Elgar Fleisch
Friedemann Mattern (Hrsg.)

Das Internet der Dinge

Ubiquitous Computing und RFID in der Praxis

Springer

Elgar Fleisch · Friedemann Mattern (Hrsg.)

Das Internet der Dinge

Elgar Fleisch · Friedemann Mattern (Hrsg.)

Das Internet der Dinge

Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen

Mit 101 Abbildungen und 21 Tabellen

Springer

Elgar Fleisch
Universität St. Gallen
Institut für Technologiemanagement
Dufourstr. 40 A
9000 St. Gallen, Schweiz
ETH Zürich
Departement für Management, Technologie und Ökonomie
elgar.fleisch@unisg.ch

Friedemann Mattern
ETH Zürich
Departement für Informatik, Institut für Pervasive Computing
Haldeneggsteig 4
8092 Zürich, Schweiz
mattern@inf.ethz.ch

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN-10 3-540-24003-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-24003-7 Springer Berlin Heidelberg New York

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

Satz: Druckfertige Daten der Autoren
Herstellung: LE-TeX Jelonek, Schmidt & Vöckler GbR, Leipzig
Umschlaggestaltung: KünkelLopka Werbeagentur, Heidelberg

Gedruckt auf säurefreiem Papier 33/3142/YL - 5 4 3 2 1 0

Vorwort

Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Silent Commerce – eine Vielzahl neuer Termini kursiert in diesen Tagen und kündet von einer grundsätzlich neuen Qualität der rechnergestützten Informationsverarbeitung. Allen Begriffen gemeinsam ist die Vision einer Welt smarter Alltagsgegenstände, welche mit digitaler Logik, Sensorik und der Möglichkeit zur Vernetzung ausgestattet ein „Internet der Dinge" bilden, in dem der Computer als eigenständiges Gerät verschwindet und in den Objekten der physischen Welt aufgeht. War zu Zeiten des Mainframe und des PCs Rechenkapazität noch eine knappe Ressource, so versprechen neuartige Technologien und weitere Fortschritte im IT-Bereich eine allgegenwärtige Verfügbarkeit von Informationen und Diensten, in deren Zentrum nicht mehr die Maschine mit ihren technischen Möglichkeiten und Grenzen, sondern der Benutzer mit seinen individuellen Anforderungen steht.

Die zunehmende Informatisierung und Vernetzung physischer Dinge beschäftigt heute die Forschung weltweit. Während sich die Vordenker des Ubiquitous Computing vor Jahren noch den Vorwurf des Utopismus gefallen lassen mussten, rückt die technische Machbarkeit aufgrund der rasanten Miniaturisierung mikroelektronischer Komponenten und des damit einhergehenden Preisverfalls mehr und mehr in greifbare Nähe. Gleichzeitig ist in der Wirtschaft ein starkes Interesse am praktischen Einsatz zu verzeichnen, welches abseits von dem in den Medien zwar häufig zitierten, aber doch naiven „intelligenten Kühlschrank" auf die Verbesserung betrieblicher Prozesse und die Vermarktung smarter Produkte und Dienstleistungen abzielt – eine Domäne, die mittel- bis langfristig das Potenzial für enorme Wirkungen besitzt.

Mit RFID steht zum ersten Mal eine Basistechnologie zur Realisierung smarter Dinge vor dem Masseneinsatz. Die automatische Identifikation physischer Güter durch Funketiketten bietet eine Reihe von Vorteilen gegenüber dem klassischen Barcode und trägt zur Optimierung und Verbesserung zahlreicher bisher aufwendiger und fehleranfälliger Abläufe bei. Darüber hinaus ermöglicht RFID aber auch eine Vielzahl völlig neuer Lösungen betriebswirtschaftlicher Probleme, etwa zur Produktrückverfolgung oder Fälschungssicherheit. Die Fähigkeit eines Objekts, eine eindeutige Kennung zu speichern und seiner Umwelt mitzuteilen, stellt so gesehen einen ersten Schritt in Richtung eines „Internets der Dinge" dar, auf dem zusätzliche Funktionalität aufbauen kann.

Wie auch bei anderen einflussreichen Technologien vollziehen sich die beschriebenen Entwicklungen jedoch keineswegs im gesellschaftspolitischen Vakuum. Während die betriebliche Praxis als Technikbefürworter aus einer ökonomischen Perspektive heraus argumentiert, verstärkt sich in der öffentlichen Wahrnehmung der Eindruck eines Risikos für Individuum und Gesellschaft. Vor allem Datenschützer befürchten eine zunehmende Überwachung des Bürgers seitens des Staats oder einzelner Unternehmen durch RFID und fordern Konzepte zur Sicherung der Privatsphäre auf technischer, organisatorischer und rechtlicher Ebene.

Vor diesem Hintergrund setzt sich das vorliegende Buch – durch den in den Einband integrierten RFID-Transponder selbst ein smartes Objekt – mit den Visionen und Technologien des Ubiquitous Computing auseinander, beschreibt zahl-

reiche Anwendungsszenarien aus der Praxis, diskutiert mögliche Risiken und gibt Anwendern Handlungsanleitungen für die Umsetzung. Insbesondere die vorgestellten Fallstudien skizzieren dabei nicht allein das technisch Machbare, sondern den aus Nutzersicht bereits heute wirtschaftlich sinnvollen Einsatz.

Ausgangspunkt für das Entstehen dieses Buches ist das M-Lab, im Jahr 2001 als Gemeinschaftsprojekt des Instituts für Technologiemanagement der Universität St. Gallen und des Instituts für Pervasive Computing der Eidgenössischen Technischen Hochschule (ETH) Zürich gegründet. Das M-Lab beschäftigt sich in Kooperation mit namhaften Industriepartnern mit der Identifikation und Gestaltung betriebswirtschaftlicher Anwendungen smarter Dinge – von der Idee bis zum Demonstrator. Die Unternehmen bringen Problemstellungen ihrer Branchen, Experten sowie finanzielle Mittel ein und erstellen gemeinsam mit dem universitären Forscherteam Analysen, Konzepte und Prototypen. Mit dieser Vorgehensweise konnte sich das M-Lab als eines von weltweit sechs Auto-ID Labs profilieren und maßgeblich zur Etablierung der RFID-Technologie beitragen. Zusammen mit internationalen Forschungspartnern wie dem amerikanischen MIT, der Universität Cambridge, der Keio University, der Fudan University und der Universität Adelaide entstand neben Analysen zum Thema RFID auch eine Reihe von Standards rund um den „Electronic Product Code“, die heute in den Roll-out-Projekten vieler Großunternehmen Verwendung finden.

Das vorliegende Buch profitiert vom Erfahrungsschatz, Praxisbezug und der internationalen Vernetzung der Autoren und Wissenschaftler aus dem M-Lab. Beim Identifizieren wirtschaftlich relevanter Problemstellungen sowie beim Validieren der Ergebnisse sind die Forscher allerdings auf die Mitarbeit der Unternehmenspraxis angewiesen; ein solches Buch wäre daher ohne die Unterstützung der verschiedenen M-Lab-Partnerunternehmen nicht möglich gewesen. Wir möchten uns deswegen herzlich bei folgenden Firmen für die wertvolle und angenehme Zusammenarbeit im M-Lab bedanken, von denen viele in kooperativer Weise beim Verfassen der Buchbeiträge auf direkte oder indirekte Art mitgewirkt haben: Deutsche Telekom, Gillette, Infineon Technologies, Migros, Novartis, Paul Hartmann, SAP, SAP SI, SIG Combibloc, Swiss Re, Swisscom, UBS und Volkswagen.

Nicht zuletzt hängt das Gelingen eines solchen Vorhabens auch vom Engagement einzelner Personen ab. Unser besonderer Dank gilt in dieser Hinsicht neben den Autoren vor allem Herrn Christian Tellkamp und Dr. Frédéric Thiesse für ihren Einsatz bei der Aufbereitung der Manuskripte. Wir danken auch dem Springer-Verlag für die angenehme Zusammenarbeit bei der Herausgabe unseres Buches zum kommenden Internet der Dinge.

Elgar Fleisch und Friedemann Mattern
St. Gallen / Zürich, im Mai 2005

Inhaltsverzeichnis

Teil A: Visionen

Die betriebswirtschaftliche Vision des Internets der Dinge

Elgar Fleisch
Institut für Technologiemanagement, Universität St. Gallen und
Departement „Management, Technology, and Economics“, ETH Zürich

Oliver Christ
SAP AG, Walldorf

Markus Dierkes
Intellion AG, St. Gallen

Kurzfassung. Dieser Beitrag beschreibt die Entwicklung und Konsequenzen des nächsten Schritts der betrieblichen Informationsverarbeitung aus ökonomischer Perspektive: Mit Radio Frequency Identification (RFID) und anderen Ubiquitous-Computing-Technologien bekommen Informationssysteme erstmals Augen und Ohren. Bisher mussten sie aufwendig von Menschen mit Hilfe von Tastatur und Barcode-Leser mit Daten gefüttert werden. Nun können Informationssysteme Daten aus der realen Welt automatisch in Echtzeit zu einem Bruchteil der Kosten sammeln. Dies ermöglicht einerseits die wirtschaftliche Gewinnung von wesentlich feingranulareren Daten und andererseits deutlich differenziertere Managementregelkreise. Denn Unternehmen können nur managen, was sie auch messen können, und nur wer Out-of-Stock und Schwund messen kann, kann wirksame Gegenmaßnahmen einleiten. In einem ersten Schritt führt der Technologieeinsatz damit zu sichereren, schnelleren und effizienteren Prozessen, in einem zweiten Schritt zu neuen „smarten“ Produkten und Dienstleistungen.

1 Die Lücke zwischen realer und virtueller Welt

Die betriebswirtschaftliche Informationsverarbeitung hat in den letzten vier Jahrzehnten viel zur Geschwindigkeit, Effizienz und Genauigkeit unternehmensinterner wie -übergreifender Prozesse beigetragen. Einige unternehmerische Problemstellungen konnte sie bisher jedoch nur sehr limitiert lösen. Dazu zählen:

- Im Einzelhandel sind 5 bis 10 % der nachgefragten Produkte nicht verfügbar [BGC02], bei speziell beworbenen Produkten sogar 15 % (Out-of-Stock) [GMA02]. Einzelhändler und Produzenten verlieren dadurch 3 bis 4 % ihres Umsatzes und empfehlen ihre Kunden an die besser organisierte Konkurrenz [IBM02].

- Diebstahl durch Mitarbeiter, Lieferanten und Kunden, Betrug durch Lieferanten und administrative Fehler führen zu ungeplanten Bestandsreduktionen (Shrinkage), die etwa bei US-amerikanischen Einzelhändlern jährlich Kosten von 33 Milliarden USD (1,8 % des Umsatzes) verursachen [HoD01].
- Der Handel mit gefälschten Produkten ist bereits für 5 bis 7 % des Welthandelsvolumens verantwortlich [OECD98]. Der Wert gefälschter Waren beläuft sich auf über 500 Milliarden EUR jährlich [ICC04]. In den Entwicklungsländern werden ca. 30 % aller pharmazeutischen Produkte gefälscht [IDT04]. Neben den primären Schäden durch entgangenen Umsatz bei den Originalmarken entstehen etwa im Bereich Medikamente und Flugzeugersatzteile hohe Risiken bei der Verwendung von qualitativ minderwertigen Fälschungen.
- Aufgrund vermeidbarer falscher Medikation sterben in den Spitälern der USA jährlich zwischen 44 000 und 98 000 Menschen [IDT04].
- Die Kosten für Rückrufaktionen sind etwa in der Automobilindustrie fester Bestandteil jeder Neueinführung geworden. Im Jahr 2003 musste die deutsche Automobilindustrie 144 offizielle Rückholaktionen initiieren [KBA04], im Jahr 2000 musste Firestone 14,4 Millionen Reifen zurückholen [Bri00].
- Ab 2005 sind zahlreiche Branchen in der EU verpflichtet, das Recycling ihrer Produkte professionell und transparent zu organisieren. Automobilhersteller müssen Altwagen zurücknehmen und 85 % des Gewichts recyceln [EuU00]. Die Elektronikschrottverordnung zwingt Hersteller von Elektrogeräten zur Übernahme der Kosten aus der Elektronikverschrottung [EuU02]. Die eindeutige Zuordnung zwischen Bauteil und Unternehmen wird zum Schlüssel der Abrechnungssysteme.
- Der physische Lagerbestand stimmt mit den Lagerbestandsdaten in den entsprechenden Informationssystemen im Durchschnitt bei über 30 % aller Produkte nicht überein (Einzelfallbeispiel) [RDT01]. Die Realität unterscheidet sich maßgeblich vom ihrem digitalen Abbild, das die Grundlage für Managemententscheidungen liefert.

Der gemeinsame Nenner dieser Probleme ist die bis heute mangelhafte Integration zwischen der realen, physischen Welt bzw. der Wirklichkeit aus Molekülen auf der einen Seite und der digitalen Welt der Informationssysteme, des Internets bzw. der Wirklichkeit der Daten und Bits auf der anderen Seite. Diese „Lücke“ zwischen den beiden Welten hat 1999 zur Gründung des Auto-ID Centers[1] und 2001 zur Gründung des M-Labs[2] geführt. Unternehmen wie Wal-Mart, Tesco, Gillette, Metro, Novartis und Volkswagen haben sich an diesen Initiativen aktiv beteiligt. Sie wollten damit die Grundlagen für die Lösung obiger Probleme auf Basis des Ubiquitous Computing (UbiComp) schaffen. Heute, 2005, scheinen die Ankündigungen der großen Einzelhändler, Industrie-, Konsumgüter- und Softwarehersteller dieser Welt, von den USA über Europa bis Japan und China, die nächste Generation der betriebswirtschaftlichen Informationsverarbeitung und den Wandel zum Echtzeitunternehmen einzuläuten.

[1] www.autoidcenter.org bzw. www.autoidlabs.org und www.epcglobalinc.org

[2] www.m-lab.ch

2 Der Beitrag von UbiComp

Dieser Aufsatz liefert vier miteinander verzahnte Modelle zur Erklärung, warum UbiComp ein logischer nächster Schritt in der betrieblichen Informationsverarbeitung ist. Ausgangspunkt der Überlegungen ist der im Beitrag von Mattern beschriebene technologische Fortschritt in verschiedenen Bereichen.

Die Entwicklungsphasen der betrieblichen Informationsverarbeitung (Modell 1, siehe unten) zeigen, dass mit jeder neuen Informationssystemgeneration eine Erweiterung des Integrationsbereichs einhergeht. Das zweite Modell beschreibt die enge Verknüpfung von realer und virtueller Welt mit Hilfe von Sensoren und Aktuatoren als nächste Ausbaustufe des Integrationsbereichs. Die Folge ist ein geschlossener digitaler Managementregelkreis (Modell 3), der erstmals vollautomatisierte Führungsregelkreise ermöglicht und damit dem Begriff Echtzeitmanagement die bisher vermisste Substanz gibt. Eine weitere Konsequenz der Integration von realer und virtueller Welt ist die kostengünstige Verfügbarkeit von Daten über den Zustand der realen Welt. Sie führt dort, wo zusätzliche Daten Nutzen stiften, zu einer hohen Datengranularität (Modell 4), die neue Geschäftsprozesse und Geschäftsmodelle ermöglicht.

2.1 Entwicklungsphasen der betrieblichen Informationsverarbeitung (Modell 1)

Abbildung 1 zeigt die Phasen der Informatisierung anhand der Entwicklung des Integrationsbereichs [FlÖ00, Fle02]. Der Integrationsbereich beschreibt die Anzahl der Aufgaben, die ein Unternehmen bzw. ein Unternehmensnetzwerk in einem integrierten Informationssystem ausführt [ÖBW92]. Die Aufstellung zeigt, dass der Integrationsbereich mit zunehmender Entwicklung der Technologie größer wird. Er wächst entsprechend den Phasen von der isolierten Aufgabe über Unternehmensfunktion und innerbetrieblichem Prozess zum überbetrieblichen Prozessnetzwerk.

Phase 1. Ziel der Informatisierung isolierter Funktionen war es, einzelne Geschäftsfunktionen wie z.B. die Fakturierung zu automatisieren. Manuelle Vorgänge werden dabei in unveränderter Weise dem Computer übertragen. Das Ergebnis sind isolierte Lösungen, d.h. separate Informationssysteme, die Einzelvorgänge effizient unterstützen.

Phase 2. Durch die Informatisierung von Funktionsbereichen, wie z.B. Produktion, Finanzbuchhaltung oder Distribution, wurde eine Integration innerhalb der wichtigsten Geschäftsfunktionsbereiche erreicht und damit die Effizienz ganzer Abteilungen verbessert. IT ermöglichte erstmals die Anwendung neuer Methoden, wie z.B. Produktions- und Finanzplanung, durch die Geschäftsprozesse neu gestaltet und Mitarbeiter mit neuen Herausforderungen konfrontiert wurden.

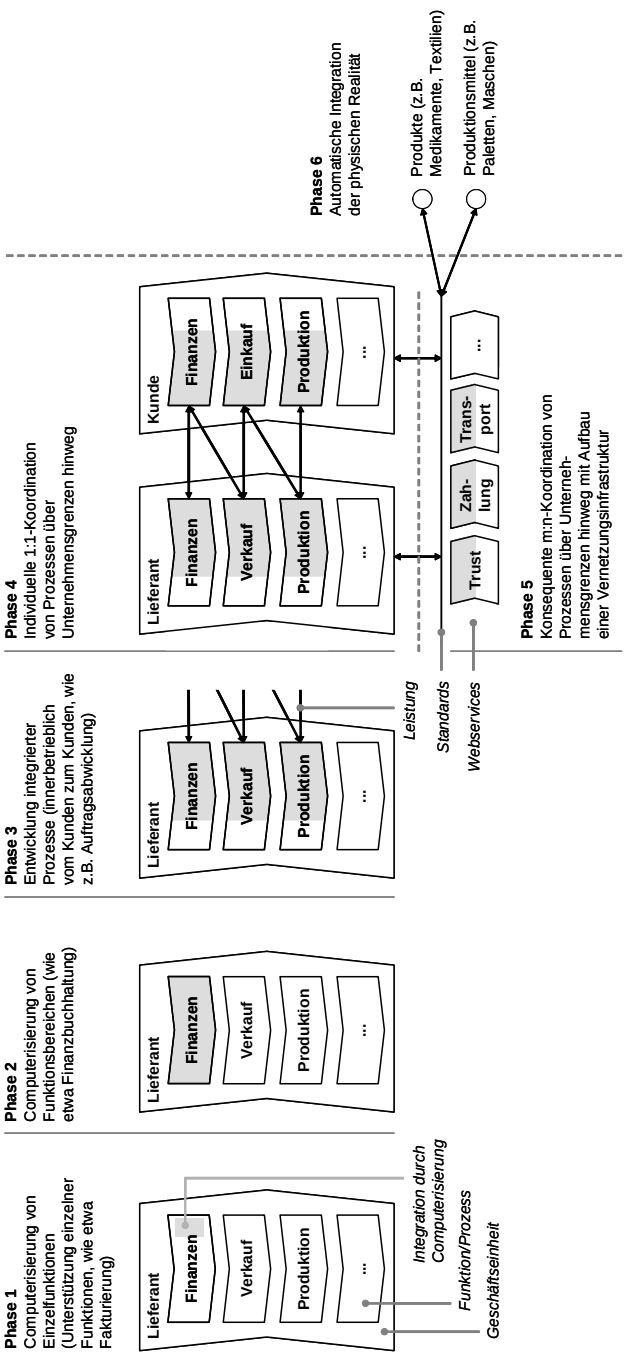


Abb. 1. Phasen der Informatisierung von Unternehmen

Phase 3. Die Entwicklung von Enterprise-Resource-Planning-Systemen (ERP-Systemen) bot den Unternehmen die Möglichkeit, abteilungs- bzw. funktionsübergreifend integrierte Prozesse einzuführen. Damit konnten durchgängige Prozesse (z.B. Auftragsbearbeitung) vom Kunden (z.B. Verkauf, Auftragserfassung) und zum Kunden (z.B. Vertrieb, Rechnungsstellung, Zahlungseingang) eingerichtet werden. ERP-Systeme wurden bald zum Nervensystem der Unternehmen und ermöglichten jedem (berechtigten) Mitarbeiter unverzögerten Zugang zu allen abgebildeten Betriebsinformationen.

Phase 4. Parallel zur Einführung von ERP-Systemen gingen einige Unternehmen dazu über, Verflechtungen mit ihren Kunden oder Lieferanten zu schaffen. Sie begannen in einem ersten Schritt, Systeme zum elektronischen Datenaustausch (Electronic Data Interchange, EDI) einzusetzen, um Massentransaktionen effizient abzuwickeln. Dies führte zum Aufbau aufwendiger 1:1- oder 1:n-Beziehungen – einer der wichtigen Gründe, weshalb EDI nicht die erwartete flächendeckende Verbreitung fand.

Phase 5. In dieser Phase verlangt der Käufermarkt einen neuen kundenorientierten Ansatz. Es sind nun die Prozesse der Kunden des Unternehmens, die den Ausgangspunkt für die Gestaltung eigener Dienstleistungen und Prozesse bilden. Neue Informationssysteme für Supply Chain Management und Electronic Commerce erfüllen diese Voraussetzungen, indem sie die überbetriebliche Integration von Informationen und Prozessen und damit einen Schritt hin zur Vision des grenzenlosen Unternehmens ermöglichen. Diese m:n-Vernetzung interner und externer Geschäftseinheiten stützt sich auf eine Vernetzungsinfrastruktur, die analog dem Straßennetz aus der physischen Welt funktioniert: Enthalten sind Normen (z.B. Straßenbreite, Verkehrsschilder, Verkehrsvorschriften), Koordinationstechnologien und -systeme (z.B. Ampeln, Navigationssysteme) und Dienstleistungen (z.B. Polizei, Straßenwartung, Gebühren, Mautabgaben, Automobilklubs).

2.2 Integration der Realität (Modell 2)

Bis heute konzentrieren sich Forschung und Praxis der betrieblichen Informationsverarbeitung primär auf die Vernetzung von Unternehmen, Prozessen, Informationssystemen und Menschen. Sie verfolgen das Ziel, mit wachsenden Integrationsbereichen immer mehr Medienbrüche zu eliminieren (vgl. Tabelle 1). Ein Beispiel für einen Medienbruch ist die mehrfache Erfassung eines Auftrags in unterschiedlichen betrieblichen Informationssystemen innerhalb einer Wertschöpfungskette. Ein Medienbruch ist vergleichbar mit einem fehlenden Glied einer digitalen Informationskette und ist Mitursache für Langsamkeit, Intransparenz, Fehleranfälligkeit etc. inner- und überbetrieblicher Prozesse.

UbiComp-Technologien haben das Potenzial, den Medienbruch zwischen physischen Prozessen und deren Informationsverarbeitung zu vermeiden. Sie ermöglichen eine vollautomatisierbare Maschine-Maschine-Beziehung zwischen realen Dingen und Informationssystemen, indem sie Ersteren einen Minicomputer zufügen. Sie helfen, die Kosten der Abbildung realer Ressourcen und Vorgänge in Informationssystemen zu reduzieren (vgl. Abbildung 2), sie übernehmen die Auf-

gaben eines Mediators zwischen realer und virtueller Welt. Physische Ressourcen können so ohne zusätzliche menschliche Intervention über die unternehmensinternen und -externen Rechnernetze kommunizieren.

Aus der Perspektive des sich erweiternden Integrationsbereichs ist UbiComp ein logischer nächster Entwicklungsschritt der betrieblichen Informationsverarbeitung. Während integrierte Informationssysteme und E-Business-Systeme die Verknüpfung von immer mehr Applikationen und Datenbanken verfolgen, strebt UbiComp die Integration dieser Applikationen und Datenbanken mit der realen betrieblichen Umgebung wie etwa dem Lagerhaus an. UbiComp schließt die heute in vielen Fällen sehr kostspielige Lücke zwischen Informationssystem und Realität. Mittels Sensorik (und Aktuatorik) können UbiComp-basierte Systeme Zustandsänderungen in der realen Welt automatisch erkennen (bzw. herbeiführen) [AEG02]. Sie treffen ihre Entscheidungen aufgrund faktenbasierter Echtzeitdaten aus der Realität und nicht auf Basis fortgeschriebener buchhalterischer Werte aus den Informationssystemen.

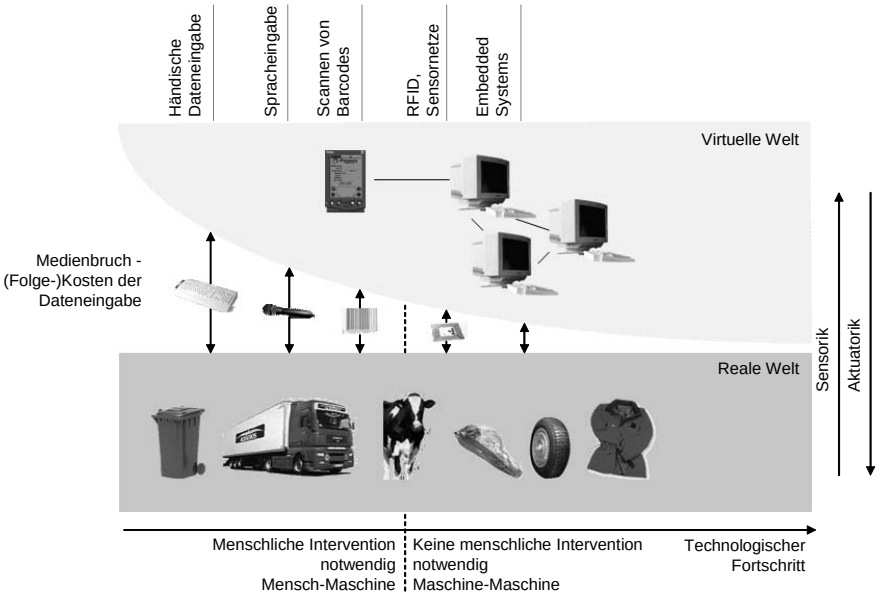


Abb. 2. Integration von realer und virtueller Welt

Tabelle 1 zeigt die enge Verknüpfung zwischen technologischen Möglichkeiten und betriebswirtschaftlichen Konzepten. Erst unternehmensweit integrierte ERP-Systeme haben eine Prozesssicht zugelassen und ihr so zum Durchbruch verholfen. Mit den E-Business-Systemen sind die unternehmensübergreifenden Ansätze wie beispielsweise Supply Chain Management in den Vordergrund gerückt. UbiComp-Technologie, etwa die an anderer Stelle des Buches genauer besprochenen Auto-ID-Systeme, liefern die Grundlage zu Echtzeitkonzepten oder zu den etwas vollmundig formulierten Konstrukten *Silent Commerce* bzw. *Ubiquitous Commerce*. In einem neuen Garten möchte eben jeder einen Baum pflan-

zen. Die folgenden Abschnitte sollen zur Klärung beitragen, ob die neuen Begriffe gerechtfertigt sind.

Tabelle 1 interpretiert die Integration der beiden Welten als die nächste Entwicklungsphase der Informatisierung von Unternehmen. Die zunehmende Miniaturisierung von Informationsverarbeitungs- und Kommunikationsgeräten führt zu einer neuen Ära der Vernetzung, in der die physische Realität automatisch mit deren Abbildung in den betrieblichen Informationssystemen kommuniziert. Mit UbiComp-Technologie aufgeladene Dinge wie Verbrauchsgüter (Medikamente, Textilien), Rohstoffe (Boden, Wasser, Holz) und Produktionsmittel (z.B. Container, Paletten, Schachteln, Werkzeugmaschinen) eröffnen neue Perspektiven in der Innovation von Produkten, Dienstleistungen und Prozessen (vgl. Abbildung 3).

Tabelle 1. Medienbrüche, betriebliche Informationssysteme und betriebswirtschaftliche Konzepte

Phase	Integrationsbereich	Informationssysteme zur Überwindung der Medienbrüche	Betriebswirtschaftliche Konzepte
Phasen 1 & 2	Einzelne Unternehmensfunktionen (mehr Integrationsreichweite, vgl. Abbildung 14)	Funktionsorientierte Standardsoftwarepakete wie z.B. Finanzpakete oder Produktionsplanungs- und Steuerungssysteme	Automatisierung
Phase 3	Unternehmensweite Prozesse (mehr Integrationsreichweite)	ERP-Systeme wie z.B. R/3 von SAP	Business Process Redesign, Business Process Engineering, Business Engineering
Phasen 4 & 5	Unternehmensübergreifende Prozesse (mehr Integrationsreichweite)	Unternehmensübergreifende Systeme wie z.B. E-Procurement- und Supply-Chain-Management-Systeme	e-Business, Business Networking, Supply Chain Management, Adaptive Enterprise
Phase 6	„Reale“ Prozesse (mehr Integrationstiefe)	Anwendungen des UbiComp, z.B. auf Basis von Radio Frequency Identification (RFID)-Technologie und Sensornetzen	Echtzeitmanagement, Ubiquitous Commerce, Silent Commerce

2.3 Digitalisierung des Managementregelkreises (Modell 3)

Die Verschmelzung der realen mit der virtuellen Welt erlaubt das Schließen des digitalen Managementregelkreises, wie im Folgenden am Modell eines Echtzeitunternehmens beschrieben (vgl. Abbildung 4).

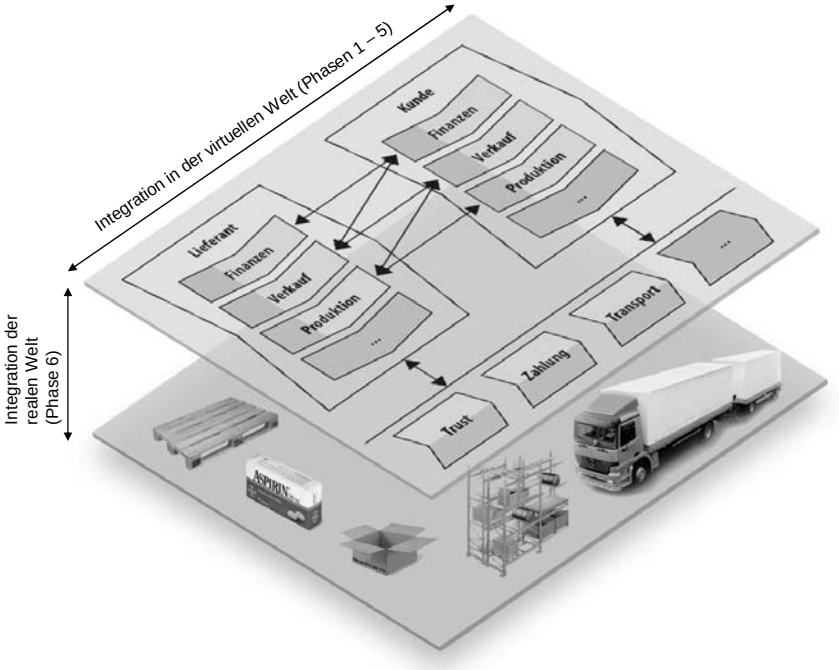


Abb. 3. Integration der Realität als 6. Phase der betrieblichen Informationsverarbeitung

In idealtypischen Echtzeitunternehmen stehen Informationen unmittelbar nach ihrer Entstehung am so genannten „Point-of-Creation“ (POC) sowie an den Orten ihrer Verwendung bzw. „Point-of-Action“ (POA) zur Verfügung [FlÖ03]. Sowohl POC als auch POA können dabei unterschiedlichen Organisationseinheiten zugeordnet sein und dementsprechend inner- und überbetriebliche Informationsflüsse bedingen. Der POC kann beispielsweise die Scannerkasse eines Einzelhändlers sein, die dazugehörigen POA sind neben der Scannerkasse das interne Warenwirtschafts- und Logistiksystem sowie das überbetriebliche Beschaffungs- und Prognosesystem, das den Einzelhändler mit seinen Lieferanten verbindet.

Wenn ein Verkäufer eine Packung Kompottringe über den Verkaufstisch schiebt oder wenn sich auf einer der Autobahnen im Raum Stuttgart ein Stau bildet, dann generieren die Ereignisse Informationen, die vor ihrer Weiterverarbeitung in Informationssystemen digital erfasst werden müssen.

Wie am Beispiel des Einzelhandels ersichtlich, lassen sich in Wertschöpfungsketten zahlreiche POC und POA identifizieren – immer genau dann, wenn eine Information entsteht oder verwendet wird. Die Wahl der POC und POA orientiert sich an der Domäne, die es zu steuern gilt – in der Mess- und Regeltechnik *Regelstrecke* genannt. Infrage kommen hier einzelne Aufgaben, interne wie überbetriebliche Prozesse, Unternehmensbereiche, Wertschöpfungsketten und Unternehmensnetzwerke. Auf sie wirken laufend Störgrößen wie Maschinenausfälle, Schwund, Qualitäts- und Nachfrageschwankungen, welche die Regelgrößen (Istgrößen) wie beispielsweise Prozess- oder Unternehmenskennzahlen beeinflussen

und ein zeitnahes Management verlangen. Am POA vergleicht der Entscheider (Regler) Sollgrößen (Führungsgrößen) mit Istgrößen und definiert Maßnahmen (Stellgrößen), welche die Regelstrecke so beeinflussen sollen, dass die Regelgrößen den Zielvorgaben besser entsprechen.

Jede Unterbrechung des Regelkreises führt zu Verzögerungen und zusätzlichen Störgrößen. Prozesse, Unternehmen und Unternehmensnetzwerke sind dann nicht in Echtzeit führbar. UbiComp-Technologien, insbesondere automatische Identifikation, Sensorik und Aktuatorik, sind die technischen Grundlagen zur Digitalisierung und Automatisierung von POC und POA. Sie sind notwendige Voraussetzungen zur Schaffung von geschlossenen digitalen Managementregelkreisen.

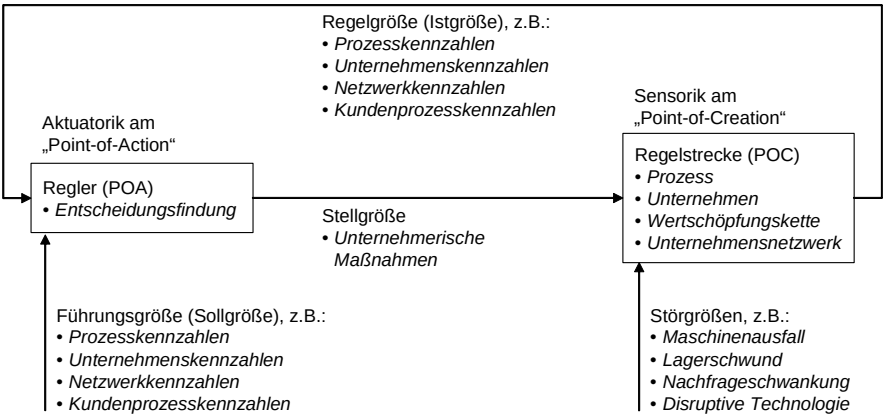


Abb. 4. Der digitale Managementregelkreis

Die durchgängige Digitalisierung des Regelkreises ermöglicht die Vollautomatisierung eines Regelzyklus. Bei gegebener Infrastruktur sind die Kosten eines solchen Zyklus, beispielsweise einer automatischen Regalinventur, bei der Regal und Produkte miteinander kommunizieren, niedriger als bei einer manuellen Inventur. Diese Kostendifferenz führt nicht nur zu einer Substitution des manuellen Regelkreises durch einen automatisierten Regelkreis, sondern aufgrund der Nachfrageelastizität auch zu einem Anstieg an kostengünstigen Prüfzyklen [MaC94]. Während die kostenintensive manuelle Inventur je nach Anwendungsfall nur ein Mal pro Periode (z.B. Tag, Woche oder Jahr) stattfindet, kann die automatische Inventur laufend erfolgen.

UbiComp-Lösungen übernehmen in der Regel kostenintensive Aufgaben an der Schnittstelle zwischen Informationssystemen und der realen Welt in eine Infrastruktur, die in der Lage sein soll, dieselben Aufgaben vollautomatisch und damit kostengünstiger und laufend durchzuführen. Solche Schnittstellenaufgaben sind Teil zahlreicher Prozesse, welche die reale Welt, also materielle Dinge und Menschen, einbeziehen. Sie sind häufig Daueraufgaben, die, wenn auch meistens im Hintergrund, ständig aktiv sind. Ihre Durchführung ist dementsprechend aufwendig.

2.4 Steigerung der Datenqualität (Modell 4)

Die heute eingesetzten Informationssysteme lösen schon zahlreiche Integrationsprobleme. Die Vision des Echtzeitunternehmens ist jedoch noch lange nicht erreicht. Unternehmen arbeiten immer noch mit hohen Ineffizienzen aufgrund schlechter Datenqualität. Beispiele sind die eingangs erwähnte schlechte Produktverfügbarkeit, unverkäufliche Ware, Diebstahl und Fälschungen. Wenn ein Einzelhändler genau wüsste, welche Produkte sich auf dem Verkaufsregal befinden und welche im filialeigenen Lager, könnte er seine Produktverfügbarkeit deutlich erhöhen [BGC02, IBM02]. Warum also sammeln Einzelhändler nicht einfach diese Daten oder leiten sie aus den Barcode-basierten Kassensystemen ab? Die Antwort auf diese Frage geht Hand in Hand mit dem oben skizzierten Integrationsproblem: Auf der Basis heutiger Technologie ist die Vollerhebung von Daten aus der realen Welt in vielen Fällen zu teuer.

Daher entwickelten Unternehmen Methoden zum Sammeln und Verarbeiten von Daten, die ihr Auskommen mit Teilerhebungen bzw. Stichproben finden. Weil die zuverlässige Vollerhebung eines Inventars teuer und zeitaufwendig ist, findet die Inventur eben nur ein Mal im Jahr statt. Weil die vollständige Überprüfung der ein- bzw. ausgehenden Lieferungen gegen die Daten in den entsprechenden Informationssystemen zu kostenintensiv ist, führen Unternehmen solche Checks auf statistischer Basis durch.

Die hohen Integrationskosten resultieren unweigerlich in Entscheidungen am POA, die auf Daten mit niedriger Qualität aufbauen. Entscheider am POA stützen sich heute stark auf Statistik, die ihre Aussagen aus Verarbeitung historischer Daten gewinnt.

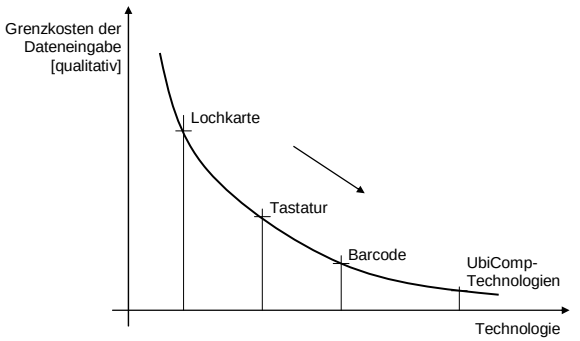


Abb. 5. Sinkende Grenzkosten der Integration der realen Welt

UbiComp kann die Kosten der Integration der Realität reduzieren (vgl. Abbildung 5). Am POC nehmen Sensoren automatisch Daten von ihrer Umwelt auf, beispielsweise lesen RFID-Lesegeräte die Identifikationsnummern aller Objekte in Lesedistanz. Am POA übersetzen Aktuatoren die Daten von unterschiedlichen POC automatisch in Nutzen stiftende Aktionen, beispielsweise durch das Versenden einer „Out-of-Stock“-Nachricht an ein anderes Informationssystem oder einen Mitarbeiter. Wenn POC und POA die Daten automatisch sammeln und verarbei-

ten können, ist menschliche Intervention nicht mehr notwendig. Im dann digitalen Managementregelkreis können Daten in Echtzeit gesammelt, verarbeitet und verteilt werden.

Mit sinkenden Preisen von Sensoren und Aktuatoren substituieren UbiComp-Technologien die konventionellen Datenein- und -ausgabemethoden. Zusätzlich zum Substitutionseffekt kommt der Elastizitätseffekt zum Zug: Unternehmen setzen zusätzliche Sensoren und Aktuatoren dort ein, wo höhere Datenqualität Wert stiftet, d.h. wo der Nutzen aus zusätzlicher Datenqualität die entstehenden Kosten übersteigt.

Die hier benutzte Definition für Datenqualität setzt sich aus den vier Dimensionen *Zeit*, *Objekt*, *Ort* und *Inhalt* zusammen. Die folgenden Abschnitte beschreiben die Dimensionen und liefern damit eine weitere Grundlage zur Ableitung der betriebswirtschaftlichen Anwendungen des UbiComp.

Dimension „Zeit“

Zwei Faktoren bestimmen die zeitliche Qualität von Information (vgl. Abbildung 6 und 8). Erstens, die Häufigkeit der Dateneingabe bzw. Granularität auf der Zeitachse: Die zeitliche Granularität ist niedrig bzw. grobkörnig, wenn, wie im Beispiel der Inventur bereits beschrieben, die Dateneingabe so kostenintensiv ist, dass sie sich unter Anwendung wirtschaftlicher Prinzipien nur bei vereinzeltem Einsatz rechnet. Die zeitliche Granularität ist hoch, wenn Grenzkosten und Grenznutzen der Sensorik eine laufende Integration der Realität aus wirtschaftlichen Gründen favorisieren. Informationssysteme mit einer feinen zeitlichen Körnung müssen sich nicht auf statistische Methoden abstützen. Sie gründen ihre Entscheidungen immer auf Fakten.

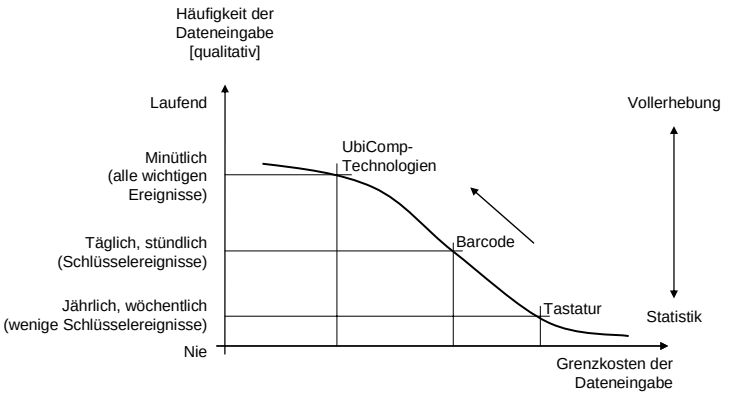


Abb. 6. Verfeinerung der zeitlichen Granularität

Zweitens, die Zeitspanne, die zwischen POC und POA, also der Erzeugung und Verwendung des Datums, verstreicht: Auch die feinkörnigsten Daten stiften nur dann Nutzen, wenn sie hinreichend zeitnah am Ort der Entscheidung zur Verfü-

gung stehen und nicht etwa in einem Datenspeicher auf die manuelle Weiterverarbeitung warten.

Dimension „Objekt“

Auch die Qualitätsdimension „Objekt“ wird von zwei Faktoren bestimmt. Der erste Faktor beschreibt den Objekttyp. Die Weiterentwicklung der Kostenstruktur von UbiComp-Technologien erlaubt eine Integration der Technologie in immer kleinere und weniger wertvolle Objekte (vgl. Abbildung 7). Bereits heute sind die Return-on-Investment-Rechnungen (ROI) im Bereich Behältermanagement für wieder verwendbare Behälter wie Kleincontainer überwiegend stark positiv. Mit dem Mandat von Wal-Mart, dem US-amerikanischen Verteidigungsministerium, Metro, Tesco, Gillette u.a. steigt auch die Wahrscheinlichkeit, eine kritische Masse von mit Funkchips ausgestatteten Paletten und Schachteln zu erreichen [Rfi03, Met04, DoD03]. Diese Schwelle ist einerseits notwendig, um die Chippreise durch Skaleneffekte bei der Produktion weiter zu senken, andererseits, um die notwendigen Infrastrukturinvestitionen der Anwenderunternehmen wirtschaftlich rechtfertigen zu können. Die Entwicklung in einigen Industriebereichen, beispielsweise der Bekleidungsindustrie, die sich durch stark individuelle Produkte mit hohen Margen auszeichnet, deutet bereits heute auf eine positive ROI-Rechnung bei der Ausstattung von einzelnen Produkten mit RFID-Tags hin [Kau03].

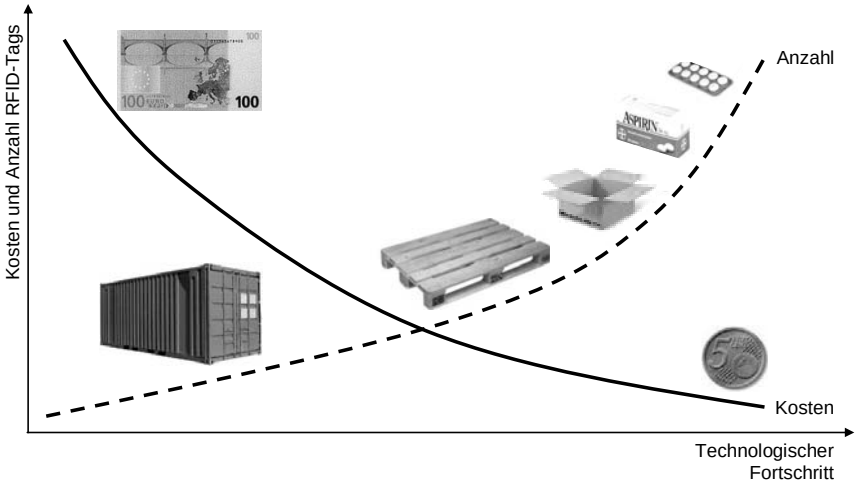


Abb. 7. Verfeinerung der Objektgranularität

Der zweite Faktor beschreibt, wie viele Objekte einer Klasse (z.B. Schachteln) integriert sind. Bei sinkenden Technologiekosten und gegebenem Nutzen aus der Integration der Realität werden mehr Objekte (Instanzen von Schachteln) innerhalb einer Objektklasse (alle Schachteln) mit UbiComp-Technologie ausgestattet. Wenn beispielsweise ein Versandhandel 5 % seiner Videokameraschachteln mit

RFID-Tags ausstattet, ist diese Objektgranulariät im Vergleich zu den möglichen 100 % relativ gering. Schon eine solche Lösung kann jedoch sehr wohl Nutzen stiften: etwa um festzustellen, an welchen Orten der Supply Chain hochwertige Lieferungen verloren gehen, verzögert oder gestohlen werden.

Dimension „Ort“

Wenn die Integration von realen Objekten kostengünstig wird, findet sie nicht nur zeitlich öfter statt, sondern auch an mehr Orten. Wie am Beispiel der Einzelhandelsfiliale ersichtlich, findet die Integration nicht mehr nur an der Scannerkasse statt, sondern auch am Regal, das in Zukunft mit RFID-Sensoren ausgestattet sein mag, bzw. beim Wareneingang im Filiallager. Mit der Ausbreitung von UbiComp-Standards und -Infrastruktur kann die Datensammlung über die Unternehmensgrenzen hinweg quer durch die gesamte Wertschöpfungskette erfolgen – im Lebensmittelbereich etwa von der Rinderfarm über die Fleisch verarbeitende Industrie hin zu Verteilzentren, Verkaufsstätten und schließlich dem Endkunden – immer unter Einbezug der Kühlkettenlogistik.

Dimension „Inhalt“

Die vierte Dimension der Datenqualität, die mittels UbiComp-Technologien erhöht werden kann, ist die Datenvielfalt bzw. der Inhalt der automatisch gesammelten Daten. Als Minimum verlangt die Integration der realen Welt einen eindeutigen Identifikator der Objektklasse oder der Objektinstanz. Vor 25 Jahren begannen EAN/UCC dem Einzelhandel weltweit eindeutige Klassenidentifikatoren zur Verfügung zu stellen. In 2003 stellte das Auto-ID Center den Electronic Product Code (ePC) vor, einen eindeutigen Identifikator auf Instanzenebene [AsS03]. Seit 2004 können Unternehmen ePC-Nummernkreise von EPCglobal, einer 100%-Tochter von EAN/UCC, beziehen.

Viele UbiComp-Applikationen, beispielsweise in der Automobil- und Hightechindustrie, sammeln zusätzliche objektspezifische Daten. So speichern etwa Funkchips auf internen Transportbehältern Qualitätsdaten, nächste Produktionsschritte, Kundenname und Zielkonfiguration. Der Einbezug weiterer Sensoren zur Messung von Temperatur, Helligkeit, Feuchtigkeit etc. ermöglicht die zusätzliche Integration von Daten über die unmittelbare Umgebung des Objektes. Die Datenvielfalt steigt dadurch erneut an.

Zusammenfassend lässt sich festhalten, dass UbiComp die Kosten der Integration der realen Welt reduziert. Es ermöglicht damit Informationssystemen die Sammlung wesentlich detaillierterer Daten am POC und verhilft Mitarbeitern und Maschinen am POA, ihre Entscheidungen auf hochwertigen Echtzeitdaten zu basieren.

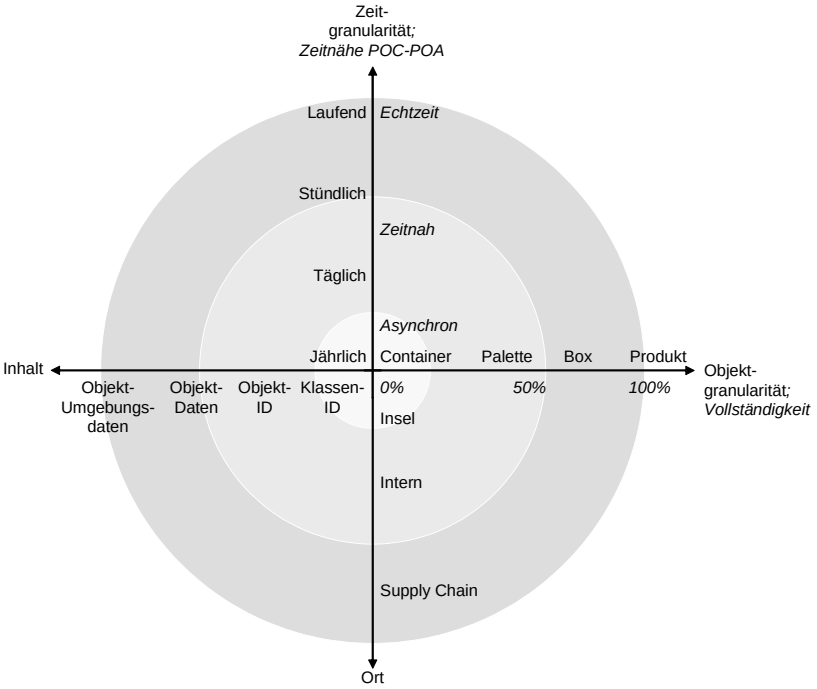


Abb. 8. Dimensionen der Datenqualität

3 Betriebswirtschaftliche Konsequenzen

Den Modellen zur Beschreibung und Erklärung der Verknüpfung zwischen Ubi-Comp-Technologie und betriebswirtschaftlichen Konzepten folgen nun Überlegungen zur Gestaltung. Als Gegenstand der Gestaltung kristallisieren sich unternehmerische Kontrollaufgaben in Geschäftsprozessen, Produkten und Dienstleistungen heraus. Prozess, Produkt und Dienstleistung gehören untrennbar zusammen, denn Produkt und Dienstleistung sind Ergebnisse von Prozessen [Öst95]. Die folgende Darstellung muss daher einige wenige Überschneidungen zulassen. Sie beginnt mit einer kurzen Einführung in die aufgabenorientierte Datenqualität, die unter dem Begriff Abbildungsqualität den Kern der weiteren Argumentation bildet. Im Weiteren zeigt der Abschnitt auf, wie sich steigende Abbildungsqualität auf Prozesse, Produkte und Dienstleistungen auswirkt. Abbildung 9 stellt die diskutierten Wirkungsfelder im Überblick dar.

Wirkungsfelder gesteigerter Abbildungsqualität durch Ubicomp				Nutzen aus gesteigerter Abbildungsqualität
Automatische Prozesskontrolle	Supply Chain Management • Warenbuchungen • Warencheck • Warenbewegungen • Produktionssteuerung • Diebstahlverhinderung • Schadenverhinderung • Fälschungsvermeidung	Produktlebenszyklusmanagement • Rückverfolgung / Herkunftsnachweis • Rückholaktionen • Wartung • Reparatur • Recycling / Entsorgung	Customer Relationship Management • Bezahlvorgang • Marktforschung • Nutzungsverhalten • Verkaufsförderung	• Kostenreduktion (Bestand, Personal, Fehler) • Geschwindigkeit (Echtzeit) • Prozessqualität und -sicherheit
Smarte Produkte	• Funktionen aus Nachbarschaft von Produkten • Funktionen aus Verwandtschaft von Produkten • Funktionen aus der Geschichte von Produkten • Emotionale Produkte • Produkt-Dienstleistungs-Bündel			–
Smarte Dienstleistungen	• Produkt-Dienstleistungs-Bündel • Kontrolldienstleistungen • Verrechnung der faktischen Verwendung (Leasing) • Verrechnung des faktischen Risikos • Informationsdienstleistungen • Komplexe Dienstleistungen			–
				• Umsatzsteigerung (Zusatzfunktionen, neue Dienstleistungen)

Abb. 9. Wirkungsfelder des Ubiquitous Computing

3.1 Kontrollaufgaben, Abbildungsqualität und Technologie

Im Kern der Gestaltung neuer Prozesse, Produkte und Dienstleistungen auf Basis von UbiComp-Technologien steht die Abbildungsqualität der realen in die virtuelle Welt. Die Abbildungsqualität erweitert den oben skizzierten Begriff Datenqualität um ein Abbildungsmodell zur zweckmäßigen Interpretation der Daten: Die Abbildungsqualität, beispielsweise die Erkennungsrate einer automatischen Eingangskontrolle per Videokamera, ist Ergebnis der Datenqualität (Bildauflösung) und des gewählten Abbildungsmodells (Modell zur Mustererkennung, wie etwa der Abstand zwischen Nase, Augen und Mund).

Die Abbildung eines Sachverhalts der realen Welt entspricht der Messgröße bzw. Istgröße eines Managementregelkreises. Die Güte der Abbildung entscheidet somit maßgeblich über die Qualität eines Managementregelkreises. Denn nur was gemessen werden kann, kann auch geführt werden.

Neue Technologie wie beispielsweise UbiComp kann die Abbildungsqualität erhöhen und damit neue Kontrollaufgaben ermöglichen, die ihrerseits neue Prozesse, Produkte und Dienstleistungen erlauben. Die Technologie bestimmt somit letztlich die maximale Qualität der Kontrollaufgabe (siehe Abbildung 10). Wenn die Technologie „Scannerkasse“ in den Einzelhandelsfilialen nicht in der Lage ist, die Regalfüllung hinreichend genau zu messen und damit abzubilden, dann ist das Management der Regalbeschickung eben unmöglich. Wenn eine einfache Beschriftung die eindeutige Bestimmung von Patienten und Medikamenten nicht zulässt, wird Falschmedikation in US-amerikanischen Spitälern weiterhin die achthäufigste Todesursache bleiben. Denn alle Abbildungstechnologien bzw. alle Abbildungsverfahren haben ihre natürlichen Grenzen. Ein Barcode wird beispielsweise nie dynamische Daten speichern können und wird nie ohne Sichtverbindung oder im Pulk erfasst werden können.

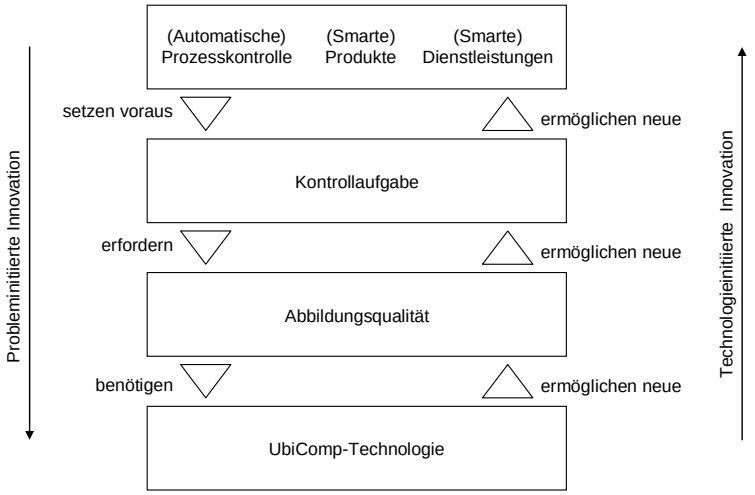


Abb. 10. Technologie, Abbildungsqualität und Kontrollaufgaben

Mit jedem Technologiesprung kommen Eigenschaften dazu, die die Abbildungsqualität erhöhen und die Einschränkungen der alten Technologie schrittweise auflösen, wie im Folgenden am Beispiel der visuellen Abbildung der realen Welt für das menschliche Auge dargestellt wird (vgl. Abbildung 11):

Zu den ersten Verfahren der visuellen Abbildung der realen Welt zählt die Malerei (deren Technologie Farbe, Pinsel, Leinwand, Lack, Staffelei sich erst über Millionen Jahre von der Höhlenmalerei her entwickelt hat). Sie erfordert bis heute eine Kunstfertigkeit, die nur wenige Menschen besitzen, ist relativ ungenau, statisch, zeitintensiv und fehleranfällig. Die chemische Fotografie löste die Malerei zu reinen Abbildungszwecken im 20. Jahrhundert völlig ab. Durch stetige Verbesserung der Technologie (Farbe, Film, Zoomobjektiv) wurde die Bildauflösung drastisch gesteigert und durch die Digitaltechnik sofort weiterverarbeitbar. Zudem integrierten die Technologiehersteller das Expertenwissen bezüglich Foto- und Filmerstellung und -bearbeitung in ihre Produkte und Dienstleistungen. So wurde die Fotografie für jeden eine einfach zugängliche Abbildungstechnologie. Mit dem Übergang vom Foto zum Film wurde aus Einzelinformationen ein Informationsstrom, der mit dem Live-Streaming (Live-Sendungen im Fernsehen wie Fußballspiele oder Schützengraben-Reportagen „eingebetteter" Reporter, Überwachungskameras, Webcams) den zeitlichen Abstand zwischen Ereignis (POC) und dem Zuschauer (POA) auf nahezu null reduziert.

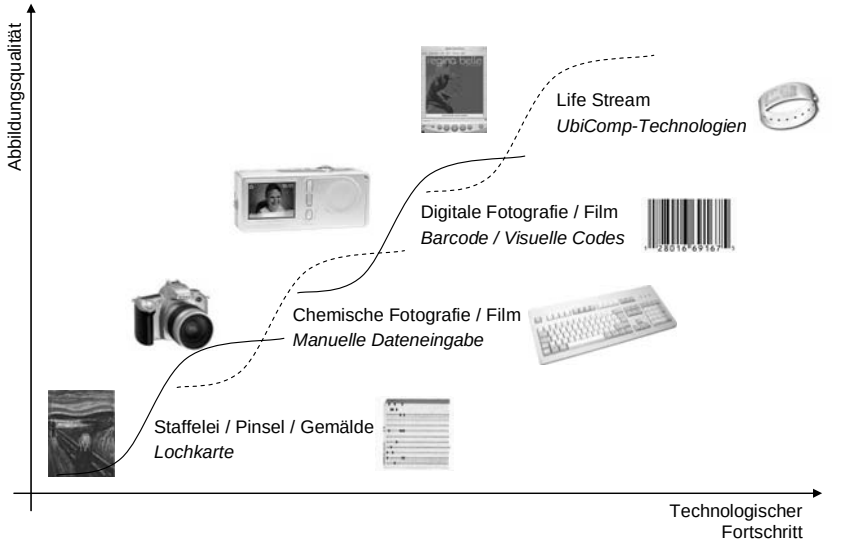


Abb. 11. Technologieentwicklung

So wie für die Technologien und Verfahren zur Abbildung der realen Welt für das menschliche Auge, lässt sich für die letzten 50 Jahre auch die Entwicklung der Abbildungsverfahren der realen Welt für den Computer nachvollziehen. Mit jedem Technologiesprung werden alte Technologien und mit ihnen Arbeitsschritte, Arbeitsplätze, Wissen und Unternehmen verdrängt. Allerdings verlieren diese

Technologien nicht immer vollständig ihre Existenzberechtigung, wie dies etwa bei der Lochkarte geschehen ist. Denn Unternehmen setzen für jede Kontrollaufgabe die jeweils kostengünstigste hinreichend genaue Technologie ein. Daher werden händische Dateneingabe und Barcodes noch lange einen großen Teil der Abbildungsverfahren ausmachen und nur dort ersetzt, wo sie aufgrund der Anforderung der Kontrollaufgaben an ihre natürlichen Grenzen stoßen bzw. höhere Kosten generieren.

3.2 Automatisierung der Prozesskontrolle

Die Innovation aufgrund neuer Abbildungsqualität kann, wie in Abbildung 10 dargestellt, aus zwei Richtungen erfolgen. Einerseits kann sie ihren Ursprung in betriebswirtschaftlichen Problemstellungen wie beispielsweise Diebstahl oder Fälschungen finden. Dann müssen sich die Innovatoren die Frage stellen, welche Messungen bzw. Abbildungsqualität notwendig sind, um einen Prozess unter Kontrolle halten zu können, und mit Hilfe welcher Technologien diese Messungen kostengünstig durchführbar sind.

Solche *probleminitiierte Innovationen* führen meist zu inkrementellen Prozessverbesserungen, nicht aber zu radikalen Veränderungen. Sie gehen von einem bestehenden Problem aus und versuchen, dieses durch höhere Abbildungsqualität zu reduzieren, eventuell sogar vollständig zu beheben. Sie setzen dort an, wo bisherige Technologien zu wenig Abbildungsqualität erreicht haben und hoher Nutzen aus zusätzlicher Abbildungsqualität zu erwarten ist. Im Bereich Supply Chain Management sind dies Kontrollaufgaben bei Warenbuchungen, Warenchecks, Warenbewegungen, Produktionssteuerung, Diebstahlverhinderung, Schadensverhinderung und Fälschungsvermeidung. Im Bereich Produktlebenszyklusmanagement sind es Kontrollaufgaben bei Rückverfolgung/Herkunftsnachweis, Rückholaktionen, Wartung, Reparatur, Recycling/Entsorgung, und im Bereich Customer Relationship Management sind es Kontrollaufgaben bei Bezahlvorgang, Marktforschung, Nutzungsverhalten und Verkaufsförderung.

Die Kontrollaufgaben (vgl. Abbildung 9) werden typischerweise vor, während oder kurz nach kritischen Prozessschritten wie beispielsweise Eigentumswechsel oder Ereignissen, die Wert zerstören oder generieren können, durchgeführt. In der typischen manuellen Kontrollaufgabe misst eine Arbeitskraft den aktuellen Wert in der realen Welt und vergleicht ihn mit dem vorher definierten Sollwert bzw. den zulässigen Ober- und Untergrenzen, die sie im relevanten Informationssystem findet. Beispielsweise öffnet ein Arbeiter in der Versandabteilung mancher Bekleidungshersteller jede auszuliefernde Schachtel und überprüft, ob Anzahl, Typ und Größe der Kleidungsstücke mit dem Lieferschein im Computer übereinstimmt. Dieser manuelle Qualitätscheck ist sehr zeit- und kostenaufwendig und außerdem fehleranfällig. Aus diesem Grund überprüfen viele Unternehmen nur einen kleinen Anteil ihrer Lieferungen detailliert. Sie vertrauen auf Stichprobenmessungen und versuchen so, vom optimalen Verhältnis aus Kontroll- und Fehlerkosten zu profitieren.

Gerry Weber hat diese Kontrollaufgaben auf Basis von RFID-Technologie automatisiert und damit die Kontrollkosten gesenkt und gleichzeitig die Kontroll-

aufgabe schneller und sicherer durchgeführt (vgl. den Beitrag von Tellkamp und Quiede in diesem Buch). Wie in vielen anderen Fällen rechnet sich die Automatisierung der Kontrollaufgabe hier (vgl. Fall A in Abbildung 12), wenn die entsprechenden Voraussetzungen gegeben sind. Zu diesen zählen, dass die Kosten einer manuellen Kontrolle bei steigender Abbildungsqualität wesentlich stärker ansteigen als bei einer automatischen Kontrolle und dass die Prozesskosten inklusive der Fehler- und Folgekosten entsprechend niedrig werden. Die optimale Abbildungsqualität bei manueller Kontrolle ist dann im Verhältnis zur automatischen Kontrolle geringer und dies bei gleichzeitig höheren Kosten.

Fall B in Abbildung 12 zeigt jedoch auch, dass es Konstellationen gibt, in denen die Automatisierung von Prozesskontrollen keinen Zusatznutzen stiftet. Dies ist vor allem dann der Fall, wenn die Kostenschere aus manueller und automatischer Kontrolle gering ausfällt und die zu erwartenden Einsparungen niedrig sind.

Das geeignete Suchfeld für Prozessverbesserungen auf Basis von UbiComp-Technologien sind demzufolge wenig automatisierte Prozesse, deren Probleme durch genauere Messungen und bessere Abbildungsqualität weitgehend gelöst werden können. Hier entscheidet das Problem über die einzusetzende Technologie und nicht umgekehrt. Wie in zahlreichen Beispielen belegt, kann eine RFID-Machbarkeitsstudie ohne Weiteres zu einer Empfehlung zur sorgfältigen Einführung von Barcode inklusive der notwendigen Lieferantenanbindung über EDI führen.

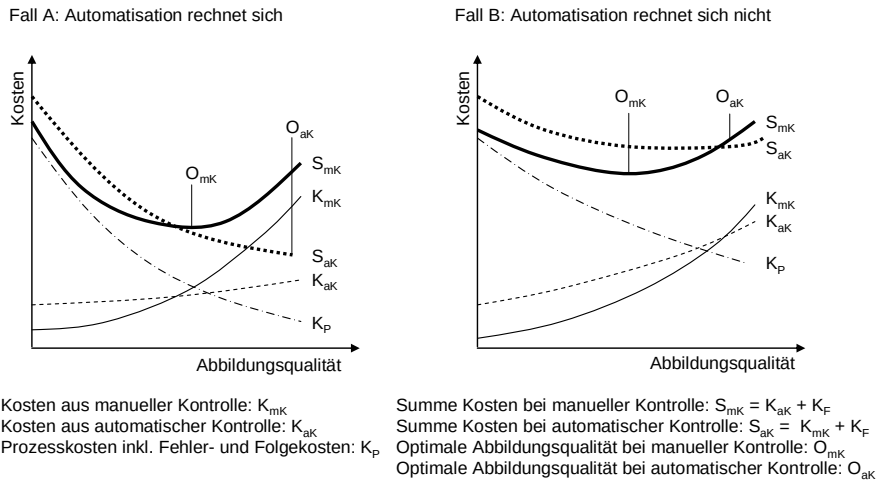


Abb. 12. Kosten manueller und automatischer Kontrollaufgaben

Die meisten heute diskutierten RFID-Projekte verfolgen diesen *Top-down-Ansatz*. Sie versuchen, ein ihnen bekanntes Prozessproblem mit einer neuen Technologie zu lösen. Das Ergebnis sind inkrementelle Prozessverbesserungen, welche den großen Teil der Potenziale einer neuen Technologie oft nur sehr limitiert nutzen.

3.3 Smarte Produkte

Die *technologieinitiierte* bzw. *Bottom-up-Innovation* (vgl. Abbildung 10) geht den anderen Weg. Sie beginnt mit der technologischen Möglichkeit der hoch qualitativen Abbildung und sucht nach bisher nicht kontrollierbaren Aufgabenstellungen, die nun messbar und damit managebar werden. Sie geht davon aus, dass alles, was durch neue Technologie messbar wird, prinzipiell auch bewirtschaftet werden kann. Diese Bewirtschaftung führt zu neuen bisher nicht handelbaren Leistungen, die im Fall von UbiComp in Zukunft in Form von smarten Produkten bzw. smarten Dienstleistungen am Markt angeboten und nachgefragt werden.

Der Begriff „smart" drückt dabei aus, dass der Mensch einen Teil seiner Kontrollaufgaben, die er bislang aufgrund seiner Fähigkeit zur Generierung von qualitativ hochwertigen Abbildungen selber durchgeführt hat („darf dieses Giftfass neben jenem Chemikalienfass stehen?"), an Dinge und Dienstleistungen abgibt. Mit der Gewöhnung an diesen zumindest zum Teil gewünschten Kontrollverlust dürfte dann auch der Begriff „smart" wieder verschwinden.

Smarte Produkte sind in diesem Sinne Produkte, die Zusatzfunktionen aus der neuen höheren Abbildungsqualität durch UbiComp-Technologie erzielen. Sie machen ihre Funktionen abhängig von der unmittelbaren Umgebung, von der Nachbarschaft, Verwandtschaft, Vertrautheit und Geschichte der Bauteile, Betriebsmittel, Verbrauchsteile, Ersatzteile und Werkzeuge, mit denen sie interagieren. Die neue Abbildungsqualität erlaubt ihnen beispielsweise, folgende Fragen zu beantworten:

- **Verbrauchsteile.** Welche Verbrauchsteile sind die richtigen? Welche Funktion muss ich pro Verbrauchsteil starten?
- **Ersatzteile.** Welche Ersatzteile sind die richtigen? Wann muss ich sie ersetzen? Wann verfallen sie oder eine ihrer Funktionen?
- **Bauteile.** Welche Teile gehören zusammen, d.h. dürfen nur zusammen funktionieren?
- **Lagergut.** Welche Teile dürfen nicht zusammen sein? Welche Teile müssen zusammen sein?
- **Produkte.** Welche Funktionen stelle ich an welchem Ort zur Verfügung? In Verbindung mit welchen anderen Teilen? In Verbindung mit welcher Geschichte? Welche Funktionen stelle ich unter welchen Umgebungsbedingungen zur Verfügung (Temperatur, Luftfeuchtigkeit etc.)?

Die Beantwortung dieser Fragen führt zu zahlreichen neuen Produktfunktionen. Einige von ihnen – die meisten davon sind bereits operativ in Betrieb oder befinden sich in Entwicklung – sind in folgender Liste aufgeführt:

- Waffe bzw. Kreditkarte funktioniert nur mit entsprechendem Chip am Handgelenk des Schützen bzw. Käufers [Wir04].
- Basisgerät eines Konsumguts (elektrische Zahnbürste, Drucker, Kaffeemaschine) funktioniert nur in Zusammenhang mit Original-Verbrauchsteil. Basisgerät lässt nur ein Upgrade der Verbrauchsteile zu, nicht aber ein Downgrade.

- Maschine (Werkzeugmaschine, Auto, Flugzeug) funktioniert nur, wenn Ersatzteile Originale sind. Maschine bestellt Ersatzteil nach, wenn zuvor bestimmte Belastungsgrenze erreicht ist.
- Bauteile signalisieren während der Montage, ob sie an den richtigen Baugruppen montiert sind, beispielsweise bei Druckwalzen.
- Bauteile informieren über ihre genauen Maße und vereinfachen damit das kostenintensive Konstruieren und Abstimmen von Toleranzen.
- Giftfass stellt sicher, dass es sich nicht in einem Raum mit anderen Chemikalien befindet, die zu einer erhöhten Explosionsgefahr führen würden [Int04a].
- Werkzeugkoffer überprüft sich auf Vollständigkeit [FMÖ02].
- Die Austernverpackung stellt sicher, dass die Kühlkette nicht unterbrochen wird.
- Produktionslose kommunizieren ihren Aufenthaltsort und den nächsten Arbeitsschritt. Produktionsmaschinen überprüfen vor dem nächsten Arbeitsschritt, ob das richtige Los geladen ist [Int04b].
- Der Verkaufsautomat benachrichtigt seinen Betreiber, wenn seine Bestände aufgefüllt, seine Kassen geleert oder seine Mechanik vorsorglich gewartet bzw. repariert werden soll (vgl. den Beitrag von Tellkamp und Kubach in diesem Buch).

Für Unternehmen stellt sich nun die Frage, wie sie solche Zusatzfunktionen mit Kundennutzen identifizieren können. Eine mögliche Herangehensweise bietet die Kommunikationsdimension smarter Produkte: Die These von Watzlawick et al. [WBJ69, S. 53], dass Menschen „*nicht nicht* kommunizieren können“, lässt sich auch für Produkte postulieren. Wenn Produkte *nicht nicht* kommunizieren können, dann kommunizieren sie ebenso wie Menschen immer, entweder auf der Funktions- oder aber auf der Beziehungsebene.

Für die Gestaltung der Beziehungsebene ist das industrielle Design zuständig. Sein Ziel ist die Maximierung des ästhetischen Nutzens sowie die intuitive und einfache Anwendbarkeit. Es hilft sowohl dem Kunden, der sich in der Umgebung der Maschine wohl fühlt, als auch dem Produzenten, der seine Marktposition verteidigen bzw. verbessern kann.

Für die Gestaltung des funktionalen Nutzens eines Produktes ist vor allem die Produktentwicklung zuständig. Ihr Ziel ist es, den vom Anwender wahrgenommenen funktionellen Nutzen zu maximieren.

Kommunikationsdesign und Funktionsdesign sind stark interdependent, denn je reichhaltiger die Funktionalität eines Gegenstandes, desto umfangreicher ist dessen Kommunikationsbedürfnis: Während ein Hammer heute noch gut ohne Leuchtdioden, Pfeiftöne oder Minibildschirm auskommt, sind funktional reichhaltigere Dinge wie Kaffeemaschinen, Videorekorder, Mobiltelefone, Lastkraftwagen oder Werkzeugmaschinen auf Kommunikationshilfen angewiesen. Der Zusammenhang zwischen Funktionsvielfalt und Kommunikationsbedürfnis ermutigt zum Umkehrschluss: UbiComp erhöht die Kommunikationsfähigkeit und mit ihr auch den wahrnehmbaren Nutzen aus zusätzlicher Funktionalität: Je mehr Abbildungsqualität desto mehr Kommunikation, Funktion und Nutzen. Die etwas provokant formulierte These zur Ableitung von Nutzen stiftender Funktionen lautet somit: „Gute Produkte wollen kommunizieren.“ Genauer müsste sie lauten: Pro-

duzenten wollen, dass ihre Produkte durch Kommunikation Wettbewerbsvorteile schaffen. Sie nutzen das Produkt als Agenten, dem sie die Fähigkeit mit auf den Weg geben, seiner Umgebung, insbesondere den Kunden, aber auch dem Produzenten selber, durch Kommunikation Nutzen zu stiften.

Um die neuen Funktionen abzuleiten, sehen Produzenten ihre Produkte als Schnittstelle zu ihren Kunden (vgl. Abbildung 13) und stellen folgende zwei Fragen: Welche Zusatzfunktionen können sie dem Kunden zur Verfügung stellen? Welche Zusatzfunktionen vermitteln dem Produzenten Vorteile?

Typische Informationen, mit denen ein Produkt sowohl dem Kunden als auch dem Produzenten Nutzen stiften kann, sind Statusinformationen wie etwa Ort und Produktidentifikationsnummer bzw. Umgebungszustand. So könnte ein Hammer seinem Besitzer mitteilen, wo er sich befindet, und seinem Produzenten, wie oft er schon verwendet worden ist. Liegt das Werkzeug in einem „fremden" Werkzeugkoffer, meldet es sich selbstständig. Auch beim Verlassen eines vordefinierten Raumes sendet das smarte Werkzeug eine Meldung an die betroffenen Parteien und trägt so beispielsweise zur Diebstahlsicherung bei (vgl. Abbildung 13).

Im Bereich „Business-to-Business" wenden Unternehmen UbiComp-Technologien heute i.d.R. in Produktionsmitteln an, z.B. Maschinen, Werkzeugen, Transportbehältern und Regalsystemen. Der Zusatznutzen für den Produzenten von Produktionsmitteln basiert auf den gewonnenen Daten über die Art und Weise ihrer Verwendung durch den Kunden bzw. Nutzer. Dies ist beispielsweise der Fall, wenn ein Transportbehälter laufend seine Position und Auslastung, eine Bohrmaschine ihren Betriebszustand sowie die beim Gebrauch genutzte Funktionalität und ein Regalsystem laufend seine aktuelle Belegung und derzeitigen Umschlag mitteilt.

Jedes Produktionsmittel wird damit zur Prozessschnittstelle und neuen Informationsquelle für seinen Hersteller und seine Nutzer. Auf der Herstellerseite interessieren insbesondere Informationen über die genutzte Funktionalität, Nutzungsfrequenz und -charakteristik der Produktionsmittel, die in zukünftige Produktentwicklungen und -konfigurationen sowie in die Sortimentspolitik einfließen. So können Auslastungen, Transport- und Stillstandszeiten von Transportbehältern, Paletten und Lastkraftwagen bilanziert oder Drehzahlen und Beanspruchungsspitzen von Bohrmaschinen mit dem Ziel erfasst werden, produktivere Produktionsmittel oder produktivitätsstiftende, ergänzende Produkte zu entwickeln bzw. dem Nutzer besser geeignete Produktionsmittel zur Verfügung zu stellen.

Auf der Nutzerseite interessiert beispielsweise der Ort, die Auslastung sowie die mit einem Werkzeug erzielte Produktivität für die eingesetzte Aufgabe. Zusätzlich können über mehrere Einsätze des Produktionsmittels automatisch Benchmark- und Prozessinformationen gewonnen und dem Nutzer mitgeteilt werden. Das smarte Regal weiß beispielsweise selbst, wie gut sein Nutzer das Lager organisiert und betreibt.

Dies alles verdeutlicht, dass das smarte Produkt bald im Zentrum eines Netzwerks aus Nutzern, Herstellern und verschiedenen Organisationseinheiten oder Dienstleistern wie Versicherern, Controllern, Prozessoptimierern und Qualitätsmanagern steht und die zukünftige Wettbewerbslandschaft rund um den Produktions- und Nutzungsprozess beeinflussen wird [Wal02].

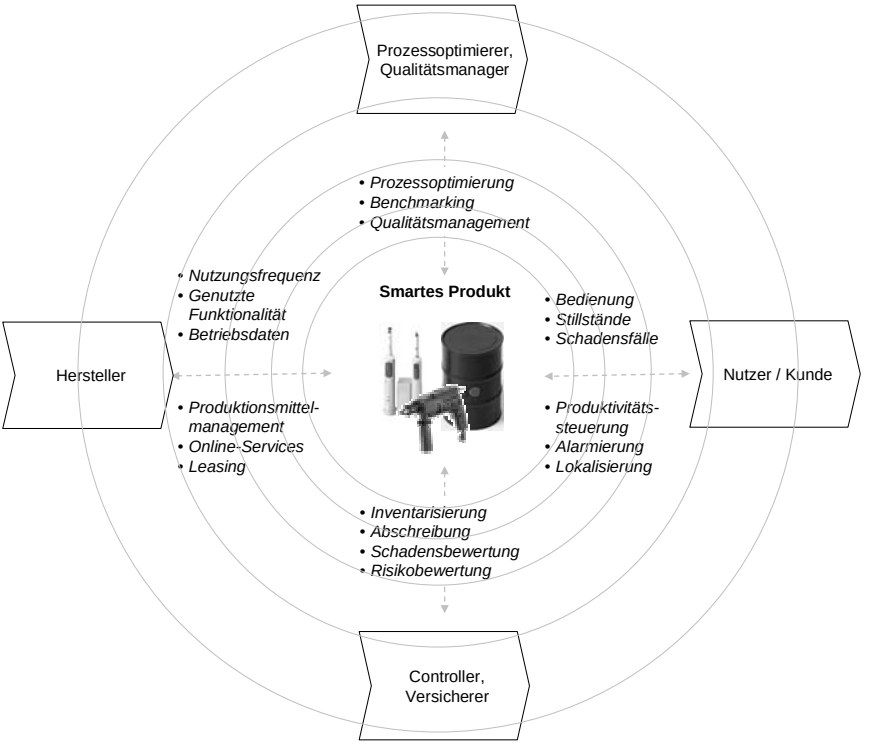


Abb.13. Das smarte Produkt und sein Kommunikationsnetzwerk

3.4 Smarte Dienstleistungen

Das Messbarmachen von bisher nicht wirtschaftlich Messbarem heißt nicht nur Steuerbarmachen von bisher nicht wirtschaftlich Steuerbarem. Es führt in letzter Konsequenz zur Bewirtschaftung, Bepreisung und damit Handelbarkeit von bisher nicht Handelbarem. Wenn die Benutzung von Straßen, Werkzeugen, Winterreifen, Aufzügen, Sitzgelegenheiten etc. nicht zuverlässig und hinreichend genau gemessen werden kann, so kann sie auch nicht nutzungsbasiert verrechnet werden. Und Leistungen, die nicht verrechnet werden können, bleiben als Gemeinkosten in derselben Bilanzhülle. Sie können nicht an externe Dienstleister ausgelagert werden.

Höhere Abbildungsqualität führt zu neuen handelbaren Dienstleistungen und infolge zu mehr Arbeitsteilung. Beispielsweise erschienen mit der kommerziellen Einführung von GPS erstmals elektronische Navigationsdienste am Markt. Als Nächstes folgten GPS-basierte Stau- und Unfallwarnungen. Bei der geplanten Steigerung der Auflösungsqualität von GPS-ähnlichen Systemen von derzeit ca. 10 auf einige wenige Meter und darunter sind weitere Services wie etwa ein War-

nungsservice vor Geisterfahrern denkbar. Die Rückverfolgung von Gütern, die Sicherstellung der Authentizität von Markenartikeln oder der Nachweis der Echtheit von Medikamenten sind auf Basis von UbiComp-Technologien bepreisbar und werden in den nächsten Jahren von neuen wie bestehenden Unternehmen als hoch spezialisierte Dienstleistungen angeboten. Smarte Dienstleistungen sind Services, die aus höherer Abbildungsqualität entstehen.

Auch Produktunternehmen haben seit einigen Jahren die Lukrativität von Dienstleistungen erkannt. Die Forschung aus dem Bereich der industriellen Dienstleistungen zeigt, dass Produktunternehmen, die auch produktbezogene Dienstleistungen verkaufen, im Durchschnitt mehr Gewinn erwirtschaften als Unternehmen, die ausschließlich Produkte vertreiben [FrG05, WiB99]. Die Gründe dazu liegen auf der Hand: Einerseits werden Produkte immer mehr zu vergleichbaren Massenartikeln mit sinkenden Margen. Außerdem verschenken viele produzierende Unternehmen zahlreiche produktbezogene Services beim Verkauf ihrer Produkte sozusagen als Rabattmarken, was die Margen weiter reduziert. Auf der anderen Seite ist der Kunde durchaus bereit, seine Koordinationsaufgaben an einen Dienstleistungsanbieter auszulagern und das Servicegeschäft selber ist wegen seinen finanziellen (Ertrag, Marge und Stabilität des Geschäfts), marketingorientierten (Cross-Selling mit Produkten) und strategischen Chancen (arbeitsintensiv und damit schwer imitierbar) lukrativ. Zahlreiche Produktunternehmen versuchen daher zurzeit, sich in Richtung Hybrid aus Produzent und Dienstleistungsanbieter zu transformieren.

UbiComp-Technologie bietet Möglichkeiten, ein Produkt mit ertragsträchtigen Dienstleistungen zu verknüpfen. Denn oft stiftet nicht der ins Produkt integrierte Minicomputer den nachgefragten Kundennutzen, sondern die mit dem smarten Produkt verknüpfte Dienstleistung. Beispielsweise plant Chep, der weltgrößte Paletten- und Container-Pool-Operator, seine über 250 Millionen wieder verwendbaren Paletten mit Funketiketten auszustatten, um seinen Kunden nicht nur Transportmittel, sondern auch Logistikinformationsservices zur Verfügung stellen zu können. Die Funketiketten sind das Bindeglied zwischen den Paletten und dem Service.

In Praxis und Forschung beginnen verschiedene Typen von UbiComp-basierten Dienstleistungen sichtbar zu werden. Zu den wichtigsten Dienstleistungstypen zählen:

- **Kontroll-Dienstleistungen.** Unternehmen lagern Kontrollaufgaben wie Track&Trace, Diebstahlsicherung, Fälschungssicherung, Rückverfolgung und Nachbestellung an hoch spezialisierte Dienstleister aus.
- **Leasing-Dienstleistungen.** Eine hohe Abbildungsqualität ermöglicht die Umstellung der Berechnungsgrundlage von Besitzerinformationen auf Nutzungsinformationen. Die Nutzung wird bezahlt, nicht mehr der Besitz. Dies kann Vorteile für Anbieter (finanzieller, marketingorientierter und strategischer Natur) wie für Nachfrager (keine hohen Anfangsinvestitionen, Flexibilität, Ausfallsicherheit etc.) mit sich bringen.
- **Risiko-Dienstleistungen.** Versicherungsunternehmen nehmen nicht nur Kontroll-Dienstleistungen in Anspruch, um Risiken vorzeitig zu erkennen und zu minimieren, sondern entwickeln Methoden zur Einschätzung und Verrechnung des de facto entstehenden Risikos. Beispielsweise ersetzen detaillierte, von

UbiComp-Technologie im Auto im Lauf des Monats erfasste Daten zu Fahrstrecke (Autobahn, Landstraße, Stadt), Tageszeit (Tag, Nacht), Geschwindigkeit etc. die sonst üblichen Schätzwerte zur Berechnung der monatlichen Versicherungskosten [Pro00].

- **Informations-Dienstleistungen.** Das Besondere an diesen Dienstleistungen ist, dass sie Menschen ermöglichen, schnell und ohne viel Zwischenschritte und Medienbrüche Information zu erhalten oder zu versenden. Eine Beispielgruppe bilden hier die Gemälde, Konsumgüter oder Denkmäler, die einem PDA bzw. Smartphone die Adresse ihrer Homepage zur Darstellung zugehöriger Informationen zusenden [RoG04]. Die schnelle Weiterleitung der mit Smartphones geschossenen Bilder von in flagranti geknipsten Verkehrssündern und Bankräubern an die Polizei oder andere Ordnungshüter wäre ein weiteres Beispiel [GeF02].
- **Komplexe Dienstleistungen.** Sie stellen eine Kombination der obigen Dienstleistungen dar. Beispielsweise verknüpft die komplexe Dienstleistung „Flottenmanagement“ für Werkzeuge Kontroll- und Leasingdienstleistungen zu einem neuen Dienstleistungsbündel.

4 Entwicklungstrends

4.1 Von der Integrationsweite zur -tiefe

Die obigen Ausführungen zeigen deutlich, dass die von Mark Weiser bereits 1991 formulierte Vision des Ubiquitous Computing ein logischer und zwingender nächster Schritt in der betriebswirtschaftlichen Informationsverarbeitung ist [Wei91]. Sie ist damit trotz des gegenwärtig zu beobachtenden RFID-Hypes keine Modeerscheinung.

Viele Begriffe mögen noch unscharf sein und sich im Laufe der Zeit den jeweils herrschenden Lehren und Marketingvokabeln anpassen, von Pervasive Computing über Ambient Intelligence und Context Aware Computing bis hin zu Silent Commerce. Unabhängig von der Namensgebung bringt das *Konzept UbiComp* aber eine neue Qualität in die betriebliche Informationsverarbeitung. Während die klassische Entwicklung der Informationsverarbeitung von lokalen Inselsystemen bis hin zu unternehmensübergreifenden E-Business-Systemen das Netz der zur besseren Organisation gewonnenen Daten in erster Linie *vergrößert* hat – von anfänglich einzelnen Abteilungen erstreckt es sich heute über ganze Wertschöpfungsketten (vgl. Abbildung 1) –, macht UbiComp das Datenerfassungsnetz *feinmaschiger*. Während der E-Business-Trend die Integrationsreichweite erhöht, steigert der UbiComp-Trend die Integrationstiefe (vgl. Abbildung 14). Mit der Erhöhung der Abbildungsqualität erlaubt UbiComp feingranulares Bewirtschaften von Massenressourcen: einzelne Produkte anstelle der üblichen Produktklassen, Transportbehälter zusätzlich zu den bisher schon bewirtschafteten Produktionsmaschinen, Zeit- und Ortspunkte anstelle von ungenauen Zeit- und Ortsräumen, Umgebungsinformation zusätzlich zu Objektinformation. UbiComp ermöglicht damit auch die kosteneffiziente Bewirtschaftung von B- und C-Ressourcen.

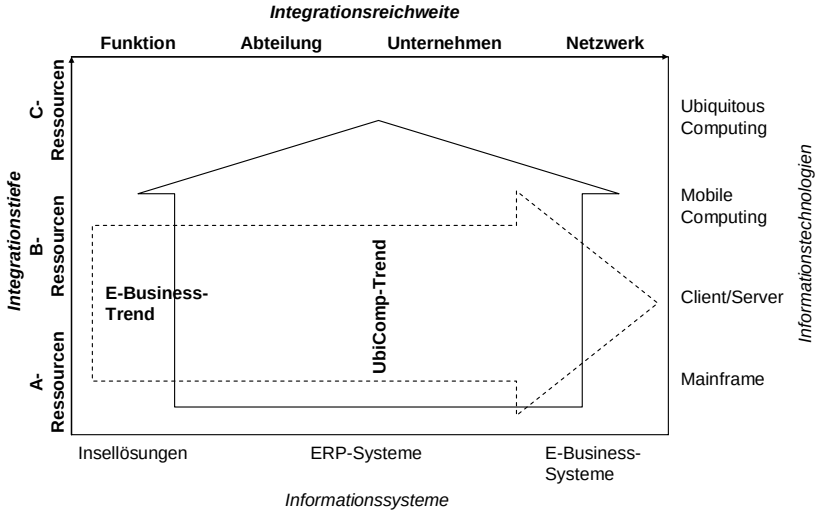


Abb. 14. Integrationsweite und -tiefe

4.2 Von geschlossenen zu offenen Kreisläufen

Eine Analyse der bisher implementierten UbiComp-Lösungen im Bereich RFID zeigt, dass die Steigerung der Integrationstiefe typischerweise in geschlossenen Kreisläufen (closed loops) beginnt (vgl. Abbildung 15). Der Grund dafür liegt erstens darin, dass die Durchsetzung innovativer Projekte innerhalb eines Unternehmens einfacher ist als in einem Netzwerk mit mehreren gleichberechtigten Partnern, die unterschiedliche Interessen verfolgen und über unterschiedliche Budgets verfügen. Hierarchischer Druck ist eben einfacher zu erzeugen als Win-Win-Situationen im Unternehmensnetzwerk. Zweitens ist die Rentabilitätsrechnung von UbiComp-Lösungen in vielen Fällen nicht trivial. Denn UbiComp-Lösungen erfordern eine neue Infrastruktur aus informationstechnischen Einrichtungen, Kommunikationsnetzen, Middleware und Datenbanken, deren kurzfristiger und quantitativer Nutzen oft genug ähnlich schwierig zu berechnen ist wie jener einer neuen Werksstraße. Die Entscheidung für oder gegen beispielsweise RFID ist eine Entscheidung für oder gegen eine neue Infrastruktur.

Herausforderungen bei der Verteilung von Kosten und Nutzen von UbiComp-Lösungen bilden den dritten Grund, der für einen Adoptionsstart innerhalb der eigenen Unternehmensgrenzen spricht. Denn in Closed-Loop-Anwendungen entstehen sowohl Kosten als auch Nutzen in derselben Bilanzhülle. Bei offenen Systemen sind dagegen Kosten und Nutzen auf unterschiedliche Bilanzhüllen verteilt. Zur Lösung der Fragen „Wer hat welchen Nutzen? Wer hat welchen Teil der Kosten bezüglich Ausrüstung, Infrastruktur und Transformation zu tragen?“ bedarf es in der Regel eines langwierigen politischen Prozesses, der von der Machtvertei-

lung innerhalb des Netzwerks aber auch von Unsicherheit über den faktischen Nutzen geprägt ist.

Sind die ersten Erfahrungen beispielsweise im internen Behältermanagement gemacht und Wissen im Umgang mit UbiComp-Technologie aufgebaut, hat sich das Unternehmen eine gute Position zur Teilnahme an offenen Lösungen erarbeitet. Allerdings nur dann, wenn es auf die richtigen Standards gesetzt hat. Denn Behälter und Produkte, die nur intern kommunizieren können, sind nur so wertvoll wie ein Haustelefon im internationalen Geschäft. Die aktive Teilnahme an Standardisierungsinitiativen, wie im Bereich RFID die Auto-ID Labs bzw. EPCglobal, ist für Erst- und Frühanwender von RFID-Technologie daher unverzichtbar.

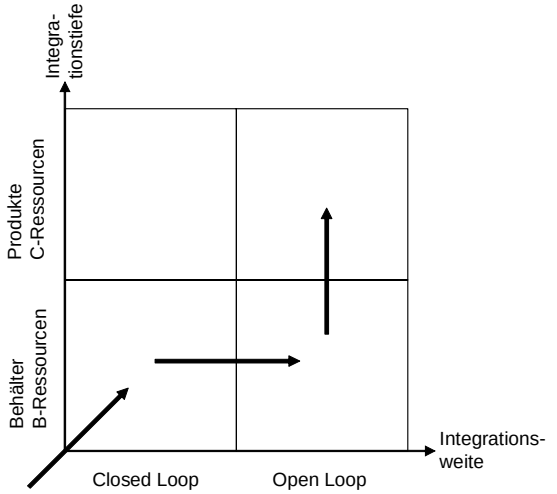


Abb. 15. Typischer Technologieadoptionspfad

4.3 Dienstleistungen folgen Prozessen und Produkten

Zahlreiche Unternehmen nutzen die hohe Abbildungsqualität der UbiComp-Technologie in einem ersten Schritt lediglich, um ihre De-facto-Prozesse („Wann und wo findet der Diebstahl statt?“) und De-facto-Verwendung ihrer Produkte („Welchen Temperaturen und Beschleunigungen ist das Produkt tatsächlich ausgesetzt?“) besser kennen zu lernen. Sie verwenden UbiComp lediglich als Monitorinstrument, wobei die damit ermittelten Fakten anschließend die Grundlage zur Analyse der Probleme und Möglichkeiten zur Gestaltung verbesserter Prozesse und Produkte bilden.

Es zeichnet sich ab, dass die Entwicklung von smarten Dienstleistungen erst in einer zweiten Phase stattfindet (vgl. Abbildung 16). Denn sie setzt nicht nur eine zumindest regional funktionierende Infrastruktur (eben das Internet der Dinge – oder aus Sicht der Telekommunikationsunternehmen das Telefon der Dinge) vor-

aus, sondern auch bereits erworbene Erfahrung im Umgang mit höherer Abbildungsqualität, insbesondere mit automatisierten Prozesskontrollen und smarten Produkten. So setzt beispielsweise ein Service, der Fußballfans, Trainer und Spieler über Ballkontakte, Schussgeschwindigkeit, Gegnerkontakte und gelaufene Kilometer pro Halbzeit informiert, neben smarten Fußbällen und smarten Fußballschuhen, auch eine funktionierende Infrastruktur in allen maßgeblichen Stadien voraus.[3] Die Interdependenzen zwischen Produkt-, Prozess-, Dienstleistungs- und Infrastrukturentwicklung nehmen zu.

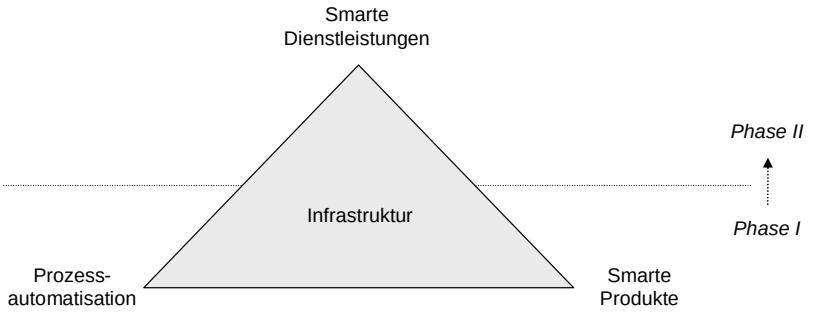


Abb. 16. Zusammenhang zwischen Prozess, Produkt, Dienstleistung und Infrastruktur

5 Ausblick

5.1 Reduktion der Wertschöpfungstiefe

Der Einsatz von UbiComp-Technologien ermöglicht eine feinmaschigere und genauere Messung der physischen Realität, erhöht damit die Abbildungsgenauigkeit und befähigt letztlich zur Steuerung, Bewirtschaftung, Bepreisung und Handelbarkeit von Leistungen, die bisher nicht wirtschaftlich messbar und steuerbar waren. Die Handelbarkeit lässt sich auf die Reduktion der Spezifität im Sinne der Transaktionskostentheorie zurückführen [Wil91], die sich aus der besseren Messbarkeit und der damit einhergehenden Digitalisierung der Leistung erklärt. Die Reduktion der Spezifität bedeutet für Leistungen, deren transaktionskostenoptimale Organisationsform bisher die Hierarchie war, dass das neue Transaktionskostenoptimum sich in Richtung Netzwerk bzw. Markt bewegt. Diese potenziell neu gewonnene Handelbarkeit bedeutet eine Reduktion der Wertschöpfungstiefe des auslagernden Unternehmens und neue Geschäftschancen für alte und neue Anbieter. Spezialisierung und Arbeitsteilung steigen. Insbesondere im Bereich Lokation, Verfolgen und Authentifizieren von Produkten entstehen am Markt derzeit neue Dienstleistungsangebote, die noch vor fünf Jahren kaum vorstellbar waren.

[3] vgl. www.cairos.de

5.2 Zunahme der Digitalisierung

Als ökonomische Gebilde sind Unternehmen stets bestrebt, ihre Prozesskosten zu minimieren. Die Gesamtkosten PK_G eines Prozesses setzen sich zusammen aus den Kosten des physischen Prozesses PK_{RW} = f (Arbeitskräfte, Lagerbestände, Anlagen etc.), jenen des digitalen Prozesses PK_{VW} = f (Software, Hardware, Einführung, Wartung) und den Kosten der Abbildung in beide Richtungen PK_A = f (Sensorik, Aktuatorik), siehe Abbildung 17 und 18. Das Kostenoptimum bezogen auf den Grad der Digitalisierung bzw. „Virtualisierung" befindet sich an der (in der Praxis im Allgemeinen eindeutigen) Stelle $(PK_{VW} + PK_{RW} + PK_A)' = 0$. Reduzieren sich nun die Abbildungskosten PK_A und sind Grenzkosten der physischen Prozesse höher als jene der virtuellen Prozesse inklusive der Abbildung, so verschiebt sich das Gesamtkostenoptimum in Richtung höherer Virtualisierung und damit Digitalisierung. Der Grad der Virtualisierung V ist das Verhältnis zwischen den virtuellen Prozesskosten inklusive den Abbildungskosten zu den Prozesskosten der physischen Realität $(PK_{VW} + PK_A) / PK_{RW}$. Dieser Wert ist im Minimum 0, z.B. in einem Handwerksbetrieb, der noch keine Informationssysteme verwendet, und „unendlich" in einem Unternehmen, das keine physischen Prozesse mehr besitzt, etwa einer idealtypischen virtuellen Bank.

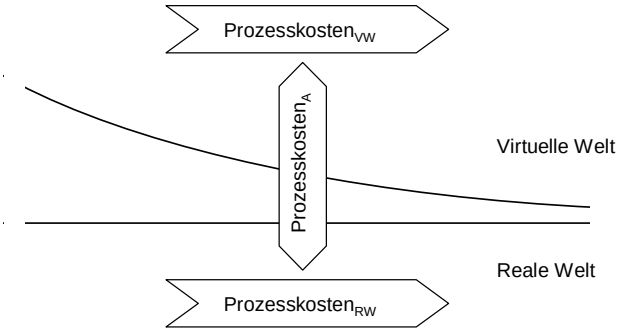


Abb. 17. Reale und virtuelle Welt und Abbildungskosten eines Prozesses

Die Geschichte der betrieblichen Informationsverarbeitung gibt Anlass zur Vermutung, dass in vielen Industriebereichen mit starkem Bezug zur physischen Welt der Grad der Virtualisierung aufgrund der sinkenden Abbildungskosten zunimmt. Digitale Prozesskontrollen sind in vielen Fällen eben kostengünstiger als physische bzw. manuelle. Wenn beispielsweise ein Basisteil sicherstellen soll, dass es nur in Zusammenhang mit gewissen Verbrauchsteilen funktioniert, so kann diese Kontrollfunktion mechanisch oder elektronisch gebaut werden. Die mechanische Lösung arbeitet etwa mit unterschiedlichen Passformen, die sich gegenseitig ausschließen. Sie ist intuitiv und damit einfach anzuwenden. Doch sie benötigt mehrere Werkzeuge, ist statisch und damit kostenintensiv. Eine elektronische Lösung kann auf ein und derselben Infrastruktur unterschiedliche digitale Passungen realisieren und diese relativ kostengünstig verändern.

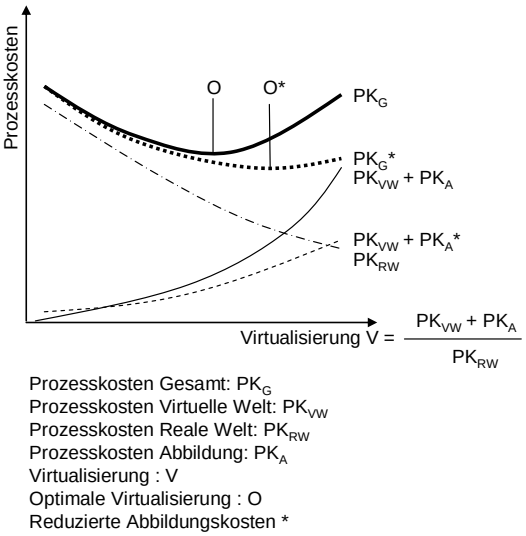


Abb. 18. Ubiquitous Computing fördert die Zunahme der Digitalisierung

5.3 Steigerung der Überlebensfähigkeit

Nach der These von Conant und Ashby „Every good regulator of a system must be a model of that system" kann eine Steuerung eines Systems nur so gut sein wie dessen Modell [CoA81]. Diese Aussage stützt sich auf ein fundamentales Gesetz der Kybernetik, das besagt, dass Varietät nur durch Varietät absorbiert werden kann („Only variety can absorb variety") [Ash56], was beispielsweise bedeutet, dass eine gute Fußballmannschaft mit Einfallsreichtum und flexiblem Spiel eben nur von einer ebenso einfallsreichen und flexiblen Fußballmannschaft besiegt werden kann oder dass jemand mit einem Wortschatz von 3000 Wörtern Shakespeare nicht ins Deutsche übersetzen kann. Übertragen auf das Management bedeutet dies, dass die Varietät des Managements immer der Varietät der aktuellen Situation entsprechen muss [Mal98, Sch01].

Die Varietät ist dabei das Maß für die Komplexität eines Systems. Sie wird in der Kybernetik definiert als die Anzahl der möglichen unterscheidbaren Zustände, die ein System haben kann. Um ein komplexes System zu kontrollieren, benötigt der Kontrollierende demnach mindestens das gleiche Maß an Komplexität. Die Anzahl der möglichen Systemzustände hängt maßgeblich von der Messgenauigkeit des Systems ab. Je höher die Messgenauigkeit und mit ihr die Abbildungsqualität, desto höher die Varietät und umgekehrt. Die Aufgabe des Managements liegt nun darin, die angemessene Varietät zu wählen. Diese wird von der aktuellen Situation am Markt bestimmt. Die Maximierung der Eigenvarietät ist dabei ein genauso falsches Patentrezept wie das oft zitierte „keep it simple".

Unternehmen wie Metro, Wal-Mart und British Petrol, die heute stark mit RFID oder Sensornetzen experimentieren, gehen von einem komplexer werden-

den Umfeld aus und versuchen – wohl mehr implizit als explizit – auch mit Hilfe engmaschigerer Messsysteme ihre Varietät und damit Wettbewerbsfähigkeit zu erhöhen, denn höhere Fähigkeiten erwachsen nur aus mehr Komplexität [Bre83].

5.4 Büchse der Pandora

Als Prometheus der Menschheit Feuer, Freiheit, Technik und Kunst geschenkt hat, wurden er und die Menschheit von Zeus dafür bestraft, denn Prometheus hatte Zeus zum Vorteil der Menschen überlistet. Zeus ließ Prometheus an seinen Felsen ketten und schickte Pandora mit einer Büchse gefüllt mit allem Übel auf die Erde. Pandora öffnete die Büchse und alles Übel entwich. Seither stehen Pandora und ihre Büchse für die Zerstörungsmacht des Fortschritts. Mit Pandora fand die Schattenseite Eintritt in das Leben, jedes Gut erhielt sein widriges Gegenstück, Gut und Böse sind seither nicht nur miteinander vermischt, sondern unauflöslich; sie sind untrennbar ineinander verwoben [Jac98].

Wenn man den griechischen Mythen Glauben schenkt, dann kann die Anwendung von UbiComp nicht nur in höherer Überlebensfähigkeit von Organisationen, in besseren Prozessen, Produkten und Dienstleistungen, kurz in einer Welt, die von Vorteilen für alle geprägt ist, münden. Sie führt gleichermaßen zu fragwürdigen Anwendungen und neuen Problemen, die genauso wenig vorhersehbar sind wie Zukunft an sich: „Unforeseen consequences stand in the way of all those who think they see clearly the direction in which a new technology will take us. Not even those who invent a technology can be assumed to be reliable prophets […]" [Pos93, S. 15].

Eine Schattenseite der Automatisierung von Kontrollaufgaben ist der ungewünschte Kontrollverlust der Anwender, der schon in der UbiComp-Bezeichnung „Human-out-of-the-loop-computing" [Ten00] seine Andeutung findet [BCL04]. Der Umgang mit dem Kontrollverlust steht auch im Zentrum der Diskussion zur Wahrung der Privatsphäre. Die Beiträge von Langheinrich sowie Thiesse in diesem Buch sind der Beschreibung, Erklärung und Gestaltung dieses Phänomens gewidmet.

Eine weitere bisher wenig diskutierte Schattenseite stellen die so genannten Sekundäreffekte der automatischen Prozesskontrolle, smarten Produkte und Dienstleistungen dar. Ein Sekundäreffekt beschreibt eine indirekte nicht unmittelbar einsichtige Konsequenz einer Entwicklung. So führt beispielsweise ein neuer Automotor, der den Benzinverbrauch um 50 % reduziert, nicht nur zu Einsparungspotenzialen bei Treibstoff, sondern aufgrund der Nachfrageelastizität auch zu mehr gefahrenen Kilometern. Der gesamte Spritverbrauch sinkt also wegen des Sekundäreffektes um weniger als 50 %.

UbiComp-Technologie führt im Effekt erster Ordnung zu automatischen, besser steuerbaren und damit sichereren Prozessen. Dies hat im Effekt zweiter Ordnung zur Folge, dass sich Mitarbeiter auf die neuen automatischen Prozesse verlassen und das Wissen über das innere Funktionieren der automatischen Steuerung vergessen. Ändern sich Rahmenbedingungen oder versagt die Steuerung ausnahmsweise aus technischen Gründen, wird der Prozess unkontrollierbar, denn der flexible Mensch ist nicht mehr Teil des Managementregelkreises oder er

hat das entsprechende Wissen nicht mehr zur Verfügung. Während die Summe an Fehlern tendenziell abnimmt, nimmt der potenzielle Effekt eines einzelnen Fehlers tendenziell überproportional zu (vgl. dazu das Konzept der Diseconomies of Risk von [Hal04]).

Die faktenbasierte Risikorechnung gibt ein weiteres Beispiel für einen Sekundäreffekt, der deutlich zeigt, dass die Einführung einer neuen Technologie ihre Grenzen finden muss. UbiComp ermöglicht einerseits die Erstellung einer genauen Versicherungsrechnung aufgrund der in Realität physisch erlebten Risiken (siehe Beispiel zur Kfz-Versicherung weiter oben). Die zweite Ableitung zeigt andererseits, dass die bis ins Detail messerscharf erfassbare Rechnung Risikoprofile offen legt, die auf ökonomischer Basis nicht mehr rechenbar und damit auch nicht versicherbar sind. Die genaue Rechenbarkeit im ersten Effekt führt zur Nichtrechenbarkeit im zweiten Effekt. Sie entzieht der Versicherung damit einen Teil der Grundlage ihres Geschäfts, das auf dem Ausgleich der Risiken aufbaut.

5.5 Aktuatorik

Im Jahr 2001 startete das M-Lab seine Forschungsaktivitäten mit dem Ziel, die betriebswirtschaftlichen Applikationen und Konsequenzen des Ubiquitous Computing zu erarbeiten. Das Forscherteam erkannte schnell, dass die erste und grundlegende Funktion einer UbiComp-Anwendung die Identifikation der Dinge ist. So vertiefte sich ein Teil des Teams in Identifikationstechnologien, allen voran RFID, und engagierte sich im Auto-ID Center, heute Auto-ID Labs/EPCglobal. Gemeinsam mit Laboratorien rund um die Welt arbeitet es als Auto-ID Lab St. Gallen/Zürich an der Infrastruktur des „Internets der Dinge“.

Die nächsten absehbaren Schwerpunktfunktionen lauten Lokalisierung und Sensorik. Mit RFID können Dinge im Wesentlichen nur mitteilen, wer sie sind. Auf ihren Ort kann nur indirekt über die Lokation der Lesegeräte geschlossen werden. Neue Lokalisierungstechnologien, wie beispielsweise energiearme GPS-Module mit integrierter Kommunikationseinheit, ermöglichen neue Abbildungsqualitäten und damit neue Applikationen. Sensoren können darüber hinaus die Zustände eines Dings und dessen Umgebung erfassen und in Sensornetzen ohne zentrale Steuereinheit kommunizieren.

Im Zentrum von RFID, Lokation und Sensorik steht die Abbildung der realen in die virtuelle Welt, nicht aber umgekehrt. Sie ist bemüht, möglichst jene Abbildungsqualität zu erzeugen, die eine neue betriebswirtschaftliche, medizinische oder militärische Anwendung benötigt. Die Abbildung der Rechenergebnisse der virtuellen Welt zurück in die reale Welt wird heute noch großteils dem Menschen überlassen. Er erhält vom Computer die Arbeitsanweisung, überprüft z.T. ihre Richtigkeit und setzt sie in der physischen Realität um. Zunehmend übernehmen Maschinen, so genannte Aktuatoren, diese Abbildung der digitalen Welt in die physische Welt (vgl. Abbildung 2), vom Auto zusammenschweißenden Industrieroboter über den Fenster schließenden Elektromotor bis hin zum Security Roboter, der nachts mit Infrarotscheinwerfern bestückt durch die leeren Werkshallen fährt und nicht vorhergesehene Aktivitäten aufdeckt. Diese Roboter haben wenig gemeinsam mit den menschenähnlichen Androiden aus den Filmen der 50er-Jahre

des letzten Jahrhunderts. Heute ist Rechenleistung so kostengünstig zu erwerben, dass sich der Bau eines Roboters für Spezialaufgaben lohnt. In der Industrie werden Roboter seit etwa 1960 eingesetzt. Heute arbeiten weltweit mehr als 800 000 solcher Maschinen. Ihre Anzahl wächst durchschnittlich mit 7 % p.a., Tendenz steigend.

Technologiefortschritt und Stückkostendegression sind dafür verantwortlich, dass sich die Preise von Industrierobotern seit 1990 auf ein Fünftel reduziert haben. Damit werden auch private Haushalte für den Robotermarkt interessant. Laut BusinessWeek [Bus04] wird der Haushaltsmarkt den Industriemarkt erstmals im Jahr 2006 übertreffen. Staubsauger (das Modell Roomba von iRobot wurde bereits über 200 000 Mal verkauft), Rasenmäher und Spielsachen wie der elektronische Hund „Aibo“ von Sony sind Vorboten einer von Robotern und anderen Aktuatoren bevölkerten Welt. Die Effekte, die Aktuatoren auf Gesellschaft, Wirtschaft und einzelne Unternehmen haben werden, sind heute allerdings so wenig bekannt wie jene von großflächig eingesetzten Lokalisierungs- und Sensorfunktionen.

Forscher aus unterschiedlichsten Disziplinen sind aufgefordert, die Vision des UbiComp konstruktiv-kritisch zu durchleuchten und über Konsequenzen und Gestaltungsmöglichkeiten aufzuklären. Das Wissen über UbiComp und dessen Einsatz darf nicht auf wenige Köpfe beschränkt sein, sondern muss, wie die zugrunde liegende Technologie, ubiquitär werden.

Literatur

[AEG02] Abowd GD, Ebling MR, Gellersen HW (2002) Context-Aware Pervasive Computing. IEEE Wireless Communications 9(5): 8–9

[Ash56] Ashby WR (1956) An Introduction to Cybernetics. Wiley

[AsS03] Ashton K, Sarma S (2003) Introducing the EPC Network. EPC Symposium, Chicago, USA, September 16, 2003

[BCL04] Bohn J, Coroama F, Langheinrich M, Mattern F, Rohs M (2004) Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications. Journal of Human and Ecological Risk Assessment 10(5): 763–786

[BGC02] Bharadwaj S, Gruen TW, Corsten DS (2002) Retail Out of Stocks – A Worldwide Examination of Extent, Causes, and Consumer Responses. Grocery Manufacturers of America, Food Marketing Institute and CIES – The Food Business Forum

[Bre83] Bresch C (1983) Zwischenstufe Leben. Evolution ohne Ziel? Piper

[Bri00] Bridgestone/Firestone (2000) Bridgestone/Firestone Announces Voluntary Recall of 3.85 million RADIAL ATX and RADIAL ATX II Tires, and 2.7 million Wilderness AT Tires. Bridgestone/Firestone Press Release, August 9, 2000, www.bridgestone-firestone.com/news/mediacenter/recall_archives/news/mediacenter/news/000809a.htm

[Bus04] BusinessWeek (2004) Robots: Today, Roomba. Tomorrow... May 6, 2004, www.businessweek.com/technology/content/may2004/tc2004056_2199_tc_168.htm

[CoA81] Conant RC, Ashby WR (1981) Every good regulator of a system must be a model of that system. In: Conant R (ed) Mechanisms of Intelligence – Ashby’s Writings on Cybernetics. Intersystems Publications, pp 205–214

[DoD03] Department of Defense (2003) DoD Announces Radio Frequency Identification Policy, www.defenselink.mil/releases/2003/nr20031023-0568.html
[EuU00] Europäische Union (2000) Richtlinie 2000/53/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über Altfahrzeuge
[EuU02] Europäische Union (2002) Richtlinie 2002/96/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 über Elektro- und Elektronik-Altgeräte
[Fle02] Fleisch E (2002) Das Netzwerkunternehmen. Springer-Verlag
[FlÖ00] Fleisch E, Österle H (2000) A Process-oriented Approach to Business Networking. Electronic Journal of Organizational Virtualness 2(2): 1–21
[FlÖ03] Fleisch E, Österle H (2003) Auf dem Weg zum Echtzeitunternehmen. In: Alt R, Österle H (Hrsg) Real-time Business. Springer-Verlag, S 3–17
[FMÖ02] Fleisch E, Mattern F, Österle, H (2002) Betriebliche Anwendungen mobiler Technologien – Ubiquitous Commerce. Computerwoche-Extra Nr. 01, 15. Februar 2002, S 12–13
[FrG05] Friedli T, Gebauer H (2005) Behavioral Implications of the Transition Process from Products to Services. Journal of Business and Industrial Marketing 20(2): 70–78
[GeF02] Gershman A, Fano A (2002) The Future of Business Services in the Age of Ubiquitous Computing. Communications of the ACM 45(12): 83–87
[GMA02] Grocery Manufacturers of America (2002) Full-Shelf Satisfaction – Reducing Out-of-stocks in the Grocery Channel
[Hal04] Haller M (2004) Je planmässiger die Menschen vorgehen, desto wirksamer vermag sie der Zufall zu treffen. Abschiedsvorlesung Universität St. Gallen, Schweiz, 8. Juni 2004,
www.ivwhsg.ch/custom/upload/docs/ewjrr3yzd6gldkbs564jjmldwaxy4t551g.pdf
[HoD01] Hollinger RC, Davis JL (2001) 2001 National Retail Security Survey – Final Report. University of Florida, web.soc.ufl.edu/SRP/NRSS_2001.pdf
[IBM02] IBM Business Consulting Services (2002) Focus on Retail – Applying Auto-ID to Improve Product Availability at the Retail Shelf. Auto-ID Center,
archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-001.pdf
[ICC04] ICC Policy Statement (2004) The fight against piracy and counterfeiting of intellectual property. Document 450/986. International Chamber of Commerce,
www.iccwbo.org/home/intellectual_property/fight_against_piracy.pdf
[IDT04] IDTechEx (2004) Smart Healthcare USA 2004 at a glance – RFID Smart Tagging and Smart Packaging, www.idtechex.com/smarthealthcareusa/index.asp
[Int04a] Intel Research (2004) Intel Research Berkeley – Collaborating to Change the World, www.intel.com/research/print/berkeley_collab.pdf
[Int04b] Intellion (2004) Product description LotTrack, www.intellion.com
[Jac98] Jacob F (1998) Die Maus, die Fliege und der Mensch. Berlin Verlag
[Kau03] Kaufhof (2003) Kaufhof AG startet RFID-Pilotprojekt mit Gerry Weber. Kaufhof Pressemitteilung, 26. Juni 2003,
www.galeria-kaufhof.de/sales/coco/co_presse_011_mit_030626_log.asp
[KBA04] Kraftfahrt-Bundesamt (2004) Pressebericht 2003/2004, www.kba.de/Stabsstelle/Presseservice/Jahrespressebericht/Jahrespressebericht_2003_20041.pdf
[MaC94] Malone T, Crowston K (1994) The Interdisciplinary Study of Coordination. ACM Computing Surveys 26(1): 87–119.
[Mal98] Malik F (1998) Komplexität – was ist das? Modewort oder mehr? Kybernetisches Führungswissen – Control of High Variety-Systems. Cwarel Isaf Institute,
www.managementkybernetik.com/dwn/Komplexitaet.pdf

[Met04] METRO Group (2004) METRO Group startet die unternehmensweite Einführung von RFID. METRO Group Presseerklärung, 12. Januar 2004, www.future-store.org/servlet/PB/menu/1002256/index.html

[OECD98] Organization for Economic Co-operation and Development (1998) The Economic Impact of Counterfeiting, www.oecd.org/dataoecd/11/11/2090589.pdf

[ÖBW92] Österle H, Brenner W, Hilbers K (1992) Unternehmensführung und Informationssystem, 2. Auflage. Teubner

[Öst95] Österle H (1995) Business Engineering, 2. Auflage. Springer-Verlag

[Pos93] Postman N (1993) Technoply – The Surrender of Culture to Technology. Vintage Books

[Pro00] Progressive Insurance (2000) Progressive Awarded Second Patent for Usage-Based Auto Insurance Rating System. Progressive Insurance Press Release, July 13, 2000, www.progressive.com/newsroom/2nd_patent.asp

[RDT01] Raman A, DeHoratius N, Ton Z (2001) Execution – The Missing Link in Retail Operations. California Management Review 43(3): 136–152

[Rfi03] RFID Journal (2003) Wal-Mart Lays Out RFID Roadmap, November 10, 2003, www.rfidjournal.com/article/view/647

[RoG04] Rohs M, Gfeller B (2004) Using Camera-Equipped Mobile Phones for Interacting with Real-World Objects. In: Ferscha A, Hoertner H, Kotsis G (eds) Advances in Pervasive Computing. Austrian Computer Society (OCG), pp 265-271

[Sch01] Schwaninger M (2001) System theory and cybernetics – a solid basis for transdisciplinary in management education and research. Kybernetes – The International Journal of Systems & Cybernetics 30(9/10): 1209–1222

[Ten00] Tennenhouse D (2000) Proactive Computing. Communications of the ACM 43(5): 43–50

[Wal02] Waldo J (2002) Virtual Organizations, Pervasive Computing, and an Infrastructure for Networking at the Edge. Information Systems Frontiers 4(1): 9–18

[WBJ69] Watzlawick P, Beavin JH, Jackson DD (1969) Menschliche Kommunikation – Formen, Störungen, Paradoxien. Verlag Hans Huber

[Wei91] Weiser M (1991) The computer for the 21st century. Scientific American 256(3): 66–75

[WiB99] Wise R, Baumgartner P (1999) Go Downstream – The New Profit Imperative in Manufacturing. Harvard Business Review 77(5): 133–141

[Wil91] Williamson OE (1991) Comparative Economic Organization – The Analysis of Discrete Structural Alternatives. Administrative Science Quarterly 36(2): 269-296

[Wir04] Wired News, No Chip in Arm, No Shot From Gun, April 14, 2004, www.wired.com/news/technology/0,1282,63066,00.html

Die technische Basis für das Internet der Dinge

Friedemann Mattern
Institut für Pervasive Computing, ETH Zürich

Es kommt mir so vor, als sei das rasante Wachstum des WWW nur der Zündfunke einer viel gewaltigeren Explosion gewesen. Sie wird losbrechen, sobald die Dinge das Internet nutzen.
Neil Gershenfeld, MIT

Kurzfassung. Der stete Fortschritt der Mikroelektronik, Kommunikationstechnik und Informationstechnologie hält weiter an. Damit rückt auch die Vision einer umfassenden „Informatisierung" und Vernetzung der Welt und ihrer vielen Gegenstände immer näher. Funketiketten auf RFID-Basis, multimediafähige Handys und Chips in Kreditkarten und Ausweispapieren sind dabei nur die ersten Vorboten des kommenden Zeitalters des Ubiquitous Computing: Denn nicht nur Mikroprozessoren und ganze Computer werden immer leistungsfähiger, kleiner und preiswerter, sondern bald lassen sich auch über Funk miteinander kommunizierende Sensoren, die ihre Umgebung erfassen, sehr billig in miniaturisierter Form herstellen und millionenfach in die Umwelt einbringen oder unsichtbar in Gegenstände einbauen. Zusammen mit neuen Technologien zur Ortsbestimmung bekommen so gewöhnliche Dinge eine noch nie da gewesene Qualität – diese können dann wissen, wo sie sich gerade befinden, welche anderen Gegenstände oder Personen in der Nähe sind und was in der Vergangenheit mit ihnen geschah. Aus ihrem Kontext können sie vielleicht sogar einfache Schlüsse über die Situation, in der sie sich befinden, ableiten. Langfristig entsteht so ein „Internet der Dinge", das gewaltige Auswirkungen auf viele Lebensbereiche haben dürfte.

1 Ubiquitous Computing

Der seit Jahrzehnten zu beobachtende stete Fortschritt der Mikroelektronik und Informationstechnologie hält weiter an und dürfte damit bald einen Punkt erreichen, der eine neue Qualität in der Computeranwendung ermöglicht: Prozessoren, Speicherbausteine und Sensoren können dann aufgrund ihrer winzigen Größe, ihres geringen Energiebedarfs und ihres fast vernachlässigbaren Preises in viele Alltagsdinge eingebaut werden und diesen einen Mehrwert verleihen, indem sie sie zu einem an die jeweilige Situation angepassten Verhalten befähigen. Informationsverarbeitung und drahtlose Kommunikationsfähigkeit dringen so fast überall ein, selbst in Gegenstände, die zumindest auf den ersten Blick keine elektrischen

---

Einige Teile dieses Beitrags beruhen auf dem Aufsatz [Mat03] sowie anderen früheren Veröffentlichungen des Autors.

Geräte darstellen[4]. Damit sind auch die technischen Voraussetzungen für die Kooperationsfähigkeit „smarter" Dinge untereinander und das Entstehen eines „Internets der Dinge" gegeben.

Für die zu erwartende Durchdringung der Welt mit Informationstechnologie prägte Mark Weiser, seinerzeit leitender Wissenschaftler am Xerox-Forschungszentrum im Silicon Valley, bereits Anfang der 1990er-Jahre den Begriff „Ubiquitous Computing". Weiser erkannte früh das Potenzial, das im nachhaltigen Fortschritt der Mikroelektronik und Informatik liegt, und propagierte in seinem visionären Artikel *The Computer for the 21st Century* [Wei91] den ubiquitären Computer, der den Menschen unsichtbar und unaufdringlich bei seinen Tätigkeiten unterstützt und ihn von lästigen Routineaufgaben weitgehend befreit. Dabei soll der Computer als sichtbares Gerät nach Weisers Auffassung in den Hintergrund treten oder durch Verschmelzen mit den Dingen sogar ganz verschwinden, dessen informationsverarbeitende Funktionalität im Sinne einer „elektronischen Hintergrundassistenz" aber überall verfügbar sein.

Die visionäre Aussage von Marc Weiser *„in the 21st century the technology revolution will move into the everyday, the small and the invisible"* kann in Bezug auf die Computertechnik heute auf zwei Arten interpretiert werden: Kleine und preiswerte Prozessoren, Sensoren, Speicher und Kommunikationsmodule lassen sich einerseits in Alltagsgegenstände integrieren, was als *embedded computing* bezeichnet wird. Stattet man andererseits die Umwelt damit aus, dann erhält man so genannte *Sensornetze*. Auf beide Aspekte wird weiter unten (Kapitel 4) eingegangen.

Während Weiser den Begriff „Ubiquitous Computing" als eine unaufdringliche, humanzentrierte Technikvision versteht, die sich so erst in der ferneren Zukunft realisieren lässt, hat die Industrie dafür inzwischen den Begriff „Pervasive Computing" [BHR01, HMN03] mit einer leicht unterschiedlichen Akzentuierung geprägt: Auch hier geht es um die überall eindringende und omnipräsente Informationsverarbeitung, allerdings mit dem primären Ziel, diese schon kurzfristig im Rahmen von Mobile-Commerce-Szenarien und Web-basierten Geschäftsprozessen nutzbar zu machen. Die sich damit ergebenden Perspektiven (und kommerziellen Hoffnungen) wurden vor einigen Jahren von Lou Gerstner, seinerzeit Chairman von IBM, fast schwärmerisch so beschrieben: *„A billion people interacting with a million e-businesses through a trillion interconnected intelligent devices."*

Als Reaktion auf die weitgehend US-amerikanisch geprägte Szene um die Begriffe „Ubiquitous Computing" und „Pervasive Computing" ist in Europa in den letzten Jahren der Terminus „Ambient Intelligence" [AHS02, AaM03, DBS04, Mat04] entstanden, der verstärkt auch Aspekte der Mensch-Maschine-Interaktion und der Künstlichen Intelligenz umfasst. Man stellt sich dabei vor, dass eine „intelligente" Technologie den Menschen über intuitive Schnittstellen unterstützend zur Verfügung steht, die Technik selbst jedoch zurückgezogen und nur auf eine behutsame und nahezu unmerkliche Weise wirkt. Eine räumliche Umgebung soll

[4] *„Es wird in wenigen Jahrzehnten kaum mehr Industrieprodukte geben, in welche die Computer nicht hineingewoben sind, etwa so, wie das Nervensystem in Organismen hineingewoben ist"*, schrieb Karl Steinbuch schon 1966 in seinem viel beachteten Buch „Die informierte Gesellschaft" [Ste66].

zum Beispiel fähig werden, die Anwesenheit unterschiedlicher Personen zu erkennen und mit diesen individuell in unaufdringlicher Weise zu interagieren. Auch Alltagsgegenstände sollen sich von passiven Objekten zu aktiven, kommunikationsfähigen Subjekten wandeln und der dinglichen Welt eine ganz neue Eigenschaft verleihen: Diese wird „sensibel“ und reaktionsfähig, passt sich den aktuellen Bedürfnissen des Menschen an und steigert damit dessen Leistungsfähigkeit und Lebensqualität.

Langfristig soll Ambient Intelligence praktisch alle Lebensbereiche umfassen: Ein mit Ambient Intelligence ausgestattetes Haus erhöht Komfort und Sicherheit und trägt zur automatischen Energieeinsparung bei; im Bürobereich wird die Arbeitseffizienz durch eine aufmerksame, lernfähige und personalisierte Assistenz gesteigert; der Verkehr wird durch intelligente Autos, Straßen und Züge sicherer, ressourcenschonender und stressfreier; und auch der medizinische Bereich soll durch die neue Technik revolutioniert werden – Sensoren in der Kleidung erstellen Langzeitdiagnosen, und kommunikationsfähige Implantate adaptieren sich an die aktuelle Situation.

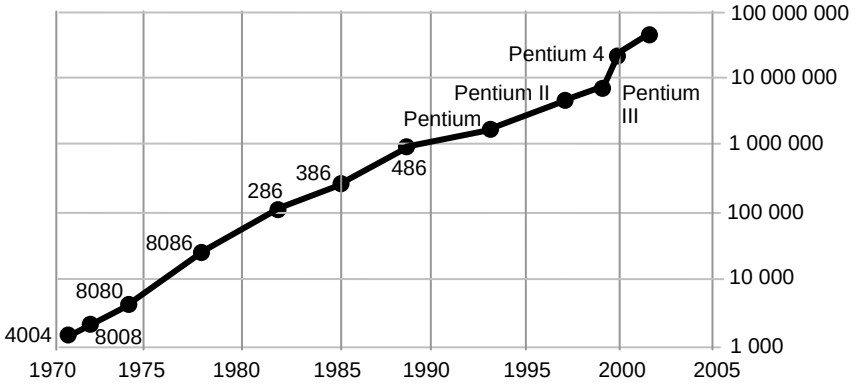


Abb. 1. Anzahl integrierter Transistoren ausgewählter Mikroprozessoren

Noch stecken allerdings die Technologien zur Realisierung solcher Zukunftsträume in den Kinderschuhen, und es besteht ein erheblicher Forschungsbedarf beispielsweise bei neuartigen Nutzungsschnittstellen wie der Sprach- und Gestenerkennung sowie bei der Realisierung eines adaptiven und lernfähigen Verhaltens „smarter“ Dinge. Konkreter sind hier die Szenarien aus dem Bereich des Ubiquitous und Pervasive Computing, die im Wesentlichen nur inkrementelle Verbesserungen bereits etablierter Technologien, wie sie weiter unten beschrieben werden, voraussetzen. In vielerlei Hinsicht bleibt die Unterscheidung zwischen den drei Begriffen „Ubiquitous Computing“, „Pervasive Computing“ und „Ambient Intelligence“ indes eher akademisch. Gemeinsam ist allen das Ziel einer unaufdringlichen, aber nachhaltigen Unterstützung des Menschen im Alltag sowie einer durchgängigen Automatisierung und Optimierung wirtschaftlicher Prozesse. Erreicht werden soll dies durch die Integration einer Vielzahl von miniaturisierten Prozessoren, Sensoren und Funkmodulen in Räumen, Umgebungen und Alltagsdingen, ergänzt durch unterstützende Infrastruktursysteme.

2 Das Gesetz von Moore

Im Computerbereich hat in den letzten Jahrzehnten eine dramatische technische Entwicklung stattgefunden, einhergehend mit einer substanziellen Veränderung der Kostenrelationen, die aus dem teuren wissenschaftlichen Instrument „Rechner“ das Massenprodukt „PC“ gemacht hat und damit die Informationsverarbeitung im wahrsten Sinne des Wortes popularisiert hat. Ursache hierfür ist der stete Fortschritt in der Mikroelektronik, welcher weiterhin andauert und uns inzwischen fast zur Selbstverständlichkeit geworden ist: Mit erstaunlicher Präzision und Konstanz scheint das bereits Mitte der 1960er-Jahre von Gordon Moore aufgestellte „Gesetz“ zu gelten [Moo65], welches besagt, dass sich die Zahl der auf einen Chip integrierbaren elektronischen Komponenten (wie z.B. Transistoren) alle 18 bis 24 Monate verdoppelt (Abb. 1, Quelle: Intel).

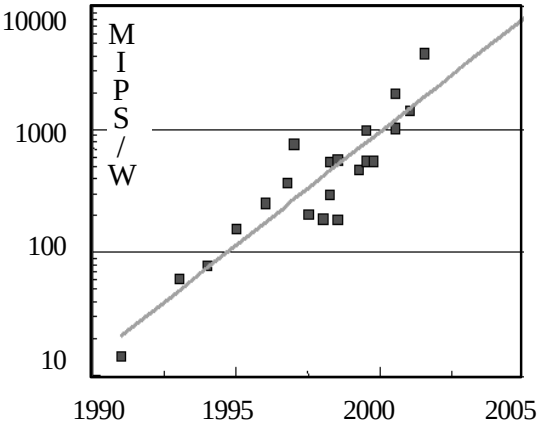


Abb. 2. Leistungsentwicklung von Prozessoren in MIPS/W

Populärer ist eine Kurzform des mooreschen Gesetzes, welches ausdrückt, dass sich die *Leistungsfähigkeit* von Prozessoren (bei konstanter oder sogar eher abnehmender Größe und Preis) etwa alle anderthalb Jahre verdoppelt. Dies ist aber eher eine Konsequenz aus der ursprünglichen Fassung, wobei neben den niedrigeren Schaltzeiten der kleineren Transistoren, die eine höhere Taktrate ermöglichen, auch Architekturprinzipien wie Pipelining, Parallelität und Cachegrößen ins Spiel kommen, mit denen die größeren Transistorzahlen in eine höhere Prozessorgeschwindigkeit umgesetzt werden.

Die Verkleinerung der Strukturbreiten elektronischer Komponenten auf den Mikrochips hat weitere interessante Konsequenzen. Moore meint dazu in [Moo95]: *„By making things smaller, everything gets better simultaneously. There is little need for tradeoffs. The speed of our products goes up, the power consumption goes down, system reliability improves, ... the cost drops.“* Abbildung 2 zeigt beispielhaft den Effizienzgewinn beim Energiebedarf pro Computerinstruktion (angegeben als Reziprokwert „MIPS pro Watt“ für ausgewählte Prozessoren) – ein wichtiges Ergebnis, da die Energiedichte von Batterien leider

relativ zu den Steigerungsraten, die man in der Mikroelektronik gewohnt ist, nur langsam anwächst.

Auch wenn immer wieder vor Fehlinterpretationen und dem baldigen Ende des mooreschen Gesetzes gewarnt wird (vgl. z.B. [Tuo02]), scheint kein unmittelbarer Anlass zu Fortschrittspessimismus gegeben zu sein: Noch während einer ganzen Reihe von Jahren dürften Prozessoren und Speicherkomponenten immer leistungsfähiger, kleiner und billiger werden. Bei vielen Anwendungen aus dem Bereich des Ubiquitous Computing geht es auch nicht primär um höchste Rechenleistung, vielmehr stehen billige Herstellungsverfahren und ein niedriger Energiebedarf im Vordergrund.

Das mooresche Gesetz ist übrigens nicht nur durch physikalische Grenzen bedroht, sondern auch durch ökonomische, da die Kosten für die innerhalb weniger Jahre abzuschreibenden Produktionsstätten laufend steigen und bereits mehrere Milliarden US-Dollar betragen. Aber selbst wenn die Chipindustrie die exponentielle Zunahme von integrierten Komponenten auf Mikroprozessoren nicht mehr lange garantieren kann, dürfte aufgrund anderer Faktoren die tatsächlich spürbare Computerleistung in nächster Zeit insgesamt dennoch weiter stark anwachsen. Hierfür sorgen neben neuen Architektur- und Verarbeitungsprinzipien auch die zu erwartenden Leistungssteigerungen bei der Kommunikation und dem Speichervermögen.

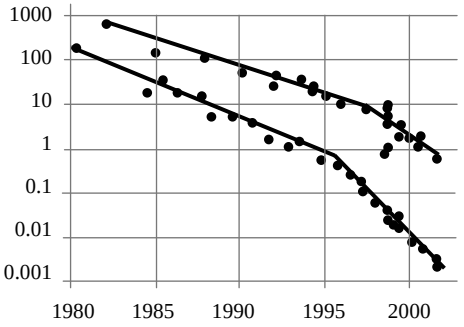


Abb. 3. Preisentwicklung Speicher (RAM bzw. Festplatten in US-Dollar/MByte)

Interessanterweise lässt sich das mooresche Gesetz auf andere wichtige Technologieparameter ausdehnen. So verdoppelte sich Ende der 1990er-Jahre die Bandbreite von Glasfaserverbindungen etwa jährlich. Erstaunlich ist ferner die Entwicklung bei Speichern, für die das „verallgemeinerte" mooresche Gesetz[5] voll zutrifft. Abbildung 3 [Hay02] zeigt die Kosten bei konkreten Festplatten und Halbleiterspeichern. In den letzten zwei Jahrzehnten fiel bei Magnetplatten (3,5-Zoll, untere Linie) der Preis für 1 MByte von ca. 100 US-Dollar auf einige zehntel Cent. Die Datendichte verdoppelte sich über lange Zeit etwa alle 2 Jahre, ab 1997

[5] *„For some reason anything that changes exponentially in the technology world now gets lumped under Moore's Law – but I'm happy to take credit for all of it"*, sagte der 74-jährige Gordon Moore im Februar 2003 anlässlich der International Solid-State Circuits Conference – und verlängerte gleichzeitig die Gültigkeit seines Gesetzes um weitere 10 Jahre.

aber sogar jährlich, was sich in der Abbildung im Preisknick widerspiegelt – dieser Trend scheint momentan ungebrochen [GrH03]. Abbildung 4 illustriert, wie klein Festplatten hoher Kapazität, die sich in mobilen Geräten wie Handys oder MP3-Playern finden, inzwischen geworden sind.

Abb. 4. Eine 4-GB/0,85-Zoll Harddisk von Toshiba (2004)

Halbleiterspeicher (RAM) wurden, wie die obere Linie von Abb. 3 zeigt, ebenfalls laufend billiger – wenn auch nicht mit der gleichen Rate wie Magnetplattenspeicher. Bei RAM erwartet man in nächster Zeit übrigens einen Qualitätssprung, wenn MRAM (Magnetic Random Access Memory) in hohen Stückzahlen erhältlich wird, denn MRAM kombiniert die besten Eigenschaften derzeit verfügbarer Halbleiter-Speichertechnologien: die Geschwindigkeit von statischem RAM (SRAM), die Speicherdichte und die niedrigen Kosten von DRAM und die Persistenz von Flash-Memory. Letzteres bedeutet, dass der Speicherinhalt beim Ausschalten nicht verloren geht, und ist daher vor allem für portable Geräte von Bedeutung, da dies ein Instant-on-Verhalten und damit einen Hot-stand-by-Betrieb ermöglicht. Da außerdem der Stromverbrauch von MRAM sehr niedrig ist (im Unterschied zu DRAM ist kein Refreshing nötig), halten auch die Akkumulatoren in Mobiltelefonen, PDAs und Laptops deutlich länger.

Längerfristig erwartet man von Technologien, die heute eher exotisch erscheinen, wie beispielsweise der Holografie, nochmals deutlich höhere Speicherdichten.

3 Weitere technologische Treiber

Vieles treibt den Fortschritt der Informationstechnik auf ganz unterschiedlichen Ebenen voran: technische Perfektionierungen von Lasern und Displays, effizientere Methoden zum Erstellen von Software, bessere Programmiersprachen und Betriebssysteme, neue physikalisch-chemische Prozesse für Batterien, innovative Konzepte für die Mensch-Maschine-Interaktion, flexiblere Fertigungsverfahren und noch manches mehr. Das alles wiederum beruht wesentlich auf dem kontinuierlichen Zuwachs an Erfahrung und Wissen sowie einem steten Erkenntnisgewinn in der grundlagenorientierten Forschung.

Der Fortschritt ist im Detail nicht planbar, und einzelne Entdeckungen geschehen eher zufällig. Dennoch lassen sich auf hoher Ebene, wo viele Einzelbeiträge zusammenfließen, klare Trends ausmachen, die über lange Zeit anhalten. Durch Extrapolation solcher Trends kann mit einer gewissen Wahrscheinlichkeit darauf geschlossen werden, was in näherer Zukunft möglich ist. Das oben diskutierte mooresche Gesetz stellt einen solchen Trend dar – die Mikroelektronik, die in den letzten Jahrzehnten bezüglich ihres Leistungszuwachses diesem Gesetz treu geblieben ist, ist die wohl wichtigste treibende Kraft hinter den Visionen des Ubiquitous Computing.

Für das sich abzeichnende Internet der Dinge sind aber auch andere Technologiebereiche sowie indirekte Konsequenzen des mikroelektronischen Fortschritts wichtig. So sollten smarte Dinge zum Beispiel untereinander und eventuell sogar mit Nutzern kommunizieren können. Einige Dinge wollen vielleicht außerdem etwas über ihre Umgebung erfahren, ihre Identität weitermelden oder wissen, wo sie sich befinden. Auf diese Aspekte und die dabei erkennbaren technischen Trends soll nachfolgend kurz eingegangen werden.

3.1 Neue Materialien und Ausgabemedien

Schon immer haben Werkstoffe ganze Zeitalter geprägt, denken wir nur an Bezeichnungen wie *Steinzeit* oder *Eisenzeit*. Die zweite Hälfte des letzten Jahrhunderts war wesentlich durch Silizium bestimmt – das Grundmaterial der Halbleiterindustrie und der Stoff, aus dem der Mikroprozessor besteht.

Jetzt aber, zu Beginn des einundzwanzigsten Jahrhunderts, zeichnet sich etwas Neues ab: Es sieht so aus, als ob demnächst Polymere, also „Plastik“, eine wesentliche Rolle spielen werden und – etwa im Bereich der Polymerelektronik – Dinge ermöglichen, die man früher nie erwartet hätte. Hier wären unter anderem *lichtemittierende Polymere* („leuchtendes Plastik“) zu nennen, die Displays aus dünnen und hochflexiblen Plastikfolien ermöglichen.

Es wird auch an *elektronischer Tinte* gearbeitet, welche Papier und Stift zum vollwertigen, interaktiven und hoch mobilen Ein- und Ausgabemedium mit einer uns wohl vertrauten Nutzungsschnittstelle erheben. Hier gibt es verschiedene technische Möglichkeiten, wovon eine auf folgendem Prinzip beruht: Eingeschlossen in Mikrokapseln, die etwa den Durchmesser eines menschlichen Haares haben, „schwimmen“ weiße und schwarze, elektrisch unterschiedlich geladene Pigmente. Diese „Tinte“ wird auf eine sehr dünne Plastikfolie aufgetragen. Legt man an einer Stelle der Folie eine positive oder negative Spannung an, dann fließen entweder die weißen oder respektive die schwarzen Pigmente an die Oberfläche und erzeugen an dieser Stelle einen kleinen Punkt. Auf diese Weise kann dynamisch etwas geschrieben und später wieder gelöscht werden. Werden zudem Farbfilter eingesetzt, ist sogar eine farbige Darstellung möglich.

Da eine Energiezufuhr lediglich zur Änderung, nicht aber für die Aufrechterhaltung des Bildes nötig ist, dieses nicht flimmert und die Substratfolien nur ca. 0,2 mm dünn sind, bietet sich diese Technologie für roll- und faltbare Bildschirme geradezu an. Prototypen existieren bereits, und an der Behebung diverser Mängel bezüglich Haltbarkeit, Pixelgröße oder Preis wird gearbeitet. Die Bedeutung für

die Praxis kann wohl kaum hoch genug eingeschätzt werden, wenn durch elektronische Tinte die Vorteile von Bildschirm und Papier verschmelzen und damit letztlich Papier, ein uns auch kulturell wohl vertrautes und klassisches Medium, quasi zum Computer mutiert oder umgekehrt der Computer als Papier daherkommt!

Laserprojektionen aus einer Brille direkt in das Auge stellen eine weitere gegenwärtig untersuchte Möglichkeit zur Substitution klassischer Ausgabemedien von Computern dar. Bei diesen so genannten *Retinaldisplays* erzeugt ein im Brillengestell eingebauter Laser ein computergeneriertes Bild, das auf ein kleines Prisma im Brillenglas gelenkt wird. Von dort wird es in das Auge gespiegelt und auf die Retina projiziert. Das Bild entsteht also nicht auf einem „Schirm", sondern wird Punkt für Punkt direkt ins Auge geschrieben.

Solche Brillen eröffnen nun ganz neue Möglichkeiten zur Informationsdarstellung – Computer (und vielleicht auch Fernseher) könnten damit z.B. auf ihre Bildschirme verzichten. Richtig interessant wird es dann, wenn der Brillenträger Informationen eingeblendet bekommt, die in der jeweiligen Situation für ihn nützlich sind. Dies hat Mahadev Satyanarayanan auf nette (und vielleicht nicht so ganz ernst gemeinte) Weise einmal wie folgt beschrieben [Sat01], wobei er davon ausgeht, dass neben einer kleinen Kamera, wie man sie bei Foto-Handys ja bereits findet, zukünftig auch ein Softwaresystem zur visuellen Objekterkennung in Brillen eingebaut werden kann: *„You could wear a pair of glasses with a small amount of face recognition built-in, look at a person, and his name would pop up in a balloon above his head. You could know instantly who the person is, even if you don't immediately recognize him. I look at my tree, and a little balloon pops up saying, 'Water me,' I look at my dog, it says, 'Take me out,' or I look at my wife, it says, 'Don't forget my birthday!'"*

Generell kann man sich leicht vorstellen, dass in Zukunft immer mehr elektronisches Gerät in miniaturisierter Form in Kleidung, Armbanduhren und Schmuckstücke eingebaut wird. Letztlich geht es beim so genannten *wearable computing* allerdings weniger darum, medienwirksame Cyborg-Fantasien oder Jacken mit eingebautem MP3-Player zu realisieren, sondern langfristig dem einzelnen Menschen in persönlicher Weise zu dienen: seinen Gesundheitszustand zu überwachen, seine Sinne zu schärfen und ihn jederzeit mit Informationen zu versorgen – ihn also sicherer und mächtiger zu machen – zwei bedeutende Triebkräfte!

3.2 Sensoren

Entwicklungen der Mikrosystemtechnik und vermehrt auch die Nanotechnik ermöglichen kleinste Sensoren, die unterschiedlichste Parameter der Umwelt aufnehmen und die gemessenen Werte in elektrischer Form weitermelden. Sensoren stellen gewissermaßen die „Sinnesorgane" smarter Dinge dar, mit denen diese ihre Umwelt wahrnehmen können. Bei der Sensortechnik wurden in den letzten Jahren bedeutende Fortschritte erzielt; neuere Sensoren reagieren nicht nur auf die klassischen Größen Licht, Beschleunigung, Temperatur, Feuchtigkeit, Druck, Magnetfeld etc., sondern können durch integrierte Rechenleistung auch Gase und Flüssigkeiten analysieren und den sensorischen Input vorverarbeiten.

In etwas verallgemeinerter Form kann man auch Kameras zu den Sensoren rechnen – diese sind mittlerweile ja so klein, dass sie problemlos in Handys eingebaut werden können. Vor allem aber sind sie auch so billig, dass sich nicht nur James Bond eine Spezialanfertigung leisten kann. Und auch hier ist das Ende des technisch Möglichen noch nicht erreicht – so bemüht man sich derzeit, neben dem CCD-Element auch die zugehörige Elektronik und die Linse auf einem einzigen Chip zu integrieren. Physikalisch spricht auch nichts dagegen, dass Kameras in Zukunft so weit verkleinert werden können, dass sie mit bloßem Auge praktisch nicht mehr zu erkennen sind.

Eine interessante Entwicklung sind ferner Funksensoren, die ohne explizite Energieversorgung ihre Messwerte einige Meter weit melden können. Die dazu nötige Energie beziehen sie aus der Umgebung oder direkt aus dem Messvorgang, indem beispielsweise piezoelektrische oder pyroelektrische Materialien bei Druck- bzw. Temperaturmessungen eingesetzt werden. Andere Typen batterieloser Funksensoren beruhen auf einer Variante der RFID-Technik, bei der der Sensor in Abhängigkeit vom gemessenen Wert ein jeweils spezifisches Funkecho zurücksendet, wenn er mit einem Hochfrequenzsignal bestrahlt wird.

Funksensoren mit einer akkumulatorbetriebenen Stromversorgung, die ihre Messwerte via GSM-Mobilfunknetz über größere Distanzen weitermelden, werden im Logistikbereich vereinzelt bereits eingesetzt, so etwa zur Überwachung von Containern oder Eisenbahn-Güterwagen und oft in Verbindung mit GPS-basierten Lokalisatoren. Kürzlich hat Siemens unter dem Namen „MyAy“ aber auch für den Consumer-Markt ein eiförmiges Gerät vorgestellt, das diverse Sensoren besitzt und vielfältige Fernüberwachungsfunktionen wahrnehmen kann. So erkennt beispielsweise ein Infrarotsensor, wenn sich in der Umgebung etwas rührt, und ein Beschleunigungssensor registriert, wenn das Gerät selbst bewegt wird. Eingebaut sind auch ein Temperatur- und ein Geräuschsensor. Konfiguriert wird MyAy via Handy oder Internet. Es kann dann, wenn sich in seiner Umgebung etwas Ungewöhnliches tut, per SMS mit dem Handy des Besitzers Kontakt aufnehmen oder ihn auf andere Weise alarmieren. Im Unterschied zu einem Mobiltelefon ist ein solches Gerät also nützlich, wenn man es *nicht* mit sich herumträgt. Propagiert werden Anwendungsmöglichkeiten als mobiles Babyphon oder als Alarmanlage im Urlaub, etwa um das Zelt auf dem Campingplatz zu schützen.

Ob die Sensor- und Kommunikationstechnik bereits weit genug fortgeschritten ist, um Systemen wie MyAy einen Markterfolg zu bescheren, wird sich noch zeigen müssen. Langfristig darf man aber davon ausgehen, dass Funksensoren eine wichtige Rolle spielen werden, z.B. in Form von Sensornetzen, die weiter unten (Kapitel 4.1) thematisiert werden.

3.3 Kommunikationstechnik

Wenn man das Internet aus historischer Perspektive betrachtet und die dabei erkennbaren Trends extrapoliert, erscheint das Entstehen eines „Internets der Dinge“ konsequent und fast unvermeidlich. Tatsächlich ist die Geschichte des Internets nicht nur durch einen stürmischen, exponentiell verlaufenden Zuwachs hinsichtlich der angeschlossenen Rechner charakterisiert. Interessanter ist in die-

sem Kontext die damit einhergehende *qualitative* Entwicklung: War das Internet in den 1970er-Jahren zunächst noch ein Experimentier- und Forschungsnetz, das Nutzer im Wesentlichen für remote login und Dateitransfer, also den entfernten Zugriff auf Computerressourcen, verwendeten, so wurde es in den 1980er-Jahren zunehmend als Kommunikationsmedium von *Mensch zu Mensch* benutzt – E-Mail entwickelte sich zur dominierenden Anwendung. Die 1990er-Jahre brachten mit dem WWW dann aber eine ganz andere Nutzungsform hervor: Nun kommunizierten *Menschen* via Browser auf der einen Seite mit *Maschinen*, nämlich WWW-Servern, auf der anderen Seite. Dies hatte eine Vervielfachung des Datenverkehrs zur Folge und stellte gleichzeitig die Voraussetzung für die schnelle Kommerzialisierung und Popularisierung des Internets dar. Die gegenwärtige Dekade lässt sich dadurch charakterisieren, dass mit internetfähigen Mobiltelefonen und PDAs, aber auch mit neueren Fernsehgeräten, Fotokopierern und anderen elektronischen Medien und Geräten das Internet sich über seine klassische Domäne hinaus ausbreitet und einen ganz neuen Markt und Tummelplatz für innovative Anwendungen erschließt.

Nun zeichnet sich am Horizont aber bereits ein weiterer Qualitätssprung ab, der die Internetnutzung der kommenden Dekade bestimmen dürfte und völlig neue Möglichkeiten eröffnet: Das Internet wird bald auch für die autonome Kommunikation von *Maschine zu Maschine* und schließlich sogar von *Ding zu Ding* verwendet werden. Kommunikationsprotokolle und Infrastrukturdienste, die Web-Informationen maschinenlesbar machen, wie beispielsweise XML und Web-Services, sind erste Anzeichen dafür. Auch das Semantic Web und die Bemühungen, geeignete Ontologien zur Klassifikation und Strukturierung von Daten im Web zu erhalten, dienen letztlich dem Zweck, kooperative Prozesse im Internet automatisch ausführbar zu machen. Vor allem aber werden in Zukunft viele in Alltagsgegenstände eingebettete Prozessoren und Sensoren im Verbund mit neuen technischen Möglichkeiten der drahtlosen Datenkommunikation dafür sorgen, dass gewöhnliche Dinge miteinander kommunizieren können und diese z.B. ihren Aufenthaltsort oder ihre Sensorwerte anderen interessierten und dazu befugten Dingen mitteilen.

Damit dürfte das Internet einen weiteren drastischen Wandel erleben: Nachdem mittlerweile so gut wie alle Computer der Welt daran angeschlossen sind, steht nun quasi seine Verlängerung bis in die letzten Alltagsgegenstände hinein an – es entsteht ein *Internet der Dinge*! Tatsächlich hat Neil Gershenfeld vom MIT im Rahmen seines „Internet 0"-Projekts eine Leichtgewichtsimplementierung des IP-Internetprotokolls realisiert, welche auf kleinen Hardware-Knoten zum Preis von etwa 3 US-Dollar ausführbar sein soll [GKC04]. Dabei wurde aber viel Funktionalität abgespeckt, sodass nur noch einfachste Anwendungen (wie z.B. Lichtschalter) möglich sind. Generell ist wohl eher nicht davon auszugehen, dass bei der Vernetzung smarter Dinge überall das klassische Internet-Protokoll zum Einsatz kommt – da die Implementierung dieses Protokolls für banale Dinge geringer Funktionalität nicht adäquat sein mag, könnte die konkrete Internetanbindung stattdessen von einem in der Nähe befindlichen „Proxy" (Mobiltelefon, RFID-Lesegerät, WLAN-Hotspot etc.) übernommen werden, welcher dann in geeigneter Weise mit den smarten Dingen kommuniziert.

Für die Realisierung der Vision vom Internet der Dinge ist – insbesondere zur Überbrückung der letzten Meter – vor allem die drahtlose Kommunikation von

großer Bedeutung. Auf diesem Gebiet werden anhaltende technische Erfolge erzielt. Interessant sind, neben Fortschritten hinsichtlich höherer Datenraten bei der mittlerweile großflächig etablierten und auf teurer Infrastruktur beruhenden Handy-Technik (GSM, UMTS) und der eher dezentral wachsenden WLAN-Technik (WiFi, IEEE802.11), insbesondere neuere Kommunikationstechniken im Nahbereich.

Mit *ZigBee* (IEEE802.15.4), in gewisser Weise eine Fortentwicklung der bekannten Bluetooth-Kurzstreckenfunktechnik im 2,4-GHz-Band mit Übertragungsraten von bis zu 250 kbit/s, können in einem Bereich von einigen zig Metern dichte Netze aus mehreren hundert Knoten aufgebaut werden. ZigBee benötigt sehr wenig Energie und ermöglicht kleine und billige Bauformen der Kommunikationsmodule. Vorrangiges Anwendungsgebiet ist die drahtlose Vernetzung im Bereich der „consumer electronics“. Aber auch bei der Gebäudeautomation und im medizinischen Bereich ergeben sich interessante Einsatzmöglichkeiten.

Ultra Wide Band (UWB, IEEE802.15.3) andererseits ermöglicht hohe Datenraten. Das verwendete Prinzip basiert auf extrem kurzen Energieimpulsen, die über ein breites Frequenzspektrum ausgesandt werden. Dadurch ist UWB nicht nur relativ störungsunempfindlich und durchdringt Hindernisse besser als andere Funktechnologien, sondern kann auch ähnlich wie Radar benutzt werden und erlaubt damit prinzipiell die Lokalisierung von Objekten mit einer Präzision im Zentimeterbereich.

Interessant im Hinblick auf eine intuitive Nutzerinteraktion mit Geräten und smarten Dingen ist auch die *Near Field Communication*[6] (NFC), ein Standard, der im Jahr 2004 von Nokia, Philips und Sony etabliert wurde. Technisch gesehen handelt es sich um ein Kommunikationsprinzip, das die induktive Kopplung verwendet und analog zu RFID (bzw. kontaktlosen Chipkarten), allerdings nur über Distanzen von wenigen Zentimetern, funktioniert. Es wird der 13,56-MHz-Frequenzbereich mit eher geringen Datenraten von 106, 212 oder 424 kbit/s genutzt, wobei nur sehr wenig Energie benötigt wird. Bei der Kommunikation ist ein Partner im so genannten aktiven Modus, der andere kann im aktiven oder passiven Modus sein. Aktive Geräte generieren ein Magnetfeld (ähnlich zu RFID-Lesegeräten), mit dem die Daten übertragen werden, während passive Geräte sich als batterielose RFID-Transponder verhalten und ihre Daten nach dem Prinzip der Lastmodulation übermitteln.

Verfügen bei NFC die beiden Kommunikationspartner zusätzlich über drahtlose Kommunikationsschnittstellen höherer Übertragungsleistung, wie z.B. WLAN oder Bluetooth, so kann NFC auch lediglich zur Herstellung des Kontaktes, zur Identifikation der Geräte und zum Austausch der Parameter für die automatische Konfiguration des schnelleren Mediums genutzt werden. Die eigentliche Datenkommunikation erfolgt dann in transparenter Weise über die so eingerichtete leistungsfähigere Verbindung.

Aktive NFC-Einheiten sind klein genug, um beispielsweise in einem Mobiltelefon untergebracht zu werden; passive Einheiten sind als RFID-Tags noch wesentlich kleiner und vor allem sehr billig. Damit ermöglicht NFC ein neues Kommunikationsparadigma: Kommunikation durch physische Nähe. Aus Nutzersicht sieht es dabei so aus, als ob sich zwei benachbarte Geräte erkennen und miteinan-

[6] www.nfc-forum.org

der kommunizieren, sobald sie sich berühren oder zumindest sehr nahe kommen. Auf diese Weise soll eine mühelose und intuitive Datenübertragung zwischen den vielen persönlichen (und meist kleinen und mobilen) „information appliances“ eines Nutzers wie Digitalkamera, Mobiltelefon, PDA, Spielkonsole, Fernseher oder PC möglich werden. Das Problem der Sicherheit und Authentifikation wird alleine dadurch wesentlich entschärft, dass NFC nur über sehr kurze Distanzen wirkt und praktisch ein physischer Kontakt hergestellt werden muss.

Sehr interessant ist aber auch noch eine andere potenzielle Nutzungsart von NFC: Indem beispielsweise ein mit einer aktiven NFC-Einheit ausgestattetes Mobiltelefon an ein Objekt gehalten wird, das einen RFID-Chip enthält, kann dieser ausgelesen werden. Das Handy kann die gelesenen Daten dann entweder direkt interpretieren und anzeigen oder ergänzende Information über das Mobilnetz besorgen bzw. sogar mit einem zugehörigen Server im Internet interagieren, dessen Internetadresse auf dem RFID-Chip gespeichert ist. Dadurch sind etwa Szenarien denkbar, wo man mit einer Reklametafel oder einem Filmplakat interagiert und dabei Videoclips zugespielt bekommt, Kinokarten reserviert oder Musik herunterlädt und dies mit der Telefonrechnung bezahlt.

Die fernere Zukunft lässt über UWB, ZigBee und NFC hinaus noch wesentlich weiter gehende Möglichkeiten bei der drahtlosen Kommunikation erwarten. Einerseits etwa WLAN-Hotspots mit Datenraten von über 1 Gbit/s, andererseits extrem kleine und energiesparsame Funktechnologien für Sensornetze, bei denen nur sehr geringe Datenraten erforderlich sind. Indem Sender und Empfänger mit mehr „Intelligenz“ ausgestattet werden, um sich an die momentane Situation anzupassen, kann das verfügbare Frequenzspektrum auch wesentlich ökonomischer genutzt werden, als es mit den bisherigen, auf analoger Technik beruhenden Verfahren möglich war, sodass insgesamt in viel größerem Umfang als heute „gefunkt“ werden kann.

3.4 Lokalisierung

Damit „smarte“ Alltagsdinge sich situationsangepasst verhalten können, ist der Kontext, in dem sie sich befinden, von großer Relevanz. Zu den wichtigsten Kontextaspekten eines Gegenstandes gehört sein momentaner Ort (bei fast allen Dingen, die wir besitzen und die uns wichtig sind, handelt es sich schließlich nicht um „Immobilien“, sondern um prinzipiell bewegliche Objekte) und seine Nähe zu anderen Dingen. Festzustellen, wo sich ein Gegenstand befindet, ist daher eine wichtige Aufgabe für viele Anwendungen im „Internet der Dinge“.

Zur Lokalisierung mobiler Objekte existieren verschiedene technische Ansätze [HiB01]. Eine einfache – wenn auch etwas grobe – Möglichkeit besteht darin, festzustellen, in welchen Empfangsbereichen bzw. Funkzellen von Sendern man sich befindet, deren Positionen bekannt sind. Da die Signalstärke mit zunehmender Entfernung von Sender und Empfänger abnimmt, kann dieser Faktor ebenfalls berücksichtigt werden; allerdings ist dieses Prinzip ungenau, da die Signalstärke durch viele Störeffekte beeinflusst wird. Eine etwas aufwendigere aber präzisere Methode besteht in der Laufzeitmessung von Funksignalen und daraus abgeleitet der Entfernungsbestimmung, wobei im Allgemeinen der Abstand zu drei oder

mehr Punkten bekannt sein muss, um die Position im Raum festlegen zu können. Das „Global Positioning System“ (GPS) und das ähnlich konzipierte europäische Galileo-System, das zwischen 2009 und 2011 einsatzbereit sein soll, beruhen beispielsweise auf einer solchen Entfernungsmessung zu momentan sichtbaren Satelliten – eine Einschränkung stellt dabei allerdings die Tatsache dar, dass dies bisher nur bei „Sichtkontakt“ zu den Satelliten, also im Freien, funktioniert.

An verbesserten Möglichkeiten zur Positionsbestimmung mobiler Objekte wird derzeit intensiv gearbeitet. Neben einer Erhöhung der Genauigkeit (derzeit einige Meter beim GPS-System) besteht das Ziel vor allem in einer deutlichen Verkleinerung der Module (einige passive Bauelemente und vor allem die Antenne stellen bei GPS-ähnlichen Systemen noch eine Herausforderung dar), einer Reduktion des Energiebedarfs sowie der Entwicklung von Techniken, die auch in geschlossenen Räumen funktionieren. Es wird erwartet, dass schon 2006 Chips für die satellitenbasierte Positionsbestimmung auf den Markt kommen, die wesentlich schwächere Signale verarbeiten können und deutlich weniger Energie benötigen, womit die Verwendung in Mobiltelefonen und ähnlichen Geräten möglich wird. Außerdem sollte so auch im Fall einer nicht vorhandenen Sichtverbindung zu einem Satelliten oftmals noch eine Ortsbestimmung durchführbar sein.

Zur Ortung von Handys (oder Dingen, die sich diesbezüglich wie ein Handy verhalten) kann auch das Mobilfunknetz verwendet werden, das in vielen Ländern flächendeckend vorhanden ist. Beispielsweise ist bei GSM die Funkzelle bekannt, in der sich ein Handy aufhält. Zwar ist die Funkzellendichte nur in Agglomerationsbereichen relativ hoch (mit typischerweise einigen wenigen hundert Metern Abstand zwischen den Antennen) und beträgt im ländlichen Raum bis zu 35 km, allerdings kennt die Basisstation einer Funkzelle die Entfernung der Handys zu ihrer Sendeantenne mit einer Granularität von etwa 550 m. Dies ist aus technischen Gründen (Synchronisation) notwendig und wird durch Laufzeitmessungen des Funksignals ermittelt. Befindet sich ein Handy im Überlappungsbereich mehrerer Funkzellen, kann die Position durch Messung der Laufzeitunterschiede im Prinzip auf etwa 300 m genau ermittelt werden. Bei UMTS, dem Mobilfunksystem der nächsten Generation, das zurzeit eingeführt wird, wäre in technischer Hinsicht sogar eine bis zu 10 Mal genauere Lokalisierung möglich.

Interessant ist eine neuere Lokalisierungsmöglichkeit, die auf WLAN-Zugangspunkten beruht: In vielen städtischen Gebieten sind WLAN-Basisstationen schon sehr dicht vorhanden, sodass man sich fast überall im Bereich eines oder mehrerer solcher Funknetze mit typischen Zellengrößen von einigen zig Metern befindet. Für Seattle wurde zum Beispiel im Herbst 2004 eine Dichte von ca. 1200 Stationen pro Quadratkilometer gemessen. Kennt man die Ortskoordinaten der festen Stationen (öffentlich zugängliche Datenbanken enthalten bereits über eine Million Netze mit deren eindeutiger Kennung und Ortskoordinaten), so kann damit eine Lokalisierungsgenauigkeit von 20 bis 40 Meter erreicht werden – auch in Gebäuden, wo GPS bisher versagt [LCC05]. Städtische Bereiche können damit schon zu fast hundert Prozent abgedeckt werden.

Je genauer und einfacher der Ort eines kleinen, preiswerten Gerätes ermittelt werden kann, umso vielfältiger und interessanter sind natürlich die möglichen Anwendungen. Manch einer mag davon träumen, in Zukunft kaum mehr etwas zu verlieren bzw. das Verlorene fast immer wiederzufinden, weil ein Gegenstand stets weiß, wo er ist, und dies bei Bedarf mitteilen kann – das ist beim jetzigen

Stand der Technik allerdings unrealistisch. Noch sind Lokalisierungsmodule für viele Anwendungen zu groß, zu teuer, zu ungenau und zu energiehungrig. Bei allen vier Parametern erzielt man allerdings kontinuierliche Fortschritte. Für größere und wertvolle Dinge wie beispielsweise Mietautos rechnet sich die Verwendung von Lokalisierungstechnologien schon heute, und mit dem Fortschritt der Technik werden nach und nach dann auch einfachere Gegenstände von dieser Möglichkeit profitieren.

Damit ist vorstellbar, dass sich in Zukunft für viele Dinge eine Art „Fahrtenschreiber" realisieren lässt: Weiß ein Gegenstand, wo er sich befindet, dann braucht er dies nur regelmäßig zusammen mit der momentanen Uhrzeit abzuspeichern oder weiterzumelden, womit sich auch im Nachhinein die „Lebensspur" des Gegenstandes einfach rekonstruieren lässt. Durch den Abgleich mehrerer solcher Lebensspuren kann der gemeinsame Kontext verschiedener Dinge ermittelt werden, oder es kann über diese Historie einfach Zugang zu damit assoziierten Informationen (z.B. das Hotel, in dem sich eine ortsbewusste Reisetasche befand) erlangt werden.

Ist eine Lokalisierung von Dingen zukünftig einfach, billig und genau machbar, dann finden sich dafür vielfältige Verwendungsmöglichkeiten. Nicht nur Schlüssel, Haustiere, Koffer, Postsendungen, Container, Waffen, mautpflichtige Fahrzeuge, diebstahlgefährdete Objekte, umweltschädliche Stoffe und untreue Ehepartner wollen oder sollen lokalisiert werden, sondern auch Eltern könnten es sehr schätzen, wenn Kleidungsstücke der Kinder ihren Aufenthaltsort verraten oder wenn sogar Alarm ausgelöst wird, falls sich außer Haus die Jacke zu weit vom Schuh entfernt. Ein Vorbote einer solchen Möglichkeit ist ein seit einiger Zeit in Deutschland angebotener Lokalisierungsdienst für Mobiltelefone[7], über den im März 2004 „Bild.de" folgendermaßen berichtete: *Neuer Handy-Dienst sagt Ihnen immer, wo Ihr Kind ist. Ist es auch wirklich in der Schule? Mit „Track your kid" finden Sie es heraus. Deutschlandweit können Sie so bis auf 250 m genau feststellen, wo sich der Nachwuchs aufhält. Das kann gerade für berufstätige Eltern oder Alleinerziehende eine Erleichterung sein. Denn diese sanfte Kontrolle verschafft Ihnen Sicherheit – und das Kind merkt gar nichts davon!* Rechtlich ist an diesem Dienst übrigens nichts auszusetzen, da das Telekommunikationsgesetz die Weitergabe der Standortinformation zulässt, wenn der Handybesitzer dem zustimmt. Vermutlich wird aber einen kritischen Zeitgenossen oder einen Bürger in einem totalitären Staat eine solche Zustimmungspflicht nicht ganz beruhigen können.

Tatsächlich dürfte in Zukunft der „location privacy" besondere Beachtung zukommen [Mat05]. Denn wissen Dinge, wo sie sind oder wo sie waren, dann kann damit leicht auf den Aufenthaltsort einer Person geschlossen werden, wenn die persönlichen Gegenstände dies „ausplaudern". Lokalisierungstechnologien bergen also einiges an sozialem Sprengstoff: nicht nur, weil man damit Leuten hinterherspionieren kann, sondern weil dies auch ein bewusst eingesetztes Kontrollinstrument werden kann. Dobson und Fisher drücken dies in ihrem Artikel „Geoslavery" [DoF03] mit drastischen Worten so aus: *„Society must contemplate a new form of slavery, characterized by location control."* Andererseits kann das Wissen um den Aufenthaltsort anderer oder gar die Kontrolle darüber manchmal natürlich auch nützlich und sozial akzeptabel sein – nicht nur bei Kindern, sondern zum

[7] www.trackyourkid.de

Beispiel auch bei zeitweilig geistig verwirrten Personen, wie dies etwa im Bereich der Altenpflege gehäuft vorkommt: Statt solche Personen vorsichtshalber einzuschließen, kann man z.B. virtuelle Sicherheitszonen definieren, bei deren Verlassen Alarm geschlagen wird. Dies ermöglicht es den Betroffenen, innerhalb gewisser Grenzen ein selbstbestimmteres Leben zu führen – auch wenn die Trennlinie zwischen Schutz und Freiheit einerseits und Überwachung und Eingriff in die Privatsphäre andererseits dabei einen diffizilen Verlauf annehmen kann.

Solange nur einfache Handys lokalisierbar sind, wie zum Beispiel beim oben erwähnten „Track your kid"-System, kann man dies (wenn man daran denkt!) als Betroffener noch kontrollieren und das Gerät notfalls – allerdings zum Preis der Nichterreichbarkeit – ausschalten. Schon gibt es aber erste Produkte in Form von Armbanduhren[8], mit denen man aus der Ferne den Aufenthaltsort seiner Kinder feststellen kann. Diese Uhren sind noch nicht so bequem, genau und energiesparend, wie man es sich wünscht, aber die Technik macht ja Fortschritte! Nun mag ein 8-Jähriger das Tragen einer solchen Uhr „cool" finden. Aber ist auch die 15-jährige Tochter bereit, sich damit auf Schritt und Tritt verfolgen zu lassen? Muss sie sich rechtfertigen, wenn sie die Fernlokalisierungsmöglichkeit einmal abschaltet – sofern dies überhaupt geht? Sollte man nicht „vorsichtshalber" auch auf Bewährung freigelassene Sträflinge verpflichten, eine solche Uhr zu tragen? Oder, falls die Technik zukünftig klein genug wird, Ausländern („zum eigenen Schutz") in das Visum integrieren?

Die Lokalisierung von Strafgefangenen und Kindern wird in ersten Projekten jedenfalls bereits betrieben. Die Firma Technology Systems International in Arizona hatte beispielsweise im Sommer 2004 schon vier Gefängnisse mit Lokalisierungstechnologie und Armbändern für die Insassen, die alle zwei Sekunden die Position melden, ausgestattet. Angeblich nahmen dadurch die Gewalttaten um 60 % ab, und Greg Oester, der Präsident der Firma, begründete dies so [Kan04]: *„Inmates know they are being monitored and know they will get caught. The word spreads very quickly. It increases the safety in facilities."* Ebenfalls ein ortsbewusstes Armband bekommen die Kinder beim „Kidspotter"-System[9] im dänischen Legoland. Damit können Eltern im Falle eines Falles eine SMS-Nachricht an das System schicken und bekommen als Antwort die Ortskoordinaten ihres Kindes, welches sie dann mittels einer Karte lokalisieren können. Nebenbei erfährt Legoland so auch, mit welchen Attraktionen sich ihre jungen Besucher vorwiegend vergnügen und welche Teile des Parks eher übersehen werden.

3.5 Energie

Im Vergleich zur rasanten Effizienzsteigerung bei Prozessorleistung, Kommunikationsbandbreite und Speicherdichte macht die Batterietechnik eher langsame Fortschritte. Immerhin konnte die Kapazität jedoch durchschnittlich um ca. 5 % pro Jahr gesteigert werden; bei den verbreiteten AA-Mignonzellen in den letzten 20 Jahren beispielsweise von ca. 0,6 auf 1,8 Wattstunden [Est02]. Batterien lassen

[8] www.wherify.com

[9] http://blogger.iftf.org/Future/cat_rfid.html

sich mittlerweile in dünner (0,5 mm) und biegsamer Bauform herstellen und können in ihrer Gestalt daher den jeweiligen Gegebenheiten angepasst werden.

Der Energiehunger elektronisch realisierter Funktionalität und der Wunsch, Batterien nicht oder möglichst selten wechseln zu müssen (was praktisch unabdingbar für die Realisierung der Vision autonomer smarter Alltagsgegenstände ist), hat zur intensiven Suche nach alternativen Energiequellen geführt. Brennstoffzellen haben hinsichtlich ihres Energieträgers (z.B. Methanol) eine 10 bis 40fach höhere Energiedichte als Batterien, allerdings lassen sie sich derzeit nicht beliebig klein verwirklichen, und es tritt bei der Umwandlung in elektrische Energie ein Verlust von ca. 50–80 % auf. Typische Solarzellen erreichen bei Sonnenschein maximal 10 mW/cm^2, bei Kunstlicht ist die Ausbeute leider um fast 3 Größenordnungen kleiner. Weitere Möglichkeiten, Energie in geringem Umfang aus der Umwelt abzuschöpfen, bestehen z.B. bei mechanischer Energie (vibrierende Fensterscheiben, Körperbewegungen etc.). Dies mag in Zukunft zumindest in einigen spezifischen Anwendungskontexten sinnvoll sein, wenn Prozessoren, Speicher und Kommunikationsmodule dann deutlich weniger Energie als heute benötigen. Eine explizite drahtlose Energieversorgung ist zwar prinzipiell auch möglich, funktioniert aber nur über kurze Distanzen – immerhin nutzen jedoch kontaktlose Chipkarten, RFID-Chips sowie die passiven Komponenten von NFC das Prinzip der magnetischen Induktion erfolgreich zu diesem Zweck.

Eine noch nicht voll ausgeschöpfte Option im Umgang mit dem Energieproblem besteht auch im Energiesparen. Dies betrifft nicht nur schaltungstechnische Maßnahmen in der Hardware, sondern auch energiebewusste Software, die auf „intelligente“ Weise mit Energie verantwortungsvoll umgehen und einzelne Systemkomponenten zeitweise abschalten oder mit reduzierter Leistung betreiben kann. Hier dürften in nächster Zeit noch einige Fortschritte zu erwarten sein.

Da Energie generell eine sehr kostbare Ressource ist – für kleine und portable Geräte ist vor allem die Maßeinheit „Energie pro Gewicht“ relevant – und sich nur beschränkt speichern lässt, macht ein sparsamer Umgang damit ausgeklügelte Maßnahmen im Bereich der Kommunikationsprotokolle sowie der Soft- und Hardwarearchitekturen notwendig und erfordert im Allgemeinen eine verteilte Bearbeitung der Anwendung auf unterschiedlich ausgestatteten Geräten. Grob kann man in einem solchen vernetzten Systemverbund drei Klassen von Geräten unterscheiden: Zum einen „Mikrowattknoten“, die über Monate hinweg autonom betrieben werden können und nur einfachste sensorische Aufgaben wahrnehmen. Sie sind im Wesentlichen für die „awareness“ umgebungsbewusster Systeme zuständig, verbringen lange Zeit im energiesparenden Tiefschlaf und melden ihre Erkenntnisse nur sporadisch über kurze Funkdistanzen weiter. Des Weiteren lassen sich „Milliwattknoten“ identifizieren, die einige Tage mit einer Batterie oder Akkuladung auskommen. Und schließlich gibt es „Wattknoten“, welche an das Stromnetz angeschlossen sind und Serverfunktionen wahrnehmen oder Gateways zum Internet darstellen. Die Milliwattknoten sind in der Form von Mobiltelefonen, PDAs, Retinaldisplays und ähnlichen mobilen und persönlichen Geräten für die Nutzungsschnittstelle und den ubiquitären Audio- und Video-Zugang zuständig, kommunizieren über größere Funkdistanzen mit Wattknoten und können (z.B. im Bereich des wearable computings) auch Daten von nahe gelegenen Mikrowattknoten entgegennehmen. Während Wattknoten und Milliwattknoten technisch bereits gut beherrscht werden und etabliert sind, ist die Mikroelektronik erst

jetzt so weit, dass langsam auch Mikrowattknoten (und zugehörige Kommunikationstechnologien wie z.B. ZigBee) möglich werden – Anwendungsmöglichkeiten dafür werden weiter unten im Kapitel über Sensornetze diskutiert.

3.6 RFID

Bei RFID („Radio Frequency Identification“) handelt es sich um eine Technologie, um Dinge aus der Ferne zu identifizieren. Bekannt geworden sind in letzter Zeit vor allem die ohne eigene Energieversorgung funktionierenden elektronischen Etiketten. Dabei verwendet man technisch gesehen Transponder, die mit einem Hochfrequenzsignal bestrahlt werden, dieses Signal decodieren, aus ihm (z.B. nach dem Prinzip der magnetischen Induktion) auch die Energie für sich selbst beziehen und eine Antwortnachricht (etwa eine eindeutige Identifikationsnummer) als Funksignal zurücksenden. In gewisser Weise handelt es sich bei dieser Technik um eine Weiterentwicklung der bekannten Türschleusen zur Diebstahlsicherung von Kaufhäusern und Boutiquen. Allerdings geht es hier nicht mehr nur um eine binäre Information „bezahlt/gestohlen“, sondern es können „durch die Luft“ innerhalb von Sekundenbruchteilen einige hundert Bits gelesen und bei manchen Typen sogar geschrieben werden – je nach Bauform und zugrunde liegender Technik bis zu einer Distanz von einigen wenigen Metern.

RFID-Chips sind typischerweise weniger als ein Quadratmillimeter groß und dünner als ein Blatt Papier. Die meist flache Antenne kann aus sehr dünnem Kupfer oder auch aus leitfähiger Tinte bestehen. In der Form von flexiblen Selbstklebeetiketten („smart labels“) kosten sie mit fallender Tendenz derzeit zwischen 10 Cent und 1 Euro pro Stück und haben dadurch das Potenzial, in manchen Anwendungsbereichen die klassischen Strichcodeetiketten zur Identifikation von Waren abzulösen. Von Vorteil ist dabei vor allem, dass im Unterschied zu anderen Technologien, wie etwa den aus dem Supermarkt bekannten Laserscannern, keine Sichtverbindung zum Lesegerät bestehen muss. Neben den für den Masseneinsatz geeigneten passiven RFID-Transpondern existieren auch batteriegespeiste *aktive* Transponder mit wesentlich größeren Reichweiten, die z.B. in regelmäßigen Zeitabständen ein eindeutiges Funksignal aussenden, das von der Umgebung erkannt wird. Aktive Transponder sind allerdings wesentlich größer und teurer als die passiven RFID-Labels.

Wir gehen an dieser Stelle nicht näher auf die Funktionsweise der RFID-Technik ein; genauere Erläuterungen dazu finden sich im Beitrag von Lampe, Flörkemeier und Haller sowie im Buch von Finkenzeller [Fin02]. Es sei nur noch bemerkt, dass die Idee an sich zwar schon über 50 Jahre alt ist [Sto48], die Technik aber erst in den 1980er-Jahren weit genug fortgeschritten war, um erste kommerzielle Anwendungen wie kontaktlose Zugangskontrollsysteme, Maut-Systeme oder die Markierung von Tieren zu ermöglichen. Erst in den 1990er-Jahren standen dann preiswerte Realisierungen für Massenapplikationen wie Skipässe, elektronische Wegfahrsperren und Artikel-Diebstahlsicherungen sowie RFID-Transponder in Form von elektronischen Etiketten (etwa für Bibliotheksanwendungen) zur Verfügung.

Konkrete Anwendungsmöglichkeiten der RFID-Technik ergeben sich zunächst vor allem im Bereich der Logistik: Wenn Produkte oder zumindest ganze Paletten ihre Identität jedes Mal automatisch preisgeben, wenn sie das Tor einer Lagerhalle oder die Laderampe eines LKW passieren, dann kann ohne manuelles Zutun eine lückenlose Verfolgung der Warenströme über die gesamte Lieferkette hinweg sichergestellt werden. Dies ist natürlich von erheblicher wirtschaftlicher Bedeutung. Andererseits muss man sich bewusst sein, dass es bei dieser prinzipiell empfindlichen und für den Masseneinsatz relativ „billig" konzipierten Technik vielfältige Störeinflüsse wie Beeinflussungen durch benachbarte Funkgeräte, Frequenzverschiebungen, nicht ausreichende Lesedistanzen, abträgliche Umgebungsbedingungen (Reflexionen, Absorptionen, Abschattungen), defekte Labels etc. geben kann. Daher gelingt insbesondere das gleichzeitige Auslesen vieler Transponder (Pulkerfassung) nicht immer zu 100%, was Szenarien wie den kassenlosen Supermarkt-Check-out derzeit noch infrage stellt, da man dort aus wirtschaftlichen Gründen auf Erkennungsraten von über 99% angewiesen ist.

Mit preiswerten RFID-Labels sind allerdings auch Anwendungen jenseits des Logistikbereichs vorstellbar, wo ein gelegentliches Misslingen des Lesevorgangs eher unkritisch ist. Enthält beispielsweise die Bordkarte eines Flugreisenden einen RFID-Chip, so kann beim Passieren geeignet instrumentierter Stellen automatisch festgestellt werden, in welchem Flughafenbereich sich dieser befindet. Ein säumiger Fluggast braucht dann nicht mehr überall per Lautsprecher ausgerufen zu werden, und die Airline kann entscheiden, ob es sich lohnt, die Maschine noch einige Minuten warten zu lassen – nämlich dann, wenn der Fluggast nicht mehr weit vom Gate entfernt ist, und es sich um einen guten Kunden handelt.

Da über die eindeutige Identifikation von RFID-Labels Objekte in Echtzeit mit einem im Internet oder in einer entfernten Datenbank residierenden Datensatz verknüpft werden können, kann letztendlich beliebigen Dingen eine spezifische Information zugeordnet werden. Wenn Alltagsgegenstände auf diese Weise flexibel mit Information angereichert werden können, eröffnet dies in Zukunft aber Anwendungsmöglichkeiten, die weit über den vordergründigen Zweck der automatisierten Lagerhaltung oder des kassenlosen Supermarktes hinausgehen. Eine nette Einsatzmöglichkeit stellen beispielsweise RFID-Chips im Abfall dar: Hier kann ein Produkt der Müllsortieranlage in einer „letzten Willensmitteilung" kundtun, aus was es besteht und wie seine Überreste behandelt werden sollen [SaT03].

Längerfristig lassen RFID und andere Verfahren zur Identifikation von Objekten zusammen mit Techniken der Mobilkommunikation und des entfernten Informationszugriffs Möglichkeiten zu, die auf eine umfassende Informatisierung der Welt hinauslaufen. Insbesondere kann auf diese Weise mit Dingen „kommuniziert" werden, wie es weiter oben bei der Diskussion von NFC schon angedeutet wurde: Es ist z.B. vorstellbar, dass fast jedes Produkt ein Web-Portal oder eine Homepage im Internet hat, die der Hersteller gleich mit eingerichtet hat. Die zugehörige Internetadresse ließe sich mit einem handlichen Gerät – man denke an ein Handy in Form eines Stiftes – ermitteln, indem man damit auf den Gegenstand zeigt und auf diese Weise dessen Identität bzw. die darin kodierte Internetadresse ausliest. So kann dieser „Handystift" von sich aus und ohne weitere Zuhilfenahme des anvisierten Objektes die entsprechende Homepage über das Funknetz besorgen und anzeigen [Kin02]. Zur Darstellung der Information mag in Zukunft vielleicht ein Retinaldisplay genutzt werden – oder der Zeigestift fungiert gleich auch

als Laserbeamer, mit dem man die Information einfach auf eine beliebige Fläche projizieren kann [Zac04].

Für den Nutzer entsteht so jedenfalls der Eindruck, als habe ihm der Gegenstand selbst eine Information „zugefunkt", obwohl diese tatsächlich vom Zeigegerät aus dem Internet besorgt wurde [BaM98]. Bei der Information kann es sich beispielsweise um eine Gebrauchsanweisung handeln, um ein Kochrezept für ein Fertiggericht oder auch um den Beipackzettel eines Arzneimittels. Was im Einzelnen angezeigt wird, mag vom Kontext abhängen – also etwa davon, ob der Nutzer ein guter Kunde ist und viel für das Produkt bezahlt hat, ob er über oder unter 18 Jahre alt ist, welche Sprache er spricht, wo er sich gerade befindet oder welchen „Welterklärungsservice" eines Lexikonverlags er abonniert hat.

3.7 Was noch?

Im Rahmen dieses Beitrages kann nicht näher auf jede einzelne der vielen „enabling technologies" eingegangen werden, die zum Internet der Dinge beitragen. Ein wichtiges zu diskutierendes Gebiet wären zum Beispiel noch *„intelligente" Mensch-Maschine-Schnittstellen* – schließlich ist ja a priori nicht klar, wie wir in intuitiver Weise mit unsichtbaren Computern und smarten Dingen in unserer Umgebung interagieren sollen. Gefragt sind hier Ergebnisse aus den Bereichen Bild- und Gestenerkennung, Sprachverstehen, Nutzermodellierung, kognitive Psychologie etc., die teilweise eng mit dem Gebiet der Künstlichen Intelligenz zusammenhängen. Fortschritte in der Künstlichen Intelligenz sind aber hinsichtlich der Modellierung und partiellen Simulation der menschlichen Intelligenz notorisch zäh; hier sind vor allem Erkenntnisse grundlegender Forschung gefragt. Gelegentlich helfen im Bereich von Mensch-Maschine-Schnittstellen aber auch schon gute "Engineering"-Lösungen weiter, wie z.B. das „PenPhone" von Siemens, das ein Handy in Form eines Stiftes mit Handschriftenerkennung darstellt. Platz für Tasten gibt es nicht – um einen Anruf zu tätigen, wird die Telefonnummer einfach auf eine beliebige Unterlage geschrieben.

Eine Herausforderung stellt auch vieles dar, was mit dem Begriff des *„context computing"* zusammenhängt. Einerseits sollen sich smarte Dinge typischerweise kontextbezogen verhalten, andererseits gelingt dies bisher nur gut bei einem recht eingeschränkten Verständnis von „Kontext". So lässt sich etwa, wie oben diskutiert, der Ort eines mobilen Gerätes innerhalb gewisser Grenzen relativ eindeutig ermitteln. Viel schwieriger ist es aber, aus einigen wenigen Sensorwerten auf die momentan relevante *Situation* zu schließen und situationsadäquat zu reagieren. Einen Koffer, der beim Packen an wichtige vergessene Utensilien erinnert, darf man sich wünschen – aber kann man ihn auch realisieren? Welches Weltwissen benötigt er, um zu erkennen, dass bei einer Geschäftsreise nach Florida auch im Februar an die Badehose erinnert werden sollte? „Intelligente" Vermutungen über die Absichten eines Nutzers anzustellen, aus früheren Situationen zu lernen und sich adaptiv zu verhalten, scheint inhärent schwierig [Lue02]. Hier zeichnet sich keine generelle Lösung ab, auch wenn in den Bereichen Nutzer-, Kontext- und Weltmodellierung intensiv geforscht wird.

Schließlich gäbe es auch zu den Forschungen aus den Bereichen *Middleware* und *Infrastrukturen zur Kooperation smarter Objekte* einiges zu berichten. Hier geht es darum, dass alles zusammenpasst, dass die vielen smarten Dinge sich verstehen und aufeinander verlassen können und dass ihnen die Grunddienste bereitgestellt werden, die sie typischerweise zur Erfüllung ihrer Aufgaben erwarten oder benötigen. Dazu gehören Protokolle und Standards wie XML, UDDI, OSGI, UPnP, Jini, HAVi etc. Zum Thema „Middleware" sei auf den Beitrag von Thomas Schoch verwiesen.

4 Die Informatisierung und Instrumentierung der Welt

Fasst man die oben skizzierten Techniktrends und Entwicklungen zusammen – extrem miniaturisierte Sensoren, die vielfältige Umgebungsinformation erfassen, stecknadelgroße Kameras hoher Auflösung, allerkleinste, energieeffiziente und preiswerte Prozessoren mit integrierter drahtloser Kommunikationsfähigkeit, Fernidentifikation von Dingen durch passive und praktisch unsichtbare Elektronik, präzise Lokalisierung von Gegenständen, flexible Displays auf Polymerbasis, elektronische Tinte etc. – so wird deutlich, dass damit die technischen Grundlagen für eine spannende Zukunft gelegt sind. Dies auch ungeachtet der Tatsache, dass etwa hinsichtlich der adäquaten Verarbeitung von Kontextinformation oder einer „intelligenten" Mensch-Maschine-Interaktion noch viele grundlegende und schwierige Fragen ungelöst sind. Die Devise für die von der Ubiquitous-Computing-Gemeinde propagierten smarten Alltagsdinge und Umgebungen heißt, sich „schlau", also situationsangepasst, zu verhalten, ohne tatsächlich „intelligent" im Sinne von „vernunftbegabt" zu sein.[10]

Konkret schälen sich zurzeit zwei unterschiedliche Stoßrichtungen heraus, die durch den massiven Einsatz von Mikroelektronik die Welt informatisieren und – im wörtlichen Sinne – instrumentieren wollen: Zum einen sind es die Sensornetze, bei denen eine große Zahl kleinster und sich typischerweise zu drahtlosen Ad-hoc-Netzen formierender Sensoren in die Umwelt eingebracht wird, um diese im weitesten Sinne zu überwachen. Zum anderen sind es smarte Alltagsgegenstände, die ihren Nutzern aufgrund autonomer „Intelligenz" (oder besser „Smartness") und der Kooperationsfähigkeit mit anderen smarten Dingen und Hintergrundservices einen Zusatznutzen stiften. Beide Aspekte sollen nachfolgend diskutiert werden.

4.1 Sensornetze

Mit miniaturisierten und energieeffizienten Sensoren, die ihre Werte vorverarbeiten und – zumindest über kurze Distanzen – drahtlos übermitteln können, wird es möglich, vielfältige Phänomene der Welt in bisher nie da gewesener Genauigkeit zu beobachten [Aky02, CES04]. Indem viele solche Sensoren großflächig in die

[10] Matthias Horx bringt dies in netter Form auf den Punkt: *„Ich will nicht, dass mein Kühlschrank intelligent wird. Ich will, dass er blöd ist, aber schlau funktioniert."*

Umwelt oder in physische Strukturen wie Brücken, Straßen oder Wasserversorgungssysteme eingebracht werden, erhält man dichte Überwachungsnetze für unterschiedlichste Zwecke.

Die Aufgabe eines einzelnen Sensorknotens in einem solchen Verbund besteht zunächst nur darin, seine unmittelbare Umgebung zu beobachten. Die Sensoren können sich aber mit benachbarten Sensoren vernetzen, ihre Arbeit untereinander abstimmen und relevante Beobachtungen austauschen. Die Kooperation der Sensoren ist entscheidend, denn nur dadurch ist es im Allgemeinen möglich, wesentliche Eigenschaften eines Phänomens (wie Aufenthaltsort, räumliche Orientierung, Bewegungsrichtung- und Geschwindigkeit, Größe und Form von Objekten) zu erkennen und über die Zeit hinweg zu beobachten. Wird es bei einem Sensor zum Beispiel heiß, kurze Zeit später bei einem benachbarten Sensor, und wieder etwas später bei einem dritten Sensor, so lässt sich daraus auf ein Feuer schließen, und es kann mit weiteren geeigneten Daten der Umfang sowie die Ausbreitungsrichtung und -geschwindigkeit des Brandes berechnet werden.

Durch die geringe Größe der Sensoren und dadurch, dass sie keine physische Infrastruktur wie Verkabelung und Stromanschlüsse benötigen, kann die Instrumentierung in flexibler und nahezu unsichtbarer Weise geschehen, ohne die beobachteten Aspekte wesentlich zu beeinflussen. In gewisser Weise handelt es sich dabei um einen Paradigmenwechsel im Einsatz von Computern: Verarbeitete man früher (mit einer „EDV-Anlage“) Daten, die typischerweise manuell eingegeben wurden, so erfasst man jetzt, wo Computer Augen, Ohren und andere Sinnesorgane bekommen, die physischen Phänomene unmittelbar – und zwar automatisch, online und in Realzeit. Tatsächlich sendet die Umwelt eine Vielzahl von Signalen unterschiedlicher „Modalitäten“ aus; messen oder beobachten kann man akustische Phänomene, visuelle Phänomene wie die Bewegung von Objekten oder aber einfach nur Helligkeit, Beschleunigung, Temperatur, Feuchtigkeit und viele andere Parameter.

Hinsichtlich der technischen Aspekte und der Informatikkonzepte, die für einen großräumigen Einsatz vernetzter Sensoren notwendig sind, zeichnet sich die Machbarkeit inzwischen ab, auch wenn noch eine Vielzahl von Problemen auf der Ebene der Hardware und der Softwarearchitektur zu lösen ist, bevor Sensornetze einfach angewendet werden können. Estrin et al. [Est02] schreiben dazu: *„Interfacing to the physical world is arguably the single most important challenge in computer science today.“*

Letztendlich erwartet man von Sensornetzen in Zukunft Gewaltiges: Statt Experimente in einem Labor voller Instrumente durchzuführen, soll es dann – quasi umgekehrt – oft möglich sein, die extrem miniaturisierten Beobachtungsinstrumente am Vorgang in der Natur selbst anzubringen. Ökosysteme beispielsweise sollten sich so viel leichter und umfassender beobachten lassen. Allgemein dürften die stark sinkenden Kosten zur Überwachung und Informationsgewinnung viele Anwendungen ermöglichen, die bisher unwirtschaftlich gewesen wären – vor allem im industriellen Bereich. William A. Wulf, Präsident der US-amerikanischen Academy of Engineering, meinte kürzlich zum Beispiel [Wul04]: *„Over the life of a bridge, it costs more to check for corrosion than to build the bridge itself. So we built a chip that had a small amount of computing power, a corrosion sensor, and a radio transceiver. The idea was to put a shovel-load of these chips in every mix of concrete, so that you'd be able to ask the sensors*

whether or not the reinforcing bars were corroding. It's hard to think of a more mundane product than a concrete bridge; yet we're talking about how to make it smart." Andere, wie Priscilla Nelson von der US-amerikanischen National Science Foundation sprechen sogar von einer „Revolution" [Nel04]: *„Distributed sensing is about being able to observe freshly and innovatively the world around us, both the constructed and the natural environments, and indeed our own organizational and social environments. We're right on the edge of what I think of as the Sensing Revolution, and it's very exciting."* Selbstverständlich ist auch das Militär an sich autonom konfigurierenden Sensornetzen – insbesondere in der Form von „smart dust" [Kah99] – sehr interessiert, da diese ein ideales Aufklärungsmittel darstellen.

Christoph Podewils hat die Zukunftsaussichten mit Sensornetzen auf witzige und fast poetische Art unlängst so beschrieben [Pod04]: *„Computer kaufen, das könnte in einigen Jahren so ähnlich sein wie heute Bonbons aussuchen in der Süßwarenabteilung. Der Verkäuferin wird man sagen: '50 Gramm von den Temperaturchips, bitte sehr! Und dann geben Sie mir noch ein Pfund von den Feuchtigkeitssensoren, es hat ja schon seit ein paar Wochen nicht mehr geregnet.' Im Garten wird man dann in die Chipstüte greifen, eine Hand voll Körner herausnehmen und über den Boden verstreuen, ganz so wie Blumensamen. Die winzigen Computer merken dann, dass sie auf den Boden gefallen sind, schalten sich ein und wachen fortan darüber, wie feucht oder wie warm es im Beet oder auf der Wiese ist. Wird es zu trocken oder zu kalt, so alarmieren sie per Funk einen Nachbarcomputer, der seinerseits einen weiteren Nachbarn anfunkt und so weiter – per Inselspringen erreicht der Hilferuf schließlich einen Gartenroboter, der sich dann mit der Gießkanne auf den Weg macht oder auch eine Pflanze ins Warme holt."*

Die Hauptaufgabe von Sensornetzen ist das feinmaschige und umfassende Monitoring. Werden damit nicht Ökosysteme, Produktionsprozesse oder physische Infrastrukturen überwacht, sondern in indirekter oder direkter Weise Menschen, dann zieht eine solche einfach anzuwendende Technik eventuell massive gesellschaftliche Probleme nach sich – es könnte damit die delikate Balance von Freiheit und Sicherheit aus dem Gleichgewicht gebracht werden, weil die qualitativen und quantitativen Möglichkeiten zur Überwachung derart ausgeweitet werden, dass auch Bereiche erfasst werden, die einem dauerhaften und unauffälligen Monitoring bisher nicht zugänglich waren. Viele Wünsche totalitärer Machthaber, staatlicher Institutionen oder neugieriger Zeitgenossen würden damit wohl mehr als zufrieden stellend erfüllt. Insofern erscheinen drahtlos kommunizierende Sensoren langfristig gesehen als viel größere Bedrohung für die Privatsphäre als die in dieser Hinsicht gegenwärtig kontrovers diskutierte RFID-Technologie[11]. Schließlich handelt es sich bei den Sensoren um nahezu unsichtbare, aber äußerst mitteilsame „Spione". Wenn diese ein billiges Massenprodukt werden, dann lässt sich ihr Einsatz kaum kontrollieren und ein Missbrauch nur schwer verhindern.

---

[11] *„Da der RFID an der Kaugummi-Packung in seiner Jackentasche nicht im Supermarkt zerstört wurde, wird er als Kaugummi-Kauer identifiziert und die Tanksäule spielt ihm während des Wartens Werbespots für Konkurrenz-Kaugummis vor"*, so eines der Szenarien, die im Rahmen der Verleihung des „BigBrother Awards" an die Metro AG für das Projekt "Future Store" propagiert wurden, siehe www.big-brother-award.de/2003/.cop

4.2 Smarte Dinge

Smarte Dinge sind Alltagsgegenstände, die mit Informationstechnologie zum Sammeln, Speichern, Verarbeiten und Kommunizieren von Daten „aufgerüstet" sind. Sie erhalten so eine gegenüber ihrem ursprünglichen Zweck erweiterte Funktionalität und damit eine neue, zusätzliche Qualität. Idealerweise erscheint der informationsverarbeitende Anteil eines smarten Dings dem Nutzer als vollkommen in den Gegenstand und seine herkömmliche Funktionalität integriert, bietet aber darüber hinausgehende Eigenschaften. Um ihre Aufgabe gut zu erfüllen, müssen smarte Dinge typischerweise (z.B. über Sensoren) mit Informationen ihrer Umgebung versorgt werden und kommunizieren können, weil erst dadurch eine Wechselwirkung zwischen Computer und „Cyberspace" einerseits und der realen Umwelt andererseits möglich wird.

Beispiele für smarte Dinge sind Autoreifen, die den Fahrer benachrichtigen, wenn der Luftdruck abnimmt, oder Medikamente, die sich rechtzeitig bemerkbar machen, bevor ihr Haltbarkeitsdatum abläuft [ScS03]. Idealerweise können smarte Dinge nicht nur mit Menschen und anderen smarten Gegenständen in geeigneter Weise kommunizieren, sondern zum Beispiel auch erfahren, wo sie sich befinden, welche anderen Gegenstände in der Nähe sind, was in der Vergangenheit mit ihnen geschah und was in ihrer Umgebung los ist.

Smarte und kommunikationsfähige Dinge haben ein hohes Anwendungspotenzial – welche konkreten Ideen wirtschaftlich sinnvoll sind, wird sich aber erst noch zeigen müssen. Zum Beispiel könnte ein Auto das andere auf der Gegenfahrbahn vor einem Stau warnen. Oder mein Mobiltelefon könnte sich daran erinnern, wann und wo es zuletzt in unmittelbarer Nähe meines Schlüsselbundes war. Ferner mag eine Mülltonne neugierig auf die Recyclingfähigkeit ihres Inhaltes sein, ein Arzneischrank mag um die Verträglichkeit seiner Medikamente und deren Haltbarkeit besorgt sein, und eine Wohnungsheizung könnte mit dem Auto oder anderen persönlichen Gegenständen der Bewohner „konspirieren" wollen, um zu erfahren, ob mit deren baldiger Rückkehr zu rechnen ist.

Die eben genannten Beispiele sind noch Zukunftsmusik, Vorläufer smarter Alltagsdinge existieren allerdings bereits und sind unter dem Begriff „eingebettete Systeme" bekannt. Dabei handelt es sich um Mikroprozessoren und andere Computerelemente, die zu Steuerungsaufgaben in Maschinen und Geräte eingebaut werden. Einfache Prozessoren, die nicht höchste Leistung für Multimedia-PCs erzeugen müssen, können billig und klein hergestellt werden. Über 98 % der vielen Milliarden Mikroprozessoren, die jedes Jahr produziert werden, finden sich auch nicht in PCs oder sonstigen Computern, sondern in irgendwelchen anderen Geräten – Autos, Nähmaschinen, Spielkonsolen, Heimtrainern, elektrischen Zahnbürsten, Waschmaschinen, Verkaufsautomaten und Fotokopiergeräten zum Beispiel [PaM04].

Praktisch alle Geräte, die eine digitale Schnittstelle haben, beruhen auf einem eingebetteten System. Oft ist dessen Steuerung so komplex, dass hierfür ein Betriebssystem notwendig ist. Auf dem Markt gibt es zu diesem Zweck einige Systeme und Sprachplattformen wie zum Beispiel embedded Java, Symbian (das aus dem Bereich der Mobiltelefone stammt), Windows CE oder embedded Linux. Die ersten Versionen von Symbian und vergleichbaren Systemen (z.B. PalmOS) wa-

ren aufgrund der anfangs stark beschränkten Hardwareressourcen mit einem sehr reduzierten Funktionsumfang ausgestattet. Erst im Laufe der Zeit gesellten sich Funktionen typischer Betriebssysteme (z.B. Speicherschutz oder multi threading) hinzu, sodass komplexere und portable Anwendungen möglich wurden. Gerade umgekehrt verläuft die Entwicklung bei Windows und Linux: Diese klassischen Server- und PC-Systeme wurden so weit abgespeckt und adaptiert, dass sie mit reduziertem Funktionsumfang auch auf Hardwareplattformen geringerer Leistung laufen. Die Entwicklung der Softwareplattformen (und der Kampf um Marktanteile) ist noch voll im Gang – insbesondere, was die oben definierten „Milliwattknoten" betrifft. Für die kommende Generation der „Mikrowattknoten", also die Systeme für smarte Alltagsdinge und Sensorknoten, existieren erst einige Forschungsprototypen; noch ist weitgehend unklar, welche Anforderungen die zukünftigen Anwendungen smarter Dinge an die Software-Grunddienste stellen werden.

Was die Hardware eingebetteter Systeme für smarte Dinge betrifft, stellen die verschiedenen Basistechnologien von Sensorik, Verarbeitungseinheit und Kommunikationseinheit, nämlich Analog-, Digital- und Hochfrequenztechnologie, recht unterschiedliche Anforderungen an den Herstellungsprozess. Daher ist eine Integration derzeit noch teuer, technisch aber nicht unmöglich. Ziel ist ein einziger kleiner Chip, der Umgebungsparameter wahrnimmt, diese verarbeitet und gegebenenfalls gleich weitermeldet – an einen Menschen, an ein informationstechnisches System oder an andere smarte Dinge. Da der technische Fortschritt mit seinen Konsequenzen hinsichtlich Energiebedarf, Größe, Leistungsfähigkeit und Kosten der mikroelektronischen Funktionalität auch hier ungebremst ist, darf man erwarten, dass in ferner Zukunft fast beliebige Alltagsgegenstände mit eingebetteter Informationstechnologie „smart gemacht" werden, sofern dies im jeweiligen Fall einen Nutzen stiftet und einen wirtschaftlichen Sinn ergibt.

Die Zweckmäßigkeit konkreter Anwendungen smarter Dinge einzuschätzen ist schwierig, und auch Experten[12] sind sich nicht darüber im Klaren, welche der vielen oft zunächst absurd klingenden Ideen – angefangen vom Fertiggericht, das Rezeptvorschläge (und natürlich Werbung) auf die Kühlschranktür projiziert, bis hin zur schlauen Unterwäsche, die eine kritische, vom individuellen Normalfall abweichende Puls- und Atemfrequenz dem Arzt weitermeldet – letztlich eine wichtige Rolle in der Zukunft spielen könnten. Generell scheint das Potenzial hinsichtlich sinnvoller Anwendungen jedoch groß, wenn Gegenstände miteinander kooperieren können und drahtlosen Zugriff auf externe Datenbanken haben oder passende Internet-basierte Services nutzen können. So gewinnt offenbar ein automatischer Rasensprinkler nicht nur durch eine Vernetzung mit Feuchtigkeitssensoren im Boden an Effizienz, sondern auch durch die Konsultation der Wetterprognose im Internet.

Viele weitere Anwendungen „schlauer" und kommunizierender Alltagsdinge sind denkbar. Allgemein ist zu erwarten, dass zunehmend hybride Produkte ent-

[12] *„Naturwissenschaftler und Techniker gehen davon aus, dass neue technische Möglichkeiten (für die sie aus ihrer Lebenswelt bestimmte Nutzungsformen sehen) nicht nur genutzt werden, sondern so genutzt werden, wie sie sich das gedacht haben. Dies war – insbesondere was die Geschichte der Informations- und Kommunikationstechnik angeht – häufig genug ein Irrtum."* Gernot Wersig

stehen werden, die sich aus physischer Leistung (z.B. ein Medikament mit seinen biochemischen und medizinischen Wirkungen) und Informationsleistung (bei diesem Beispiel etwa aktuelle Hinweise zum Verlauf einer Grippeepidemie) zusammensetzen. Anfangs werden von den Möglichkeiten des Ubiquitous Computing sicherlich eher solche hochpreisigen Geräte und Maschinen profitieren, die durch sensorgestützte Informationsverarbeitung und Kommunikationsfähigkeit einen deutlichen Mehrwert erhalten. Sind die Grundtechniken und zugehörigen Infrastrukturen dann erst einmal eingeführt, könnten bald darauf auch viele andere und eher banale Gegenstände ganz selbstverständlich das Internet mit seinen vielfältigen Ressourcen für die Durchführung ihrer Aufgaben nutzen, selbst wenn dies uns als Anwender gar nicht immer bewusst ist.

Mittel- und langfristig dürften die diversen Techniken des Ubiquitous Computing sicherlich eine große wirtschaftliche Bedeutung erlangen und zu gravierenden Veränderungen in Geschäftsprozessen führen. Denn werden industrielle Produkte (wie z.B. Haushaltsgeräte, Werkzeuge, Spielzeug oder Kleidungsstücke) durch integrierte Informationsverarbeitung „schlau“, oder erhalten sie auch nur eine fernabfragbare elektronische Identität beziehungsweise Sensoren zur Wahrnehmung des Kontextes (wissen also z.B., wo und in welcher Umgebung sie sich gerade befinden), so sind dadurch nicht nur innovative Produkte, sondern auch zusätzliche Services und neue Geschäftsmodelle möglich: Der digitale Mehrwert eigener Produkte kann diese beispielsweise von physisch ähnlichen Erzeugnissen der Konkurrenz absetzen sowie Kunden stärker an eigene Mehrwertdienste und dazu kompatible Produkte binden. Ferner werden durch technisch ausgefeilte Methoden, welche die tatsächliche Nutzung von physischen Produkten ermitteln und weitermelden, neue Abrechnungs- und Leasingmodelle möglich, wie im Beitrag von Fleisch et al. genauer ausgeführt wird. Generell dürfte die zunehmende Informatisierung von Produkten auch zu einer stärkeren Serviceorientierung führen, denn smarte Dinge können nur dann ihr ganzes Potenzial ausspielen, wenn sie vernetzt werden und in eine umfassende Struktur von Dienstleistungen eingebunden sind.

5 Fazit

Die durch den Fortschritt der Informationstechnologie induzierten Veränderungen geschehen nicht über Nacht. Vielmehr handelt es sich bei diesem Prozess um eine schleichende Revolution, die immer größere Teilbereiche des täglichen Lebens erfasst und durch die dynamische Entwicklung der Mikroelektronik und der Informatik ständig weiter angetrieben wird. Der allgemeine Technologietrend zeigt dabei eindeutig in Richtung einer umfassenden Informatisierung der Welt, die dadurch ungewohnte oder gar bizarre Formen annehmen kann: Alltagsgegenstände werden kommunikativ, vernetzen sich untereinander, wissen über ihre Situation Bescheid und teilen ihre Erkenntnisse anderen Dingen mit, die daraufhin ihr Verhalten ändern können.

Langfristig mag sich damit auch unser Verhältnis zur Welt wandeln. Mike Kuniavsky meint zum Beispiel [Kun04]: *„Once these technologies are widely distributed in everyday objects, the environment they create will become too diffi-*

cult for us to explain in purely functional ways. When we don't have a good functional model to explain how things work, we anthropomorphize them. And when enough things around us recognize us, remember us, and react to our presence I suspect we'll start to anthropomorphize all objects. In other words, because we have no other way to explain how things work, we will see the world as animist. Animism is, in its broadest definition, the belief that all objects have will, intelligence, and memory and that they interact with and affect our lives in a deliberate, intelligent, and (in a sense) conscious way."

Selbst wenn es nicht so weit kommt – die langfristigen Auswirkungen einer tief greifenden Integration von Informationstechnologie in unseren Alltag und einer durch smarte Dinge geschaffenen „augmented reality" dürften jedenfalls gewaltig sein, und es ergeben sich insbesondere im nichttechnischen Bereich viele spannende Herausforderungen [BCL04]. Im Vordergrund steht dabei der Schutz der Privatsphäre [LaM02, Mat05], denn smarte Gegenstände und sensorbestückte Umgebungen häufen potenziell eine große Menge teilweise sensibler und intimer Daten an, um ihren Nutzern jederzeit situationsgerecht dienen zu können. Eine einzelne solche Information mag für sich genommen zwar unscheinbar sein, aber wenn verschiedene an sich harmlose Beobachtungen kombiniert werden, kann dies zu unerwarteten Erkenntnissen führen und eine folgenschwere Verletzung der Privatsphäre nach sich ziehen.

Damit ein Internet der Dinge und eine von Informationstechnik im wahrsten Sinne des Wortes durchdrungene Welt wirklich Nutzen stiften, bedarf es daher mehr als nur mikroelektronisch aufgerüsteter und miteinander kooperierender Gegenstände. Ebenso nötig sind sichere und verlässliche IT-Infrastrukturen, geeignete ökonomische und rechtliche Rahmenbedingungen sowie ein gesellschaftlicher Konsens darüber, wie die neuen technischen Möglichkeiten verwendet werden sollen. Hierin liegt eine große Aufgabe für die Zukunft.

Literatur

[AHS02] Aarts E, Harwig R, Schuurmans M (2002) Ambient Intelligence. In: Denning PJ (ed) The invisible future – the seamless integration of technology in everyday life, McGraw-Hill, S 235–250

[AaM03] Aarts E, Marzano S (2003) The New Everyday – Views on Ambient Intelligence. 010 Publishers

[Aky02] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Computer Networks 38: 393–422

[BaM98] Barrett E, Maglio P (1998) Informative Things: How to Attach Information to the Real World. In: Proceedings UIST '98, pp 81–88

[BCL04] Bohn J, Coroama V, Langheinrich M, Mattern F, Rohs M (2004) Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications. Human and Ecological Risk Assessment 10(5): 763–786

[BHR01] Burkhardt J, Henn H, Hepper S, Rindtorff K, Schaeck T (2001) Pervasive Computing. Addison Wesley

[Bre10] Brehmer A (Hrsg) (1910) Die Welt in 100 Jahren. Verlagsanstalt Buntdruck GmbH

[CES04] Culler D, Estrin D, Srivastava M (2004) Overview of Sensor Networks. Computer, 37(8): 41–49

[DBS04] Ducatel K, Bogdanowicz M, Scapolo F, Leijten J, Burgelman J-C (2004) Dafür sind die Freunde da – Ambient Intelligence und die Informationsgesellschaft im Jahre 2010. In: Zerdick A, Picot A, Schrape K, Burgelman J-C, Silverstone R, Feldmann V, Heger DK, Wolff C (Hrsg): E-Merging Media – Kommunikation und Medienwirtschaft der Zukunft, Springer-Verlag, S 195–218

[DoF03] Dobson JE, Fisher PF (2003) Geoslavery. IEEE Technology and Society Magazine 22(1): 47–52

[Est02] Estrin D, Culler D, Pister K, Sukhatme G (2002) Connecting the Physical World with Pervasive Networks. Pervasive Computing Magazine 1(1): 59–69

[Fin02] Finkenzeller K (2002) RFID-Handbuch. Hanser-Verlag

[GrH03] Grochowski E, Halem R (2003) Technological impact of magnetic hard disk drives on storage systems. IBM Systems Journal 42(2): 338–346

[GKC04] Gershenfeld N, Krikorian R, Cohen D (2004) The Internet of Things. Scientific American, October, pp 76–81

[Hay02] Hayes B (2002) Terabyte Territory. American Scientist 90(3): 212–216

[HiB01] Hightower J, Borriello G (2001) Location Systems for Ubiquitous Computing, IEEE Computer Magazine, August, pp 57–66

[HMN03] Hansmann U, Merk M, Nicklous M, Stober R (2003) Pervasive Computing Handbook (2nd ed.). Springer-Verlag

[Kah99] Kahn JM, Katz RH, Pister KSJ (1999) Mobile Networking for Smart Dust. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom ’99), pp 271–278

[Kan04] Kanellos M (2004) Human chips more than skin-deep. CNET News.com, 23. August 2004, zdnet.com.com/2100-1103-5319869.html

[Kin02] Kindberg T, Barton J, Morgan J, Becker G, Caswell D, Debaty P, Gopal G, Frid M, Krishnan V, Morris H, Schettino J, Serra B, Spasojevic M (2002) People, Places, Things: Web Presence for the Real World. Mobile Networks and Applications 7(5): 365–376

[Kun04] Kuniavsky M (2004) User Expectations in a World of Smart Devices. www.adaptivepath.com/publications/essays/archives/000272.php

[LaM02] Langheinrich M, Mattern F (2002) Wenn der Computer verschwindet – Was Datenschutz und Sicherheit in einer Welt intelligenter Alltagsdinge bedeuten. digma – Zeitschrift für Datenrecht und Informationssicherheit 2(3): 138–142

[LCC05] LaMarca A, Chawathe Y, Consolvo S, Hightower J, Smith I, Scott J, Sohn T, Howard J, Hughes J, Potter F, Tabert J, Powledge P, Borriello G, Schilit B (2005) Place Lab: Device Positioning Using Radio Beacons in the Wild. Pervasive 2005, Springer-Verlag, pp 116–133

[Lue02] Lueg C (2002) On the Gap between Vision and Feasibility. In: Mattern F, Naghshineh M (eds) Pervasive 2002, Springer-Verlag, pp 45–57

[Mat03] Mattern F (2003) Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern F (Hrsg) Total vernetzt – Szenarien einer informatisierten Welt, Springer-Verlag, S 1–41

[Mat04] Mattern F (2004) Ambient Intelligence. In: Bullinger H-J (Hrsg): Trendbarometer Technik, Hanser-Verlag, S 18–19

[Mat05] Mattern F (2005) Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen. In: Taeger J, Wiebe A (Hrsg): Mobilität, Telematik, Recht (DGRI-Jahrestagung 2004), Verlag Dr. Otto Schmidt

[Moo65] Moore G (1965) Cramming more components onto integrated circuits. Electronics 38 (April 1965), pp 114–117

[Moo95] Moore G (1995) Lithography and the Future of Moore's Law. Proceedings SPIE 2440, pp 2–17

[Nel04] Nelson PP (2004) In: The View From the Top. IEEE Spectrum, November 2004, pp 36–51

[PaM04] Payne R, Macdonald B (2004) Ambient technology – now you see it, now you don't. BT Technology Journal 22(3): 119–129

[Pod04] Podewils C (2004) In: Berliner Zeitung vom 27.03.2004

[Sat01] Satyanarayanan, M (2001) Interview: M. Satyanarayanan on Mobile and Pervasive Computing. IEEE Distributed Systems Online, 2(6) http://ads.computer.org/dsonline/0106/departments/int0106_print.htm

[SaT03] Saar S, Thomas V (2003) Toward Trash That Thinks – Product Tags for Environmental Management. Journal of Industrial Ecology 6(2): 133–146

[ScS03] Schoch T, Strassner M (2003) Wie smarte Dinge Prozesse unterstützen. HMD 229: 23–32

[Ste66] Steinbuch K (1966) Die informierte Gesellschaft – Geschichte und Zukunft der Nachrichtentechnik. DVA

[Sto48] Stockman H (1948) Communication by Means of Reflected Power. Proceedings of the IRE, pp 1196–1204

[Tuo02] Tuomi I (2002) The Lives and Death of Moore's Law. First Monday 7(11)

[Wei91] Weiser M (1991) The Computer for the 21st Century. Scientific American 265(3): 66–75

[Wul04] Wulf AW (2004) In: The View From the Top. IEEE Spectrum, November 2004, pp 36–51

[Zac04] Zacks R (2004) Portable Projectors. Technology Review 107(10): 72

Teil B: Technologien

Einführung in die RFID-Technologie

Matthias Lampe, Christian Flörkemeier
Institut für Pervasive Computing, ETH Zürich

Stephan Haller
SAP Research, Karlsruhe, SAP AG

Kurzfassung. Die öffentliche Thematisierung der RFID-Technik und die Standardisierungsbemühungen des Auto-ID Centers haben dazu geführt, dass den Potenzialen der Technologie zur Verbesserung betriebswirtschaftlicher Prozesse zunehmende Bedeutung geschenkt wird. Dabei steht die Vermeidung von Medienbrüchen, d.h. das Überwinden der Lücke zwischen der realen Welt und der digitalen Welt, im Vordergrund. Der vorliegende Beitrag gibt eine Einführung in die RFID-Technik und beschreibt dabei die Komponenten eines RFID-Systems wie Lesegerät und RFID-Transponder. Zum Verständnis der Funktionsweise eines RFID-Systems wird genauer auf die zugrunde liegenden Technologien und darauf aufbauend auf wichtige Auswahlkriterien für RFID-Systeme eingegangen. Abschließend liefert der Beitrag eine Übersicht über relevante RFID-Standards.

1 Einleitung

Während die Radiofrequenz-Identifikation (RFID) in der Vergangenheit vor allem zur Tieridentifikation, in Wegfahrsperren und zur Zugangskontrolle u.a. bei Ski-Anlagen eingesetzt wurde, erweitert sich das Anwendungsfeld nun zunehmend. Die öffentliche Thematisierung der RFID-Transpondertechnik durch das Auto-ID Center und der geplante Einsatz in der Lieferkette von Handelsunternehmen (wie beispielsweise Wal-Mart und Metro) oder in den Logistikprozessen des amerikanischen Verteidigungsministeriums haben dazu geführt, dass den Potenzialen der Technologie zur Verbesserung betriebswirtschaftlicher Prozesse zunehmende Bedeutung geschenkt wird.

Insbesondere die Vermeidung von Medienbrüchen steht hier im Vordergrund, da die kontaktlose, automatische Identifikation durch die RFID-Transpondertechnik es erlaubt, die Lücke zwischen der realen Welt der physischen Objekte und Produkte einerseits und der digitalen Welt in Form von Warenwirtschaftssystemen und SCM-Lösungen andererseits zu verkleinern. Die Folge sind u.a. niedrigere Fehlerquoten, höhere Prozesseffizienz, gesteigerte Produktqualität sowie Kosteneinsparungen durch schnellere und bessere Informationsverarbeitung. Darüber hinaus bildet RFID die Grundlage für zahlreiche weitere Anwendungen, die über reine Identifikation hinausgehen, wie z.B. lückenlose Kühlkettenüberwa-

chung mittels Sensorik oder Echtzeitlokalisierung von Objekten in Produktions- oder Logistikprozessen.

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.

Das Ziel dieses Beitrages ist es, einen Überblick über die RFID-Technik zu liefern. Dabei soll die Funktionsweise der verschiedenen RFID-Systeme aufgezeigt werden, wobei der Fokus vor allem auf den Möglichkeiten und Grenzen der verschiedenen Systeme liegt.

2 Komponenten eines RFID-Systems

Ein typisches RFID-System besteht aus den folgenden drei Komponenten: Rechner, Lesegerät mit Kopplungseinheit (Spule bzw. Antenne) und RFID-Transponder (siehe Abbildung 1).

Das Lesegerät ist über eine serielle Schnittstelle oder Netzwerkverbindung mit dem Rechner, z.B. einem PC, verbunden und dient je nach RFID-System als reines Lesegerät bzw. im erweiterten Sinne als Schreib-/Lesegerät. Die Applikation auf dem Rechner schickt Kommandos und Daten an das Lesegerät und erhält wiederum Antwortdaten vom Lesegerät zurück. Beispiele für Kommandos sind das Auslesen der Identifikationsnummern aller RFID-Transponder im Lesebereich, oder das Beschreiben eines RFID-Transponders mit Daten. Die Kommandos werden dann vom Lesegerät kodiert und auf ein magnetisches bzw. elektromagnetisches Wechselfeld moduliert, das zusätzlich zu den Daten die RFID-Transponder mit Energie versorgt[13]. Alle RFID-Transponder, die sich im Feld des Lesegeräts befinden, empfangen die vom Lesegerät ausgesandten Befehle und Daten und schicken ihre jeweiligen Antwortdaten an das Lesegerät zurück.

[13] Dies gilt nur für passive RFID-Transponder, aktive RFID-Transponder besitzen eine eigene Energieversorgung (vgl. Abschnitt 3.1).

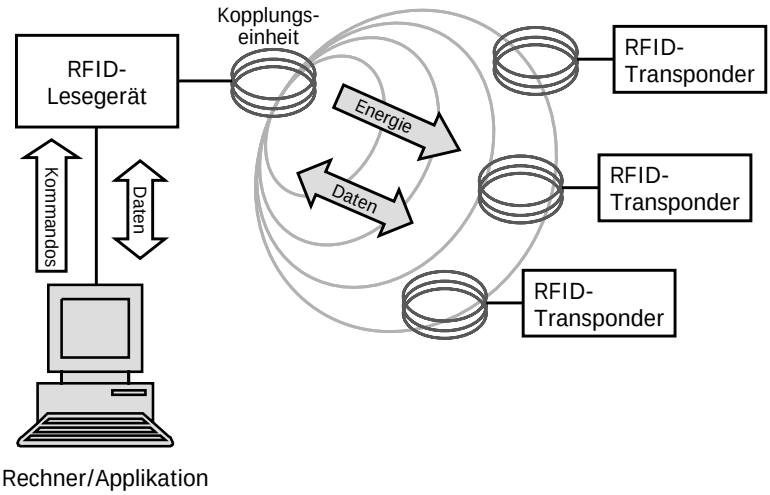


Abb. 1. Komponenten eines RFID-Systems

Ein RFID-Transponder besteht typischerweise aus einem Mikrochip und einer Kopplungseinheit und ist der eigentliche Informationsträger. Man unterscheidet je nach Technologie zwischen RFID-Transpondern, die eine Spule oder eine Antenne als Kopplungseinheit haben. Bei den RFID-Transpondern gibt es eine Vielzahl von Bauformen, die sowohl von der verwendeten Technologie als auch vom Einsatzgebiet des RFID-Transponders abhängen. Abbildung 2 zeigt eine Auswahl verschiedenster Bauformen.

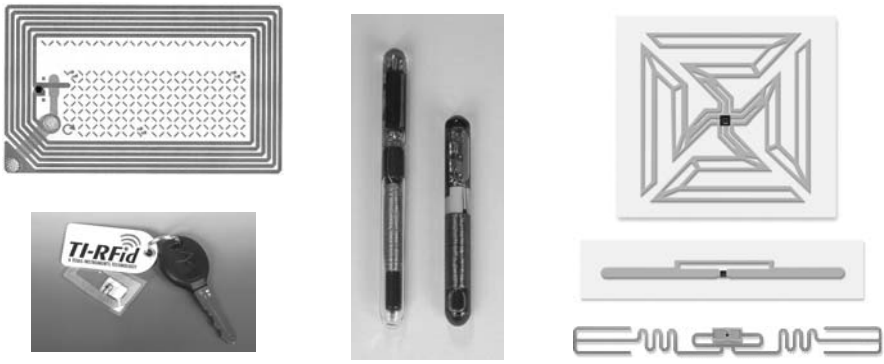


Abb. 2. RFID-Transponder in verschiedenen Bauformen (Quellen: Infineon, Texas Instruments, Symbol, Alien)

Stark verbreitet sind zum einen die so genannten „Smart Labels“, bei denen die Spule mit RFID-Chip auf einer Klebefolie aufgebracht ist, und zum anderen die kontaktlosen Chipkarten. In anderen Bauformen ist der RFID-Transponder in

Kunststoffe oder andere Materialien eingebracht. Eine solche Spezialverpackung macht die RFID-Transponder resistent gegenüber Schmutz oder Säuren und erlaubt den Einsatz unter hohen Temperaturen und anderen widrigen Umweltbedingungen, wie sie häufig im industriellen Umfeld anzutreffen sind. Für Zugangskontrollen oder Wegfahrsperren werden RFID-Transponder oft in Schlüsselanhänger oder Uhren integriert. Bei der Tieridentifikation werden RFID-Transponder in kleinen Glasröhrchen eingesetzt, die den Tieren unter die Haut injiziert werden.

Abb. 3. Bauformen von Lesegeräten mit Kopplungseinheiten (Quellen: Symbol, Alien, Infineon)

Bei den Lesegeräten macht hauptsächlich die Größe und Form der Kopplungseinheit die Bauform aus (siehe Abbildung 3). Bei mobilen Lesegeräten ist das eigentliche Lesegerät und die Kopplungseinheit mit dem Rechner in einem gemeinsamen Gehäuse integriert, um das mobile Auslesen von RFID-Transpondern zu ermöglichen. Lesegeräte mit Flachantennen in typischen Größen von DIN A3/A4 werden z.B. in Bibliotheken bei der Buchausleihe und -rückgabe eingesetzt. Bei einem „Gate“ sind Lesegerät und Kopplungseinheit räumlich getrennt. Die Anordnung von zwei Kopplungseinheiten bei einem Gate ermöglicht einen größeren Lesebereich zwischen den beiden Einheiten. Anwendung finden Gates in der Warensicherung und in der Lieferkettenüberwachung, z.B. beim Wareneingang und -ausgang. Anwendungen, die viele RFID-Transponder erkennen müssen, die sich ungeordnet auf engem Raum befinden, werden oft durch Tunnelleser realisiert, wie z.B. in der Materialflussverfolgung oder bei der Paketsortierung. Bei einem Tunnelleser sind mehrere Kopplungseinheiten in einem Tunnel angebracht, der nach außen abgeschirmt ist, sodass innerhalb des Tunnels größere Feldstärken möglich sind als bei einem nicht abgeschirmten System und deshalb auch bessere Leseraten erzielt werden.

3 Funktionsweise

Die Funktionsweise eines RFID-Systems lässt sich durch grundlegende technische Eigenschaften wie Energieversorgung und Speicherstruktur der RFID-

Transponder, Sendefrequenz des Lesegeräts, Kopplung und Datentransfer zwischen Lesegerät und RFID-Transponder und eingesetztem Vielfachzugriffsverfahren beschreiben und klassifizieren. Im Folgenden wird auf diese Aspekte genauer eingegangen; für eine umfassende Darstellung sei der Leser jedoch auf das RFID-Handbuch von Klaus Finkenzeller [Fin02] verwiesen.

3.1 Energieversorgung

RFID-Transponder benötigen Energie zum einen, um ihren Mikrochip zu betreiben, und zum anderen, um Daten zum Lesegerät zu senden. Dabei unterscheidet man die folgenden drei Arten von RFID-Transpondern:

- *Passive* RFID-Transponder benutzen die Energie des Feldes, das vom Lesegeräte erzeugt wird, sowohl für das Betreiben des Mikrochips als auch zum Senden der Daten.
- *Semi-aktive* RFID-Transponder haben eine interne Batterie, mit der sie ihren Mikrochip versorgen. Sie benutzen aber zum Senden der Daten die Energie des Feldes des Lesegeräts.
- *Aktive* RFID-Transponder haben eine interne Batterie, die sie für beide Zwecke benutzen.

3.2 Sendefrequenz und Kopplung

Die Sendefrequenzen der meisten RFID-Systeme liegen in den lizenzfreien ISM-Bändern (Industrial-Scientific-Medical), die für industrielle, wissenschaftliche und medizinische Anwendungen weltweit freigehalten sind. Hinzu kommt der Frequenzbereich unterhalb 135 kHz und um 900 MHz. Damit fallen die typischen Sendefrequenzen eines RFID-Systems in die folgenden vier Bereiche (siehe Abbildung 4):

- 100–135 kHz (Niederfrequenz, LF)
- 13,56 MHz (Hochfrequenz, HF)
- 868 MHz (Europa) / 915 MHz (USA) / 950–956 MHz (Japan, geplant) (Ultrahochfrequenz, UHF)
- 2,45 GHz und 5,8 GHz (Mikrowelle, MW)

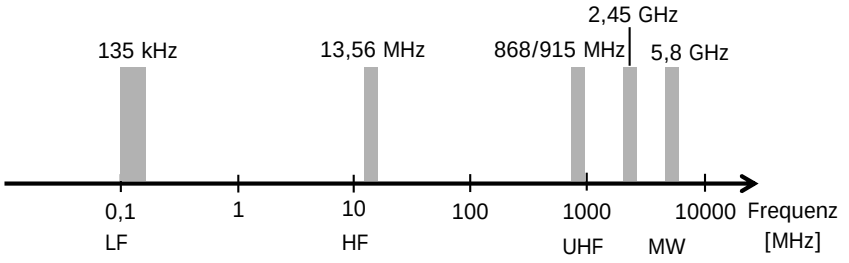


Abb. 4. RFID-Frequenzbänder

Die Funktionsweise von RFID-Systemen wird innerhalb der erlaubten Frequenzbänder durch Vorschriften weiter eingeschränkt. Für den weltweiten Einsatz eines RFID-Systems sind die folgenden Vorschriften relevant: Das Harmonisierungsdokument CEPT/ERC REC 70-03 [ERC02] des European Radiocommunications Office[14] mit den Normen EN 300 330, EN 300 220 und EN 300 440 des European Telecommunications Standards Institute[15], für die USA die Zulassungsvorschrift „FCC Part 15“ [FCC01] der Federal Communications Commission[16] (FCC) und für Deutschland die Verfügungen 61/200 [RTP00a] und 73/2000 [RTP00b] der Regulierungsbehörde für Telekommunikation und Post[17] (RegTP). Die Vorschriften geben maximal zulässige Sendeleistungen bzw. Feldstärken, erlaubte Seitenbänder, sowie standardisierte Messverfahren vor. Die Frequenzen im Bereich um 135 kHz und 13,56 MHz stehen weltweit für RFID-Systeme zur Verfügung. Bei den Frequenzen im UHF-Bereich ist dies nicht der Fall. Während in den USA eine Sendeleistung von vier Watt möglich ist, erlauben die europäischen Zulassungsbeschränkungen bisher nur eine Sendeleistung von einem halben Watt (in Japan ist dieses Frequenzband für RFID-Systeme nicht zugelassen). Allerdings gibt es Bestrebungen, innerhalb Europas die Bandbreite in diesem Frequenzband zu vergrößern und die Sendeleistung auf 2 W zu erhöhen bzw. dieses Frequenzband in Japan neu zu etablieren [Rfi03]. In Zukunft kann daher davon ausgegangen werden, dass das UHF-Frequenzband mit entsprechender Sendeleistung zumindest in den USA, Europa und Japan verfügbar sein wird.

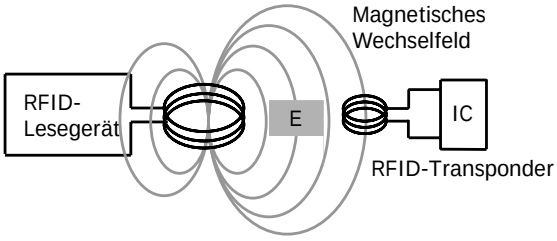


Abb. 5. Energieversorgung durch induktive Kopplung

Bei RFID-Systemen mit *Sendefrequenzen von 135 kHz und 13,56 MHz* findet die Energieübertragung mittels induktiver Kopplung durch ein Magnetfeld ähnlich wie bei einem Transformator statt. Der Kopplungsfaktor bei RFID-Systemen ist jedoch sehr viel kleiner als bei einem Transformator und liegt bei ca. 1 %. Die Spule des Lesegeräts erzeugt ein magnetisches Wechselfeld mit der Sendefrequenz, das eine Wechselspannung in der Spule des RFID-Transponders induziert (siehe Abbildung 5). Die Spannung wird im RFID-Transponder gleichgerichtet und dient dann bei passiven RFID-Transpondern zur Energieversorgung des Mikrochips. Auf dem Schaltkreis des RFID-Transponders befindet sich typischerwei-

[14] www.ero.dk
[15] www.etsi.org
[16] www.fcc.gov
[17] www.regtp.de

se ein Schwingkreis, dessen Frequenz auf die Sendefrequenz des Lesegeräts eingestellt ist. Bei Resonanz wird dadurch die induzierte Spannung im Vergleich zu Frequenzen außerhalb des Resonanzbandes erheblich verstärkt, was zu einer erhöhten Lesereichweite führt.

Die induzierte Spannung im RFID-Transponder hängt unter anderem von der Anzahl der Windungen in der Spule des RFID-Transponders und der Sendefrequenz ab. Daraus ergibt sich, dass bei einer Sendefrequenz von 135 kHz sehr viel mehr Windungen benötigt werden, als bei 13,56 MHz, um bei gleicher Feldstärke auf die nötige Spannung im RFID-Transponder zu kommen. Bei 135-kHz-Transpondern liegt die Anzahl der Windungen typischerweise um die 1000, bei 13,56-MHz-Transpondern um die 10.

Der Verlauf des distanzbezogenen Abfalls der Feldstärke des magnetischen Feldes hängt von der Ausgangsleistung des Lesegeräts, der Sendefrequenz und auch vom Durchmesser der Spule des Lesegeräts ab. Die Feldstärke nimmt dabei innerhalb eines gewissen Bereiches, dem so genannten Nahfeld, proportional zur dritten Potenz der Entfernung ab, außerhalb des Nahfeldes, dem so genannten Fernfeld, nur direkt proportional zur Entfernung. Die Ausdehnung des Nahfeldes lässt sich mathematisch ermitteln und ist umgekehrt proportional zur Sendefrequenz. Da die induktive Kopplung nur im Nahfeld funktioniert, stellt sie somit eine theoretische Grenze für die maximale Reichweite dar. Die typische Reichweite liegt in der Praxis jedoch immer deutlich unter dieser Grenze, da die induzierte Spannung im RFID-Transponder bei dieser Grenze zu niedrig ist, um den Mikrochip zu betreiben. Bei einem RFID-Transponder im Kreditkartenformat entspricht die maximale Reichweite eines Lesegeräts ungefähr dem Durchmesser der Spule des Lesegeräts.

Die Übertragung der Daten vom RFID-Transponder zum Lesegerät wird mittels Lastmodulation verwirklicht. Die Daten werden dabei als ein digitales Signal kodiert, das einen Lastwiderstand ein- und ausschaltet. Die Veränderungen des Widerstandes ändern dabei die Gegeninduktivität des RFID-Transponders, die vom Lesegerät in Form kleiner Spannungsänderungen wahrgenommen wird. Diese so aufmodulierten Daten werden vom Lesegerät demoduliert, dekodiert und weiterverarbeitet.

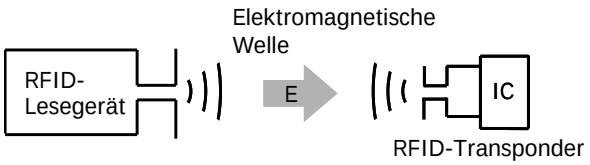


Abb. 6. Energieversorgung durch elektromagnetische Kopplung

Bei RFID-Systemen mit *Sendefrequenzen von 868 bzw. 915 MHz, 2,45 GHz und 5,8 GHz* findet die Energieübertragung durch elektromagnetische Kopplung statt. Die Antenne des Lesegeräts erzeugt eine elektromagnetische Welle, die sich im Raum ausbreitet und in der Antenne des RFID-Transponders eine Wechselspannung erzeugt (siehe Abbildung 6). Die Spannung wird im RFID-Transponder

gleichgerichtet und dient dann bei passiven Systemen zur Energieversorgung des Mikrochips.

Die maximale Reichweite hängt u.a. von der Sendeleistung des Lesegeräts ab. Da die Energie im Fernfeld umgekehrt proportional zum Quadrat der Entfernung von der Antenne abnimmt, sind der maximalen Reichweite jedoch Grenzen gesetzt. Die Sendeleistung ist durch Zulassungsvorschriften beschränkt und damit ergeben sich unter idealen Bedingungen für passive Systeme Reichweiten von 5–7 m, für semi-aktive Systeme bis zu 15 m und für aktive Systeme Reichweiten von bis zu 100 m.

Die Übertragung der Daten zum Lesegerät wird bei passiven Systemen durch die Variation des Rückstrahlquerschnittes erreicht. Wie bei LF- und HF-Systemen werden die Daten als ein digitales Signal kodiert, das einen Widerstand parallel zur Antenne ein- und ausschaltet. Die Veränderungen des Widerstandes ändern dabei die Eigenschaften der reflektierten elektromagnetischen Welle und modulieren so die Daten auf die Welle auf. Die reflektierte Welle wird vom Lesegerät demoduliert und das daraus erhaltene Signal dekodiert.

3.3 Vielfachzugriffsverfahren

Viele Anwendungen fordern von RFID-Systemen, dass eine größere Anzahl von Objekten gleichzeitig erkannt wird, z.B. alle Waren auf einer Palette im Wareneingang. Verglichen mit RFID-Systemen, bei denen sich immer nur ein einziger RFID-Transponder im Lesebereich befindet, z.B. bei der Zugangskontrolle, bedingt dies ein komplexeres Kommunikationsverfahren.

Ein solches Verfahren, das es mehr als einem RFID-Transponder ermöglicht, gleichzeitig auf das Übertragungsmedium zuzugreifen, nennt man Vielfachzugriffsverfahren. In der Funktechnik sind Raummultiplex (SDMA), Zeitmultiplex (TDMA), Frequenzmultiplex (FDMA) und Codemultiplex (CDMA) als Vielfachzugriffsverfahren bekannt. Da RFID-Transponder nur über eine beschränkte Leistungsfähigkeit verfügen und möglichst günstig hergestellt werden sollen, wird dabei hauptsächlich TDMA, seltener auch FDMA (oder eine Kombination aus TDMA und FDMA) eingesetzt. Die technische Umsetzung eines Vielfachzugriffsverfahrens wird auch als Antikollisionsverfahren bezeichnet und lässt sich in zwei Klassen unterteilen [SWE02]: deterministische und probabilistische Verfahren.

Bei den *deterministischen Verfahren* sucht das Lesegerät alle RFID-Transponder im Lesebereich anhand der eindeutigen Seriennummer der RFID-Transponder ab. Das am häufigsten eingesetzte Verfahren ist der Baumtraversierungsalgorithmus, bei dem der Binärbaum aller möglichen dual kodierten Seriennummern in systematischer Weise durchlaufen wird. Bei jedem Anfrageschritt werden alle RFID-Transponder, deren Seriennummer in einem bestimmten Intervall liegen, aufgefordert, mit ihrer Seriennummer zu antworten. Kommt es zu einer Kollision, d.h. haben mehrere RFID-Transponder geantwortet, wird das Intervall halbiert. Dieser Schritt wird so lange wiederholt, bis nur noch ein einziger RFID-Transponder antwortet. Alle noch verbleibenden Intervalle werden dann auf dieselbe Art und Weise abgesucht. Deterministische Antikollisionsalgorith-

men stellen also sicher, dass nach einer gewissen Zeit alle im Bereich des Lesegeräts befindlichen RFID-Transponder erkannt werden. Allgemein kann gesagt werden, dass das Baumtraversierungsverfahren auf hohe Datenübertragungsraten vom Lesegerät zum RFID-Transponder angewiesen ist, um hohe Erkennungsraten zu ermöglichen. Existierende Zulassungsvorschriften ermöglichen dies momentan nur im UHF-Band.

Bei den *probabilistischen Verfahren* antworten die RFID-Transponder zu einem zufällig gewählten Zeitpunkt. Es wird dabei hauptsächlich eine Variante des ALOHA-Algorithmus angewandt, bei dem das Lesegerät den RFID-Transpondern ein Zeitfenster zum Antworten zur Verfügung stellt. Beim Framed-slotted-ALOHA-Algorithmus ist dieses Zeitfenster in eine vorgegebene Anzahl so genannter „Zeitslots“ unterteilt, aus denen jeder RFID-Transponder zufällig einen für seine Antwort auswählt. Zu einer Kollision kommt es, falls mehr als ein RFID-Transponder im selben Zeitslot antwortet. Dies kann von den RFID-Transpondern nicht verhindert werden, da sie nicht erkennen können, ob im selben Zeitslot ein anderer RFID-Transponder antwortet. Um nun bei mehreren Anfragerunden die Zahl der Kollisionen zu minimieren, können RFID-Transponder, die erfolgreich erkannt wurden, für die folgenden Runden stumm geschaltet werden. Bei der Wahl der Größe des Zeitfensters sollte die erwartete Anzahl RFID-Transponder mit in Betracht gezogen werden, da bei einem zu großen Zeitfenster viele Zeitslots ungenutzt bleiben [Vog02]. Ist das Zeitfenster jedoch zu klein gewählt, kommt es häufig zu Kollisionen und die Zahl der nötigen Anfragerunden, um alle RFID-Transponder zu erkennen, steigt stark an. Bei probabilistischen Antikollisionsalgorithmen ist generell nicht sichergestellt, dass nach einer gewissen Zeit alle im Bereich des Lesegeräts befindlichen RFID-Transponder erkannt werden.

4 Auswahlkriterien

Bei der Wahl eines geeigneten RFID-Systems für eine bestimmte Anwendung spielen die folgenden Kriterien eine wichtige Rolle: die Lesereichweite, die Datentransferrate, die Geschwindigkeit, mit der verschiedene RFID-Transponder im Ansprechbereich erkannt werden, die Störanfälligkeit für Rauschen und andere Fehlerquellen sowie die Kosten von RFID-Transpondern und Lesegeräten. Diese Auswahlkriterien hängen direkt von den grundlegenden, technischen Eigenschaften eines RFID-Systems, wie sie in Kapitel 3 beschrieben wurden, ab. Tabelle 1 fasst einige der Eigenschaften, gegliedert nach Frequenzbereichen, nochmals zusammen.

4.1 Lesereichweite

Die Lesereichweite ist eines der wichtigsten Auswahlkriterien für ein RFID-System. Betrachtet man die typische Lesereichweite, so werden RFID-Systeme in drei Klassen unterteilt: Systeme, die bis zu einer Reichweite von 1 cm arbeiten, werden als *Close-Coupling-Systeme* bezeichnet. Sie arbeiten mit induktiver Kopp-

lung und werden hauptsächlich in sicherheitsrelevanten Anwendungen wie Zugangskontrollsystemen oder Bezahlsystemen eingesetzt. *Remote-Coupling-Systeme* arbeiten ebenfalls mit induktiver Kopplung, aber im Entfernungsbereich von bis zu einem Meter. Die Sendefrequenz liegt je nach Anwendung typischerweise bei 135 kHz oder 13,56 MHz. Systeme mit einer Reichweite von über einem Meter werden als *Long-Range-Systeme* bezeichnet. Sie arbeiten typischerweise mit Sendefrequenzen von 868/915 MHz oder 2,5 GHz. Verschiedene Hersteller bezeichnen jedoch auch RFID-Systeme mit einer Reichweite von bis zu einem Meter als Long-Range-Systeme. Generell hängt die erzielbare Lesereichweite von sehr vielen Faktoren ab, unter anderem von:

- der Sendefrequenz des Lesegeräts,
- dem Energieverbrauch des integrierten Schaltkreises (Mikrochip) des RFID-Transponders,
- der Verbindung zwischen Mikrochip und Antenne des RFID-Transponders,
- der Größe, Form und Qualität der Antenne des RFID-Transponders,
- der Orientierung der Antenne des RFID-Transponders zum Lesegerät,
- dem Design der Antenne des Lesegeräts,
- der Empfindlichkeit des Lesegeräts,
- der Sendeleistung des Lesegeräts,
- den zur Anwendung kommenden Zulassungsbestimmungen des Einsatzlandes,
- den Umgebungsbedingungen (in Gebäuden bzw. im Freien) und
- der Anfälligkeit gegenüber anderen Funk-Signalquellen.

Tabelle 1. RFID-Eigenschaften

	LF 0–135 kHz	HF 3–30 MHz	UHF 200 MHz–2 GHz	MW > 2 GHz
Art der Kopplung	Induktive Kopplung (wirkt im Nahfeld)		Elektromagnetische Kopplung (wirkt im Fernfeld)	
Typische Frequenz	134,2 kHz	13,56 MHz	868 MHz (EU) 915 MHz (USA)	2,45 GHz 5,8 GHz
Typische Lesereichweite	< 1,5 m	< 1,0 m	Passive Transponder: < 3 m (EU bei 0,4 W) ca. 3–5 m (EU bei 2 W, geplant) ca. 5–7 m (USA bei 4 W)	
Negative Umgebungseinflüsse	• Abschirmung • leitfähige Materialien (z.B. Metall)		• Abschirmung • Absorption, Reflexion, Brechung	
Einflüsse der Transponder untereinander	Antennen-Verstimmung bei eng liegenden Transpondern		Verzerrung der Funkmuster aufgrund von Antennenkopplung	

Es ist daher schwierig, die Lesereichweite verschiedener RFID-Systeme zu vergleichen. Unter idealen Bedingungen, d.h. einer perfekten Ausrichtung von

RFID-Transponder und Antenne des Lesegeräts, einer Sichtverbindung zwischen RFID-Transponder und Lesegerät, Vorschriften für Sendeleistungen der USA, wenig Rauschen, keiner Absorption oder Reflexion durch Objekte in der Nähe und einem Durchmesser der Antenne des RFID-Transponders von ca. 15 cm, kann ein RFID-System, das im UHF-Band operiert, eine Lesereichweite von 5 bis 7 m erreichen. Unter realen Bedingungen ist diese Reichweite nur selten zu erzielen. Für semi-aktive RFID-Systeme liegt die Lesereichweite bei bis zu 15 m, bei aktiven Systemen bis zu 100 m. LF- und HF-Systeme haben eine typische Lesereichweite von 1–1,5 m. Verglichen mit UHF-Systemen sind sie allerdings weniger fehleranfällig gegenüber Umwelteinflüssen.

4.2 Datenübertragungs- und Erkennungsrate

Hohe Datenübertragungsraten sind wichtig, falls eine große Datenmenge vom Speicher des RFID-Transponders in kürzester Zeit gelesen werden soll. Für LF- und HF-Systeme (ISO-Standards 15 693 und 14 223) liegt die Datenübertragungsrate bei ca. 5 kbit/s. Allerdings erlauben neuartige RFID-Systeme im HF-Bereich, die dem ISO-Standard 18 000 Part 3 Mode 2 entsprechen, Datenraten von über 100 kbit/s. UHF-Systeme des ISO-Standards 18000 Part 6 Mode A erreichen ca. 50 kbit/s. Die Datenübertragungsrate beeinflusst unter anderem auch, wie viele RFID-Transponder pro Sekunde erkannt werden können. Die Erkennungsrate hängt zusätzlich noch von der Wahl des Antikollisionsalgorithmus, der Länge der Seriennummern auf den RFID-Transpondern und den Abfertigungszeiten der Nachrichten ab. Typische Erkennungsraten liegen bei 10–30 RFID-Transpondern pro Sekunde für LF- und HF-Systeme und bei 100–500 RFID-Transpondern pro Sekunde für UHF-Systeme.

4.3 Störungsanfälligkeit

Da es sich bei RFID-Transpondern um kostengünstige elektronische Elemente handelt und die passiven Systeme ohne eigene Energieversorgung arbeiten, sind sie relativ anfällig für verschiedene Störungen wie Übertragungsfehler, Kollisionen bei nichtdeterministischen Antikollisionsalgorithmen, ungünstige Ausrichtung und Verstimmung der Transponder-Antennen sowie Flüssigkeiten und Metall in der Umgebung.

Übertragungsfehler manifestieren sich als Bit-Fehler, die auftreten, falls Daten, wie die Seriennummer des RFID-Transponders, über einen Frequenzkanal übertragen werden, auf dem starkes Rauschen herrscht. Damit das Lesegerät Bit-Fehler in den Daten erkennen kann, übertragen RFID-Transponder zusätzlich zu den Daten eine Prüfsumme. Am häufigsten kommt dabei der Cyclic-Redundancy-Check (CRC) zum Einsatz. Die Wahrscheinlichkeit für Bit-Fehler ist in einer Umgebung mit starkem Rauschen offensichtlich größer als in rauschfreien Umgebungen. Im LF-Bereich wird normalerweise stärkeres Rauschen durch atypische Sender wie z.B. Schweißanlagen oder Motoren hervorgerufen. Im HF- und UHF-Bereich wird Rauschen hauptsächlich durch andere Datensender verursacht, die

auf dem gleichen Frequenzkanal wie das RFID-System übertragen. Im 2,45-GHz-Band sind dies z.B. Bluetooth- und WLAN-Systeme.

Manche RFID-Systeme verwenden nichtdeterministische Antikollisionsalgorithmen basierend auf dem ALOHA-Prinzip (siehe Kapitel 3.3). Da sich bei diesen Algorithmen die RFID-Transponder zufällig einen Zeitpunkt zum Senden aussuchen, kann es zu fortgesetzten Störungen durch Kollisionen kommen und das Lesegerät kann dann die RFID-Transponder, die zur selben Zeit gesendet haben, nicht erkennen. Bei RFID-Systemen, die einen deterministischen Antikollisionsalgorithmus einsetzen, treten solche Probleme nicht auf.

Bei induktiv gekoppelten RFID-Systemen hängt die induzierte Spannung im RFID-Transponder von der Ausrichtung der Fläche der Spule des RFID-Transponders zum Magnetfeld, das vom Lesegerät erzeugt wird, ab. Bei einer senkrechten Ausrichtung ist die Spannung maximal, bei einer parallelen Ausrichtung wird dagegen keine Spannung induziert und der RFID-Transponder ist daher vom Lesegerät nicht zu erkennen. Das bedeutet, dass es bei einer zufälligen Ausrichtung der RFID-Transponder vorkommen kann, dass bestimmte RFID-Transponder nicht erkannt werden. Dieses Problem lässt sich durch mehrere Leserantennen, die verschiedene räumliche Ausrichtungen haben, lösen. Auch bei elektromagnetisch gekoppelten Systemen tritt dieses Problem auf, jedoch hat es hier eine andere Ursache. Da die ausgesendete elektromagnetische Welle polarisiert ist, wird die Spannung im RFID-Transponder maximal, sobald die RFID-Transponderantenne auf die Polarisationsrichtung der Leseantenne ausgerichtet ist. Ist sie nicht ausgerichtet, wird nur eine geringere Spannung im RFID-Transponder erzeugt. Dies kann im Extremfall dazu führen, dass er nicht vom Lesegerät erkannt wird. Dieses Problem wird durch zirkulär polarisierte Antennen des Lesegeräts oder durch mehrere Antennen, die verschiedene räumliche Ausrichtungen haben, gelöst, wobei dies in einer reduzierten Reichweite resultiert.

Bei passiven induktiv gekoppelten RFID-Systemen befindet sich auf dem Schaltkreis des RFID-Transponders normalerweise ein Schwingkreis, um die induzierte Spannung zu verstärken und damit die Lesereichweite zu erhöhen (siehe Kapitel 3.2). Dadurch sind diese RFID-Transponder jedoch empfänglich für bestimmte Verstimmungseffekte. Der Schwingkreis ist in diesem Fall nicht mehr auf die Sendefrequenz des Lesegeräts gestimmt, was die Lesereichweite stark reduzieren kann. Solche Effekte werden unter anderem durch eng aufeinander liegende RFID-Transponder, oder auch durch Metall und dielektrische Medien in der Umgebung, hervorgerufen.

Metalle in der Umgebung haben auch noch einen anderen negativen Effekt auf induktiv gekoppelte RFID-Transponder: Sie stören den magnetischen Fluss und schwächen damit die Energiekopplung zwischen Lesegerät und RFID-Transponder, was eine weitere Verringerung der Lesereichweite zur Folge hat. Werden RFID-Transponder direkt auf eine Metalloberfläche aufgebracht, können sie meistens überhaupt nicht mehr gelesen werden. Unter bestimmten Bedingungen können metallische Objekte das Antennenfeld auch verzerren und damit die Lesereichweite in bestimmten Richtungen sogar erhöhen. Bei Anwendungen, die auf einen definierten Lesebereich vertrauen, kann es somit zu Erkennungen von RFID-Transpondern kommen, die sich eigentlich außerhalb des erwarteten Lesebereiches befinden.

Bei elektromagnetisch gekoppelten RFID-Systemen werden elektromagnetische Wellen, die vom Lesegerät ausgesandt werden, nicht nur von den RFID-Transpondern reflektiert, sondern auch von allen anderen Objekten in der Umgebung. Die reflektierten Wellen überlagern sich mit den vom Lesegerät ausgesandten Wellen und führen auf der einen Seite zu lokalen Dämpfungen bis hin zu Auslöschungen, auf der anderen Seite zu Verstärkungen. Die Reflexionen resultieren so in einem unberechenbaren Verhalten der elektromagnetischen Wellen und damit in einer unvorhersagbaren Lesereichweite. Diese Effekte sind insbesondere in Umgebungen mit großen, metallischen Objekten zu erwarten.

Bei Flüssigkeiten oder organischen Materialien in der Umgebung kann es ferner zu Absorptionen des magnetischen oder elektromagnetischen Feldes kommen. Während im LF-Bereich Absorption keine Rolle spielt und im HF-Bereich nur eine geringe, kommt es im UHF- und MW-Bereich jedoch zu starken Absorptionen der elektromagnetischen Wellen und damit zu einer bedeutenden Verringerung der Lesereichweite, wenn das Signal organische oder wasserhaltige Materialien durchdringen muss.

4.4 Speicherstruktur

RFID-Transponder kann man anhand ihrer Speicherstruktur und ihres Datenzugriffs grob in die folgenden drei Kategorien einteilen:

- RFID-Transponder, die nur eine Identifikationsnummer besitzen. Das Beschreiben kann bei der Herstellung in der Fabrik bzw. später vor der ersten Benutzung geschehen. Da der Datenspeicher für die Identifikationsnummer nur einmalig beschrieben und dann beliebig oft ausgelesen wird, handelt es sich um einen WORM-Speicher (write-once-read-many-times).
- RFID-Transponder mit einer Identifikationsnummer und einem zusätzlichen Datenspeicher, der beschrieben und gelesen werden kann. Üblicherweise ist die Reichweite für Schreibzugriffe geringer als für Lesezugriffe, da hierfür mehr Energie benötigt wird.
- RFID-Transponder mit einer komplexen Speicherstruktur und Sicherheitsmerkmalen. Üblicherweise ist der Datenspeicher solcher RFID-Transponder in verschiedene Bereiche unterteilt, für die der Zugriff durch Schlüssel oder Challenge-Response-Verfahren geregelt werden kann.

Je nach Anwendungsanforderungen genügen RFID-Transponder, die nur eine Identifikationsnummer besitzen. Diese Identifikationsnummer dient dann als Referenz auf weitere Daten in einer Datenbank oder einem Informationssystem. RFID-Transponder mit zusätzlichem Datenspeicher werden hauptsächlich dann eingesetzt, falls ein Zugriff auf eine Datenbank aus Zeit- oder Verbindungsgründen nicht möglich ist. In diesem Fall sind die Daten direkt im Speicher des RFID-Transponders abgelegt.

4.5 Transponderkosten

Die Gesamtkosten eines RFID-Transponders werden, neben den anteiligen Kosten für das Design des Mikrochips und weiterer Gemeinkosten, durch die folgenden Einzelkosten bestimmt:

- Herstellungskosten für den Mikrochip
- Herstellungskosten für die Spule bzw. Antenne des RFID-Transponders
- Kosten für das Zusammensetzen der Spule bzw. Antenne und des Mikrochips des RFID-Transponders
- Kosten für das Aufbringen des RFID-Transponders auf den Träger

Die Herstellungskosten für den Mikrochip des RFID-Transponders hängen von der Größe des Mikrochips, der Anzahl herzustellender Mikrochips und der Verarbeitungstechnologie ab. Da der Datenspeicher bei der Chipherstellung zu Buche schlägt, nehmen die Kosten mit steigender Komplexität der Speicherstruktur zu, insbesondere für Datenspeicher mit Sicherheitsmerkmalen. Da sich eine Spule mit wenigen Windungen drucktechnisch herstellen lässt, bei vielen Windungen aber gewickelt werden muss, sind die Herstellungskosten eines 135-kHz-RFID-Transponders, der eine höhere Windungszahl benötigt, höher als die eines 13,56-MHz-RFID-Transponders. Die Kosten für RFID-Transponder im Lowcost-Bereich (nur mit Seriennummer und einfacher Bauform) liegen derzeit bei ca. 20–50 Cent, für komplexere RFID-Transponder im Euro-Bereich. Der Preis, den ein Anwender für einen RFID-Transponder zu bezahlen hat, ist zusätzlich abhängig von der Anzahl der bestellten Transponder. Der für die nächsten Jahre erwartete verstärkte Einsatz der RFID-Technologie wird dazu führen, dass dank Massenproduktion die RFID-Transponderpreise weiter fallen werden.

5 Standards für die Schnittstelle zwischen RFID-Transpondern und Lesegeräten

Die verschiedenen Normen, die die Schnittstelle zwischen RFID-Transpondern und Lesegeräten spezifizieren, beschreiben die grundlegende Funktion eines RFID-Systems und sollen garantieren, dass RFID-Transponder und Lesegeräte verschiedener Hersteller miteinander kommunizieren können. Dabei definieren die Normen sowohl die physikalische Schicht mit Trägerfrequenz, Kodierung, Timing, Modulationsverfahren und Datenübertragungsraten als auch das Vielfachzugriffsverfahren und den Befehlsumfang. Die entsprechenden Standardisierungsbemühungen sind vor allem vom Joint Technical Committee 1 (JTC1) der International Standards Organisation (ISO) und der International Electrotechnical Commission (IEC), sowie in jüngster Zeit vom Auto-ID Center bzw. von der Nachfolgeorganisation EPCglobal unternommen worden.

Im HF-Frequenzband wurde Mitte 2001 vom ISO-Gremium ISO/IEC JTC SC17 („Contactless integrated circuit cards“) der ISO-Standard 15 693 veröffentlicht, der unter dem Titel „Identification cards – contactless integrated circuit(s) cards“ die Funktionsweise von kontaktlosen Chipkarten beschreibt (siehe Tabel-

le 2). Obwohl diese Norm eigentlich auf die Standardisierung von Chipkarten mit einer Reichweite bis zu einem Meter abzielt, die z.B. zur Zugangskontrolle verwendet werden können, bildet sie die Basis vieler Smart-Label-Produkte (siehe Abbildung 2), da die Funktionsweise identisch ist. Die Energieversorgung der induktiv gekoppelten RFID-Transponder erfolgt dabei durch ein magnetisches Wechselfeld, das vom Lesegerät mit einer Sendefrequenz von 13,56 MHz erzeugt wird. Bei den Datenübertragungsraten kann zwischen einem „long-distance-mode“ und einem „fast-mode“ unterschieden werden. Der „fast-mode“ kann vor allem bei Lesegeräten mit verminderter Reichweite oder mit zusätzlicher Abschirmung, wie z.B. Tunnellesern, zum Einsatz kommen.

Der Vorteil von RFID-Systemen, die auf dem ISO-Standard 15 693 basieren, liegt vor allem in der weltweiten Verfügbarkeit des Frequenzbandes. Allerdings erlaubt die im Verhältnis zum Trägersignal niedrige maximale Feldstärke der Modulationsseitenbänder nur eine relativ geringe Übertragungsrate zwischen Lesegerät und RFID-Transpondern (1,6 kbit/s bzw. 6,6 kbit/s im „long-distance-mode“) und eine eingeschränkte Reichweite (üblicherweise weniger als einen Meter). Die Reichweite eines RFID-Systems ist allerdings wie oben beschrieben von vielen Faktoren abhängig, sodass unter Umständen auch Reichweiten von über einem Meter möglich sind. Die geringe Datenübertragungsrate resultiert auch in einer relativ geringen Anzahl von RFID-Transpondern, die pro Zeiteinheit erkannt werden können (ca. 20 Transponder pro Sekunde).

Das für die Normung von Chipkarten verantwortliche ISO-Gremium SC17 hat im gleichen Jahr noch eine weitere Norm veröffentlicht (ISO 14 443), welche sich von ISO 15 693 vor allem durch eine höhere Datenübertragungsrate (106 kbit/s) und eine geringere Reichweite (weniger als 15 cm) unterscheidet. Wegen der relativ hohen Datenübertragungsrate werden RFID-Transponder dieser Norm vor allem bei Applikationen eingesetzt, wo größere Datenmengen zwischen Lesegerät und RFID-Transponder bzw. kontaktloser Chipkarte ausgetauscht werden müssen.

Neben dem hauptsächlich für die Normierung von Chipkarten zuständigen ISO-Gremium SC 17 ist für die weitere Normierung im RFID-Umfeld die Arbeitsgruppe 4 des ISO-Gremiums SC 31 verantwortlich. Dort werden zurzeit für die verschiedenen Frequenzbereiche LF, HF, UHF und MW weitere Normen für die Luftschnittstelle erstellt (siehe Tabelle 2). Dabei ist zu beachten, dass eine einzige Norm, wie z.B. ISO 18 000 Part 3, aus mehreren miteinander nichtkompatiblen RFID-Protokollen, in diesem Fall Mode 1 und Mode 2, bestehen kann, die außer der Sendefrequenz wenig gemeinsam haben.

ISO 18 000 Part 3 Mode 1 ist mit der zuvor vorgestellten Norm ISO 15 693 kompatibel. Mode 2 erlaubt durch ein anderes Modulationsverfahren und ein Vielfachzugriffsverfahren, bei dem die RFID-Transponder auf bis zu acht verschiedenen Frequenzkanälen antworten, eine deutlich höhere Datenübertragungsrate. Dieser „High-Performance-Mode“ ist daher besonders geeignet für Anwendungen, bei denen in kurzer Zeit eine große Anzahl von RFID-Transpondern erkannt bzw. ausgelesen werden muss.

Obwohl beim Auto-ID Center bzw. der Nachfolgeorganisation EPCglobal der Fokus auf der Entwicklung von Standards für das UHF-Frequenzband liegt, gibt es dort ebenfalls eine Norm im HF-Bereich. Die Class-1-HF-Norm unterscheidet sich – zumindest auf der physikalischen Schicht – allerdings nur geringfügig von ISO 15 693 bzw. ISO 18 000 Part 3 Mode 1.

Tabelle 2. Übersicht über die verschiedenen Normen, die die Schnittstelle zwischen RFID-Transpondern und Lesegeräten spezifizieren

Frequenz	Gremium	Bezeichnung	Name	Veröffentlichung
LF	ISO	11 785	Radio-Frequency Identification of Animals – Technical Concepts	1996
LF	ISO	14 233	Radio-Frequency Identification of Animals – Advanced Transponders	2003
LF	ISO	18 000 Part 2 Type A/B	Parameters for Air Interface Communications below 135 kHz	2004
HF	ISO	15 693	Identification Cards – Vicinity Cards	2001
HF	ISO	14 443 Type A/B	Identification Cards – Proximity Cards	2001
HF	ISO	18 000 Part 3 Mode 1/2	Parameters for Air Interface Communications at 13.56 MHz	2004
HF	EPCglobal	Class 1	13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification	2003
UHF	ISO	18 000 Part 6 Mode A/B	Parameters for Air Interface Communications at 860 to 930 MHz	2004
UHF	EPCglobal	Class 0 (Gen. 1)	860 MHz–935 MHz Class 0 Radio Frequency Identification Tag Protocol Specification	2003
UHF	EPCglobal	Class 1 (Gen. 1)	860 MHz–960 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification	2002
UHF	EPCglobal	Class 1 (Gen. 2)	UHF Class 1 Generation 2 Protocol	2004
MW	ISO	18 000 Part 4	Parameters for Air Interface Communications at 2.45 GHz	2004

Im UHF-Bereich gibt es eine ganze Reihe verschiedener Normen (siehe Tabelle 2), die nicht miteinander kompatibel sind. EPCglobal plant allerdings langfristig die beiden Protokolle erster Generation durch das Protokoll der zweiten Generation abzulösen [EPC04]. Außerdem wird vonseiten EPCglobals darüber nachgedacht, das UHF-Class-1-Protokoll der zweiten Generation als weiteren Mode in die ISO-Norm 18 000 Part 6 einzubringen [EPC04].

Die verschiedenen UHF-Protokolle unterscheiden sich in der physikalischen Schicht, im verwendeten Vielfachzugriffsverfahren sowie im Befehlsumfang, der unterstützt wird. Ein direkter Leistungsvergleich hinsichtlich Reichweite und Störungsempfindlichkeit, aber auch Kosten von RFID-Transpondern und Lesegeräten, ist nur schwer möglich, da diese Eigenschaften auch von standardunabhängigen Faktoren, wie z.B. der Leistungsaufnahme des Mikrochips, den verwendeten Fertigungsprozessen, bzw. vom Antennen- und Lesegerätdesign beeinflusst werden.

Neben den Standardisierungsbemühungen im HF- und UHF-Bereich gibt es unter ISO 18 000 auch Normen für den LF- und MW-Frequenzbereich (siehe

Tabelle 2). Der LF-Teil entspricht dabei im Wesentlichen der früheren Norm ISO 11 785 und deren Weiterentwicklung ISO 14 233.

Bei der Datenorganisation auf den RFID-Transpondern kann man grundsätzlich zwischen zwei verschiedenen Ansätzen unterscheiden. In sämtlichen Teilen der ISO-Norm 18 000 wird der einzelne RFID-Transponder durch eine eindeutige Identifikationsnummer gekennzeichnet, die bereits während des Herstellungsprozesses auf den Mikrochip des RFID-Transponders geschrieben wird. Informationen über das mit dem RFID-Transponder gekennzeichnete Produkt können vom Anwender im Speicher des RFID-Transponders abgelegt werden, wobei die Größe des Speichers variabel ist und lediglich ein Maximalwert spezifiziert ist (z.B. 8 kB für ISO 18 000 Part 6 Mode A). Die RFID-Transponder, die einer der Spezifikationen des Auto-ID Centers bzw. der Nachfolgeorganisation EPCglobal entsprechen, enthalten lediglich eine eindeutige Identifikationsnummer, den „Electronic Product Code“ (EPC), jedoch keinen zusätzlichen Speicher. Im EPC selbst sind Informationen zu dem Produkt, an dem der RFID-Transponder befestigt ist, kodiert, wie z.B. Herstellercode, Produkttyp und Seriennummer [EPC03].

Darüber hinaus gibt es neben den Normen für die Luftschnittstelle auch solche, die die Kommunikation zwischen Lesegerät und IT-Infrastruktur betreffen. 2003 wurde unter der Bezeichnung ISO 19 789 damit begonnen, ein solches „Application Program Interface“ zu entwickeln. Basierend auf der amerikanischen Norm ANSI NCITS 256:2001 wurde hierzu ein bereits bestehender, vollständiger Vorschlag eingereicht [Wal04]. Im Rahmen von EPCglobal wird zurzeit ebenfalls an einem „Reader Protocol“ gearbeitet, das den standardisierten Zugriff auf die Lesegeräte erlauben soll.

Literatur

[EPC03] EPCglobal (2003) EPC Tag Data Standards 1.1 Rev.1.24. www.epcglobalinc.org/ standards_technology/EPCTagDataSpecification11rev124.pdf

[EPC04] EPCglobal (2004) Review of Hardware Action Group's UHF Generation 2 Protocol Working Group Activities

[ERC02] European Radiocommunications Committee (2002) ERC recommendation 70-03 relating to the use of short range devices, www.ero.dk/documentation/docs/docfiles.asp?docid=1622

[FCC01] Federal Communications Commission (2001) Part 15 – Radio Frequency Devices. Code of Federal Regulations, Title 47, Vol 1, Chapter 1: 667ff, www.ero.dk/documentation/docs/docfiles.asp?docid=1622

[Fin02] Finkenzeller K (2002) RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3., aktualisierte und erweiterte Auflage. Carl Hanser Verlag

[Rfi03] RFID Journal (2003) Japan Opens Up UHF for RFID Use. June 30, 2003, www.rfidjournal.com/article/view/477

[RTP00a] Regulierungsbehörde für Telekommunikation und Post (RegTP) (2000) Verfügungen 61/2000: Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für induktive Funkanlagen des nichtöffentlichen mobilen Landfunks, Amtsblatt 12

[RTP00b] Regulierungsbehörde für Telekommunikation und Post (RegTP) (2000) Verfügungen 73/2000: Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für Funkanlagen geringer Leistung des nichtöffentlichen mobilen Landfunks in ISM-Frequenzbereichen, Amtsblatt 18

[SWE02] Sarma SE, Weis SA, Engels DW (2002) RFID Systems and Security and Privacy Implications. In: Cryptographic Hardware and Embedded Systems, Springer-Verlag, Lecture Notes in Computer Science, 2523: 454-469

[Vog02] Vogt H (2002) Multiple Object Identification with Passive RFID Tags. IEEE International Conference on Systems, Man and Cybernetics

[Wal04] Walk E (2004) Aktuelle Situation der RFID Standards für die Logistik. Jahrbuch ident 2004, ident Verlag und Service

EPC-Technologie – vom Auto-ID Center zu EPCglobal

Christian Flörkemeier
Institut für Pervasive Computing, ETH Zürich

Kurzfassung. Seit seiner Gründung im Jahr 1999 hat das Auto-ID Center die Vision verfolgt, ein auf der RFID-Transpondertechnik basierendes „Internet der Dinge“ zu realisieren. Dabei wurde in enger Kooperation mit den Industriepartnern des Auto-ID Centers nicht nur das Potenzial der Transpondertechnik für betriebswirtschaftliche Prozesse erforscht, sondern auch an den entsprechenden Normen für Transponder, Lesegeräte und die unterstützende Infrastruktur gearbeitet. Diese Aufgabe wird seit Ende 2003 von der Nachfolgeorganisation EPCglobal fortgeführt, die sich vor allem mit der Kommerzialisierung der EPC[18]-Technologie beschäftigt. In diesem Beitrag wird ein Überblick über die Technologiestandards und deren Status gegeben, ferner werden die einzelnen Komponenten der Auto-ID-Center-Infrastruktur vorgestellt. Anschließend werden die Vorschläge des Auto-ID Centers mit anderen existierenden Ansätzen verglichen.

1 Das Auto-ID Center und EPCglobal

Das Auto-ID Center wurde 1999 am Massachusetts Institute of Technology (MIT) mit der Absicht gegründet, die Vision des „Internets der Dinge“ weiterzuentwickeln und zu implementieren [Aut02a]. Dabei sollte die RFID-Technologie als Grundlage dienen, um Alltagsgegenstände eindeutig zu identifizieren und somit IT-Systeme in die Lage zu versetzen, ohne menschliches Zutun mit der realen Welt zu interagieren. Jeder produzierte Gegenstand sollte dabei mit einem preiswerten RFID-Transponder versehen sein, damit „sich sein Aufenthaltsort mithilfe einer globalen Infrastruktur über Unternehmens- und Ländergrenzen hinweg bestimmen lässt“ [Aut02a]. Durch ein derartiges globales „EPC Network“ zur automatischen Identifikation – benannt nach dem elektronischen Produktcode (EPC), der auf den Transpondern gespeichert ist – erhofft man sich insbesondere Verbesserungen der betrieblichen Prozesse in der Fertigung [CGS02], der Lieferkette [AGG02] und der Warenbewirtschaftung [CDG02].

In der Entwicklung der entsprechenden Standards für Transponder, Lesegeräte und das zugehörige Informationssystem wurden die beteiligten Universitäten, u.a. das MIT, die Universität Cambridge und die Universität St. Gallen, von über 100 industriellen Partnern unterstützt. Die mehrheitlich aus dem Handel und der Kon-

[18] EPC ist ein geschütztes Markenzeichen von EPCglobal

sumgüterindustrie stammenden „End-User-Sponsoren“, wie Coca-Cola, Gillette, Proctor&Gamble und Wal-Mart, legten dabei die Anforderungen an die Technologie fest, während die beteiligten Technologieunternehmen in Zusammenarbeit mit den Universitäten die verschiedenen Technologiekomponenten und Standards entwickelten und diese als Produkte realisierten.

Ende Oktober 2003 hat das Auto-ID Center seine Forschungsarbeit planungsgemäß beendet [CaB02]. Die Kommerzialisierung und weitere Entwicklung der Normen und Standards wird von einem Joint Venture des Uniform Code Council (UCC) und EAN International – zwei der ersten Sponsoren des Centers, die u.a. auch die internationalen Standards für Barcodes festlegen – weiterverfolgt. Diese Nachfolgeorganisation agiert unter dem Namen *EPCglobal* und hat Mitte 2003 seine Arbeit aufgenommen [EPC03a]. Die am Auto-ID Center beteiligten Universitäten setzen als Auto-ID-Labs ihre RFID-Forschungsaktivitäten weiter fort.

Im folgenden Kapitel wird zunächst ein Überblick über die verschiedenen Systemkomponenten, die im Rahmen des Auto-ID Centers entwickelt wurden bzw. zurzeit von EPCglobal entwickelt werden, gegeben. Daraufhin wird auf jede einzelne Systemkomponente des EPC Network im Detail eingegangen. Anschließend werden die Arbeiten des Auto-ID Centers mit existierenden und teilweise konkurrierenden Ansätzen verglichen. Am Ende liefert dieser Beitrag einen Ausblick auf die Herausforderungen, die für eine erfolgreiche Realisierung der Vision, mit der das Auto-ID Center 1999 gegründet wurde, noch gemeistert werden müssen.

2 Übersicht über das „EPC Network“

Das Herzstück der Auto-ID-Center-Technologie ist der *Electronic Product Code* (EPC). Im Unterschied zu den Ziffernfolgen auf Barcodes, die auf Verpackungen im Einzelhandel zu finden sind, enthält der EPC neben einer Hersteller- und Produktnummer auch eine Seriennummer, mit der die Artikel einzeln und individuell nummeriert werden können. Dieser EPC wird auf den RFID-Transpondern gespeichert und erlaubt die eindeutige Identifikation einzelner Transponder und der damit assoziierten Gegenstände.

Das Ziel des Auto-ID Centers war es, nicht nur das Datenformat auf den Transpondern und die Kommunikation zwischen den Transpondern und Lesegeräten zu standardisieren, sondern auch den Transport der RFID-Daten zu den entsprechenden Applikationen und das Auffinden von Informationen zu den identifizierten Gegenständen zu standardisieren [SBA01] (siehe Abbildung 1). In einer Welt, in der jeder Artikel durch einen Transponder gekennzeichnet wäre, würden Lesegeräte große Datenmengen aufzeichnen. Um diese Daten zu bearbeiten und an die entsprechenden Anwendungen zu übermitteln, wurde eine Software namens *Savant* entwickelt. Diese RFID-Middleware sollte sowohl die Vielzahl unterschiedlicher Lesegeräte steuern als auch Anwendungen, wie z.B. Warenwirtschaftssysteme, mit entsprechend aufbereiteten Daten versorgen. Da auf den Transpondern selbst keine über die Identifikationsnummer hinausgehenden Daten gespeichert werden, gibt es einen *Object Naming Service (ONS)*, der unter Angabe des EPC an die entsprechenden Datenquellen weiterleitet. Diese Datenquellen sollen dabei u.a. vom *EPC Information System (EPC IS)* angeboten werden. Da-

mit die von Transpondern und Lesegeräten gesammelten Daten in einem einheitlichen Format externen Anwendungen und anderen Komponenten des EPC Networks zur Verfügung gestellt werden können, ist unter dem Begriff *Physical Markup Language (PML)* ein XML-basiertes Vokabular definiert worden.

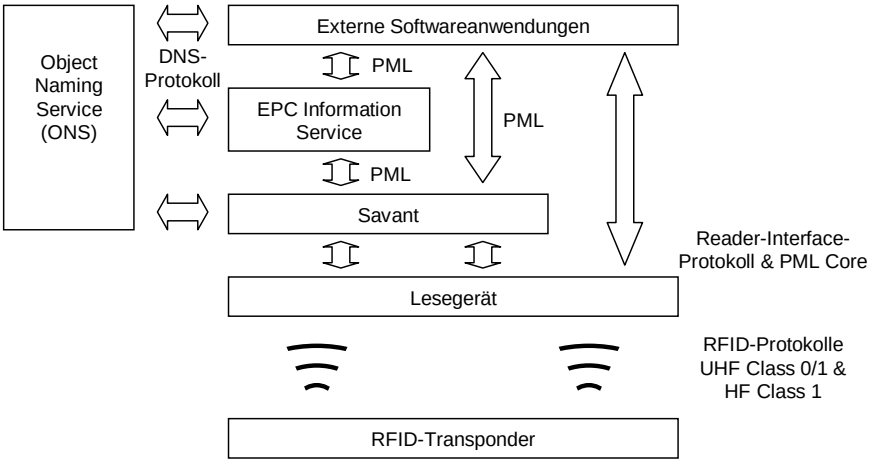


Abb. 1. Vom Auto-ID Center konzipiertes EPC Network mit den einzelnen Systemkomponenten

Das EPC Network umfasste ursprünglich Transponder, den Identifikationscode, der auf diesen gespeichert ist, Lesegeräte und Infrastrukturkomponenten, wie den Lookup-Service ONS, die RFID-Datenübermittlungssoftware Savant, das Datenarchiv EPC IS und die Auszeichnungssprache PML. In den folgenden Kapiteln werden diese einzeln erläutert. Mit dem Übergang zu EPCglobal hat sich die Architektur des EPC Network jedoch verändert, sodass nicht nur die ursprünglich vom Auto-ID Center konzipierten Technologien vorgestellt werden, sondern auch Veränderungen seit der Übergabe an EPCglobal.

3 Der Electronic Product Code (EPC)

Der Electronic Product Code (EPC) ist die Ziffernfolge, die in der Auto-ID-Infrastruktur, dem so genannten EPC Network, die Basis dafür liefert, dass die einzelnen Objekte eindeutig identifiziert werden können. Da die Transponder keinerlei Daten außer dem EPC tragen, fungiert der Code damit auch als Referenz auf weitere Datensätze, die auf anderen Speichermedien zur Verfügung stehen. Ursprünglich war der EPC als universeller Identifizierungscode konzipiert, der gleichermaßen für verschiedene Industriebranchen und Anwendungsgebiete gelten sollte [Bro01a]. Es sollte sowohl auf die Integration von Attributen des Gegenstandes, wie Gewicht oder Preis, als auch auf die direkte Anpassung an exis-

tierende Nummernformate, wie beispielsweise die EAN-Nummer, verzichtet werden.

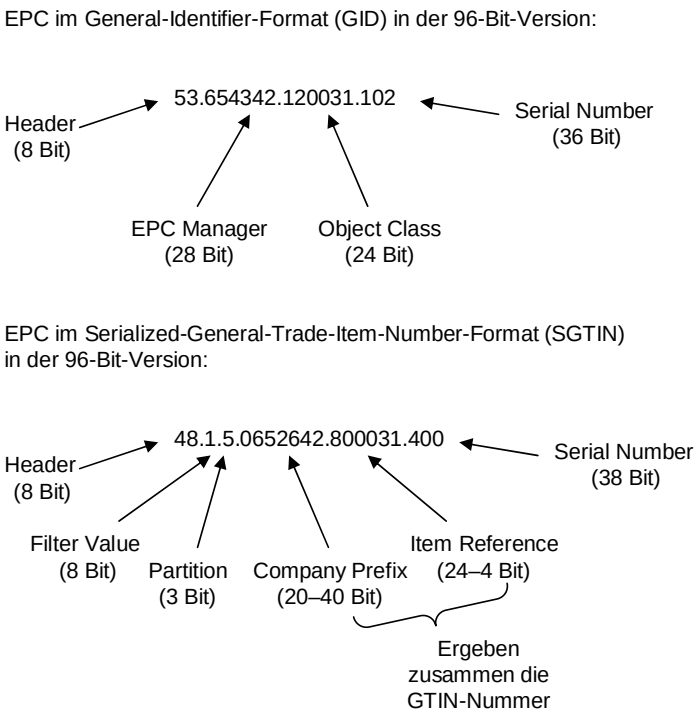


Abb. 2. Vergleich des universellen EPC-Formats (GID) mit dem EPC-Format für die General Trade Item Numbers (GTIN)

Da ein Nummernformat ohne jegliche Partitionierung bei dem großen Adressraum von mindestens 64 Bit allerdings zu Skalierungsproblemen führt, haben sich die Entwickler für eine Unterteilung in *Header*, *EPC Manager*, *Object Class* und *Serial Number* entschieden. Der *Header* definiert dabei das EPC-Format, während das *EPC Manager*-Feld dazu verwendet wird, das Unternehmen bzw. die Organisation zu identifizieren, die die Nummern der folgenden Felder verwaltet. Das *Object Class*-Feld enthält eine Nummer, die einen Typ von Objekten dieses EPC Managers eindeutig identifiziert, und die *Seriennummer* wird zur eindeutigen Identifikation eines einzelnen Objektes dieses Objekttyps benutzt. Während die ersten Transponder nur einen 64 Bit langen EPC unterstützten, sind heute 96 Bit standardmäßig vorgesehen. Der *Header* ist allerdings so konzipiert, dass der Adressraum zu einem späteren Zeitpunkt erweitert werden kann. Brock liefert in [Bro01a] eine gute Übersicht zu den weiteren Überlegungen, die zu diesem Format geführt haben.

Das Konzept eines universell einsetzbaren EPC wurde unter dem Druck der End-User-Sponsoren durch domänenspezifische EPC-Formate [EPC03b] ergänzt, da die beteiligten Unternehmen die Kompatibilität mit ihren existierenden Daten-

schemata gewährleistet sehen wollten. Die im Handel und der Konsumgüterindustrie weit verbreiteten Nummernformate des Uniform Code Council und der EAN International, d.h. der Universal Product Code (UPC), die European Article Number (EAN) [UCC03], der Serialized Shipping Container Code (SSCC) [UCC02a] und die Global Location Number (GLN) [UCC02b], sollten so weit wie möglich direkt im EPC Verwendung finden. Abbildung 2 zeigt das ursprüngliche EPC-Format (General Identifier GID-96) und das EPC-Format SGTIN-96, das speziell für die General Trade Item Number (GTIN) – den UPC-Code und die EAN-Nummer – entwickelt wurde. Da der UPC und die EAN-Nummer über keine Produktseriennummer verfügen, wurden die in diesen Codes typischen Felder für den Herstellercode und den Produkttyp in diesen EPC-Typ übernommen und durch eine Produktseriennummer ergänzt. Weiterhin kann man bereits durch ein Feld für den Objekttyp erkennen, ob es sich um eine Palette, eine Kiste oder einen Einzelartikel handelt. Dieser „Filter Value“ ermöglicht beispielsweise, dass Lesegeräte lediglich Paletten, aber keine Einzelartikel erfassen. Der EPC-Typ für die Nummern des EAN-UCC-Systems umfasst zusätzlich noch EPC-Formate für SSCC und GLN. In Zukunft sollen auch für andere Branchen, wie z.B. die Automobilindustrie und das Militär, domänenspezifische Typen des EPC folgen [EPC03b].

4 Transponder

Die Kosten eines RFID-Transponders ergeben sich nach Sarma aus den Herstellungskosten für den Mikrochip und die Antenne sowie den Kosten für die Platzierung des Mikrochips auf der Antenne [Sar01]. Um die Kosten des Mikrochips möglichst gering zu halten und somit den Einsatz von Transpondern zu fördern, propagiert das Auto-ID Center ein Transponderdesign, das lediglich Speicherplatz für eine 96 Bit lange Identifikationsnummer – den EPC – vorsieht und keinerlei weiteren Speicher enthält. Dies soll die Größe und dementsprechend die Kosten des Chips niedrig halten [Sar01]. Außerdem wird der Einsatz von neuen Fertigungsmethoden, wie Fluid Self Assembly [ATC99] und Vibratory Assembly, [KhS03] untersucht, um die Kosten des Zusammenfügens von Chip und Antenne zu reduzieren.

Am Auto-ID Center bzw. bei EPCglobal wird der Einsatz der Transpondertechnologie in der Lieferkette als das Anwendungsgebiet mit dem größten Potenzial angesehen. Die dafür notwendigen Lesedistanzen von mehr als einem Meter lassen sich meist nur mit passiven RFID-Transpondern realisieren, die im UHF-Frequenzbereich operieren. In den USA erlauben die dortigen Grenzwerte der Sendeleistung im UHF-Bereich typischerweise eine Lesedistanz von bis zu 7 m. Da dieses Frequenzband allerdings bisher weltweit nicht für den RFID-Einsatz mit entsprechender Leistung und Bandbreite zugelassen ist [Fin02], wurde am Auto-ID Center ein Kommunikationsprotokoll für den HF-Frequenzbereich entwickelt, das zwar weltweit eingesetzt werden kann, allerdings bei derzeitiger Technologie eine deutlich geringere Reichweite aufweist (typischerweise unter 1 m). Die bisher vom Auto-ID Center/EPCglobal veröffentlichten Normen zur

Standardisierung der Kommunikation zwischen Transpondern und Lesegeräten sind in folgenden Spezifikationen definiert:

- UHF Class 0 [Aut03a]
- UHF Class 1 [Aut02b]
- UHF Class 1 Generation 2 [EPC04a]
- HF Class 1 [Aut03b]

Die UHF-Protokolle der Class 0 and Class 1 sind so genannte Reader-talks-first-Protokolle, die im Fernfeld des Lesegerätes operieren und über Modulation des Rückstreuquerschnittes der Transponderantenne mit dem Lesegerät kommunizieren (zur Erklärung der technischen Begriffe sei der Leser auf den Beitrag von Lampe et al. in diesem Buch verwiesen). Die Kommunikation zwischen Lesegerät und Transponder geschieht im Halbduplex-Modus. Als Vielfachzugriffsverfahren kommt bei beiden Protokollen eine Variante des Baumtraversierungsverfahrens [SLL00] zum Einsatz. Neben verschiedenen Signalkodierungen und Modulationsverfahren unterscheiden sich die beiden Protokolle vor allem dadurch, dass die Transponder der Class 1 vor Ort mit dem EPC einmalig beschrieben werden können, während Transponder der Class 0 schon beim Transponderhersteller mit dem entsprechenden EPC programmiert werden müssen. Beide Protokolle unterstützen keine Transponder mit Schreibfunktion, sondern lediglich das Auslesen des EPC.

Das Ende 2004 verabschiedete UHF-Protokoll Class 1 Generation 2 soll in Zukunft die beiden oben genannten UHF-Protokolle in einem gemeinsamen Protokoll vereinigen und insbesondere auf die Eigenheiten der europäischen und asiatischen Richtlinien eingehen.

Das HF Class 1 Protokoll [Aut03b] ist ebenfalls ein Reader-talks-first-Protokoll, wobei hier die Transponder über induktive Kopplung mit Energie versorgt werden und über Lastmodulation mit dem Lesegerät kommunizieren. Anstelle des Baumtraversierungsverfahrens kommt hier eine Variante des ALOHA-Verfahrens [Fin02] zum Einsatz. Aufgrund des HF-Frequenzbandes sind die typischen Lesedistanzen allerdings deutlich geringer.

5 Lesegeräte

Das Auto-ID Center hat zusammen mit der Firma ThingMagic LLC ein Referenzdesign für ein Lesegerät entwickelt [RRP02]. Während viele der heute erhältlichen Lesegeräte nur für ein einzelnes Frequenzband ausgelegt sind, sollten die Auto-ID-Center-Lesegeräte sowohl die Auto-ID-Center-Protokolle im HF- als auch im UHF-Bereich unterstützen. Dabei wurde nicht nur auf Flexibilität bezüglich der zu unterstützenden Frequenzbänder, sondern auch auf die Anpassungsfähigkeit an die Eigenheiten der verschiedenen Protokolle geachtet. Außerdem sollte eine TCP/IP-Schnittstelle für die Kommunikation zwischen Lesegerät und Host zur Verfügung stehen, sodass die bekannten Internetprotokolle für den Datenaustausch mit den Lesegeräten verwendet werden können. Dieser Ansatz eines frei verfügbaren Referenzdesigns mit HF- und UHF-Unterstützung wurde schlussendlich aber verworfen. Man konzentrierte sich stattdessen auf die Schnittstelle zwi-

schen Lesegeräten und IT-Systemen. Um die Kommunikation zwischen Lesegerät und Host zu standardisieren, wurde daher an der Entwicklung eines Reader-Interface-Protokolls gearbeitet [EPC05]. Dieses Protokoll spezifiziert die Konfigurationsparameter des Lesegerätes und die Datenübermittlung von erkannten EPCs an den Host.

6 Object Naming Service

Um ein Adressschema, wie den EPC, sinnvoll zu nutzen, ist ein Lookup-Mechanismus notwendig, der es erlaubt, Datenquellen, die weitere Informationen zu dieser Identifikationsnummer speichern, aufzufinden. Im EPC Network wird diese Lookup-Funktion vom Object Naming Service (ONS) bereitgestellt [Mea03]. Unter Angabe eines EPC liefert der ONS eine einzelne bzw. mehrere Internetadressen (URLs) zurück. Diese Internetadressen können dabei auf einen EPC Information Service verweisen. Sie erlauben allerdings auch die Verknüpfung mit anderen Datenquellen, wie z.B. einfachen Web-Seiten im HTML-Format. Der ONS basiert dabei auf dem Domain Name Service (DNS), der bereits zu einer der Basistechnologien des Internets gehört. Daher müssen bei Anfragen an den ONS die EPCs auch erst in gültige Domänennamen umgewandelt werden, bevor sie als DNS-Anfragen weitergeleitet werden können. Die Antwort des DNS ist dann dementsprechend ein gültiger DNS Resource Record. Ein typischer Anfrageablauf könnte folgendermaßen aussehen [Mea03]:

1. Eine Bitfolge, die einen EPC beinhaltet, wird vom Transponder an das Lesegerät übertragen.
2. Das Lesegerät sendet diese Bitfolge an einen lokalen Server, der sie in das EPC-URI-Format umwandelt und zum lokalen ONS Resolver schickt.
3. Der Resolver übersetzt die URI in einen DNS-Namen, schickt eine DNS-Anfrage ab und erhält einen DNS Resource Record als Antwort, in dem die zugehörigen Internetadressen enthalten sind.

Die Version 1.0 der ONS-Spezifikation [Mea03] erlaubt keine Anfragen für einzelne EPCs, sondern nur für um die Seriennummer verkürzte EPCs. Anfragen zu Informationen für einen einzelnen EPC sollen von den jeweiligen Applikationsservern aufgelöst werden, die nach Angabe des um die Seriennummer verkürzten EPC vom ONS-System aufgelistet werden. Eine Anfrage, die auch die Seriennummer beinhaltet, soll in zukünftigen Versionen der Spezifikation ermöglicht werden, sobald die Architektur- und Skalierungsfragen, die sich aus der erheblichen Größe des Adressraumes ergeben, geklärt sind. Das ONS-System wird im Auftrag von EPCglobal zurzeit von der Firma Verisign betrieben [EPC04b].

Abschließend wäre noch zu betonen, dass es sich bei dem ONS-System um einen reinen Lookup-Service handelt, dessen Aufgabe darin besteht, die Internetadresse einer Datenquelle anzugeben. Die Funktion eines globalen Track&Trace-Systems beispielsweise, das die Positionsbestimmung über Länder- und Unternehmensgrenzen hinweg möglich machen würde, kann das ONS-System daher nicht selbst erfüllen.

7 Savant

Die Savant-Software war ursprünglich die eigentliche Middlewarekomponente des EPC Networks, deren Hauptaufgabe es sein sollte, die Datenströme von den Lesegeräten und möglichen weiteren Sensoren zu verarbeiten und an die entsprechenden Anwendungen weiterzuleiten [CTA03]. Dabei sollte die Software insbesondere die von den Lesegeräten generierten Datenmengen filtern und bündeln, damit die gefilterten Daten dann den entsprechenden Unternehmenssoftwaresystemen zur Verfügung gestellt werden können, ohne diese mit den großen Datenmengen zu überlasten.

Ursprünglich sollte die Savant-Software als Open-Source-Software zur Verfügung gestellt werden. Diese Pläne wurden jedoch nicht weiterverfolgt. Vielmehr hat man sich dazu entschlossen, keine Referenzimplementation oder Softwarespezifikation zu liefern, sondern lediglich die Schnittstelle zwischen RFID-Middleware und Anwendungssoftware zu normieren [TBO04]. Wie entsprechende RFID-Middleware die einzelnen Funktionen, wie z.B. das Filtern der EPC-Daten, implementiert, bleibt dadurch den jeweiligen Software-Anbietern überlassen. Diese Schnittstelle zwischen RFID-Middleware und Applikation wird von EPCglobal als Application-Level-Events-Spezifikation (ALE) bezeichnet [TBO04]. Diese enthält Funktionalität, die das einfache Filtern und Bündeln der aggregierten Daten unterstützt. So können beispielsweise Filter spezifiziert werden, die nur EPCs mit bestimmten Bitmustern weiterleiten. Außerdem sind Filter angedacht, die die mehrfache Erkennung eines Transponders in einem kurzen Zeitraum zu einem einzigen Eingangsereignis bündeln. Durch eine Verknüpfung solcher Filter sollten die Daten, die von den verschiedenen angeschlossenen Lesegeräten geliefert werden, aufbereitet und in die entsprechenden Ereignisse für die Anwendung umgewandelt werden. So könnte beispielsweise eine Vielzahl von Transpondererkennungen an einem Lesegerät in ein einziges Wareneingangsereignis für eine Lieferung zusammengefasst werden.

8 Physical Markup Language (PML)

Die Physical Markup Language (PML) wurde ursprünglich konzipiert, um physische Objekte, die mit EPC-Transpondern gekennzeichnet sind, zu beschreiben [Bro01b]. Ähnlich der HTML-Sprache des World Wide Webs, die das Layout von Web-Seiten standardisiert, sollte hier eine Beschreibungssprache entwickelt werden, die allgemein gültige Attribute von Objekten, Prozessen und Umgebungen beinhaltet, wie z.B. Informationen zum Besitzer oder Aufenthaltsort eines Objektes. Da sich die Entwicklung einer anwendungsunabhängigen Beschreibungssprache, die aber trotzdem den Anforderungen verschiedener Anwendungsgebiete gerecht wird, als schwierig herausstellte, wurde zunächst unter dem Namen PML Core ein Vokabular entwickelt, das den Austausch von Daten, die von den Lesegeräten und eventuell von anderen Sensoren im EPC Network geliefert werden, standardisiert [FAH03]. Durch PML Core soll ein standardisierter Datenaustausch zwischen den einzelnen Komponenten des EPC Networks gewährleistet sein,

wobei der Fokus auf Sensordaten liegt, die unter anderem von RFID-Lesegeräten generiert werden. Diese XML-basierte Markup-Sprache ist dabei durch ein XML-Schema definiert [W3C01], sodass die syntaktische Korrektheit der übertragenen Daten automatisch mit den geeigneten XML-Tools überprüft werden kann. Das folgende Beispiel zeigt, wie die Tatsache, dass ein Lesegerät zwei RFID-Transponder erkannt hat, in PML Core repräsentiert wird:

```
<pmlcore: Sensor>
 <pmluid:ID>urn:epc:1:4.16.36</pmluid:ID>
 <pmlcore:Observation>
      <pmlcore:DateTime>2002-11-06T13:04:34-06:00</pmlcore:DateTime>
      <pmlcore:Tag>
           <pmluid:ID>urn:epc:1:2.24.400</pmluid:ID>
      </pmlcore:Tag>
      <pmlcore:Tag>
           <pmluid:ID>urn:epc:1:2.24.401</pmluid:ID>
      </pmlcore:Tag>
 </pmlcore:Observation>
</pmlcore:Sensor>
```

Die Weiterentwicklung der PML wurde nach dem Übergang zu EPCglobal eingestellt, wobei die PML-Core-Konzepte zum Teil im Reader-Interface-Protokoll weiterverfolgt wurden.

9 EPC Information Service

Der EPC Information Service, der ursprünglich unter dem Namen PML Service entwickelt wurde, soll verschiedene Daten zu den einzelnen mit Transpondern gekennzeichneten Objekten liefern [HaM03]. Bei den zur Verfügung gestellten Daten wird insbesondere an die Historie von Transpondererkennungen gedacht, da sie eine Objektrückverfolgung (Track&Trace) ermöglichen. Außerdem sollen instanzenbezogene Daten von allgemeinem Interesse, wie z.B. Herstellungsdatum und Mindesthaltbarkeit, verfügbar gemacht werden. Der EPC Information Service soll dabei nicht nur auf eigene Datenquellen zurückgreifen können, sondern auch Informationen aus anderen Datenquellen anbieten, die unternehmensweit zur Verfügung gestellt werden, wie z.B. Produktkataloge. Eine detaillierte Spezifikation des EPC Information Service liegt allerdings zurzeit noch nicht vor.

10 Diskussion

In diesem Kapitel werden die Technologiekonzepte des Auto-ID Centers diskutiert und mit ähnlichen Ansätzen verglichen. Dabei wird zwischen der Transpondertechnik und der diese unterstützende IT-Infrastruktur unterschieden.

10.1 Transpondertechnik

Im Umfeld der Transpondertechnik gibt es eine Vielzahl weiterer Standardisierungsbemühungen, die auf die Normung der Kommunikation zwischen Transponder und Lesegerät abzielen (siehe auch den Beitrag von Lampe et al. in diesem Buch). Insbesondere die verschiedenen ISO-Protokolle sind hierbei von Bedeutung. Während die ISO-Standards im Bereich von 13,56 MHz (z.B. ISO 15693) bereits heute verbreitet sind und durch entsprechende Produkte unterstützt werden, sind die Normen der ISO-18000-Familie teilweise noch in der Entwicklung. Eine weitere Initiative, GTAG, die auch vom Uniform Code Council und EAN International unterstützt wurde, ist ebenfalls zum Teil in den ISO-18000-Standard eingeflossen [Fin02].

Eines der Merkmale der EPC-Technologie ist der Verzicht auf jeglichen Datenspeicher außer der EPC-Identifikationsnummer auf den Transpondern, um damit die Transponderkosten zu reduzieren. Kritiker merken diesbezüglich an, dass die Kosten der Transponder vor allem durch das entsprechende Produktionsvolumen bestimmt werden. Der Verzicht auf größeren Speicher hat nachteilig zur Folge, dass eine Netzverbindung zu entsprechenden Datenquellen immer vor Ort beim Lesegerät vorhanden sein muss. Insbesondere im militärischen Bereich ist dies jedoch oft nicht der Fall.

Um auch solchen Anforderungen gerecht zu werden, hat sich das Auto-ID Center entschlossen, in Zukunft auch Transponder mit erweiterter Funktionalität zu unterstützen. Diese Entwicklung soll Transponder mit Speicher und Sicherheitsfunktionen (Class 2), semiaktive Transponder mit Batteriebetrieb (Class 3) und Transponder mit integrierten Sensoren (Class 4) umfassen.

Die Unterschiede der von verschiedener Seite vorgeschlagenen Protokolle liegen häufig im Detail und erfordern umfassende Tests für eine Evaluation, sodass eine genauere Analyse hier nicht möglich ist. Generell kann jedoch gesagt werden, dass es folgende charakterisierende Eigenschaften und Hauptunterscheidungsmerkmale gibt:

- Lesedistanz
- Speicherorganisation auf den Transpondern
- Anzahl von Transpondern, die pro Zeiteinheit erkannt werden können
- Störanfälligkeit z.B. gegenüber hohem Rauschpegel oder Metall in der Umgebung
- Unterstützung spezifischer Kommandos, wie z.B. eines Kill-Kommandos, das einen Transponder unbrauchbar macht
- Erfüllung der Zulassungsvorschriften in den einzelnen Ländern

Die oben angesprochenen neuartigen Fertigungsmethoden befinden sich zurzeit noch in einem Entwicklungsstadium, sodass ihr Nutzen in der Praxis bisher noch nicht nachgewiesen worden ist. Die genannten Design- und Fertigungsansätze für die integrierten Schaltkreise werden allerdings nur dann zu den erhofften Kostenreduktionen führen, wenn die Chips in großen Mengen produziert werden können. Die Nachfrage der Endkunden wird daher ein wesentliches Element in der Hoffnung auf langfristig günstigere RFID-Chips bleiben.

Neben den verschiedenen Identifikationsnummernformaten, die außerhalb der Transpondertechnik verbreitet eingesetzt werden [Bro01a], gibt es auch im RFID-Umfeld einige Standards zu Identifizierungscodes. So spezifiziert z.B. der ISO-Standard 11784 Identifizierungscodes für Tiere und ISO 15963 definiert das Nummernformat für die ISO-18000-Serie, die die Anforderungen der Waren- und Güterwirtschaft berücksichtigt.

Abschließend wäre zu den Transpondern und zugehörigen Protokollen zu bemerken, dass EPCglobal Unterstützung durch viele große Firmen aus der Konsumgüterbranche, wie z.B. Wal-Mart [RFI03], erfährt. Diese Tatsache stellt einen nicht zu vernachlässigenden Aspekt im Hinblick darauf dar, welche Protokolle und Codestrukturen sich langfristig in diesem Industriesegment durchsetzen werden.

10.2 IT-Infrastruktur

Die Vision einer „Networked Physical World“ und eines „Internets der Dinge“, wie sie das Auto-ID Center propagierte [SBA02], wird bereits seit Beginn der 1990er-Jahre auch in anderen Forschungsprojekten untersucht. Im Bereich des Ubiquitous Computing konzentriert man sich dabei allerdings nicht allein auf die RFID-Transpondertechnik, sondern beschäftigt sich auch mit alternativen Identifikations- und Positionierungstechnologien. Gemeinsam ist allerdings allen Ansätzen, dass sie versuchen, die physische, reale Welt mit der virtuellen Welt des Internets, der Datenbanken und der Web-Services zu verbinden und dafür die entsprechende Infrastruktur zu entwerfen. Im Cooltown-Projekt [KiB00], das von der Firma HP initiiert wurde, wurde beispielsweise eine Internet-basierte Infrastruktur entwickelt, die Webressourcen mit physischen Objekten verbindet. Benutzer können dabei Internetadressen (URL) über Sensoren, wie Infrarotschnittstellen und Barcodes von Objekten, die entsprechend gekennzeichnet sind, abrufen und über das Internet die virtuellen Repräsentationen dieser Objekte in Form von Webseiten anfordern. Ähnlich wie beim Auto-ID-Center-Ansatz wird dabei auf klassische Middleware, wie CORBA und Java RMI, verzichtet und es werden stattdessen Internettechnologien, wie HTTP, URLs und DNS, eingesetzt. Bei Cooltown stehen allerdings eher die Mobilität des Benutzers und die Interaktion mit stationären Gegenständen im Vordergrund, und nicht so sehr die autonome Lokalisierung und Verfolgbarkeit von augmentierten Objekten.

Von den Technologien des Auto-ID Centers, die auf der klassischen Netzinfrastruktur aufbauen, wie die Physical Markup Language, die Savant-Software, das EPC IS und das ONS-System, wurde nur ein Teil nach der Übergabe an EPCglobal weitergeführt. Die Savant-Software wurde dabei durch die Application-Level-Events-Spezifikation und die Physical Markup Language zumindest teilweise durch das Reader-Interface-Protokoll ersetzt. Da diese Spezifikationen erst kürzlich veröffentlicht wurden, bleibt abzuwarten, ob diese Standardisierungsbemühungen, die lediglich die RFID-Transpondertechnik unterstützen, schlussendlich von Erfolg gekrönt sind.

Für die Vision einer globalen Infrastruktur, die es erlaubt, die mit Transpondern gekennzeichneten Objekte automatisch überall zu verfolgen, ist die Funktio-

nalität des ONS-Systems zurzeit nicht ausreichend. Während die heutige Version lediglich ein Auffinden eines Servers für weitere Produktinformationen vorsieht, wird ein globales Track&Trace nicht unterstützt. Hierzu müsste ähnlich der GSM-Infrastruktur Funktionalität so spezifiziert werden, dass der momentane Aufenthaltsort der identifizierten Objekte an ein System gemeldet wird.

11 Schlussfolgerung

Zusammenfassend lässt sich festhalten, dass die Standardisierungsbemühungen des Auto-ID Centers bzw. der Nachfolgeorganisation EPCglobal zum jetzigen Zeitpunkt noch nicht abgeschlossen sind. Am weitesten fortgeschritten sind dabei die Protokolle, die die Kommunikation zwischen Lesegeräten und den Transpondern sicherstellen. Die erste Generation dieser Protokolle ist dabei in Form von Produkten bereits heute verfügbar. Für die zweite Generation wird zudem mit einer breiten Unterstützung durch die verschiedenen Chiphersteller gerechnet, da zumindest durch den geplanten Einsatz der Technologie im Einzelhandel die entsprechenden Umsätze zu erwarten sind. Weit fortgeschritten sind ebenfalls die Standardisierungsbemühungen bzgl. der EPC-Datenstruktur und des ONS-Systems.

Mit dem Übergang vom Auto-ID Center zu EPCglobal hat sich der Fokus von Forschung in Richtung Realisierung verschoben. Dabei ist es möglich, dass die ursprüngliche Vision eines Internets der Dinge, die sich bisher in der Entwicklung der Transpondertechnik, aber auch der entsprechenden Netzinfrastruktur geäußert hat, zukünftig in den Hintergrund rückt. Die Standardisierungsbemühungen würden sich dann vor allem auf Transponder und Lesegeräte konzentrieren und es bliebe abzuwarten, ob sich diejenigen Entwicklungen, die nicht die Luftschnittstelle betreffen, in der ursprünglich vorgesehenen Weise durchsetzen werden.

Um die Vision zu realisieren, mit RFID-Transpondern gekennzeichnete Objekte überall automatisch verfolgen zu können, ist es noch ein weiter Weg. Das Auto-ID Center hat in den fünf Jahren erfolgreich diese Vision in den verschiedenen Industriebereichen bekannt gemacht und die Möglichkeiten der Transpondertechnik aufgezeigt. Die Hauptaufgabe der Nachfolgeorganisation EPCglobal und der beteiligten Unternehmen wird in nächster Zeit darin bestehen, die Standards zu vervollständigen, durch geeignete Produkte zu unterstützen und für die entsprechende Nachfrage bei Anwendern zu sorgen. Nicht zu unterschätzen ist dabei der Datenschutzaspekt, der sich durch eine Allgegenwärtigkeit der RFID-Transpondertechnik ergeben dürfte − kritische Presseberichte und einige Ereignisse im Umfeld erster Anwendungen im Einzelhandel haben in letzter Zeit die Öffentlichkeit hinsichtlich des Problems des Privatsphärenschutzes sensibilisiert (siehe dazu auch die Beiträge von Langheinrich und von Thiesse in diesem Buch).

Literatur

[AGG02] Alexander K, Gilliam T, Gramling K, Kindy M, Moogimane D, Schultz M, Woods M (2002) Focus on the Supply Chain: Applying Auto-ID within the Distribution Center. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-002.pdf

[ATC99] Alien Technology Corporation (1999) Fluidic Self Assembly. www.alientechnology.com/library/pdf/fsa_white_paper.pdf

[Aut02a] Auto-ID Center (2002) Das neue Netzwerk. archive.epcglobalinc.org/new_media/brochures/GERMAN_AUTO_ID_CENTER.pdf

[Aut02b] Auto-ID Center (2002) 860 MHz–960 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Recommended Standard, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

[Aut03a] Auto-ID Center (2003) 860 MHz–935 MHz Class 0 Radio Frequency Identification Tag Protocol Specification Candidate Recommendation, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[Aut03b] Auto-ID Center (2003) 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0, archive.epcglobalinc.org/publishedresearch/mit-autoid-tr011.pdf

[Bro01a] Brock D (2001) The Electronic Product Code. MIT Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-002.pdf

[Bro01b] Brock D (2001) The Physical Markup Language. MIT Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-003.pdf

[CaB02] Carr CT, Brown S (2002) Auto-ID Center of 2003 - Steps Towards Delivering the Future. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-EB-005.pdf

[CDG02] Chappell G, Durdan D, Gilbert G, Ginsburg L, Smith J, Tobolski J (2002) Auto-ID on Delivery: The Value of Auto-ID Technology in the Retail Supply Chain. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/ACN-AUTOID-BC-004.pdf

[CGS02] Chappell G, Ginsburg L, Schmidt P, Smith J, Tobolski J (2002) Auto-ID on the Line: The Value of Auto-ID Technology in Manufacturing. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/ACN-AUTOID-BC-005.pdf

[CTA03] Clark S, Traub K, Anarkat D, Osinski T (2003) Auto-ID Savant Specification 1.0. Auto-ID Center, www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-savant-1_0-20030911.doc

[EPC03a] EPCglobal (2003) About EPCglobal. www.epcglobalinc.org/about/about.html

[EPC03b] EPCglobal (2003) EPC Tag Data Standards Version 1.1 Rev.1.24. www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf

[EPC04a] EPCglobal (2004) EPCTM Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz.

[EPC04b] EPCglobal (2004) EPCglobal Selects VeriSign to Provide Root Directory for EPCglobal Network. www.epcglobalinc.org/news/pr_01132004.html

[EPC05] EPCglobal (2005) Reader Protocol 1.0.

[FAH03] Floerkemeier C, Anarkat D, Harrison M, Osinski T (2003) Physical Markup Language (PML) Core Specification. Auto-ID Center,

www.epcglobalinc.org/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf
[Fin02] Finkenzeller K (2002) RFID-Handbuch. Hanser-Verlag
[HaM03] Harrison M, McFarlane D (2003) Development of a Prototype PML Server for an Auto-ID Enabled Robotic Manufacturing Environment. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/cam-autoid-wh010.pdf
[KhS03] Khan K, Sarma S (2003) Vibratory Assembly Update: Part Transportation Mechanics Analysis. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/mit-autoid-tr008.pdf
[KiB00] Kindberg T, Barton J (2000) A Web-Based Nomadic Computing System. HP Laboratories Palo Alto, Technical Report HPL-2000-110
[Mea03] Mealling M (2003) Auto-ID Object Name Service (ONS) 1.0. Auto-ID Center, www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-ons-1.0-20030930.pdf
[RFI03] RFID Journal (2003) Wal-Mart Draws Line in the Sand, January 1, 2005 www.rfidjournal.com/article/view/462/1/1/
[RRP02] Reynolds M, Richards J, Pathare S, Maguire Y, Tsai H, Post R, Pappu R, Schoner B (2002) Multi-Band, Low-Cost EPC Tag Reader. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-012.pdf
[Sar01] Sarma S (2001) Towards the 5¢ Tag. MIT Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-006.pdf
[SBA01] Sarma S, Brock D, Ashton K (2001) The Networked Physical World - Proposals for Engineering The Next Generation of Computing, Commerce & Automatic Identification. MIT Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-001.pdf
[SLL00] Siu KY, Law C, Lee K (2000) Efficient Memoryless Protocol for Tag Identification. MIT Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TR-003.pdf
[TBO04] Traub K, Bent S, Osinski T, Peretz SN, Rehling S, Rosenthal S, Tracey B (2004) The Application Level Events (ALE) Specification, Version 1.0. EPCglobal
[UCC02a] Uniform Code Council (2002) Serialized Shipping Container Codes Implementation Guide. www.uc-council.org/ean_ucc_system/pdf/SSCC.pdf
[UCC02b] Uniform Code Council (2002) Global Location Number Implementation Guide. www.uc-council.org/ean_ucc_system/pdf/GLN.pdf
[UCC03] Uniform Code Council (2003) Global Trade Item Numbers™ Implementation Guide. www.uc-council.org/ean_ucc_system/pdf/GTIN.pdf
[W3C01] W3C (2001) XML Schema. www.w3.org/XML/Schema

Architektur und Integration von RFID-Systemen

Frédéric Thiesse
Institut für Technologiemanagement, Universität St. Gallen

Kurzfassung. RFID-Systeme erweitern die bestehende IT-Landschaft um eine Reihe zusätzlicher Soft- und Hardwarekomponenten. RFID-Daten finden in verschiedensten Applikationen Verwendung und machen daher häufig einen hohen Integrationsaufwand erforderlich. Die gewählte Informationssystem-Architektur spielt aus diesem Grund eine entscheidende Rolle für den Erfolg einer RFID-Einführung und bedarf einer sorgfältigen Planung in frühen Projektphasen.

Der vorliegende Beitrag stellt zu diesem Zweck eine RFID-Referenzarchitektur und ihre wesentlichen Komponenten vor, die in der Analyse- und Designphase eines Einführungsprojekts als Hilfsmittel für einen strukturierten Informationssystem-Entwurf Verwendung finden kann. Darüber hinaus werden die wichtigsten, für die Implementierung notwendigen Softwaretechnologien vorgestellt. Abschließend wird das Zusammenspiel der einzelnen Bausteine anhand mehrerer Anwendungsbeispiele illustriert.

1 Einführung

In der Vergangenheit waren RFID-Systeme weitgehend Individualentwicklungen, was vor allem in der Vielzahl verschiedener Anbieter, Technologien und Anwendungsfelder begründet lag. Mit der zunehmenden Reife bzw. Standardisierung der Technologie und der damit einhergehenden Größe der zu realisierenden Systeme verlieren diese aber nach und nach ihren Prototypencharakter und es verschiebt sich der Fokus weg von den Eigenschaften der Hardware hin zum Aufbau komplexer Gesamtsysteme. Zentraler Aspekt ist dabei die Gestaltung der Softwarearchitektur zur Steuerung der eingesetzten Hardware, zur Einbindung weiterer Informationssysteme (IS) sowie zur ganzen oder teilweisen Abbildung der betroffenen Geschäftsprozesse [Kub03].

Die Anforderungen an eine derartige RFID-Softwarearchitektur lassen sich dabei wie folgt zusammenfassen:

- **Integration.** RFID-Systeme sind in den allermeisten Fällen keine isolierten Anwendungen, sondern dienen als Schnittstelle zwischen physischen Vorgängen in der realen Welt einerseits und den Informationssystemen zur Planung, Steuerung und Kontrolle dieser Vorgänge andererseits. Die Möglichkeiten zur flexiblen Integration in eine bestehende Systemlandschaft sind daher für den Nutzen von RFID-Systemen entscheidend.
- **Performance.** Insofern RFID nicht nur zur Offline-Analyse, sondern zur Prozesssteuerung in Echtzeit verwendet wird, entstehen u.U. hohe Leistungsan-

forderungen, die das System auch unter Volllast zuverlässig erfüllen muss. Dies betrifft sowohl die Fähigkeit, große Mengen an ankommenden Daten zu verarbeiten, als auch die Geschwindigkeit, mit der dies geschieht.

- **Skalierbarkeit.** Eine mit steigenden Leistungsanforderungen ebenfalls wichtiger werdende Fähigkeit ist die Skalierbarkeit, d.h. die Möglichkeit zur Erweiterung des Systems durch Verteilung auf mehrere Rechner bzw. Standorte. Entscheidend ist hierbei jeweils, inwiefern die Systemleistung von der zusätzlichen Rechenkapazität profitiert bzw. durch die evtl. redundante Datenhaltung und Notwendigkeit zum Datenaustausch zwischen mehreren Installationen negativ beeinflusst wird.
- **Robustheit.** Die Steuerung und Kontrolle physischer Vorgänge bringt eine Vielzahl möglicher Fehlerquellen mit sich, je nachdem, inwieweit es sich jeweils um geführte oder chaotische Prozesse handelt. Da unmittelbare Benutzereingriffe zumeist nicht möglich sind, muss das RFID-System jederzeit in der Lage sein, auftretende Fehler zu behandeln bzw. an übergeordnete Systeme weiterzuleiten, ohne dass die Funktionsfähigkeit des Gesamtsystems beeinträchtigt wird.
- **Sicherheit.** Nicht zuletzt ist für RFID-Systeme wie auch bei anderen Informationssystemen der Sicherheitsaspekt zu berücksichtigen, sei es zum Schutz einzelner Systemkomponenten vor Manipulation von außen oder zur Sicherung der bei Kommunikationsvorgängen übertragenen Daten. Dies gilt insbesondere bei Anwendungen, die nicht an den Grenzen einer Organisation enden, z.B. in der Lieferkette eines Industrieunternehmens.

Vor diesem Hintergrund entsteht ein wachsender Bedarf nach wieder verwendbaren Lösungsbausteinen, die schneller und zuverlässiger zum Erfolg führen, als es mit dem „Grüne Wiese“-Ansatz möglich wäre. Existierende Vorschläge für Architekturen zu Ubiquitous-Computing-Anwendungen wiederum konzentrieren sich zumeist nur auf einzelne isolierte Szenarien, um technische oder funktionale Prinzipien zu demonstrieren. Im Gegensatz dazu adressiert RFID vor allem große integrierte, häufig organisationsübergreifende Anwendungen und die wesentliche Herausforderung bei deren Implementierung besteht in der Einbettung von Technologie und Systemen in eine bereits bestehende Infrastruktur, sodass sich der Schwerpunkt mehr und mehr von der Basistechnologie in Richtung der oben genannten Punkte bewegt.

Der vorliegende Beitrag unternimmt daher den Versuch, ein Referenzmodell für die Softwarearchitektur von RFID-Systemen zu entwerfen. Ähnlich dem Einsatz wieder verwendbarer Softwarebausteine während der Implementierungsphase kann ein derartiges Architekturmodell in der Analyse- und Designphase eines Projekts eingesetzt werden und trägt zu deren Verkürzung und einer insgesamt höheren Qualität des Entwurfsergebnisses bei. Darüber hinaus kann das Modell als Grundlage für die Implementierung standardisierter Softwarekomponenten oder anderer Referenzmodelle dienen, z.B. einer Methodik zur Einführung von RFID-Systemen oder einer Reihe von Referenzprozessen, Rollen und Kennzahlen, die zu deren Betrieb notwendig sind (siehe Abbildung 1).

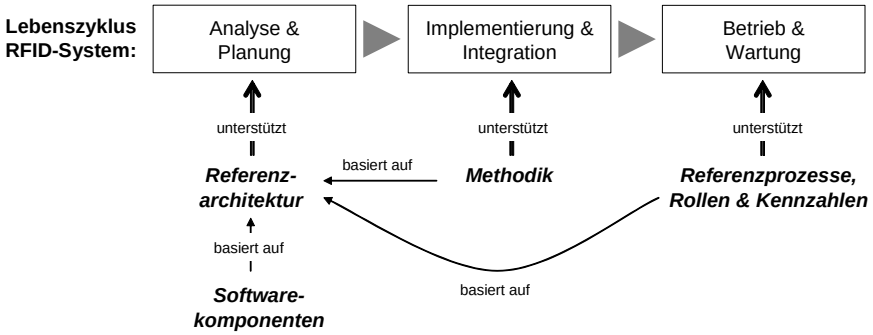


Abb. 1. Referenzarchitektur im Kontext des Lebenszyklus eines RFID-Systems

2 Referenzmodell

Vereinfacht ausgedrückt entspricht ein RFID-System den Augen und Ohren eines Informationssystems, über die unabhängig von manuellen Dateneingaben Informationen über die physische Welt erfasst werden können. Im Kern ermöglicht die dazugehörige Sensorik eine Identifikation von Objekten per Funk. Darüber hinaus ist jedoch auch eine weiter gehende Kontrolle denkbar, z.B. die Lokalisierung in Echtzeit durch Infrarot oder Ultraschall, Temperaturüberwachung, Positionsbestimmung per GPS usw.

Des Weiteren ist in der Gegenrichtung in vielen Fällen auch eine Aktuatorik notwendig, die das Objekt oder seine Umgebung beeinflusst. Die einfachste Variante ist die Speicherung von Daten auf einem Chip am Objekt; möglich ist aber auch die Steuerung physischer Vorgänge, z.B. durch Öffnen einer Schranke, Auslösen von Lichtsignalen oder Start eines Bearbeitungsschritts an einer Maschine.

Um die eingehenden Sensordaten für das Informationssystem verarbeitbar zu machen, ist eine Reihe von Bearbeitungsschritten notwendig, für die das RFID-System verantwortlich ist (siehe Abbildung 2):

- **Bereinigung.** Die von der Hardware gelieferten Daten können fehlerhaft sein, z.B. durch elektromagnetische Reflexionen oder beschädigte Sensoren. Hier können verschiedene Filtermechanismen einen je nach Anwendung hohen Prozentsatz fehlerhafter Daten aussortieren oder berichtigen. Neben der Fehlerkorrektur umfasst die Bereinigung aber auch die Entfernung irrelevanter Daten, z.B. bei der Erkennung von Transpondern, die nicht im System registriert sind.
- **Aggregation.** Nicht jeder Konsument von RFID-Informationen benötigt diese auf der gleichen Aggregationsstufe. So ist beispielsweise bei einer LKW-Zufahrtskontrolle nicht primär die einzelne atomare Objekt-Identifikation von Interesse, sondern die aus mehreren Identifikationen an verschiedenen Punkten abgeleitete Bewegungsinformation. Die Aufgabe des RFID-Systems besteht daher aus einer Zusammenfassung von Einzelinformationen zu komplexeren Aussagen.

- **Transformation.** Sowohl Lesegeräte auf der einen als auch Informationssysteme auf der anderen Seite arbeiten mit Protokollen und Datenformaten, die in den seltensten Fällen zueinander kompatibel sind. Das RFID-System dient hierbei als Vermittler auf syntaktischer, aber auch semantischer Ebene. Ein Beispiel für eine Transformation auf syntaktischer Ebene ist die Umwandlung eines vom RFID-Leser gelieferten binären Datenstroms in ein XML-Dokument, wobei sich der eigentliche Informationsgehalt jedoch nicht ändert. Eine semantische Transformation hingegen lässt Information weg oder fügt Information hinzu, z.B. bei der Ergänzung einer Transponder-ID um eine dazugehörige Produktionslosnummer.
- **Speicherung.** In vielen Fällen sind RFID-Informationen nicht zur Objektverfolgung in Echtzeit, sondern zu Analysezwecken gedacht, d.h. Informationsproduzent und -konsument arbeiten zeitlich entkoppelt voneinander. In diesem Fall ist das RFID-System für eine temporäre Pufferung oder dauerhafte Speicherung verantwortlich, um RFID-Informationen auf Anfrage bereitstellen zu können.

Analoges gilt auch in der Gegenrichtung bei der Ausführung von Kommandos, die das übergeordnete IS an das RFID-System übergibt. Hier ist das RFID-System u.a. verantwortlich für die Auswahl des jeweils geeigneten Geräts, die Umwandlung in dessen Kommunikationsprotokoll, die Zwischenspeicherung bei vorübergehender Nichtverfügbarkeit des Geräts usw.

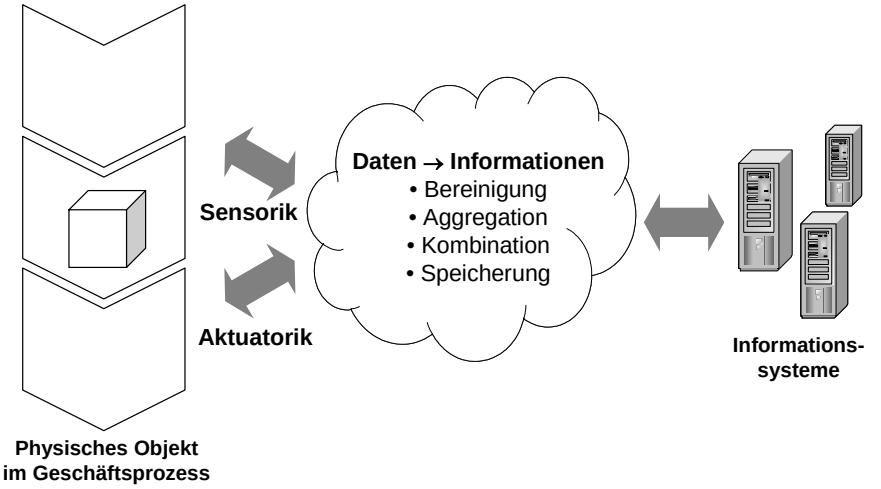


Abb. 2. Aufgaben eines RFID-Systems

Sensorik und Aktuatorik werden durch das RFID-System vollständig gekapselt, sodass das angeschlossene IS eine transparente Sicht auf reale Vorgänge erhält, ohne den inneren Aufbau des RFID-Systems kennen zu müssen.

2.1 Logische Architektur

Ausgehend von obigen Überlegungen kann die Struktur eines RFID-Systems nun durch Modularisierung weiter verfeinert werden (siehe Abbildung 3). Wichtig ist dabei im ersten Schritt, Schnittstellen nach außen festzulegen. Im Fall eines RFID-Systems handelt es sich auf der einen Seite um Schnittstellen zur RFID-Hardware, welche durch so genannte „Edgeware"-Komponenten realisiert werden. Edgeware kapselt das gesamte Kommunikationsprotokoll einer Hardware und dient so als Übersetzer zwischen dem RFID-System und den angeschlossenen Geräten. Darüber hinaus dient Edgeware zur ersten Fehlerkorrektur, wobei naturgemäß nur geräte- und nicht anwendungsbezogene Fehler erkannt werden können.

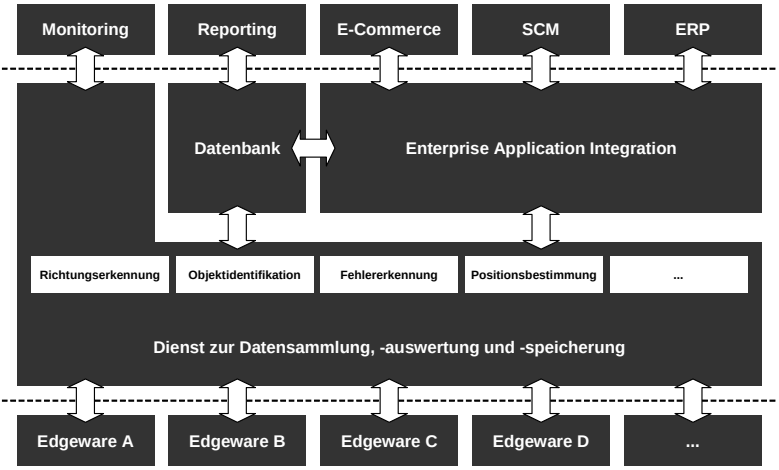


Abb. 3. Logische Architektur im Überblick

Auf der anderen Seite sind Schnittstellen zu übergeordneten Informationssystemen notwendig, welche hier als Clients des RFID-Systems agieren. Im Einzelnen können die folgenden Klassen von Clients unterschieden werden:

- **Monitoring.** Eine Monitoring-Komponente ist unmittelbar an das RFID-System angebunden und dient zur Visualisierung von Objektinformationen in Echtzeit, z.B. zur Losverfolgung in einem Produktionsprozess. Die Kommunikation erfolgt evtl. in beiden Richtungen, sodass auch die teilweise Steuerung des RFID-Systems über die Monitoring-Komponente möglich ist.
- **Reporting.** Eine Reporting-Komponente dient zur Aufbereitung und Untersuchung von Vergangenheitsdaten. In der Praxis kann es sich hier beispielsweise um einen Reportgenerator, ein Tool zur Prozessanalyse oder ein Data Warehouse handeln. Allen Varianten ist gemeinsam, dass die Kopplung mit dem RFID-System indirekt über eine Datenbank erfolgt; insbesondere funktioniert der Datenaustausch nur in einer Richtung, d.h., die Reporting-Komponente sendet im Normalfall keine Anweisungen zurück an das System.

- **E-Commerce/Supply Chain Management/Enterprise Resource Planning.** Im Gegensatz zu den zuvor genannten Komponenten verfügen die im Unternehmen bereits bestehenden Informationssysteme im Allgemeinen nicht über eigene Schnittstellen zum RFID-System und benötigen daher zwecks Integration eine zusätzliche Komponente zur Enterprise Application Integration (EAI). Die in der Praxis auftretenden Informationssysteme können dabei grob unter den Oberbegriffen E-Commerce (meist webbasierte Anwendung oder Web-Service für Kunden), Supply Chain Management (Anwendung zur organisationsübergreifenden Steuerung der Lieferkette) und Enterprise Resource Planning (Anwendung zur internen Unternehmensplanung) zusammengefasst werden. Die Übergänge sind hier selbstverständlich fließend und Systeme mit breiter Funktionalität eher die Regel als die Ausnahme. Die Aufgabe der EAI-Komponente besteht nun in der Vermittlung zwischen beiden Systemen, d.h. in der Übergabe der RFID-Informationen an das IS (durch Versand von XML-Nachrichten oder Aufruf entsprechender Transaktionen) und der Weiterleitung von Kommandos an das RFID-System. Zu diesem Zweck nutzt die EAI-Komponente eine vorhandene Messaging-Infrastruktur der Systemplattform oder stellt diese selbst bereit, an welche beliebige Systeme über Schnittstellenmodule und Datenmapping-Funktionen angekoppelt werden können. Darüber hinaus bieten manche EAI-Tools auch Workflow-Funktionen, mit denen systemübergreifende Geschäftsprozesse abgebildet werden können.

Den Kern des RFID-Systems bildet ein Dienst, welcher die eigentliche Verarbeitungslogik umfasst. Dies beinhaltet im Wesentlichen die parallel ablaufenden Prozesse zur

- Sammlung (Entgegennahme der von der Edgeware gelieferten Rohdaten),
- Auswertung (Filterung, Zusammenfassung, Kombination usw.) und
- Speicherung bzw. Bereitstellung (selbstständig oder auf Abruf)

von RFID-Informationen mit dem Ziel einer möglichst frühen Verarbeitung der Rohdaten auf dem Weg vom RFID-Leser zu den übergeordneten Informationssystemen. Ein weiterer Prozess ist für die Verarbeitung von Kommandos an die Hardware verantwortlich (z.B. „Daten XYZ auf Transponder 123 schreiben“) und übernimmt die Überwachung der korrekten Ausführung sowie die Selektion der dafür geeigneten Geräte.

2.2 Physische Architektur

Sinn und Zweck einer logischen Architektur ist die Beschreibung dessen, *was* ein RFID-System aus einer problemorientierten Sicht leisten soll, und auf welche Art und Weise diese Aufgaben durch das Zusammenspiel einzelner Module gelöst werden können. Im Gegensatz dazu zeigt die physische Architektur aus technischer Sicht, *wie* ein solches System aus Hardwarekomponenten aufgebaut ist.

Die in Abbildung 4 dargestellte Architektur stellt eine Generalisierung dar, die je nach Anwendungsfall anders ausgestaltet sein kann. Einzelne Komponenten (insbesondere DB-Server oder Webserver) sind zumeist im Unternehmen schon vorhanden und können auch für das RFID-System genutzt werden. Davon abge-

sehen ist auch die jeweilige Skalierung ein entscheidender Faktor: So werden die in der Abbildung als dedizierte Server dargestellten Komponenten bei einer kleinen Installation u.U. gemeinsam auf einer Rechnerplattform zusammengefasst, wohingegen es bei großen Systemen notwendig sein kann, besonders beanspruchte Server separat oder sogar als Cluster einzurichten.

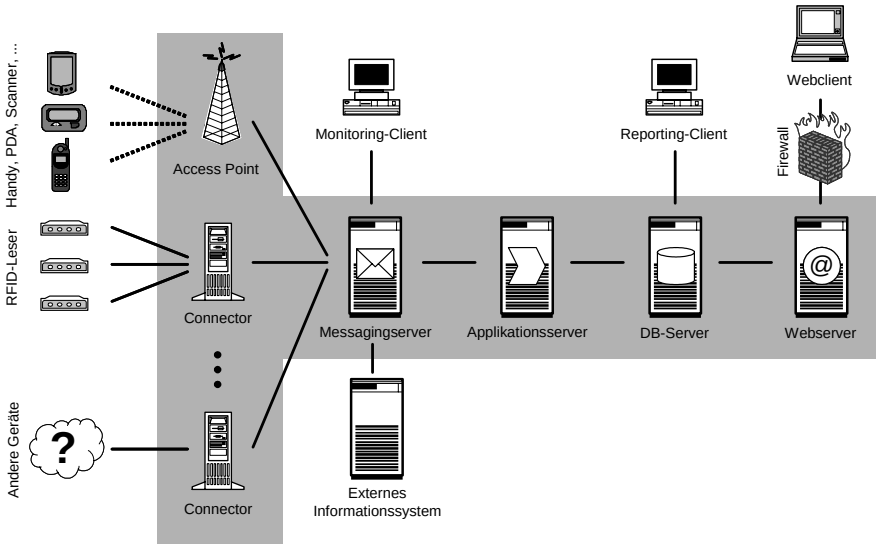


Abb. 4. Physische Architektur im Überblick

Die im Folgenden beschriebenen Komponenten sind Bestandteile der physischen RFID-Architektur:

- **RFID-Leser, Handy, PDA, mobiler Scanner usw. (Sensorik & Aktuatorik).** Die Palette der an ein RFID-System angeschlossenen Geräte deckt ein breites Spektrum ab und kann neben stationären oder mobilen RFID-Lesern auch PDAs, GPS-Empfänger, diverse Sensoren oder auch Barcode-Leser umfassen. Darüber hinaus kommen häufig auch verschiedene Geräte zum Einsatz, über die die Aktuatorik des Systems realisiert wird, z.B. zur Steuerung von Einfahrtstoren, Signallampen, Displays usw., insofern diese Aufgabe nicht bereits von einem anderen System übernommen wird. Jedes dieser Geräte verfügt im Allgemeinen über eigene Anschlüsse und Steuerungsprotokolle, sodass eine individuelle Anbindung notwendig ist, die entweder bei entsprechender Programmierbarkeit direkt auf dem Gerät oder aber über eine zusätzliche Schnittstelle realisiert wird.
- **Connector.** RFID-Leser und ähnliche Geräte werden meist als „Blackbox“ ohne Möglichkeit zur Programmierung geliefert – häufig mit einer seriellen Schnittstelle, sodass eine unmittelbare Integration in das Netzwerk nicht durchführbar ist. In solchen Fällen ist ein Rechner in der Rolle als physischer Vermittler notwendig, an den das Gerät angeschlossen ist und der mit einer pas-

senden Steuerungssoftware ausgestattet ist. Ein Zugriff auf das Gerät verläuft dann zwingend über diesen Rechner.

- **Access Point.** Im Gegensatz zu einem „dummen" RFID-Leser sind z.B. PDAs und ähnliche Geräte programmierbar und benötigen keine eigene Steuerungssoftware. Da diese Geräte andererseits in den meisten Fällen mobil eingesetzt werden und über Bluetooth, Wireless LAN oder Infrarot mit der Außenwelt kommunizieren, sind so genannte „Access Points" notwendig, die den Übergang vom drahtlosen Netz in das Unternehmens-LAN realisieren.
- **Applikationsserver.** Wie bei verteilten Systemen üblich, wird die Verarbeitungslogik unabhängig von Datenhaltung und Präsentation auf einem eigenen Server implementiert, der seine Funktionalität für Clients im Netzwerk bereitstellt. Im Fall eines RFID-Systems handelt es sich dabei um die bereits zuvor genannten Anwendungskomponenten zur Sammlung, Auswertung und Speicherung von RFID-Informationen.
- **DB-Server.** Der DB-Server dient als Datenspeicher des RFID-Systems, wobei üblicherweise einzig der Applikationsserver Daten schreiben darf und anderen Systemen nur der Lesezugriff gestattet ist.
- **Messagingserver.** In einem klassischen Client-Server-System, bei dem alle Komponenten von vornherein aufeinander zugeschnitten sind, erfolgt die Kommunikation über eine eigens definierte Schnittstelle über meist synchrone Verbindungen. In der heterogenen Systemlandschaft eines größeren Unternehmens ist die Anpassung von Anwendungen an einzelne Schnittstellen jedoch nicht mehr mit vertretbarem Aufwand machbar, sodass eine zusätzliche Middleware eingesetzt wird, deren Grundlage eine Messaging-Infrastruktur (z.B. mittels asynchroner Message Queues, siehe Abbildung 5) ist und die verschiedene Verfahren zur Datentransformation sowie Triggermechanismen bis hin zur Abbildung ganzer Geschäftsprozesse beinhaltet.

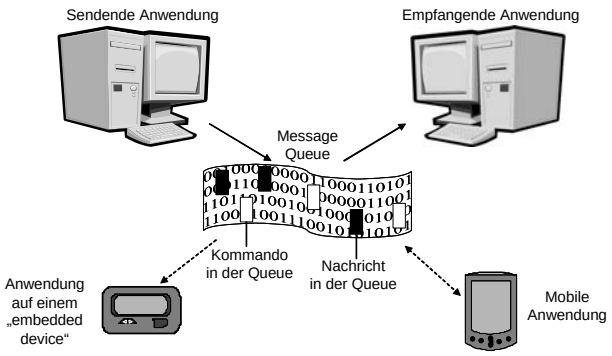


Abb. 5. Prinzip des asynchronen Messaging

- **Monitoring-Client.** Monitoring-Clients sind im Allgemeinen Endbenutzer-PCs zur Echtzeit-Überwachung und -Steuerung des RFID-Systems, welche zur Laufzeit dauerhaft mit dem System verbunden sind.

- **Reporting-Client.** Ein Reporting-Client kann sowohl ein Endbenutzer-PC sein, über den Analysen bzw. Reports erstellt werden, als auch ein Data Warehouse, welches in regelmäßigen Abständen RFID-Informationen in die eigene Datenbasis überträgt.
- **Webserver/Webclient/Firewall.** Um das RFID-System auch außerhalb der Organisation, insbesondere über das Internet, zugreifbar zu machen, ist ein Webserver als zusätzliche Middleware notwendig. Dieser realisiert entweder ein Endbenutzer-Graphical-User-Interface (GUI) oder einen Webservice. Dementsprechend kann ein Webclient entweder ein Internet-Browser sein oder eine Applikation, die den Webservice nutzt. Zur Absicherung des Systems gegen unerwünschte Zugriffe aus dem Internet wird üblicherweise eine Firewall eingesetzt.
- **Externe Informationssysteme.** Diverse externe Informationssysteme (z.B. zur Produktionsplanung, Lagerverwaltung usw.) können über den Messaging-Server mit dem RFID-System verbunden werden. Dabei werden RFID-Informationen in das Datenformat des jeweiligen Systems umgewandelt und über eine Transaktion übergeben oder direkt in dessen Datenbank geschrieben. Die Datenübertragung kann dabei sowohl vom RFID-System oder dem externen System, aber auch von der Workflow-Komponente der Middleware ausgelöst werden.

Der Zusammenhang zwischen logischer und physischer Architektur ist in Abbildung 6 dargestellt. Hier zeigt sich insbesondere, wie logische Komponenten auf Geräte verteilt werden bzw. an welchen unterschiedlichen Stellen einzelne Funktionalitäten umgesetzt werden können.

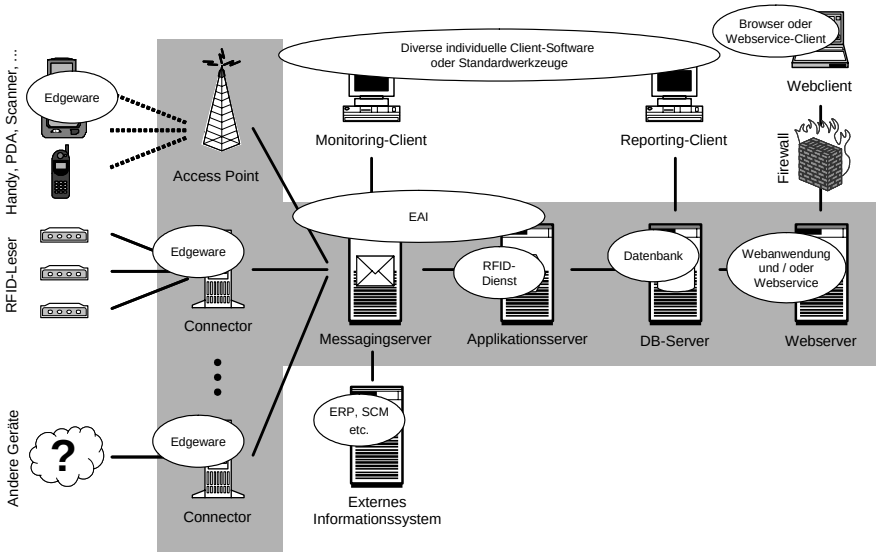


Abb. 6. Zusammenhang zwischen logischer und physischer Architektur

3 Softwaretechnologien

Zur Implementierung einer RFID-Architektur steht eine Vielzahl unterschiedlicher Softwaretechnologien zur Verfügung (siehe Abbildung 7). Im Folgenden werden deren Einsatz bei der Implementierung der beschriebenen Architekturkomponenten sowie Vor- und Nachteile kurz beschrieben.

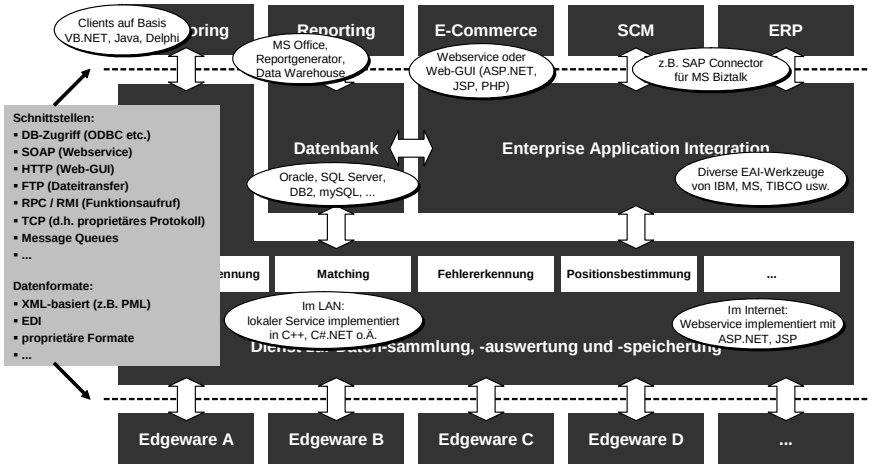


Abb. 7. Softwaretechnologien im Überblick

- **Schnittstellen zu stationären Geräten.** RFID-Leser und ähnliche Geräte arbeiten häufig nicht autonom, sondern benötigen einen zusätzlichen Rechner als Steuerung, der über eine serielle Schnittstelle angeschlossen wird. Die Steuerung des Lesers erfolgt in diesem Fall über einen herstellerspezifischen Satz an Kommandos, die als Bytefolge übergeben werden. Zur Kommunikation des Steuerungsrechners mit dem RFID-Server bietet sich ein asynchrones Messaging z.B. mit XML-Nachrichten an. Insbesondere im Bereich aktiver RFID-Systeme sind allerdings auch autonome Leser verbreitet, die über eine Ethernet-Schnittstelle verfügen und so direkt in ein Netzwerk eingebunden werden können. Auch hier erfolgt die Kommunikation über ein herstellerspezifisches Protokoll, welches auf TCP aufbaut, jedoch kann die entsprechende Softwareschnittstelle auf einem beliebigen Rechner eingerichtet werden (im Allgemeinen auf dem Applikationsserver).
- **Mobile Anwendungen.** Mobile Geräte wie PDAs oder für den industriellen Einsatz entwickelte RFID-Scanner sind üblicherweise mit einem Standard-Betriebssystem in der Art von PocketPC oder SymbianOS ausgestattet. Diese können über verschiedene Entwicklungssysteme programmiert werden, wobei für die Ansteuerung der RFID-Funktionen spezielle Libraries der Hersteller zur Verfügung stehen. Anwendungen für mobile Geräte dienen im Allgemeinen zur Datensammlung und -auswertung durch einen Benutzer. Je nachdem ob dieser einen permanenten Zugriff auf andere Systeme benötigt, kann das Gerät auch über Wireless LAN in das Netzwerk integriert sein. Dementsprechend er-

folgt die Kommunikation mit der Außenwelt entweder über ein auf TCP aufbauendes Protokoll (z.B. einen Webservice) oder mittels asynchronem Messaging. In letzterem Fall würde die mobile Anwendung alle erzeugten Nachrichten in eine Message Queue schreiben, deren Inhalt übertragen wird, sobald das Gerät wieder mit einem Access Point oder einer Docking Station verbunden ist.

- **RFID-Service.** Die Verarbeitungslogik des RFID-Systems wird in Form eines Dienstes (Windows Service, Unix Daemon usw.) implementiert, der kontinuierlich auf eingehende Nachrichten und Kommandos wartet und diese abarbeitet. Im Gegensatz zu einer herkömmlichen Anwendungssoftware arbeitet ein Dienst unabhängig von Benutzereingaben, verfügt im Allgemeinen über keine eigene GUI und kann insbesondere wesentlich flexibler administriert werden als andere Anwendungen. Aufgrund der Systemnähe von RFID-Services werden für die Implementierung üblicherweise C oder daraus abgeleitete Hochsprachen wie C++, C# oder Java eingesetzt.
- **Datenbanken.** Die überwiegende Mehrheit der heute im Einsatz befindlichen Datenbankmanagementsysteme (DBMS) verwendet relationale Modelle, d.h. Daten und die Beziehungen zwischen ihnen werden in Tabellen abgelegt, welche sich wiederum aus einigen elementaren Datentypen zusammensetzen. Im Gegensatz dazu ermöglichen objektorientierte Datenbanken die Modellierung mit allen Vorzügen der Objektorientierung (Vererbung, Kapselung, Polymorphismus usw.), die allerdings bisher nur in wenigen Spezialfällen zum Einsatz kamen. Grund hierfür ist u.a. das Fehlen einer standardisierten Abfragesprache wie SQL. Darüber hinaus haben die Hersteller relationaler Datenbanken ihre Produkte in den letzten Jahren um verschiedene objektorientierte Features erweitert, z.B. zur Definition anwendungsspezifischer Datentypen. Mit so genannten „nativen“ XML-Datenbanken existiert seit Kurzem ein weiterer DBMS-Typ, der Effizienzgewinne bei der Verwaltung von XML-Daten verspricht, da diese bei Speicherung und Abfrage nicht in bzw. aus einem anderen Datenmodell konvertiert werden müssen. Die zuletzt genannten Vertreter heutiger DBMS sind für RFID jedoch kaum relevant, da es sich hierbei mit großen Mengen stark strukturierter Daten und komplexer Abfragen um klassische Anwendungsfelder für relationale Datenbanken handelt.
- **Monitoring-Komponente.** Die Funktionalität eines RFID-Monitoring-Clients beschränkt sich meistens auf die Aufbereitung und Anzeige der vom RFID-System produzierten Daten, sodass zur Implementierung der Komponente vor allem eines der klassischen GUI-orientierten Entwicklungswerkzeuge zum Einsatz kommt. Die Art der Kopplung mit dem RFID-Service hängt vom Einsatzzweck des Clients ab. Insofern Client und Server nur punktuell miteinander kommunizieren (z.B. bei der Suche nach einzelnen Objekten), kann eine Kommunikation per Remote Procedure Call (RPC) oder einem ähnlichen Protokoll sinnvoll sein. Bei einer Echtzeitverfolgung von Objekten hingegen müssen mehrere Clients proaktiv vom Server mit Daten versorgt werden. In diesem Fall ist ein Messaging-Dienst vorzuziehen, der einen Publish/Subscribe-Mechanismus unterstützt. Der Server füllt hier eine öffentliche Message Queue mit Nachrichten, die von mehreren Clients „abonniert“ werden können. In der Gegenrichtung schreiben die Clients Kommandos an den Server in eine weitere Queue, die vom Server kontinuierlich abgefragt wird. Eine XML-Nachricht,

mit der der RFID-Server die Erkennung mehrerer Transponder durch angeschlossene Lesegeräte meldet, ist beispielhaft in Abbildung 8 dargestellt.

```
<MESSAGE Type="RFID-Events">
  <READER ID="Gebaeude A">
    <TAG ID="ABCDEF0123" Detection="In"/>
    <TAG ID="ABCDEFFFE0" Detection="NotValid"/>
  </READER>
  <READER ID="Zufahrt">
    <TAG ID="ABCDEF1111" Detection="Out"/>
  </READER>
</MESSAGE>
```

Abb. 8. XML-Nachricht eines RFID-Systems (Beispiel)

- **Reporting-Komponente.** Zur Realisierung der Reporting-Komponente steht auf dem Softwaremarkt eine große Zahl verschiedener Produkte zur Verfügung, mit denen nahezu ohne Programmierung Lösungen erstellt werden können. Die Palette reicht von Tools zur Datentransformation (z.B. zur Übertragung von Daten aus der RFID-DB in die DB eines Data Warehouse) über spezialisierte Reportgeneratoren und DB-Frontends wie MS Access (siehe Abbildung 9, die ein Beispiel der Intellion AG zeigt) bis zu diversen Tabellenkalkulationen.

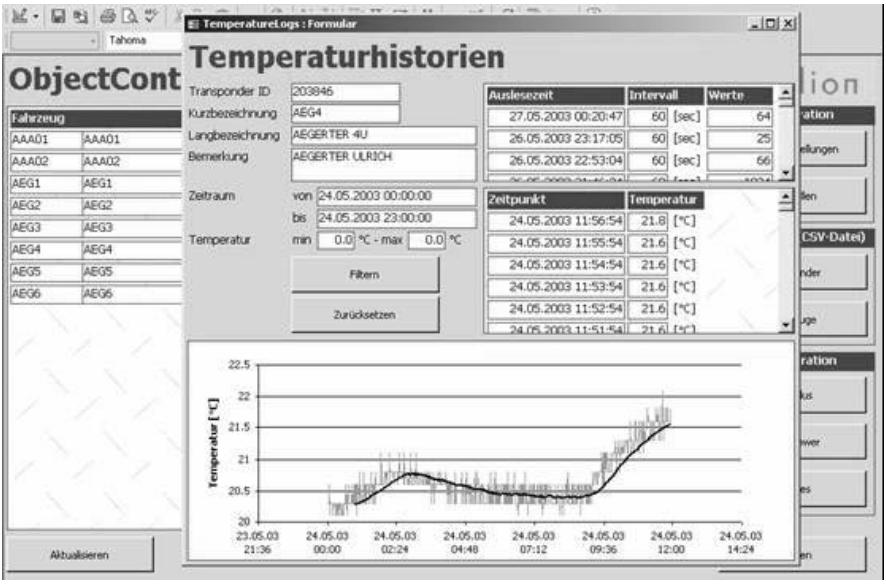


Abb. 9. Beispiel Reporting-Client

- **Ankopplung weiterer Systeme mittels Integrationstools.** Um das RFID-System mit anderen Systemen zu integrieren, können zwei Wege beschritten werden: Einerseits kann eine Integration erfolgen, indem eine entsprechende Schnittstelle direkt in eines der beiden Systeme einprogrammiert wird. Da dies aber je nach Anzahl und Komplexität der Systeme häufig nicht mit vernünftigem Aufwand machbar ist, kann alternativ auch auf spezialisierte EAI-Werkzeuge zurückgegriffen werden. Die Möglichkeiten eines EAI-Tools umfassen u.a. die Datentransformation (z.B. von XML in EDI oder von einer DB-Struktur in eine andere), die Bereitstellung von Systemfunktionen als Webservice, die Abbildung von Workflows oder der Aufruf von Transaktionen aus Standardsoftwarepaketen.

4 Anwendungsbeispiele

In den folgenden Abschnitten soll das generische Architekturmodell anhand einiger konkreter Praxisbeispiele mit Leben gefüllt werden. Dazu werden jeweils die Problemstellung und der vorgeschlagene Lösungsansatz skizziert und am Beispiel der Architektur illustriert.

4.1 Temperaturüberwachung

Problemstellung: Eine Supermarktkette möchte eine durchgehende Überwachung der Kühlkette für Produkte wie Speiseeis, Tiefkühlpizza, Frischfleisch usw. vom Produzenten über Distributionszentren bis zur einzelnen Filiale. Ziel ist es, Temperaturunter- bzw. -überschreitungen frühzeitig zu erkennen und dem Filialleiter bzw. Kunden vor Ort die vollständige Temperaturhistorie für einzelne Produkte zur Verfügung stellen zu können.
Lösungsansatz: Die für den Transport eingesetzten LKW werden mit aktiven Transpondern ausgestattet, welche über einen Temperatursensor verfügen, dessen Messwerte kontinuierlich im Transponderspeicher abgelegt werden. Die einzelnen Produkte erhalten einen passiven Transponder, der das Produkt eindeutig identifiziert. Beim Einladen werden LKW und Produkte gescannt, sodass eine Verbindung zwischen beiden hergestellt ist; beim Ausladen wird diese Verbindung durch einen erneuten Scan wieder aufgelöst und die Liste aller während der Fahrt gesammelten Temperaturdaten abgerufen. Die Abfrage erfolgt je nach örtlichen Gegebenheiten mit mobilen oder stationären Lesern, welche die gesammelten Daten als XML-Dokumente per Internet an einen zentralen Server übertragen.

Der Server legt die Temperaturdaten in einer Datenbank ab, sodass für jedes Produkt eine durchgängige Historie vorhanden ist. Zusätzlich prüft der Server, ob jeweils Temperaturunter- bzw. -obergrenzen eingehalten wurden, indem die Transponder-ID des Produkts in eine Produkttypkennung übersetzt und die dazugehörigen Grenzwerte aus einem anderen System abgerufen werden. Hierzu greift der Server über eine EAI-Komponente auf eine entsprechende Transaktion des anderen Systems zu. Die einzelnen Temperaturhistorien können anschließend

durch Eingabe einer Produktkennung oder Transponder-ID sowohl über ein DB-Frontend in der Firmenzentrale als auch über eine einfache Webanwendung im Browser abgerufen werden. Abbildung 10 zeigt die der Lösung zugrunde liegende Architektur.

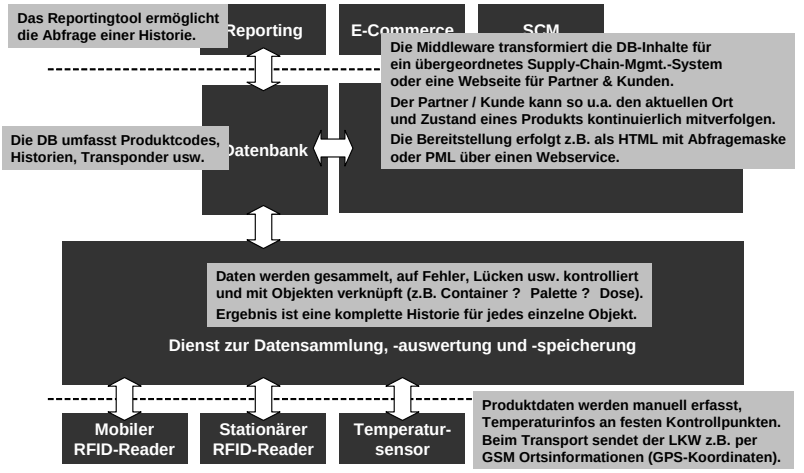


Abb. 10. Architektur am Beispiel Temperaturüberwachung

4.2 Losverfolgung

Problemstellung: Ein Unternehmen aus der Elektroindustrie möchte im Produktionsprozess die Bewegung einzelner Lose durch das Werk in Echtzeit verfolgen und zu einem späteren Zeitpunkt auch analysieren können, z.B. zur Kontrolle durchschnittlicher Durchlaufzeiten. Die Lose werden derzeit weitgehend manuell transportiert, wobei Plastikboxen unterschiedlicher Größe zum Einsatz kommen.
Lösungsansatz: An den Losboxen werden Transponder angebracht, wobei die Zuordnung von Boxen zu Losen im Produktionsplanungssystem des Unternehmens abgebildet ist. Um die Bewegung von Boxen erkennen zu können, werden an den Übergängen von einem Teil des Werks zum anderen elektromagnetische Gates installiert, d.h., das von einem RFID-Leser erzeugte Feld bildet eine Schleuse, an der RFID-Informationen über Transponder und – je nach Konfiguration der Antennen – auch Bewegungsrichtungen gesammelt werden können. Die entsprechende Architektur ist in Abbildung 11 dargestellt.

Diese Informationen werden an den RFID-Server weitergeleitet, der daraus Ortsinformationen für jeden Transponder ableitet. Die Verknüpfungen zwischen Transponder, Box und Los werden entweder regelmäßig vom RFID-Server aus dem PPS abgefragt oder aktiv vom PPS in die Datenbank repliziert.

Die Ortsinformationen der Lose werden bei Ortsänderungen vom Server über ein Messaging-System publiziert. Monitoring-Clients wiederum können diese Informationen abonnieren und stellen sie grafisch dar bzw. erlauben die Suche

nach einzelnen Losen. Mitarbeiter im Werk können sich so jederzeit über den Standort und andere Statusinformationen des Loses informieren. Daneben ist auch eine Übergabe dieser Angaben an das PPS denkbar, um so eine zusätzliche Datenbasis für die Produktionsplanung verfügbar zu haben.

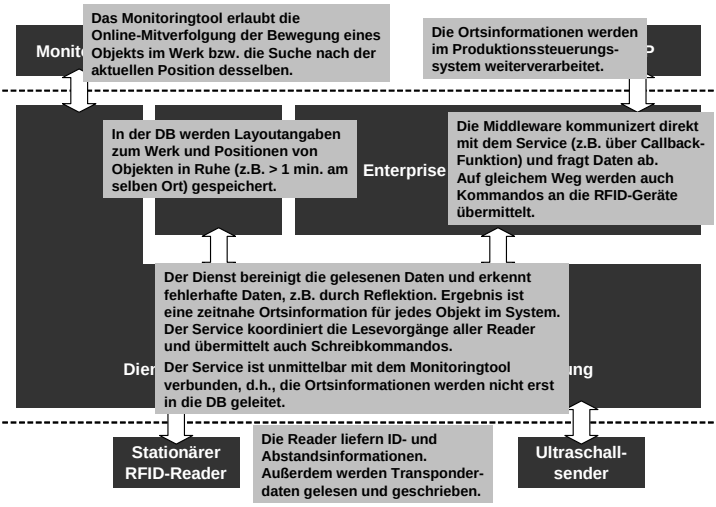


Abb. 11. Architektur am Beispiel Losverfolgung

Über ein entsprechendes Analysetool können darüber hinaus auch verschiedene Analysen auf Basis von Vergangenheitsdaten durchgeführt werden, die eine Grundlage für zukünftige Prozessverbesserungen bilden.

4.3 Inventarisierung

Problemstellung: In der Zentrale eines Finanzdienstleisters soll das zahlreich vorhandene EDV-Inventar mittels RFID kontinuierlich erfasst werden. Anlass hierfür ist neben Diebstählen auch das Problem, dass Geräte aufgrund von Umzügen oder des Wechsels von Mitarbeitern zwischen Projekten immer wieder vergessen werden und daher ungenutzt herumstehen. Eine Inventarisierung durch manuelles Einscannen von Barcodes hat sich in der Vergangenheit als zu aufwendig und fehleranfällig erwiesen.
Lösungsansatz: Da aktive Transponder zu teuer gewesen wären, werden die Geräte mit passiven Smart Labels ausgestattet. An einigen wichtigen Übergangspunkten, z.B. Fahrstühlen und Gebäudeeingängen, werden stationäre Lesegeräte installiert. Davon abgesehen erfolgt die regelmäßige Inventarisierung mit manuellen Lesern. Diese stellen einen wirtschaftlich sinnvollen Kompromiss zwischen Barcodescannern einerseits und aktiven Systemen in Form elektromagnetischer „Raumleuchten“ andererseits dar. Obwohl der manuelle Aufwand nicht völlig entfällt, ist der Scanvorgang selbst deutlich effizienter.

Neben dem Inventar selbst werden auch die Räume durch ein Smart Label am Türrahmen eindeutig identifizierbar gemacht und so beim Scannen Inventar und Equipment durch Einscannen logisch miteinander verknüpft. Die erfassten Daten werden in einer eigenen RFID-DB abgelegt und mit den Bestandsinformationen im ERP-System abgeglichen. Abbildung 12 verdeutlicht die dem Lösungsansatz zugrunde liegende Architektur.

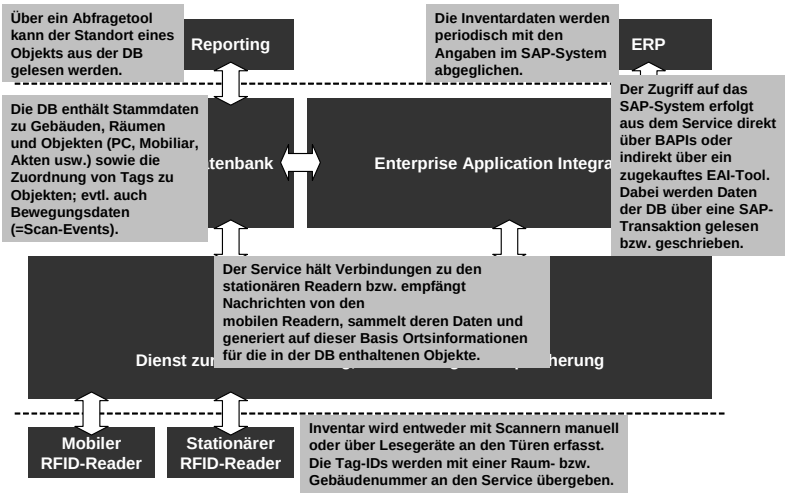


Abb. 12. Architektur am Beispiel Inventarisierung

5 Zusammenfassung und Ausblick

Die in diesem Beitrag vorgestellte Referenzarchitektur ist ein erster Schritt in Richtung einer standardisierten Infrastruktur für RFID-Lösungen. Im Gegensatz zu existierenden Ansätzen, die sich auf generische UbiComp-Anwendungen konzentrieren, berücksichtigt dieser Vorschlag Themen wie Integration und Skalierbarkeit, die für den betrieblichen Einsatz zentral sind. Das Referenzmodell hilft hier bei der Analyse- und Planungsphase von RFID-Projekten und liefert einen Bezugsrahmen für Softwarearchitekten und Projektmanager.

Zahlreiche ERP- und Middleware-Anbieter gehen mittlerweile mit entsprechenden Werkzeugen an den Markt, welche die Implementierung der resultierenden Architekturen unterstützen. Ein weiterer wichtiger Treiber für die Einführung von RFID-Systemen ist Standardisierung, insbesondere im Kontext der durch das internationale Auto-ID-Center-Projekt entwickelten EPC-Technologie, welche die Interoperabilität aller notwendigen Systemkomponenten drastisch vereinfacht. Ein wichtiger Baustein dieser Technologie ist beispielsweise die so genannte „Physical Markup Language (PML)“ [FAOH03], eine XML-basierte Spezifikation der Schnittstelle zwischen RFID-Reader und angeschlossenen Informationssystemen,

die im Rahmen der Savant-Middleware auch in Software implementiert wurde [Goy03].

Nichtsdestotrotz existiert in diesem Zusammenhang noch eine Vielzahl an Fragestellungen, welche es zu lösen gilt, u.a.

- **Algorithmen zur Auswertung von RFID-Daten.** Aufgrund der enormen Datenmengen, die durch RFID-Hardware generiert werden, ist eine Hauptaufgabe von RFID-Middleware die Ableitung von Information über Prozesse anstelle einer reinen Weiterleitung von Rohdaten an übergeordnete Systeme. Ein typisches Beispiel ist die Bewegungserkennung, bei der eine Sequenz von RFID-Sichtungen von unterschiedlichen Lesern zu einer Richtungsaussage interpretiert wird, z.B. „Objekt 123 hat das Areal X verlassen". Die Notwendigkeit einer frühzeitigen Verarbeitung der angesammelten RFID-Daten ergibt sich nicht zuletzt aus der schieren Datenmenge, die Netzwerke und übergeordnete Informationssysteme überfordern kann, wenn keine hardwarenahe Filterung durchgeführt wird.
- **Softwarekomponenten.** Teile einer RFID-Architektur bieten sich zur Implementierung als wieder verwendbarer Softwarebaustein an, was die Entwicklung von RFID-Systemen weiter vereinfachen und das Ergebnis zuverlässiger machen würde. Beispiele sind hier insbesondere Schnittstellen zur RFID-Hardware oder anderen Informationssystemen, aber auch Teile der Clientsoftware.
- **Einführungsmethodik.** Analog zur Einführung eines ERP-Systems oder einem Prozessoptimierungsprojekt umfasst auch die RFID-Einführung eine Reihe von stets ähnlich ablaufenden Aktivitäten, deren Planung und Durchführung von methodischen Werkzeugen wie Ergebnisdokumenten, Checklisten, Rollenbeschreibungen usw. profitieren können.
- **Systemmanagement.** Analog zum herkömmlichen IS-Management benötigt auch der Betrieb eines RFID-Systems Werkzeuge auf technischer und organisatorischer Ebene, z.B. ein Kennzahlensystem, welches die Güte jenes Abbilds der physischen Welt, das RFID generiert, beurteilen hilft. Andere Beispiele sind Best Practices für Betrieb und Wartung, aber auch Softwaretools, die Softwareupdates oder Statusüberwachung der Hardware ermöglichen.

Literatur

[FAH03] Floerkemeier C, Anarkat D, Harrison M, Osinski T (2003) Physical Markup Language (PML) Core Specification. Auto-ID Center, www.epcglobalinc.org/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf

[Goy03] Goyal A (2003) Savant Guide, Auto-ID Center, archive.epcglobalinc.org/publishedresearch/mit-autoid-tr015.pdf

[Kub03] Kubach U (2003) Integration von Smart Items in Enterprise-Software-Systeme. HMD – Praxis der Wirtschaftsinformatik 229: 56–67

Middleware für Ubiquitous-Computing-Anwendungen

Thomas Schoch
Institut für Pervasive Computing, ETH Zürich

Kurzfassung. Middleware für Ubiquitous Computing kommt insofern eine zentrale Rolle zu, als dass sie die Basisdienste für darauf aufbauende komplexe und hochgradig verteilte Applikationen bereitstellt. Basierend auf einer Übersicht zum Thema Middleware im Bereich Ubiquitous Computing werden charakteristische Eigenschaften solcher Middlewaresysteme beschrieben und diskutiert. Um die allgemein relevanten Gesichtspunkte zu verdeutlichen, wird zunächst kurz die Entwicklung von Middleware in klassischen verteilten Systemen dargestellt. Von diesen ausgehend, werden dann die speziellen Anforderungen für Middleware im Ubiquitous Computing erarbeitet. Anschließend wird anhand von mehreren prototypischen Middleware-Systemen, wie beispielsweise Savant, Cooltown oder GaiaOS, exemplarisch gezeigt, welche Ansätze bestehen, um den spezifischen Anforderungen für Ubiquitous-Computing-Systeme gerecht zu werden.

1 Middleware in verteilten Systemen

Middleware für Ubiquitous Computing kann als eine Weiterentwicklung von Middleware für verteilte Systeme [CDK98] aufgefasst werden. Aus diesem Grund wird nachfolgend zunächst der Begriff Middleware in allgemeiner Hinsicht erläutert und die Komponenten, aus denen sich Middleware zusammensetzt, sowie einige klassische Middleware-Systeme vorgestellt. Der Begriff „Middleware“ bezeichnet dabei eine Softwareschicht, die zwischen dem Betriebssystem und der Anwendung angesiedelt ist, und lässt sich am besten anhand einer Analogie einführend erläutern.

Für die Analogie betrachte man Abteilungen eines Unternehmens, die der internen Wertschöpfungskette zuzuordnen sind, wie beispielsweise Einkauf, Produktion und Verkauf. Dort fallen jeweils Aufgaben an, die nicht unmittelbar den Kernaufgaben der jeweiligen Abteilung zuzurechnen sind, sondern vielmehr allgemeine, von den Abteilungen unabhängige Aufgaben darstellen. Dies sind zum Beispiel die Rekrutierung neuer Mitarbeiter oder das Verbuchen von Transaktionen. Typischerweise sind in Unternehmen eigene Abteilungen dafür vorgesehen, wie die Personalabteilung oder die Buchhaltung, die diese Aufgaben als allgemeine Dienstleistungen für die anderen Abteilungen erbringen. Diese Aufteilung liegt unter anderem darin begründet, dass sich die anderen Abteilungen dadurch besser auf ihre Kernaufgaben konzentrieren können, und dass sich durch das Zusammenfassen von allgemeinen Aufgaben diese dann effizienter bearbeiten lassen.

Analog zu diesen Überlegungen wurde Middleware in verteilten Systemen eingeführt. Alle Basisaufgaben, die nicht den eigentlichen Kernaufgaben der Applikationen zuzurechnen sind, werden herausfaktorisiert, um als separate infrastrukturelle Basisfunktionalität angeboten zu werden.

1.1 Einordnung

Wie zuvor angeführt, bezeichnet der Begriff Middleware die Softwareschicht, die zwischen der Betriebssystemsschicht und der Applikationsschicht angesiedelt ist. Während das Betriebssystem dafür zuständig ist, die Ressourcen eines einzelnen Rechners zu verwalten, ist die Middleware dafür zuständig, die Ressourcen in einem Netzwerk zu verwalten. Die Grenzen zwischen der Betriebssystemschicht, der Middlewareschicht und der Applikationsschicht sind allerdings fließend, sodass einige Funktionen nicht eindeutig einer Schicht zuzuordnen sind. Orthogonal zur Einordnung in Schichten können drei Komponenten identifiziert werden, die die Basisfunktionalität der Middleware umsetzen. Zunächst sind das die Protokolle und Sprachen, die definieren, wie verschiedene Teilnehmer in einem Netz miteinander kommunizieren. Des Weiteren gehören dazu die Basisdienste, die größtenteils Verwaltungsaufgaben übernehmen. Schließlich gehören noch Entwicklungswerkzeuge wie Bibliotheken und Compiler zur Middleware, die sowohl während der Programmentwicklung als auch während der Programmausführung nützliche Dienste erbringen. Beispielsweise ermöglichen sie, dass eine Applikation über ein Netz Nachrichten austauschen kann, ohne dass der Entwickler den Nachrichtenversand explizit programmieren müsste. Sowohl die Einteilung in Schichten als auch die Einteilung in drei Komponenten ist in Abbildung 1 dargestellt.

1.2 Komponenten

Zu den Komponenten, die die Basisfunktionen von Middleware umsetzen, gehören Entwicklungswerkzeuge, Protokolle und Sprachen sowie Dienste. Basisfunktionen bezeichnen dabei Funktionen, die unabhängig von der konkreten Applikation allgemein nützliche Dienste verrichten. Zum Teil wird der Begriff Middleware so weit ausgelegt, dass auch andere Applikationen wie Datenbanksysteme dazugezählt werden. Da bei Datenbanksystemen jedoch die effiziente Speicherung und Abfrage von Daten im Vordergrund steht, welche unabhängig davon sind, ob die Datenbank in einem Netz verfügbar ist oder nur lokal auf einem Rechner, rechnen wir diese hier nicht mehr der Middleware zu.

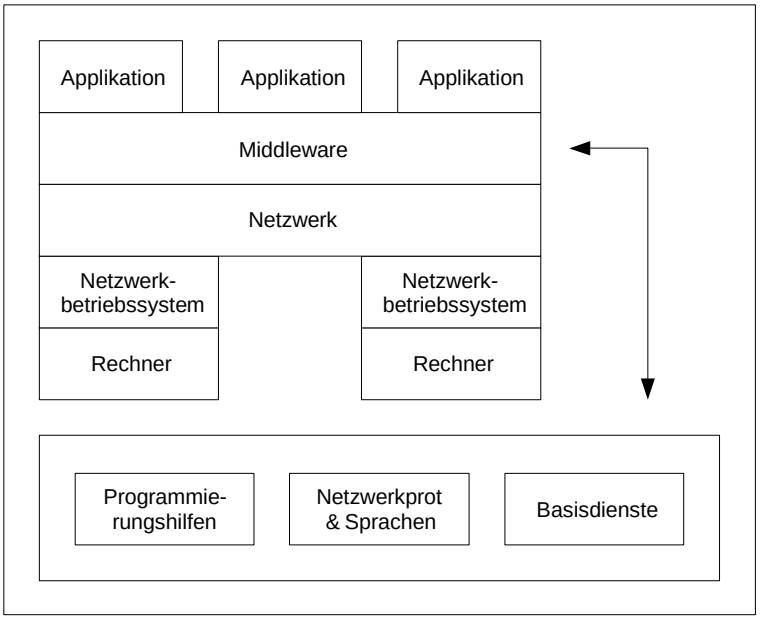


Abb. 1. Schichten und Komponenten von Middleware

Entwicklungswerkzeuge

Bei den Entwicklungswerkzeugen handelt es sich hauptsächlich um Compiler, die den Code zur Unterstützung entfernter Methodenaufrufe automatisch generieren. Ohne diese Compiler müssten Entwickler diesen meist recht umständlichen Code selbst verfassen, was einen höheren Entwicklungsaufwand sowie eine größere Fehleranfälligkeit bedeuten würde. Der automatisch generierte Code, der in die Applikation direkt eingebunden wird, greift zumeist noch auf Programmbibliotheken zurück, die sich mehrere Applikationen auf demselben Rechner teilen können, um über das Betriebssystem auf das Netz zuzugreifen und mit den Middleware-Komponenten auf dem entfernten Rechner zu kommunizieren.

Netzwerkprotokolle und Sprachen

Sowohl Netzwerkprotokolle als auch Sprachen definieren, wie Inhalte in einem Netz in strukturierter Weise übertragen werden können. Während Protokolle eng umgrenzt spezifizieren, wie die Abfolge sowie das Format von auszutauschenden Nachrichten auszusehen haben, bieten Sprachen die Möglichkeit, mit Hilfe einer Grammatik und einem Vokabular komplexere Inhalte zu formulieren, die dann übertragen werden können. Die größere Flexibilität in der Ausdrucksfähigkeit führt aber zu einem höheren Verarbeitungsaufwand. Dementsprechend werden Protokolle meist auf den unteren und Sprachen auf den oberen Kommunikationsebenen verwendet. Prominente Vertreter beider Kategorien sind das Hypertext

Transfer Protocol (http) und die Hypertext Markup Language (HTML). Hierbei definiert http, wie ein Web-Server und ein Web-Browser miteinander kommunizieren. Bei der Kommunikation tauschen sie u.a. Dokumente in HTML aus, die beschreiben, was der Web-Browser anzuzeigen hat. Analog zur Kommunikation von Web-Browsern mit Web-Servern legen Protokolle und Sprachen auch im allgemeinen Fall fest, wie Middleware-Dienste untereinander und mit den Applikationen kommunizieren.

Basisdienste

Den Schwerpunkt von Middleware bilden Basisdienste [ASC00], die ein breites Spektrum an administrativen Aufgaben übernehmen. Nachfolgend wird ein kurzer Überblick gegeben, der die wichtigsten Aufgaben aufzählt:

- **Auflösung von Namen in Adressen.** Der bekannte Domain Name Service im Internet löst einen Rechnernamen wie www.ethz.ch in seine IP-Adresse 129.132.200.35 auf.
- **Registrieren und Auffinden von Diensten.** In einer dynamischen Umgebung müssen sich Klienten und Dienste erst finden. Beispielsweise kann eine Applikation, die ein Dokument zu drucken hat, nach einem Druckdienst suchen.
- **Management und Überwachung von Netzwerkressourcen.** Dies betrifft u.a. Geräte wie Drucker, Router, Switches, aber auch Dienste wie netzwerkweite Dateisysteme. Zu den Managementaufgaben gehört z.B. ein Gerät oder einen Dienst automatisch neu zu starten, wenn ein Fehler festgestellt wurde.
- Bereitstellung von **Sicherheitsfunktionalität**, welche Authentifizierung, Autorisation, Nichtabstreitbarkeit, Integrität und Vertraulichkeit sowie Wahrung der Privatsphäre umfasst.
- **Abrechnungsfunktionen.** Abhängig vom Geschäftsmodell eines Dienstanbieters werden verschiedene Abrechnungsmodelle für seine Dienste benötigt, die beispielsweise auf der Dauer der Nutzung, der Anzahl an Nutzungen oder dem Datenaufkommen beruhen.
- Garantie von so genannten **Quality-of-Service-Kriterien** wie der Bandbreite einer Datenübertragung. Bei einer medizinischen Teleoperation muss beispielsweise die kontinuierliche Übertragung des Videobildes gewährleistet sein.
- **Transaktionsmanagement.** Das Konzept der Transaktionen, welches Gegenstand klassischer Datenbanksysteme ist, wird durch Middleware in verteilter Weise realisiert.
- **Replikation** von Diensten dient zum einen der Ausfallsicherheit eines Dienstes und zum anderen der Bewältigung hoher Lasten. Um einen Dienst zu replizieren, kann eine Middleware generische Protokolle definieren, die die Dienste unterstützen müssen. Die Middleware kann dann mit Hilfe der Protokolle je nach Bedarf Replikate des Dienstes starten oder stoppen.
- **Notifikationen** dienen u.a. dazu, Veränderungen in der realen Welt in der digitalen bekannt zu machen, sodass Applikationen dynamisch auf die Veränderungen in der realen Welt reagieren können. Beispielsweise möchte eine Lagerbewirtschaftungsapplikation über neu eintreffende Ware informiert werden.

- Definition und Durchsetzung von **Policies**. Etliche andere Basisdienste sind auf Policies angewiesen, die definieren, wie der Basisdienst auszuführen ist. Der Sicherheitsdienst benötigt beispielsweise eine Sicherheitspolicy, die u.a. definiert, welche Benutzer Zugriff auf welche Ressourcen erhalten.
- **Verzeichnisfunktionalität.** Etliche Basisdienste sind auf Verzeichnisse angewiesen, in denen sie strukturierte Daten analog einem Telefonbuch ablegen und so indirekt mit anderen Diensten kommunizieren können. Die zuvor genannte Sicherheitspolicy könnte beispielsweise in einem Verzeichnis abgelegt werden.

1.3 Middleware-Systeme

Middleware-Systeme, Middleware-Infrastrukturen und ähnliche Begriffe bezeichnen Softwarepakete, die die zuvor genannte Funktionalität implementieren. Erste Ansätze von Middleware-Systemen entstanden schon zusammen mit den ersten verteilten Systemen. Die Systeme, die nachfolgend vorgestellt werden, beschränken sich auf die prominentesten Vertreter ihrer jeweiligen Klassen, die nachhaltig die Entwicklung von Middleware-Systemen [MaS03] beeinflusst haben.

Klassische Systeme

Als klassische Systeme greifen wir diejenigen Middleware-Systeme heraus, die über die wissenschaftliche Betrachtung hinaus auch Einsatz in kommerziellen Produkten gefunden haben.

Eines der ersten Konzepte war der *Remote Procedure Call* (RPC). Früher mussten Entwickler, wenn sie Code in Form von Prozeduren auf anderen Rechnern ausführen wollten, dieses explizit ausprogrammieren, d.h. eine Kommunikationsverbindung aufbauen, die Prozedur auswählen, die Parameter, die der Prozedur zu übergeben sind, in Nachrichten verpacken und das zurückerhaltene Ergebnis entpacken. Der RPC ist entsprechend der oben diskutierten Einteilung in Komponenten ein Entwicklungswerkzeug: Der Entwickler kann mit Hilfe von RPC entfernte Prozeduren so aufrufen, als ob er eine lokale Prozedur aufruft. Der Mehraufwand wird durch einen Compiler und durch Programmbibliotheken gekapselt. Die prinzipielle Funktionsweise ist in Abbildung 2 dargestellt. Ein bekannter Dienst, der auf einer RPC-Implementierung beruht, ist das Network File System (NFS), welches es ermöglicht, Dateien netzwerkweit zu speichern und abzurufen.

Ein Problem verschiedener RPC-Systeme ist ihre Inkompatibilität bezüglich dem Ver- und Entpacken der Parameter untereinander. Jedes System hat hier sein eigenes Protokoll definiert, wie der Austausch der Parameter stattzufinden hat. Neuere Ansätze wie das *Simple Object Access Protocol* (SOAP) adressieren dieses Problem. SOAP definiert das Datenformat, bzw. das Protokoll, wie ein entfernter Prozedurenaufruf unabhängig von der zugrunde liegenden Plattform auszusehen hat, sodass SOAP-Implementierungen verschiedener Anbieter zusammenarbeiten können.

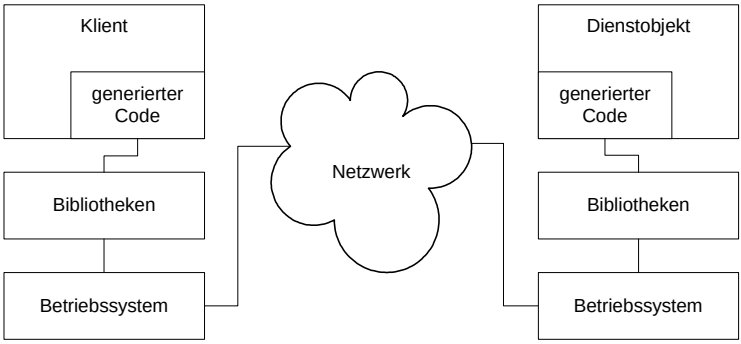


Abb. 2. Prinzipielle Funktionsweise des RPCs

Schon bald nach der Realisierung erster RPC-Systeme wurde die objektorientierte Programmierung populär, welche keine Prozeduren, sondern nunmehr Methoden kennt. Insofern musste das bisherige RPC-Konzept um objektorientierte Konzepte erweitert werden. Die *Remote Method Invocation* (RMI) ermöglicht es Java-Objekten, mit anderen Java-Objekten auf entfernten Rechnern via Methodenaufrufe zu kommunizieren.

Während die zuvor genannten Systeme hauptsächlich die Entwicklungswerkzeuge stellen und einige wenige Protokolle definieren, stellt die *Common Object Request Broker Architecture* (CORBA) eine Erweiterung dieser Systeme dar. Der Broker vermittelt hierbei zwischen Methodenaufrufen von Klienten und deren Ausführung auf einem Dienstobjekt. Daneben werden noch drei Kategorien von Diensten in CORBA definiert: auf unterer Ebene Sicherheits- oder Namensdienste, auf mittlerer Ebene allgemeine Services wie beispielsweise Druckdienste und auf oberer Ebene eher anwendungsspezifische Dienste. Damit CORBA-Systeme verschiedener Anbieter kooperieren können, wurde das General Inter-ORB-Protocol (GIOP) eingeführt, womit Broker diverser Hersteller untereinander in einheitlicher Weise kommunizieren können.

Aktuelle Systeme und Trends

Die Umgebungen, auf welche die klassischen Systeme hin optimiert wurden, sind eher statischer Natur. Das macht sich darin bemerkbar, dass der Ausfall einer Komponente oder das Hinzufügen bzw. das Entfernen eher die Ausnahme als die Regel darstellt. Die aktuellen Trends hingegen weisen darauf hin, dass die Dynamik der Systeme, d.h. das Auftauchen und Verschwinden von Geräten und Diensten, nunmehr als eine Grundannahme zu gelten hat.

Jini [Edw99], eine Middleware-Plattform der Firma Sun Microsystems, nimmt explizit Bezug auf die Dynamik und entwickelt einige Konzepte, um diese zu beherrschen. Jinis Grundannahme ist, dass Geräte, Dienste und Benutzer dynamisch auftauchen und wieder verschwinden und temporäre Föderationen bilden, in denen Klienten Dienste in Anspruch nehmen können. Die zentrale Komponente ist der *Lookup Service*. Bei diesem können sich Dienste registrieren und Klienten

nach Diensten suchen. Da in einer dynamischen Umgebung auch der Lookup Service a priori nicht bekannt ist, müssen Klienten, Dienste und der Lookup Service das *Discovery-Protokoll* implementieren. Dieses ermöglicht, dass der Lookup Service gefunden werden kann. Ein Dienst, der sich beim Lookup Service registrieren möchte, muss das so genannte *Join-Protokoll* implementieren. Ein Klient kann, nachdem er den Lookup Service ausfindig gemacht hat, diesen konsultieren, um einen Dienst anhand mehrerer Parameter auszusuchen. Der Klient erhält als Antwort auf seine Suchanfrage eine Liste so genannter Stellvertreterobjekte. Diese Stellvertreterobjekte kann der Klient nun dynamisch und automatisch in seinen eigenen Code einbinden. Wann immer er Methoden auf dem Stellvertreterobjekt aufruft, wird vom Stellvertreterobjekt automatisch der eigentliche Dienst angefragt und das Ergebnis der Anfrage über das Stellvertreterobjekt dem Klienten zur Verfügung gestellt. Dadurch kann der Klient von der Kommunikation mit dem eigentlichen Dienst abstrahieren, da diese vom Stellvertreterobjekt übernommen wird.

Um darüber hinaus der Dynamik Rechnung zu tragen, müssen alle Ressourcen, die in einer Jini-Föderation genutzt werden, geleast werden. Konkret bedeutet das, dass bevor auf die Ressource zugegriffen werden kann, ein zeitlich begrenztes *Lease* zu beantragen ist. Läuft das Lease ab, ohne dass es verlängert wurde, wird die Ressource wieder freigegeben. Somit ist gewährleistet, dass Einheiten einer Jini-Föderation, die nicht mehr zu erreichen sind, nicht unnötig Ressourcen beanspruchen.

Remote Events sind Jinis drittes Mittel, um der Dynamik zu begegnen. Bei diesem asynchronen Kommunikationsmechanismus wird, wann immer eine Änderung eines überwachten Programmzustands eintritt, derjenige benachrichtigt, der sich zuvor dafür registriert hat.

Die wichtigsten Interaktionsmechanismen – in drei Phasen unterteilt – sind in Abbildung 3 dargestellt.

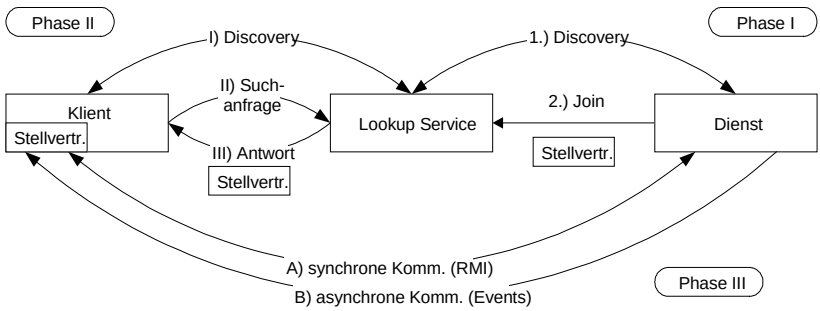


Abb. 3. Drei Phasen in Jini

Web Services, eine weitere Middleware-Plattform, sind insofern mit Jini vergleichbar, als dass auch sie die Möglichkeit bieten, dynamisch Dienste zu registrieren und aufzufinden. Während Jinis Lookup Service jeweils die im lokalen Subnetz verfügbaren Dienste verwaltet, bietet das Web-Service-Pendant, der

„Universal Discovery and Description Interface (UDDI)“-Dienst, die Möglichkeit, Dienste weltweit im Internet anzubieten. Der UDDI-Dienst muss dazu mehrfach repliziert werden, um nicht zum Flaschenhals zu werden. Ein weiterer Unterschied besteht in der zugrunde liegenden Programmiersprache. Während Jini hauptsächlich Java-basiert ist, kann bei Web Services jede Programmiersprache benutzt werden, solange sie das SOAP-Protokoll unterstützt. Der größte Vorteil der Web Services ist die Möglichkeit, Dienste in der Web Service Definition Language (WSDL) zu beschreiben, wohingegen bei Jini hierfür nur proprietäre Attribute genutzt werden können.

Vereinfacht lässt sich sagen, dass dort, wo Geräte im Einsatz sind, die dynamisch auftauchen und verschwinden, Jini eine bessere Unterstützung im Lokalen bietet, wohingegen dynamische Geschäftsanwendungen im Internet mit Web Services besser umzusetzen sind.

Ein Trend der jüngeren Zeit stellt das *Peer to Peer Computing* dar. Hierbei steht die Idee im Vordergrund, ganz ohne zentrale Dienste auszukommen. Jeder Peer ist somit immer Klient und Dienstanbieter in einem. Um die gleiche Funktionalität, z.B. die eines Lookup Services, wie in zentralen Systemen zu bieten, müssen die Peers sich untereinander abgleichen, was meist zu einer schlechteren Performanz im Vergleich zu zentralen Lösungen führt, aber die Systeme prinzipiell ausfallsicherer werden lässt. Getrieben wurde die Entwicklung anfangs hauptsächlich durch den Ansporn, Dateien wie beispielsweise Musikdateien im mp3-Format auszutauschen, ohne einen zentralen Dienst benutzen zu müssen, der wie im Fall Napster abgeschaltet werden kann. Sun widmet sich dem Thema Peer to Peer Computing mit JXTA, welches die grundsätzlichen Protokolle definiert, die in solchen Netzwerken benötigt werden.

Wie die obigen Ausführungen gezeigt haben, lässt sich in der Entwicklung der Middleware für verteilte Systeme ein Trend feststellen, der von der Unterstützung statischer Systeme hin zu dynamischen führt. Eine Ubiquitous-Computing-Middleware setzt diesen Trend fort, indem sie nun stärker die reale Welt mit ihren Benutzern, elektronischen Geräten sowie Alltagsgegenständen fokussiert.

2 Anforderungen an Ubiquitous-Computing-Middleware

Um die verschiedenen Middleware-Systeme für Ubiquitous Computing-Anwendungen evaluieren zu können, sollen zunächst wesentliche Anforderungen hierfür benannt werden. Diese leiten sich aus den Ubiquitous-Computing-Szenarien ab, die in anderen Beiträgen dieses Buches ausführlich besprochen werden.

Ubiquitous-Computing-Szenarien lassen sich in zwei Klassen einteilen, die jeweils einer anderen Unterstützung durch eine Middleware bedürfen. Das Kriterium für die Klassifizierung ist der Einbezug des Benutzers. Im einen Fall ist der Benutzer Mittelpunkt der Szenarien. Der Benutzer selbst sowie die Interaktion mit ihm muss in solchen Szenarien explizit modelliert und durch die Middleware unterstützt werden. Im anderen Fall tritt der Benutzer in den Hintergrund und die Interaktion der Umwelt und der in ihr enthaltenen Objekte untereinander tritt in den Vordergrund. Die erste Richtung bezeichnete Marc Weiser, der Pionier des Ubiquitous Computings, als Phase I des Ubiquitous Computings. In dieser ersten

Phase kommen wie im Mobile Computing [CEM02] hauptsächlich elektronische Geräte wie Mobiltelefone, Laptops oder PDAs zum Einsatz, um den Benutzer bei der Erfüllung seiner Aufgaben zu unterstützen. Der Rückgriff auf eine Sensorik spielt hier eine sekundäre Rolle. In einer möglichen Phase II treten elektronische Geräte in den Hintergrund und die Umgebung und die in ihr enthaltenen Objekte werden „smart", um den Benutzer, möglichst ohne explizite Interaktion mit ihm, bei seinen Aufgaben zu unterstützen. Die meisten Middleware-Projekte im Gebiet des Ubiquitous Computings sind der Phase I zuzuordnen, für die zweite Phase existieren erst einige Ansätze.

Eine Middleware für Ubiquitous Computing sollte die folgenden Anforderungen erfüllen, um die beiden zuvor genannten Klassen zu unterstützen. Die Aufzählung ist zwar nicht als abschließend zu betrachten, zeigt aber auf, welche Aspekte momentan von den diversen Projekten betrachtet werden:

- Überwachung der Umgebung sowie Bereitstellung dieser Informationen, damit Applikationen auf den Zustand der Umgebung zugreifen können.
- Unterstützung von impliziter und expliziter Benutzerinteraktion. Implizite Benutzerinteraktion steht für Benutzereingaben, die unbewusst erfolgen.
- Unterstützung der Migration von Software-Komponenten, um zeitnah vor Ort Berechnungen durchführen zu können.
- Unterstützung der Mobilität physischer Objekte, um ortsbasierte Dienste zu ermöglichen.
- Modellierung relevanter Weltausschnitte, um die Kommunikationsinhalte zu standardisieren.
- Bereitstellen von Kommunikationsverbindungen.
- Mechanismen zur effizienten Verwaltung von Energie, um autarke mobile Geräte möglichst lange funktionsfähig zu halten.
- Integration mit bisheriger Hard- und Software sowie klassischen Middleware-Systemen, um Redundanzen in der Entwicklung zu vermeiden.

Neben diesen Anforderungen an eine Middleware für Ubiquitous Computing im Speziellen sind weiterhin die generellen Anforderungen an eine Middleware für verteilte Systeme im Allgemeinen zu berücksichtigen:

- Gemeinsame Nutzung von Ressourcen, um diese effizienter auszulasten.
- Offenheit bezüglich des Hinzufügens neuer Einheiten.
- Nebenläufigkeit, um Berechnungen effizienter und problemadäquat zu gestalten.
- Skalierbarkeit, damit auch wachsende Systeme leistungsfähig bleiben.
- Fehlertoleranz, damit der Ausfall einzelner Einheiten nicht das gesamte System beeinträchtigt.
- Transparenz, um Entwicklern und Benutzern für sie nicht relevante Komplexität zu verbergen.

Die genannten Anforderungen sollen mit Entwicklungswerkzeugen, Netzwerkprotokollen und Sprachen sowie Basisdiensten umgesetzt werden. Zusätzlich sind noch weitere Aspekte und Entwurfsalternativen für das Design einer Middleware von Interesse. Darunter fällt unter anderem:

- Dezentrale vs. zentrale Architektur
- Synchrone vs. asynchrone Kommunikation
- Aufteilung der Rechenlast zwischen Hintergrundinfrastruktur und lokalem Gerät
- Lokale vs. verteilte Realisierung der Datenspeicherung

3 Aktuelle Middleware-Projekte

Von den nachfolgend skizzierten vierzehn Middleware-Projekten stellt noch keines ein fertiges industrielles Softwareprodukt dar. Vielmehr handelt es sich hierbei um Forschungsprojekte, die sich zum Ziel gesetzt haben, neue Konzepte zu implementieren und diese zu evaluieren. Nicht die Projekte selbst, sondern vielmehr ihre Konzepte bilden den Schwerpunkt der folgenden Ausführungen. Nähere Informationen zu den einzelnen Projekten sind den jeweils angegebenen Projektbeschreibungen zu entnehmen.

3.1 Übersicht

Um einen Eindruck von den derzeit laufenden Aktivitäten zu gewinnen, werden zunächst ausgewählte Projekte vorgestellt und die dahinter stehenden Forschungsgruppen genannt. Bei der Auswahl der Projekte wurde darauf geachtet, dass diese innerhalb der Forschungsgemeinde auf Interesse gestoßen sind und dass insgesamt ein möglichst breites Spektrum an Konzepten abgedeckt wird:

- **Aura** [SoG00], Carnegie Mellon University: Aura setzt sich zum Ziel, die Ablenkung des Benutzers durch Computer zu minimieren. Die Hauptabstraktion stellen Benutzer-Tasks dar, die transparent auf heterogener Hard- und Software ausgeführt werden.
- **Cooltown** [Dan97, KiB01, Kin01, Pra00], HP Invent: Cooltown möchte den sich von Ort zu Ort bewegenden PDA-Benutzer unterstützen. Dazu müssen Web-Technologien erweitert werden, um Pervasive-Computing-Anwendungen zu ermöglichen.
- **EasyLiving** [BMK00, BrS01, MeK00], Microsoft Research: Dieses Projekt setzt sich zum Ziel, Benutzer in so genannten intelligenten Umgebungen zu unterstützen. Dazu werden Benutzer erkannt und verfolgt, sodass automatisch Ein- und Ausgabegeräte vom System ausgewählt werden können.
- **GaiaOS** [RHC02], University of Illinois at Urbana-Champaign: Konzepte aus den Betriebssystemen werden hier auf das Gebiet des Ubiquitous Computing übertragen, um Ubiquitous-Computing-Anwendungen zu unterstützen.
- **Hive** [MGR99], Massachusetts Institute of Technology: Hive ist ursprünglich ein System, welches eine Infrastruktur für mobile Software-Agenten anbietet. Es kann auch eingesetzt werden, um Ubiquitous-Computing-Szenarien zu unterstützen.

- **iWork** [JFW02], Stanford University: Dieses Projekt bietet die nötigen Infrastrukturkomponenten, um die Interaktion mit den diversen Hard- und Softwarekomponenten in einem Sitzungsraum zu vereinfachen.
- **Nexus** [LeK99, NGS01], Universität Stuttgart: Als Erweiterung eines Geoinformationssystems modelliert das Nexus-System statische und dynamische Ortsinformationen von Objekten und deren Umwelt, um ortsbezogene Dienste zu ermöglichen.
- **one.world** [GDL01], University of Washington: Mit den drei Prinzipien Veränderungen explizit zu machen, Applikationen dynamisch zusammenzustellen sowie Daten und Code zu trennen, bietet one.world ein System-Framework für Ubiquitous Computing.
- **ParcTab** [Wei91, Wei93, WSA95], Xerox PARC: Das älteste Projekt, welches vom Ubiquitous-Computing-Pionier Marc Weiser initiiert wurde, betrachtet eine Infrastruktur für Pager-große Kleinstrechner, die auf Raumebene lokalisiert werden können.
- **Raum** [BZD02], Universität Karlsruhe: Dieses Projekt möchte die Kommunikation zwischen smarten Artefakten unterstützen. Um das zu ermöglichen, werden Alltagsgegenstände mit entsprechender Hardware ausgestattet, die einen so genannten „Raum“ aufspannen, in dem zwei Artefakte miteinander kommunizieren können.
- **Savant** [OaS02], Auto-ID Center: Die Middleware des Auto-ID Centers unterstützt das Lesen von RFID-Tags, den Bezug der dazu assoziierten Daten sowie eine Aggregation der Daten, um Firmen u.a. ein effizientes Erkennen und Verfolgen ihrer markierten Produkte zu ermöglichen.
- **Stitch** [AFP03], Xerox Research Centre Europe: Stitch ist eine Middleware, die Ubiquitous-Computing-Anwendungen mit den beiden Konzepten der Ereignisverarbeitung und der verteilten Tupel-Räume unterstützen möchte.
- **Sylph** [CMY02], University of California at Los Angeles: Sylph bietet eine Abstraktionsschicht, um Sensorwerte mittels einer beliebigen Dienstplattform wie Jini anzubieten. Es werden explizit keine Sensornetze, sondern einzelne Sensoren unterstützt.
- **Visum**, Volkswagen: Visum bietet eine Middleware an, um Applikationen Informationen über den Aufenthaltsort sowie den Speicherinhalt von RFID-Tags liefern zu können. Bei Volkswagen wird dieses Produkt bereits erfolgreich eingesetzt.

3.2 Neue Konzepte

Im Folgenden wird aufgezeigt, welche wesentlichen neuen Konzepte die oben skizzierten Projekte bieten, um die Anforderungen und Kriterien, die Middleware für Ubiquitous Computing zu erfüllen hat, umzusetzen.

Bereitstellung von Umgebungsinformationen

Ein Ziel der Überwachung der Umgebung ist, die Menschen in ihr zu erkennen, damit Applikationen diese Informationen nutzen können, um ihre Dienste zu personalisieren. Daneben wird in einigen Projekten Sensorik unterstützt, die allgemeine Daten zu Phänomenen der Umgebung liefern kann.

Während einige Projekte dedizierte Dienste anbieten, bei denen die Umgebungsinformationen abgerufen werden können, sehen andere Projekte nur ein einziges Framework vor, wie Umgebungsinformationen prinzipiell zu behandeln sind. Dabei lässt sich unterscheiden, ob ein einzelner Dienst die Umgebungsinformationen bereithält oder mehrere spezialisierte Dienste dies übernehmen. Im Fall von EasyLiving beispielsweise existieren drei Dienste, die aktuelle Zustandsinformationen zu Benutzer, Umgebung und Netzwerklast bereithalten.

Während ein Teil der Projekte nicht spezifiziert, wie die Dienste die Umgebungsinformationen erheben, sieht der andere Teil explizit Sensormodule in seinen Modellen vor, welche den Diensten die Daten zur Verfügung stellen. Bei der Abfrage der Umgebungsdaten bei den jeweiligen Diensten kann für jedes Datum eine separate Methode vorgesehen sein oder es wird mittels einer Sprache spezifiziert, welches Datum abgefragt werden soll. Die Benutzung einer Sprache ist zwar etwas komplexer, ermöglicht aber eine einfache Erweiterung um weitere Sensormodule. GaiaOS beispielsweise benutzt als Datenabfragesprache prädikatenlogische Formeln.

Auf den Umgebungsinformationen aufbauend, können personalisierte infrastrukturelle Dienste, wie beispielsweise das Context File System von GaiaOS, angeboten werden. Anstatt in klassischen Verzeichnissen werden bei GaiaOS Dateien in Abhängigkeit mehrerer so genannter Kontext-Parameter gruppiert.

Unterstützung von impliziter und expliziter Benutzerinteraktion

Die oben genannten Projekte bieten eine reichhaltige Auswahl neuer Interaktionstechniken. Neben der Sensorik, die im Hintergrund hauptsächlich für implizite Benutzereingaben verantwortlich ist, werden auch neue Eingabegeräte und -techniken unterstützt.

PointRight des iWork-Projekts erweitert beispielsweise das Mouse-Cursor-Konzept. Wird der Cursor über eine Kante einer Anzeige hinaus bewegt, springt er automatisch zur räumlich benachbarten Anzeige, sodass virtuell alle Anzeigen eines Raums eine Einheit bilden. Ähnlich wie die Gerätetreiber eines Betriebssystems kann die Middleware mittels Diensten und Event-Systemen den Zugriff auf die diversen Eingabequellen vereinfachen.

Ein Aspekt, der auch zur Middleware gezählt werden kann, ist die automatische Generierung von Benutzerschnittstellen, welche diese Aufgabe in Abhängigkeit von den aktuell zur Verfügung stehenden Ein- und Ausgabemedien ausführt.

Unterstützung der Migration von Software-Komponenten

Die Mobilität von Software-Komponenten kann in zweierlei Weise charakterisiert werden. Zum einen können Software-Komponenten spontan im Netzwerk auftau-

chen und verschwinden. Zum anderen können sie von einem Rechner zu einem anderen Rechner migrieren.

Um das Auftauchen sowie das Verschwinden von Software-Komponenten zu unterstützen, wird im Allgemeinen auf ähnliche Konzepte wie bei Jini zurückgegriffen. Ein Dienst übernimmt hierbei für gewöhnlich die Funktionalität des Jini Lookup Services, außerdem werden die Prinzipien des Discovery-Protokolls übernommen.

Die Migration von Software-Komponenten sehen die beiden Projekte one.world und Hive vor. In beiden ist neben der Migration auch eine entfernte Kommunikation möglich. Die Frage, ob eine Software-Komponente migriert werden soll oder stattdessen eine entfernte Kommunikation zu erfolgen hat, wird im Einzelfall durch Abwägung zwischen den Kommunikations- und den Migrationskosten entschieden. Eine Migration kann auch dann sinnvoll sein, wenn zu erwarten ist, dass eine Kommunikation wegen zeitweiliger Netzwerkunterbrechungen nicht regelmäßig stattfinden kann.

Unterstützung von Ortsbezug und Mobilität physischer Objekte

Unter physischen Objekten sollen sowohl elektronische Geräte als auch „smarte" Alltagsgegenstände verstanden werden. Wie eingangs erwähnt, werden Hardware-Komponenten meist durch Software-Komponenten gekapselt, sodass für das Auftauchen und das Verschwinden von Hardware-Komponenten die gleichen Mechanismen wie bei den Software-Komponenten genutzt werden können. In Jini ist das beispielsweise so vorgesehen. Damit die stellvertretende Software-Komponente eines Objekts sich bei einem Lookup-Dienst registrieren kann, muss zunächst das Objekt als solches erkannt worden sein. Häufig wird dazu eine zelluläre Überwachung eingesetzt: Für jede Zelle (einem physisch abgegrenzten Gebiet) wird überprüft, welche Objekte sich in ihr befinden. D.h., nachdem ein Objekt physisch registriert wurde, wird es, nachdem die Discovery-Protokolle einen Lookup-Dienst gefunden haben, dort registriert. Aber auch der umgekehrte Weg ist denkbar: Dem Objekt wird die Adresse des Lookup-Dienstes beispielsweise wie in Cooltown mit Infrarot-Beacons mitgeteilt, sodass sich das Objekt direkt an einen Lookup-Dienst wenden kann.

Neben der binären Information, ob ein Objekt angemeldet ist oder nicht, kann dessen genaue Position ebenfalls von Interesse sein. Oft werden auch geometrische, symbolische und hybride Ortsmodelle genutzt, mit denen die Position von Objekten angegeben werden kann. Neben der Modellierung der Ortsangaben ist die eigentliche Lokalisierung der Objekte bedeutend. Während einige der oben genannten Projekte nur eine einzige Methode der Lokalisierung verwenden, gibt es auch Projekte, die von der konkreten Methode abstrahieren und die Ergebnisse verschiedener Lokalisierungssysteme kombinieren und somit Ungenauigkeiten ausgleichen können. Das Raum-Projekt führt dazu beispielsweise den Begriff des Location Stuffings ein: Wenn das zu lokalisierende Objekt nicht selbst in der Lage ist, seine Position in einem Datenpaket anzugeben, kann dies von der Infrastruktur übernommen werden, die das ausgelassene Lokationsfeld im Datenpaket ausfüllt. Das Nexus-Projekt, welches eine Erweiterung von Geoinformationssystemen darstellt, bietet Möglichkeiten der einfachen Erweiterbarkeit und des An-

bietens verschiedener Genauigkeitsgrade – jedes System, das Geoinformationen zu einem abgegrenzten Gebiet anbieten kann und die Nexus-Protokolle implementiert, kann in die Föderation eines Nexus-Systems integriert werden.

Nachdem ein Objekt erkannt wurde, ist es zumeist noch nötig, weitere Informationen über das Objekt in Erfahrung zu bringen. Wenn die Information nicht auf dem Objekt gespeichert ist, muss zumindest ein Bezeichner (ID) des Objekts in Erfahrung gebracht werden. Das Savant-Projekt sieht hier einen Object Name Service vor, der die ID in die Adresse einer Ressource auflöst. Wenngleich diese Auflösung in den meisten Fällen ausschließlich von der ID abhängt, sieht Cooltown weitere Parameter vor, die hier einfließen können, wie beispielsweise der momentane Ort des Objekts.

Da es Objekten nicht immer möglich ist, sich ordnungsgemäß abzumelden, weil z.B. Störungen bei der Kommunikation auftreten oder die Batterie sich ihrem Ende zuneigt, muss dieser Fall eigens behandelt werden. Während in klassischen Middleware-Systemen wie CORBA meist mit Time-outs auf Kommunikationsebene gearbeitet wird, wurden in Jini Leases eingeführt, um Ressourcen entsprechend verwalten zu können. Neben diesen beiden Verfahren nutzt das Gaia-Projekt so genannte Heartbeats: Jede Komponente, die im System registriert ist, muss in einem definierten Intervall Heartbeat-Nachrichten an den Presence Service senden. Falls dies unterbleibt, werden die beanspruchten Ressourcen dieser Komponente freigegeben.

Modellierung

Die Modellierung relevanter Ausschnitte der Welt, d.h. das Festlegen, worüber Aussagen getroffen werden können und welche Zusammenhänge bestehen, ist das Fundament jeder Middleware oder Applikation. Während Versuche, große und allgemeine Bereiche der Welt zu modellieren, aussichtslos erscheinen, lassen sich Teilaspekte hingegen effizient modellieren. Einige der oben genannten Projekte widmen sich diesem Thema nicht explizit, sodass die Semantik statisch in Methoden und Protokollen definiert ist. Andere Projekte definieren ihre eigenen Sprachen, die zumeist auf XML basieren. Hive ist das einzige Projekt, das eine bereits definierte Sprache, die Resource Definition Language (RDF), benutzt. Das Nexus-Projekt versucht, eine möglichst vollständige Weltbeschreibung zu liefern. Es sieht eine generische Klassenhierarchie vor, welche Objekte der realen Welt beschreibt. Der Anwendungsentwickler kann diese Hierarchie um eigene Klassen ergänzen.

Kommunikationsmechanismen

Verantwortlich für das Einrichten von Kommunikationsverbindungen ist das Betriebssystem. Darauf bauen Middleware-Systeme wie RPC, CORBA, SOAP und dergleichen auf. Die hier betrachteten Projekte setzen meistens auf einem dieser Systeme auf, um eine Kommunikation sowohl zwischen der Anwendung mit der Infrastruktur als auch zwischen den Infrastrukturkomponenten selbst zu ermöglichen. Sensoren oder mobile Kleinstrechner sind allerdings kaum in der Lage, solche schwergewichtigen Systeme wie CORBA zu unterstützen. Diese Proble-

matik kann dadurch umgangen werden, dass diese Komponenten einen Stellvertreter („proxy“) in der Infrastruktur haben. Dieser unterstützt zur Komponente hin ein leichtgewichtiges und zur Infrastrukturseite hin ein schwergewichtiges Protokoll wie CORBA.

Neben der Nutzung des Betriebssystems oder eines anderen Middleware-Systems, um Kommunikationsverbindungen einrichten zu können, definieren einige Projekte wie das Raum- und das ParcTab-Projekt ihre eigenen Kommunikationsmechanismen. Diese legen ein eigenes Protokoll fest und verwenden auch eigene Router und Namensdienste sowie Gateways, um Zugriff auf das lokale Netzwerk zu erhalten. Damit wird es auch ressourcenbeschränkten Geräten ermöglicht, diese Protokolle zu implementieren. Insbesondere bei dezentralen Systemen wie dem one.world-System, das ein eigenes Protokoll „Remote Event Passing“ definiert, sind solche Mechanismen notwendig, da eine leistungsfähige Hintergrundinfrastruktur nicht vorhanden ist. Im Aura-Projekt wird von dem zugrunde liegenden Kommunikationssystem durch die Einführung so genannter Connector-Objekte abstrahiert, die beliebige Kommunikationssysteme als Implementierung verwenden können, aber eine einheitliche Schnittstelle nach oben bieten.

Synchrone vs. asynchrone Kommunikation

Synchrone Kommunikation liegt dann vor, wenn sich alle Kommunikationsteilnehmer bezüglich des Nachrichtenaustauschs koordinieren müssen. Beim entfernten Aufruf einer Methode bedeutet das, dass die aufrufende Seite so lange mit der Ausführung des eigenen Programms wartet, bis die aufgerufene Seite die Methode abgearbeitet und das Ergebnis zurückgeliefert hat. Da bei verteilten Methodenaufrufen der Aufrufende länger blockiert ist als bei lokalen Methodenaufrufen, könnte die Wartezeit gegebenenfalls gut anderweitig genutzt werden. Eine Möglichkeit, dieses Problem zu umgehen, ist die Nutzung von Leichtgewichtsprozessen. Während ein Leichtgewichtsprozess wartet, kann ein weiterer solcher Prozess andere Aufgaben übernehmen. Ein gänzlich anderer Ansatz ist die Nutzung von asynchroner Kommunikation, bei der sich Kommunikationsteilnehmer zeitlich nicht koordinieren müssen: Der Sender kann seine Nachricht versenden und direkt nach dem Versand mit der Programmausführung fortfahren. Diese Art der Kommunikation wird hauptsächlich durch so genannte Publish-Subscribe-Systeme implementiert, wie es bei den Remote Events von Jini der Fall ist. Asynchrone Kommunikation wird sowohl zwischen der Anwendung und der Infrastruktur als auch zwischen den Infrastrukturkomponenten selbst verwendet. Das GaiaOS-Projekt führt Event-Kanäle ein, auf die sich Komponenten separat registrieren können. Bereits im System vorgesehen sind Kanäle, die den Betriebssystemen entnommen wurden: der Standardeingabe-, Standardausgabe- und der Fehlerkanal.

In den betrachteten Projekten kommen zumeist sowohl synchrone Kommunikation mittels Methodenaufrufe als auch asynchrone Kommunikation mittels Publish-Subscribe-Systemen parallel zum Einsatz. Insbesondere bei der synchronen Kommunikation wird hier auf klassische Middleware-Systeme zurückgegriffen.

Mechanismen zur effizienten Verwaltung von Energie

Obwohl alle oben eingeführten Projekte mobile Geräte bzw. Sensoren integrieren, gibt es aufseiten der Middleware keine expliziten energiesparenden Vorkehrungen. Zwar kann jedes Gerät seinen eigenen Energieverbrauch optimieren, bzw. können seitens der Infrastruktur die Häufigkeit und die Länge der Zugriffe auf mobile Geräte minimiert werden, doch sind bei bisherigen Projekten sonst keine weiteren Maßnahmen vorgesehen, die beispielsweise auf globaler Ebene versuchen, den Energieverbrauch der einzelnen Einheiten zu balancieren und zu minimieren.

Anforderungen an verteilte Systeme

Gemeinsame Nutzung von Ressourcen, Offenheit, Nebenläufigkeit, Skalierbarkeit, Fehlertoleranz und Transparenz sind allgemeine Anforderungen an Middleware für verteilte Systeme. Die ersten drei Aspekte sind implizit in den spezifischen Anforderungen für Ubiquitous-Computing-Middleware enthalten und werden von den oben aufgeführten Systemen umgesetzt. Die letzten drei Anforderungen werden durch die Systeme nur teilweise erfüllt. Bei der *Skalierbarkeit* liegen bis auf Ausnahmen weder theoretische noch empirische Ergebnisse vor. Da manche Systeme darauf ausgerichtet sind, Ubiquitous-Computing-Anwendungen in abgegrenzten Bereichen wie Besprechungsräumen zu unterstützen und die Anzahl der dort vorhandenen Hard- und Software-Komponenten momentan noch überschaubar ist, stellt sich in diesen Szenarien die Frage bezüglich der Skalierbarkeit nicht in diesem Maße. Anders sieht es hingegen bei Systemen wie Savant aus, das prinzipiell jedes mit einem Transponder versehene Produkt auf der Welt verwalten muss. Auf *Fehlertoleranz* wird üblicherweise nur bedingt eingegangen. Zwar wird eine dynamische Umgebung unterstützt, wo Hard- und Software-Komponenten spontan auftauchen und verschwinden können, aber das Auftreten von Fehlern in der Hintergrundinfrastruktur wird nicht berücksichtigt. Bei der *Transparenz* gab es einen Wandel beim Übergang von klassischen verteilten Systemen hin zu Ubiquitous-Computing-Systemen: Während in klassischen Systemen versucht wurde, die Verteilung transparent zu halten, wird dies in den meisten Ubiquitous-Computing-Systemen nicht gewährleistet, da die Verfügbarkeit einer Ressource an einem bestimmten Ort nicht immer gegeben ist. Vielmehr besteht die Hauptabstraktion nun in einem transparenten Zugriff auf heterogene Hard- und Software.

Dezentrale vs. zentrale Architektur

Der Aspekt der Skalierbarkeit ist verwandt mit der Frage, ob die Architektur dezentral oder zentral ausgelegt ist. In zentralisierten Architekturen besteht die Gefahr, dass eine der zentralen Komponenten zum Flaschenhals wird oder das Gesamtsystem beim Ausfall einer zentralen Komponente zum Erliegen kommt. Zentrale Systeme besitzen andererseits den Vorteil, dass sie einfacher zu verwalten sind, da sowohl Daten als auch der Programmcode zentral vorliegen oder recht effizient zugreifbar sind. Die Entscheidung für eine zentrale oder dezentrale Architektur hängt hauptsächlich davon ab, ob auf eine Hintergrundinfrastruktur zu-

gegriffen werden kann. Wenn eine solche vorhanden ist, besteht die Möglichkeit, zentrale Dienste zu nutzen. Im anderen Fall, wie bei one.world, muss jede Komponente des Systems alle Basisdienste selbst vorhalten. Neben den reinen zentralen und dezentralen Realisierungsmöglichkeiten gibt es solche, die dazwischenliegen. Im Aura-Projekt beispielsweise ist vorgesehen, dass sowohl zu Hause als auch im Büro jeweils ein zentral ausgelegtes Aura-System eingesetzt wird und diese beiden Instanzen sich abgleichen. Generell stellt sich die Frage, ob ein System prinzipiell für den lokalen oder globalen Einsatz ausgelegt ist. Das Savant-System beispielsweise, welches eine baumförmige Hierarchie aufweist, müsste weltweit verfügbar sein im Gegensatz zum iWork-System, das auf einzelne Besprechungsräume ausgelegt ist. Das Visum-System ist zwar im Gegensatz zu Savant auch auf einen globalen Einsatz ausgelegt, es benutzt aber eine zentrale Datenbank.

Unabhängig davon, ob die Architektur zentral oder dezentral ausgelegt ist, kann typischerweise zwischen einer Kernkomponente und diversen Basisdiensten unterschieden werden. Die Aufgabe der Kernkomponente besteht in der Koordination der Basisdienste und den Anwendungen. In dezentralen Systemen werden sowohl die Kernkomponente als auch die Basisdienste von einer einzigen Komponente implementiert.

Verteilung der Rechenlast

Dieses Thema wird zwar in einigen Projekten wie dem ParcTab-Projekt aufgegriffen und es werden auch einzelne Applikationen dementsprechend auf mobile Geräte und die Hintergrundinfrastruktur verteilt, aber es werden keine generischen Mechanismen auf Middleware-Ebene geboten. Hive unterstützt zwar keine generische Verteilung, doch bietet es dafür die Möglichkeit, dass ein Agent beispielsweise von einem ressourcenbeschränkten Gerät in die Hintergrundinfrastruktur migriert.

Realisierung der Datenspeicherung

Wenngleich die eigentliche Speicherung der Daten transparent erfolgen kann und somit nicht von zentralem Interesse ist, wird trotzdem das Konzept der Tupelräume von einigen Projekten aufgegriffen. Tupelräume, welche erstmalig in dem System Linda implementiert wurden [CaG88], dienen der Kommunikation von nebenläufigen Prozessen. Ein Tupel ist eine geordnete Menge von Werten, und ein Tupelraum stellt einen assoziativen Speicher dar, in dem beliebige Prozesse Tupel einfügen, lesen und löschen können. Dieses Konzept lässt sich auf verteilte Systeme oder Ubiquitous-Computing-Systeme übertragen. Verschiedene Dienste oder Geräte greifen dabei auf einen Tupelraum zu, der entweder verteilt oder zentral realisiert ist. Ansonsten wird in den anderen Projekten, die keine Tupelräume verwenden, größtenteils auf klassische Datenbanksysteme zurückgegriffen.

Innovative Ansätze

Eine prinzipiell andere Architektur im Vergleich zu den klassischen Client-Server-Architekturen verfolgen u.a. one.world und Hive. one.world-Applikationen bestehen aus Komponenten, die rekursiv Environments enthalten können. Ein Environment kann Tupelräume enthalten und kommuniziert diese Tupel ausschließlich über Event Handler. Hive ist ein Agentensystem, in dem die Agenten zwischen Zellen migrieren und über Zellen hinweg kommunizieren können. Shadows abstrahieren dabei den Zugriff auf Ressourcen; auf sie kann ein Agent nur lokal zugreifen.

Neuartige Konzepte innerhalb einer Architektur bieten u.a. Gaia, iWork und Cooltown. Gaia führt das Context File System ein. Im Gegensatz zu klassischen Dateisystemen werden hier Dateien abhängig von diversen Umgebungsparametern, wie erkannter Benutzer und dessen Absichten, aufgeführt. iWork bietet mit dem DataHeap einen Dienst, der eine automatische Konvertierung von Daten zwischen verschiedenen Formaten vornimmt. Wenn beispielsweise ein Web-Browser eine Powerpoint-Präsentation anfordert, wird diese automatisch in ein Grafikformat umgewandelt, das der Web-Browser unterstützt. Cooltown schließlich führt das E-Squirt-Konzept ein, welches es ermöglicht, dass ein Benutzer mit einem PDA oder einem ähnlichen Gerät URLs aufsammeln und diese in ein physisch benachbartes Gerät elektronisch „spritzen“ kann, das dann die mit der URL bezeichnete Ressource anzeigt oder für andere Zwecke nutzt.

Basisdienste

Während Middleware-Systeme für Ubiquitous Computing auf den meisten Basisdiensten für verteilte Systeme aufbauen können oder diese selbst anbieten, bleibt insbesondere offen, wie die Quality-of-Service- sowie Sicherheitsfunktionalität in diesen Systemen umgesetzt werden soll. Bezüglich Quality of Service gibt es lediglich im Aura-Projekt erste Ansätze. Dort werden Vorhersagemodelle für den Netzwerkverkehr implementiert und evaluiert, um mobile Anwender samt ihren Anwendungen an Orte zu lotsen, wo noch ausreichend Netzwerkbandbreite zur Verfügung steht. Sicherheitskonzepte sind erst in jüngster Zeit in die Betrachtung mit einbezogen worden, Ergebnisse stehen noch aus.

Unterstützung des Entwicklers

Möglichkeiten, den Entwickler bei seiner Arbeit zu unterstützen, bestehen hauptsächlich darin, Software-Patterns, Skriptsprachen oder so genannte Application Frameworks anzubieten, die auf die besonderen Bedürfnisse des Ubiquitous Computing eingehen. Diese drei Aspekte sind klassisch eher dem Software Engineering als der Middleware zuzuordnen. Da im Bereich des Ubiquitous Computing das Software Engineering noch kein eigenes Themengebiet darstellt, können diese Aspekte hier jedoch mit in die Middleware-Betrachtung einbezogen werden.

Das Gaia-Projekt erweitert das klassische Model-Controller-View-Pattern zum Model-Controller-Presentation-Coordinator-Pattern. Das Teilkonzept „Presentation“ ist eine Verallgemeinerung des View-Teilkonzeptes, welches nun explizit multimodale Ein- und Ausgaben einbezieht, die häufig in Ubiquitous-Computing-

Szenarien Anwendung finden. Der neu hinzugekommene Coordinator ist dafür zuständig, dynamisch die drei anderen Teile den momentanen Anforderungen der Umgebung entsprechend zu kombinieren. Beispielsweise kann sich die Eingabequelle ändern, wenn sich ein Benutzer von einem PC zu einem Touchscreen bewegt. Eine eigene Skriptsprache dient dazu, die einzelnen Komponenten des neuen erweiterten Modells zu instanziieren und zu verbinden. one.world führt das Logic/Operation-Pattern ein, welches besagt, dass eine Operation-Komponente im Gegensatz zu einer Logic-Komponente fehlschlagen kann und somit zusätzlicher Fehlerbehandlungsroutinen bedarf. In Stitch ermöglicht ein Produktionensystem, wie aus der künstlichen Intelligenz bekannt, Aktionen in Form von Logikbasierten Regeln zu spezifizieren, die die sonst übliche objektorientierte Programmierung ersetzen.

Integration mit klassischen Systemen

Die Integration mit existierenden Systemen ist ein eher pragmatischer Aspekt, da bei der Einführung eines neuen Middleware-Systems nicht davon auszugehen ist, dass sämtliche bisherigen Anwendungen ersetzt oder auf das neue Middleware-System hin angepasst werden können. Bei der Integration mit bestehenden Systemen sind drei Entwicklungsrichtungen auszumachen. Im einfachsten Fall wird eine Integration mit bisherigen Systemen nicht explizit unterstützt und es bleibt dem Anwendungsentwickler überlassen, wie er bisherige Applikationen mit dem Middleware-System verbindet. Der zweite Fall bezieht sich auf die Integration von Applikationen eines bestimmten Bereichs. So unterstützen beispielsweise etliche Systeme Benutzer in Besprechungen, wobei eine Integration hauptsächlich mit Web-Browsern sowie Präsentationsprogrammen stattfindet. Im letzten und allgemeinen Fall besteht die Möglichkeit der Integration mit beliebigen Programmen. Bei Aura beispielsweise wird der Benutzer bei beliebigen Aufgaben unterstützt. Dabei spezifiziert eine Aufgabe nicht, welches Programm oder konkrete Hardware-Modul genutzt werden soll, sondern was die Aufgabe verrichten soll. Applikationen werden durch so genannte Service Supplier gekapselt und dynamisch vom Aura-System instanziiert.

Da der Zugriff auf die Hardware meistens durch Dienste oder andere Software-Einheiten gekapselt wird, läuft die Integration von verschiedenen Hardware-Einheiten auf die Integration der kapselnden Dienste hinaus, was wiederum eine Software-Integration bedeutet. Bezüglich der Integration mit bisherigen Middleware-Systemen ist festzustellen, dass die meisten Projekte auf Middleware-Systeme wie RMI oder CORBA zurückgreifen, die entfernte Methodenaufrufe erlauben. Sylph geht noch einen Schritt weiter, indem es erlaubt, von dem eingesetzten Discovery-System, wie z.B. Jini, zu abstrahieren.

4 Fazit

Die typischen Anforderungen an Middleware für Ubiquitous Computing wurden von den vierzehn betrachteten Systemen weitgehend adressiert. Einige Aspekte, wie die effiziente Verwaltung der Energie, die Verteilung der Rechenlast, Fehler-

toleranz, Quality of Service und Sicherheitsaspekte wurden bisher jedoch noch nicht oder nur ansatzweise untersucht, sodass hierzu noch Forschungsbedarf besteht.

Die Konzepte, die in Jini bereits vor einigen Jahren vorgestellt und implementiert wurden, sind in den meisten neueren Projekten in gleicher oder ähnlicher Form wiederzufinden. Das betrifft das zugrunde liegende Client/Server-Paradigma, die synchrone Kommunikation über entfernte Methodenaufrufe, die asynchrone Kommunikation mittels Remote Events, das Leasing zur Freigabe von nicht mehr benötigten Ressourcen sowie die Discovery- und Lookup-Protokolle zum Verwalten von spontan auftretenden und verschwindenden Diensten und Geräten. Umgekehrt lässt sich sagen, dass Jini etliche der Anforderungen an eine Ubiquitous-Computing-Middleware recht gut erfüllt und sich eine Ubiquitous-Computing-Middleware daher relativ leicht auf Jini oder ähnlichen Plattformen aufbauen lässt. Sylph geht hier sogar noch einen Schritt weiter, indem es von der konkreten Dienst-Middleware abstrahiert und auf einer beliebigen Dienst-Middleware aufbauen kann. Ist hingegen eine dezentrale Architektur vonnöten, die vom Client/Server-Paradigma abweicht, ist Jini oder eine ähnliche Plattform weniger hilfreich und es lohnt sich, die Konzepte der Projekte one.world und Hive näher zu betrachten und auch die aktuellen Forschungsergebnisse zu Peer-to-Peer-Computing mit einzubeziehen. Um Doppelentwicklungen gleichartiger Konzepte zu vermeiden, empfiehlt es sich, auf höhere Middleware-Systeme aufzusetzen. Interessant ist auch das Service-Supplier-Konzept des Aura-Projekts, mit dem bisherige Applikationen integriert werden.

Eine der wichtigsten Umgebungsinformationen ist der Aufenthaltsort von Benutzern und Objekten. Hier kommen in den Projekten verschiedene Lokalisierungsmethoden sowie Ortsmodelle zum Einsatz, die noch in der Praxis unter realen Bedingungen zu evaluieren sind. Allgemein lässt sich für Umgebungsinformationen sagen, dass diese recht gut mit Publish-Subscribe-Systemen kommuniziert werden können. Ein grundlegendes Problem, das mit den diversen Umgebungsinformationen einhergeht, ist die Modellierung des Kontextbereichs. Es wäre vermessen, große Teile der realen Welt mit ihren vielfältigen Abhängigkeiten modellieren zu wollen. Vielmehr sollten ganz pragmatisch nur relevante Aspekte der Welt modelliert werden, wie es bereits im Falle des Ortsbezugs gemacht wird [ChK00].

Wenngleich die Betrachtung von Sensornetzen hier außen vor gelassen wurde, ist davon auszugehen, dass die Bedeutung von Sensornetzen in der Forschung als auch in der Industrie stetig wachsen wird und in der nahen Zukunft Resultate in der Forschung zu Middleware für Sensornetze zu erwarten sind. Ebenfalls abzuwarten sind die Ergebnisse von Bestrebungen großer Software-Anbieter, eine Middleware zu schaffen, die smarte Gegenstände, z.B. eintreffende Warenlieferungen, automatisch erfasst und mit bestehenden Enterprise-Systemen verbucht.

Der vorliegende Beitrag hat versucht, die neuartigen Konzepte herauszuarbeiten, die nötig sind, um den Anforderungen an eine Ubiquitous-Computing-Middleware gerecht zu werden und die in aktuellen Projekten zum Teil bereits prototypisch realisiert sind. Jedes einzelne dieser Konzepte ist zwar nicht revolutionär, aber die Strukturierung sowie die Summe der Konzepte macht deutlich, was es bei der aktuellen Entwicklung von Middleware für Ubiquitous Computing zu beachten gilt.

Literatur

[AFP03] Arregui D, Fernström C, Pacull F, Rondeau G, Williamowski J (2003) Stitch: Middleware for Ubiquitous Applications. Proceedings of sOc'2003 (Smart Objects Conference 2003), www.grenoble-soc.com/proceedings03/Pdf/55-Arregui.pdf

[ASC00] Aiken B, Strassner J, Carpenter B, Foster I, Lynch C, Mambretti J, Moore R, Teilbaum B (2000) A Report of a Workshop on Middleware. RFC 2768

[BMK00] Brumitt B, Meyers B, Krumm J, Kern A, Shafer S (2000) EasyLiving: Technologies for Intelligent Environments. Proceedings of the 2nd International Symposium on Handheld and Ubiquitous Computing, pp 12–27

[BrS01] Brumitt B, Shafer S (2001) Topological World Modeling Using Semantic Spaces. Proceedings of the Workshop on Location Modeling for Ubiquitous Computing, pp 55–62, www.teco.edu/locationws/final.pdf

[BZD02] Beigl M, Zimmer T, Decker C (2002) A location model for communicating and processing of context. Personal and Ubiquitous Computing 6(5-6): 341–357

[CaG88] Carriero N, Gelernter D (1988) Applications experience with Linda. Proceedings of the ACM Symposium on Parallel Programming 23, S 173–187

[CEM02] Carpa L, Emmerich W, Mascolo C (2002) Middleware for Mobile Computing. Advanced Lectures on Networking, Networking 2002 Tutorials. Springer-Verlag, pp 20–58

[ChK00] Chen G, Kotz D (2000) A Survey of Context-Aware Mobile Computing Research. Dartmouth Computer Science Technical Report, TR2000-381

[CMY02] Chen A, Muntz R, Yuen S, Locher I, Park S, Srivasta M (2002) A Support Infrastructure for the Smart Kindergarten. IEEE Pervasive Computing 1(2): 49–57

[CDK98] Coulouris G, Dollimore J, Kindberg T (1998) Distributed Systems – Concepts and Design. Addison-Wesley

[Dan97] Daniel R (1997) A Trivial Convention for Using HTTP in URN Resolution. RFC 2169

[Edw99] Edwards W (1999) Core Jini. Prentice Hall

[GDL01] Grimm R, Davis J, Lemar E, MacBeth A, Swanson S, Gribble S, Anderson T, Bershad B, Boriello G, Wetherall D (2001) Programming for Pervasive Computing Environments. University of Washington Technical Report, UW-CSE-01-06-01

[JFW02] Johanson B, Fox A, Winograd T (2002) The Interactive Workspaces Project: Experiences with Ubiquitous Computing Rooms. IEEE Pervasive Computing 1(2): 67–75

[KiB01] Kindberg T, Barton J (2001) A Web-Based Nomadic Computing System. Computer Networks 35(4): 443–456

[Kin01] Kindberg T (2001) Ubiquitous and contextual identifier resolution for the real-world wide web. HP Labs Technical Report, HPL-2001-95R1

[LeK99] Leonhardi A, Kubach U (1999) An Architecture for a Distributed Universal Location Service. Proceedings of the European Wireless '99 Conference, pp 351–355

[MaS03] Mattern F, Sturm P (2003) From Distributed Systems to Ubiquitous Computing - The State of the Art, Trends, and Prospects of Future Networked Systems. In: Irmscher K, Fähnrich KP (Hrsg) Conference Proceedings der Fachtagung Kommunikation in Verteilten Systemen. Springer-Verlag, S 3–25

[MeK00] Meyers B, Kern A (2000) <Context-Aware> schema </Context-Aware>. CHI Workshop on the What, Who, When, Where, Why, and How of Context-Awareness, www.cc.gatech.edu/fce/contexttoolkit/chiws/Meyers.doc

[MGR99] Minar N, Gray M, Roup O, Krikorian R, Maes P (1999) Hive: Distributed Agents for Networking Things. Proceedings of the First International Symposium on Mobile Agents, pp 118–129

[NGS01] Nicklas D, Grossmann M, Schwarz T, Volz S, Mitschang B (2001) A model-based, open architecture for mobile, spatially aware applications. In: Jensen C, Schneider M, Seeger B, Tsotras V (eds) Proceedings of the 7th International Symposium on Spatial and Temporal Databases, pp 117–135

[OaS02] OatSystems (2002) The Savant – Version 0.1 (Alpha). Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-003.pdf

[Pra00] Pradhan S (2000) Semantic Location. Personal and Ubiquitous Computing 4(4): 213–216

[RHC02] Román M, Hess C, Cerqueria R, Ranganat A, Campbell R, Nahrstedt K (2002) Gaia: A Middleware Infastructure to Enable Active Spaces. IEEE Pervasive Computting 1(4): 74–83

[SoG00] Sousa J, Garlan D (2000) Aura: An Architectural Framework for User Mobility in Ubiquitous Computing Environments. Software Architecture: System Design, Development, and Maintenance. Conference Proceedings of the 3rd Working IEEE/IFIP Conference on Software Architecture, Montreal, pp 29–43

[SuM03] Sun Microsystems (2003) JXTA v2.0 Protocols Specification, spec.jxta.org/nonav/v1.0/docbook/JXTAProtocols.html

[WSA95] Want R, Schilit B, Adams N, Gold R, Peterson K, Goldberg D, Ellis J, Weiser M (1995) The ParcTab Ubiquitous Computing Experiment. Xerox Palo Alto Research Center Technical Report, CSL 95-1

[Wei91] Weiser M (1991) The computer for the 21st century. Scientific American 256(3): 94–104

[Wei93] Weiser M (1993) Some computer science issues in ubiquitous computing. Communications of the ACM 36(7): 75–85

Teil C: Anwendungen

Einsatz von RFID in der Bekleidungsindustrie – Ergebnisse eines Pilotprojekts von Kaufhof und Gerry Weber

Christian Tellkamp
Institut für Technologiemanagement, Universität St. Gallen

Uwe Quiede
Kaufhof Warenhaus AG, Köln

Kurzfassung. Der Einsatz von RFID in der Bekleidungsindustrie ist eine der am meisten diskutierten Anwendungen von RFID im Einzelhandel. Im Gegensatz zum Lebensmitteleinzelhandel, bei dem Händler im ersten Schritt im Wesentlichen die Nutzung von RFID auf Karton- und Palettenebene forcieren, wird bei Kleidung konkret über den Einsatz von RFID auf Produktebene nachgedacht. RFID bietet eine Reihe von Nutzenpotenzialen in der Lieferkette bis hin zum Ort des Verkaufs und darüber hinaus. Derzeit befinden sich die meisten Anwendungen allerdings noch in einem Pilotstadium.

Die Kaufhof Warenhaus AG hat in Zusammenarbeit mit dem Bekleidungshersteller Gerry Weber International AG ein RFID-Pilotprojekt durchgeführt. Der vorliegende Beitrag beschreibt die Zielsetzung und Durchführung des Projekts, die betrachteten Anwendungsszenarien, die gewonnenen Erkenntnisse, die betriebswirtschaftlichen Potenziale sowie das geplante weitere Vorgehen. Ausgehend von diesen Erfahrungen werden die Chancen für die weitere Verbreitung von RFID in der Bekleidungsindustrie diskutiert.

1 Einleitung

Die textile Wertschöpfungskette kann in die vier Stufen Faserindustrie, Textilindustrie, weiterverarbeitende Industrie und Handel unterteilt werden, wie in Abbildung 1 dargestellt [CCG02]. Zwischen den einzelnen Stufen finden Transportaktivitäten statt, die zum Teil von externen Dienstleistern erbracht werden. Der vorliegende Beitrag zum Einsatz von RFID in der Bekleidungsindustrie befasst sich mit dem Teil der Wertschöpfungskette vom Produzenten zum Einzelhandel. Der Fokus liegt dabei auf dem physischen Fluss eines fertigen Kleidungsstücks vom Lager des Herstellers bis zum Verkauf der Ware an der Kasse der Verkaufsstelle.

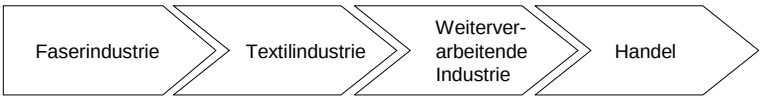


Abb. 1. Stufen der textilen Wertschöpfungskette

Wie in anderen Bereichen des Handels spielt auch in der Bekleidungsindustrie das Thema Supply Chain Management eine wichtige Rolle. Für nachbestellbare Standardartikel gilt es, eine hohe Produktverfügbarkeit auf der Verkaufsfläche bei niedrigen Kosten zu gewährleisten. Aufgrund der Nachfrage am Point-of-Sales werden Nachbestellungen ausgelöst („Pull-Konzept“). Für modische Artikel ist ein Nachschub im Allgemeinen nur beschränkt möglich. Hier kann der Händler bisher oftmals nur eine einmalige Bestellung platzieren oder ggf. die Ware innerhalb eines kurzen Zeitfensters nachbestellen. Letztlich determiniert die Entscheidung des Herstellers, wie viel er von einem Produkt herstellt, und die Entscheidung des Händlers, wie viel er davon abnimmt, was Konsumenten im Laden kaufen können („Push-Konzept“). Eine schematische Darstellung von Pull- und Push-Konzept findet sich in Abbildung 2 [CCG02].

Für modische Artikel ist die Unsicherheit bezüglich der tatsächlichen Nachfrage beträchtlich, und Nachfrageprognosen kommt eine große Bedeutung zu [Lee02]. Verschiedene Händler und Produzenten versuchen deshalb, die Prognose auf Basis der ersten Verkaufszahlen zu aktualisieren und erst dann die endgültige Produktionsmenge festzulegen. Dies setzt allerdings voraus, dass Produktion und Logistik entsprechend flexibel sind. Derzeit sind insbesondere vertikal integrierte Unternehmen wie Inditex, bekannt u.a. für die Marke Zara, dazu in der Lage [Bon02, FRM00].

Insbesondere für Basisartikel sind die Gegebenheiten und Herausforderungen im Supply Chain Management ähnlich denen für den Einzelhandel im Generellen. In der Bekleidungswirtschaft finden viele der Konzepte z.B. des Efficient Consumer Response (ECR) Anwendung. Der Einsatz von Barcodes ist ebenfalls weit verbreitet. Es gibt allerdings einige spezifische Faktoren, die die Bekleidungswirtschaft z.B. vom Lebensmittelhandel unterscheiden und die aus unserer Sicht relevant sind:

- Hohe Variantenvielfalt
- Hoher Anteil saisonaler Produkte
- Weite Verbreitung von Lagerhaltung im Laden
- In der Regel vergleichsweise hoher Preis und hohe Marge
- Erhöhte Diebstahlproblematik
- Relativ hohe Umtauschhäufigkeit

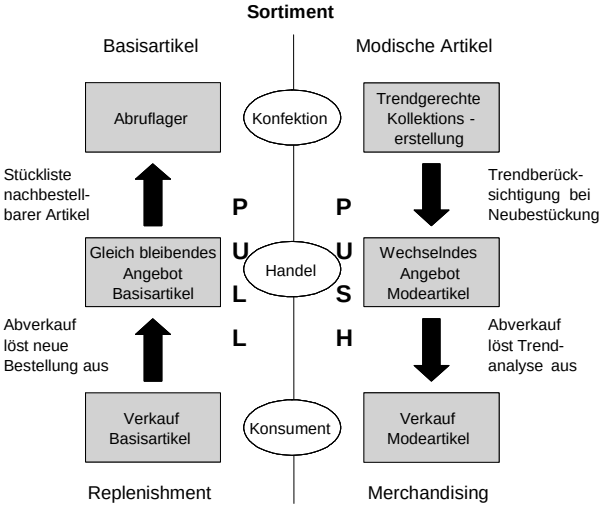


Abb. 2. Pull- und Push-Konzept

Die genannten Faktoren haben eine Reihe von Implikationen für die Lieferkette der Bekleidungsindustrie:

- Hersteller und Händler streben an, modische Artikel so schnell wie möglich in die Verkaufsstelle auszuliefern. Verzögerungen z.B. beim Transport können zu Umsatzeinbußen führen.
- Für modische Artikel und Basisartikel gilt, dass die Ware (soweit vorhanden bzw. lieferbar) immer auf der Verkaufsfläche sein soll und der Kunde die Ware dort auch finden muss. Dies betrifft nicht zuletzt Produkte, für die es eine Lagerhaltung in der Verkaufsstelle gibt. Sind Produkte nicht auf der Verkaufsfläche zu finden, drohen Einzelhändler und Hersteller Umsatzverluste. Bei modischen Artikeln besteht das Risiko, dass Ware überhaupt nicht oder nur zu einem reduzierten Preis verkauft werden kann.
- Die Kommissionierung findet häufig auf Einzelproduktebene statt und nicht auf Karton- oder Palettenebene. Dieser Prozess ist aufwendig und tendenziell fehleranfällig, insbesondere bei manueller Kommissionierung.
- Die Vermeidung von Diebstahl hat eine hohe Priorität für Hersteller und Händler.

Nicht zuletzt aufgrund dieser spezifischen Rahmenbedingungen wird in der Bekleidungswirtschaft der Einsatz von RFID nicht nur auf Karton-, sondern auch auf Produktebene diskutiert. Es gibt eine Reihe von Studien, die hier beträchtliche finanzielle Potenziale sehen (z.B. [Byr03, IBM02]). Für den Einsatz von RFID auf Produktebene sprechen zudem die physikalischen Eigenschaften von Kleidungsstücken: Das Lesen von RFID-Tags durch Stoff – unabhängig, ob es sich dabei um Natur- oder Kunstfasern handelt – ist in der Regel unproblematisch. Im Unterschied zu vielen anderen Produkten im Einzelhandel sind deshalb bei Kleidungsstücken häufig sehr gute Leseraten bei der Pulkerfassung erreichbar.

2 RFID in der Bekleidungsindustrie

2.1 Nutzenpotenziale

RFID bietet eine Reihe von Vorteilen in der Wertschöpfungskette der Bekleidungsindustrie. Eine generelle Darstellung der Nutzenpotenziale von RFID im Einzelhandel gibt der Beitrag von Tellkamp und Haller an anderer Stelle in diesem Buch. Vertieft wird hier deshalb nur auf einige für die Bekleidungsindustrie besonders relevante Anwendungsmöglichkeiten eingegangen.

Effizienzvorteile bei Wareneingang und -ausgang

Auf *Karton- oder Umverpackungsebene* liegen die Vorteile von RFID insbesondere in der schnelleren Erfassung des Wareneingangs und -ausgangs beim Hersteller, im Verteilzentrum und in der Verkaufsstelle. Manuelle Erfassungen der Liefermenge auf Kartonebene können weitgehend entfallen. In Verbindung mit elektronischen Lieferavisen kann RFID dazu genutzt werden, automatische Lieferabgleiche durchzuführen. Elektronische Lieferavis unterstützen die rechtzeitige Planung z.B. von Transportaufträgen, was zu einer Verringerung der Durchlaufzeit von Ware führen kann. Dies ist insbesondere bei Aktionsware und modischen Artikeln relevant. Mit Hilfe von RFID können Lieferavis auf Basis der tatsächlich ausgelieferten Ware erstellt werden. Diese kann unter Umständen von der geplanten Auslieferungsmenge laut Lagerverwaltungssystem abweichen, z.B. wenn Fehler bei der Kommissionierung oder unvorhergesehene Verzögerungen im Prozess aufgetreten sind. Darüber hinaus erlaubt RFID eine effiziente Verfolgung der physischen Lieferung und hilft dabei, Differenzen zwischen dem geplanten und dem tatsächlichen Status einer Lieferung aufzudecken [Ott03].

In einzelnen Fällen kann RFID auch dazu beitragen, die Transparenz im Lager zu erhöhen, wodurch unter Umständen Lagerbestände reduziert und/oder der Liefergrad erhöht werden kann. Darüber hinaus wird das Risiko reduziert, dass Ware unverkäuflich wird, weil sie nicht auffindbar ist. Der Aufwand für manuelle Inventuren kann reduziert werden, wenn die aktuellen physischen Bestände, z.B. mittels mobiler RFID-Leser, ermittelt werden können. Werden RFID-Tags auf Umverpackungsebene eingesetzt, gilt dies allerdings nur, solange die Umverpackungen noch nicht aufgebrochen wurden.

Vermeidung von Kommissionierfehlern und Reduzierung des Kontrollaufwands für Lieferungen

Bei Kleidungsstücken findet die Kommissionierung für die Verkaufsstellen, wie bereits erwähnt, häufig auf *Produktebene* statt. Mittels RFID-Tags können Kommissionierfehler weitgehend vermieden werden. Eine manuelle Lieferkontrolle durch den Hersteller und/oder Händler kann dann unter Umständen entfallen. Die Einsparungen bei Lieferkontrollen sind besonders hoch für Ware, die bereits beim Hersteller kommissioniert wird, da in diesen Fällen jedes einzelne Kleidungsstück erfasst werden muss.

Effizienteres Bestandsmanagement im Laden

Im Laden besteht die Möglichkeit, mittels RFID ein effizientes Bestandsmanagement zu realisieren. Mit Hilfe eines RFID-Lesers am Übergang zwischen Lager und Verkaufsfläche kann automatisch erfasst werden, welche Kleidungsstücke vom Lager auf die Verkaufsfläche gebracht werden. Derzeit ist eine Unterscheidung bei der Bestandsführung zwischen Ware im Lager und Ware auf der Verkaufsfläche nicht möglich, da die entsprechende Datenerfassung, z.B. mittels Scannen der Barcodes durch Mitarbeiter, zu aufwendig ist.

Beim Kauf eines Kleidungsstücks verringert sich der Bestand auf der Verkaufsfläche. Wird ein kritischer Wert unterschritten, kann nun eine Nachbefüllung aus dem Lager automatisch angestoßen werden. Bislang war man hier darauf angewiesen, dass Mitarbeiter regelmäßig die Bestände kontrollieren, um ggf. neue Ware aus dem Lager auf die Verkaufsfläche zu bringen.

Werden zusätzlich noch mobile oder stationäre Leser im Verkaufsraum eingesetzt, besteht die Möglichkeit einer automatischen Inventur. Im Fall stationärer Leser, die in Regale integriert sind, spricht man häufig von „Smart Shelves“. Inventurdifferenzen, d.h. Abweichungen zwischen dem physischen Bestand und dem Bestand laut Informationssystem, können so zeitnah aufgedeckt und korrigiert werden.

Zudem kann das System dazu verwendet werden, Produkte auf der Verkaufsfläche aufzufinden. So lässt sich genau ermitteln, ob ein bestimmtes Produkt noch verfügbar ist. Mit Hilfe mobiler oder stationärer Leser können diese Produkte sogar relativ genau lokalisiert werden. Dies kann z.B. hilfreich sein, wenn ein Kunde ein Kleidungsstück einer bestimmten Größe in einem Stapel sucht.

Vermeidung von Diebstahl

Derzeit werden bereits vielfach elektronische Diebstahlsicherungsetiketten auf Kleidungsstücken eingesetzt, die auf Hochfrequenztechnologie basieren. Anders als RFID-Tags enthalten diese Etiketten jedoch keine Nummer, die eine Identifikation und damit Unterscheidung einzelner Produkte ermöglicht. Auf RFID-Technologie basierende Systeme können wie herkömmliche elektronische Artikelsicherungssysteme (EAS-Systeme) eingesetzt werden. Das RFID-Tag erfüllt damit zwei Funktionen: Es dient sowohl der Identifikation als auch der Warensicherung. Separate Diebstahlsicherungen können entfallen.

Darüber hinaus bietet das RFID-Tag noch weitere Vorteile gegenüber herkömmlichen Diebstahlsicherungen. In Verbindung mit Smart Shelves kann zeitnah erfasst werden, wann und wo welche Kleidungsstücke verschwunden sind. Eine Analyse dieser Daten kann dazu dienen, geeignete Gegenmaßnahmen zu entwickeln, um zukünftigen Diebstahl zu verhindern. Bei einer eindeutigen Identifikation ist zudem erkennbar, ob es sich bei einem Kleidungsstück, das ein Kunde z.B. umtauschen möchte, um ein in diesem Laden gekauftes und bezahltes Produkt handelt.

Vereinfachung des Verkaufsvorgangs

Mittels RFID-Tags kann an der Kasse sofort erfasst werden, welche Kleidungsstücke der Kunde kaufen möchte. Der Mitarbeiter an der Kasse braucht die Barcodes nicht mehr manuell zu scannen. Wird das RFID-Tag auch zur Warensicherung eingesetzt, kann diese beim Lesen des RFID-Tags gleichzeitig deaktiviert werden. Der Kassiervorgang wird beschleunigt, und Wartezeiten an der Kasse werden verkürzt. Zukünftig sind auch auf RFID basierende Selbst-Check-out-Systeme denkbar.

Nutzenpotenziale außerhalb der Lieferkette

RFID bietet nicht nur eine Reihe von Vorteilen in der Lieferkette, sondern kann auch während des Auswahlprozesses im Laden und nach dem Kauf eingesetzt werden. So kann der *Beratungsprozess visuell unterstützt* werden, indem dem Kunden z.B. in der Umkleidekabine oder vor dem Spiegel passende Accessoires oder weitere Informationen zum Produkt präsentiert werden.

In Verbindung mit smarten Haushaltsgeräten sind *Zusatznutzen für den Kunden* nach dem Kauf des Kleidungsstücks denkbar. Ein häufig genanntes Beispiel ist die smarte Waschmaschine, die automatisch prüft, ob Kleidungsstücke zusammen gewaschen werden dürfen. Zudem erlaubt es das RFID-Tag zurückzuverfolgen, wann und wo das Produkt gekauft wurde. Voraussetzung ist hierbei allerdings, dass das RFID-Tag am Kleidungsstück verbleibt. Gerade in Bezug auf diesen Punkt gibt es allerdings derzeit große Bedenken einzelner Verbraucherschützer [Pri03]. Die Beiträge von Langheinrich und Thiesse in diesem Buch beschäftigen sich eingehend mit dieser Thematik.

2.2 Status quo bei Anwendungen von RFID in der Bekleidungsindustrie

Derzeit gibt es eine Reihe von Pilotanwendungen zum Einsatz von RFID-Tags auf Kleidungsstücken. Zu den öffentlich bekannten Beispielen gehören The GAP in den USA [TeI01] und Marks & Spencer in Großbritannien [Rfi04]. Der Fokus dieser Tests lag ebenso wie bei Kaufhof und Gerry Weber auf der Nutzung von RFID in der Lieferkette.

Viele der Versuche mit RFID in der Lieferkette zielen derzeit primär darauf ab, die Anwendbarkeit der Technologien in einem bestimmten Umfeld zu testen (siehe z.B. [Alb03]). Dies gilt auch für Marks & Spencer: „We are very pleased with the results of the trial. It has proved that the technology works and that it has a contribution to make, but we still have work to do on the business case and the implementation costs", wird ein Manager von Marks & Spencer zitiert [Rfi04]. Im Gegensatz dazu führt Texas Instruments – einer der weltweit größten Hersteller von RFID-Tags – an, dass in dem Test mit The GAP insbesondere die Nutzenpotenziale überprüft wurden. Bei dem dreimonatigen Feldversuch wurden Jeanswaren mit RFID-Tags ausgestattet. Aufgrund des Einsatzes von RFID sei die Effizienz in der Lieferkette und der Kundenservice verbessert worden. Die

Produktverfügbarkeit konnte auf nahezu 100 % gesteigert werden, wodurch die Umsätze gestiegen seien.

Die Firma Benetton führt ebenfalls Tests mit RFID durch. Trotz anders lautender Meldungen im Frühjahr 2003 ist, soweit bekannt, noch keine Entscheidung bei Benetton über die Einführung von RFID getroffen worden [Rfi03]. Ein weiteres Beispiel ist Prada, die Versuche mit RFID in ihrem Epicenter in New York durchgeführt haben. Anders als in den vorher genannten Beispielen ging es bei dieser Anwendung nicht primär um die Lieferkette, sondern um die Verbesserung des Kundenerlebnisses und der Kundenberatung [Rfi02]. Prada hat den Test mittlerweile beendet. Die gewählte RFID-Lösung konnte in dem Test nicht überzeugen. Ein Grund hierfür waren technische Probleme. Darüber hinaus konnten mit den Anwendungen laut Presseberichten keine wirklichen Verbesserungen beim Kundenservice und bei den Lagerhaltungsprozessen erzielt werden. Dies lag allerdings nicht primär an der RFID-Technologie, sondern an unternehmensspezifischen Charakteristika und mangelhafter Integration der Anwendungen in die internen Prozesse [Red04].

3 Einsatz von RFID im Pilotprojekt von Kaufhof und Gerry Weber

Die Kaufhof Warenhaus AG ist eine 100%-Tochter der METRO Group. Das Unternehmen betreibt in Deutschland und Belgien ca. 150 Filialen. Im Jahr 2003 machte das Unternehmen einen Umsatz von 3,8 Milliarden EUR. Ein Schwerpunkt der letzten Jahre war die Umstellung eines Großteils der Filialen auf das Galeria-Konzept [Met03].

Gerry Weber International AG ist ein börsennotierter Hersteller von Mode- und Lifestyle-Artikeln. Das Unternehmen wurde vor 30 Jahren gegründet und erzielte im Geschäftsjahr 2002/2003 einen Umsatz von 350 Millionen EUR. Unter dem Markennamen GERRY WEBER vertreibt das Unternehmen Damenoberbekleidung der gehobenen mittleren Preisklasse.[19] Das Unternehmen setzt stark auf Shop-in-Shop-Konzepte und auf den Ausbau eigener Filialen [GWI03]).

Das RFID-Pilotprojekt von Kaufhof und Gerry Weber wurde unter dem Dach der METRO Group Future Store Initiative durchgeführt. Diese Initiative ist eine Kooperation der METRO Group mit SAP, Intel und IBM und etwa 50 weiteren Partnerunternehmen aus den Bereichen Informationstechnologie und Konsumgüterindustrie. Im Rahmen der Initiative werden verschiedene Technologien und technische Systeme in der Praxis getestet. Ein Schwerpunkt der Aktivitäten ist der Einsatz von RFID in der Lieferkette. Die meisten der Anwendungen werden im Extra Future Store in Rheinberg getestet.[20]

[19] www.gerryweber-ag.de/de/index.php?movie=gerryweber
[20] www.future-store.org

3.1 Ausgangslage

Gerry Weber ist in einer Vielzahl von Galeria-Kaufhof-Filialen mit Shop-in-Shops vertreten. Bei den meisten der Produkte handelt es sich um modische Ware. Pro Jahr gibt es sieben Kollektionen, die aus insgesamt zwölf Programmen bestehen. Modische Ware wird im Regelfall nur ein Mal pro Programm bestellt und geliefert. In bestimmten Fällen (z.B. bei großer Nachfrage) ist auch eine Nachbestellung möglich. In solchen Fällen produziert Gerry Weber bestimmte Teile nach. In geringem Umfang sind auch Basisartikel im Sortiment, z.B. Kostüme, die über einen längeren Zeitraum lieferbar sind. Die Entscheidung bezüglich des Sortiments und der Bestellmenge trifft Kaufhof. Bei Anlieferung wird die komplette Bestellung direkt auf der Verkaufsfläche platziert. Eine Lagerhaltung im Warenhaus ist nicht vorgesehen.

Die Ware wird bereits vom Hersteller beziehungsweise von dem von ihm beauftragten Logistikdienstleister für die einzelnen Filialen fertig kommissioniert und über ein Kaufhof-Verteillager an die Filialen ausgeliefert. Die Kommissionierung erfolgt auf Einzelproduktebene. Die Anlieferung und Präsentation erfolgt in Abhängigkeit vom Produkt entweder hängend oder liegend.

Alle Produkte werden bereits bei Gerry Weber mit Hängeetiketten ausgestattet, auf denen neben Größe, Preis etc. auch ein Barcode aufgedruckt wird. Dieser Barcode erlaubt eine Unterscheidung der Produkte nach Typ, Größe und Farbe. Zusätzlich werden höherwertige Produkte mit Diebstahlsicherungsetiketten basierend auf Hochfrequenztechnologie ausgestattet, die an der Kasse wieder entfernt werden.

3.2 Zielsetzung und Durchführung des Pilotprojekts

Projektziele

Bei den Zielen des Pilotprojekts lassen sich zwei Kategorien unterscheiden: Zum einen ging es darum, den aktuellen Stand der Technik zu evaluieren und daraus Anforderungen an die Technologie abzuleiten, zum anderen darum, sinnvolle Einsatzmöglichkeiten für RFID zu prüfen und auf Basis dieser Erkenntnisse eine Kosten- und Nutzenabschätzung durchzuführen. Konkret haben Kaufhof und Gerry Weber folgende Projektziele formuliert [BBQ04]:

- Testen der heute vorhandenen Technik
- Prüfung der Möglichkeiten zum sinnvollen Einsatz der RFID-Technik
- Ermittlung der Investitionen für Hardware und Transponder
- Einschätzung der zu erwartenden Nutzenpotenziale durch Einsatz der Transpondertechnik
- Erstellung einer Wirtschaftlichkeitsbetrachtung
- Erstellen eines Anforderungsprofils des Textilhandels an die RFID-Industrie
- Untersuchungen zur Rückverfolgbarkeit von Produkten

Zeitlicher Rahmen

Bei Kaufhof begannen die Vorbereitungen für die Durchführung des RFID-Pilotprojekts im Sommer 2002. Zu diesem Zeitpunkt wurden auch erste Gespräche mit Gerry Weber geführt. Ideen für ein solches Projekt im Textilbereich gab es jedoch bereits seit einigen Jahren. Mit der Konzeption und Umsetzung des Piloten wurde im Oktober 2002 begonnen. Bereits im Vorfeld hatte Kaufhof Kontakte zu einigen potenziellen Technik- und Dienstleistungspartnern geknüpft. Der eigentliche Pilotversuch startete am 1. Juli 2003 und lief bis Ende November 2003. Im Anschluss an die physischen Tests in der Logistikkette und der Filiale haben Kaufhof und Gerry Weber die gewonnenen Erkenntnisse ausgewertet und Empfehlungen für das weitere Vorgehen ausgearbeitet.

Abb. 3. Verkaufsetikett mit integriertem RFID-Transponder

Teststandorte

Teststandorte waren der Logistikbetrieb Meyer & Meyer in Osnabrück, der die Kommissionierung, Auszeichnung und Auslieferung für Gerry Weber übernimmt, das Kaufhof-Lager in Neuss-Norf, die Galeria Kaufhof in Münster sowie der Kaufhof in Wesel.

Während des Versuchs wurden bei Meyer & Meyer in Osnabrück alle Textilien der Marke Gerry Weber, die für die Kaufhof-Filialen in Münster und Wesel bestimmt waren, manuell mit einem RFID-Tag versehen. Der RFID-Transponder war in ein Verkaufsetikett integriert (siehe Abbildung 3), das von Kaufhof-Mitarbeitern an der Kasse wieder entfernt wurde. Insgesamt wurden rund 5 000 Kleidungsstücke mit RFID-Tags versehen.

Im Warenausgangsbereich von Meyer & Meyer, im Kaufhof-Lager Neuss-Norf sowie im Wareneingangsbereich der Galeria Kaufhof Münster und des Kaufhof Wesel wurden stationäre RFID-Leser verwendet. Auf der Verkaufsfläche kamen sowohl mobile Leser als auch in Regale integrierte Leser zum Einsatz. Die RFID-Leser an den Kassen wurden unterhalb der Tischplatten der Kassiertische angebracht. Die einzelnen Anwendungsszenarien werden im Folgenden beschrieben.

3.3 Anwendungsszenarien

Aus Sicht von Kaufhof und Gerry Weber kann RFID dazu beitragen, die Effizienz in der Lieferkette zu erhöhen, den Kundenservice zu verbessern und eine möglichst hohe Produktverfügbarkeit sicherzustellen. Die betrachteten Anwendungsgebiete entsprechen weitgehend den in Abschnitt 2.1 beschriebenen möglichen Nutzenpotenzialen von RFID. Abbildung 4 zeigt basierend auf [BBQ04] eine Übersicht. Die folgenden Abschnitte beschreiben die im Rahmen des Pilotprojekts betrachteten Anwendungsszenarien im Detail.

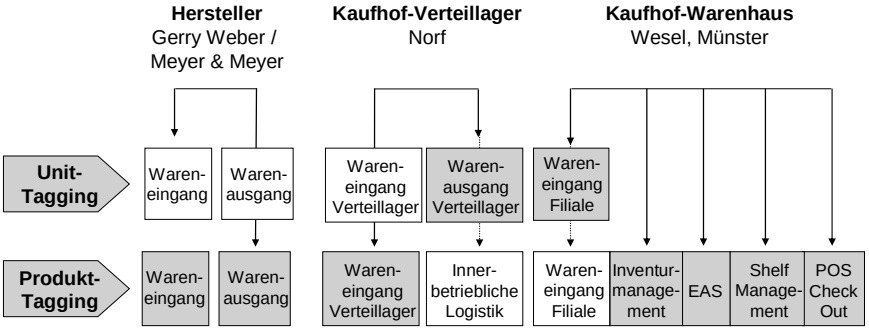


Abb. 4. Übersicht der Anwendungsgebiete

Auszeichnung der Ware beim Hersteller bzw. Logistikdienstleister

Auf Produktebene verwendeten Kaufhof und Gerry Weber Etiketten mit einem bereits integrierten RFID-Transponder, der in einem kombinierten Etikettendrucker und RFID-Schreib-/Lesegerät beschrieben wurde. Das verwendete RFID-Tag besaß neben einer bereits vom Hersteller vergebenen Seriennummer einen mehrfach beschreibbaren Speicher, in dem folgende Informationen abgelegt wurden:

- Global Trade Identification Number (GTIN)21
- Gerry-Weber-Identnummer
- Kennzeichen, ob es sich um ein Kleidungsstück oder eine logistische Einheit handelt

Dieses Etikett mit integriertem RFID-Transponder wurde zusätzlich zum herkömmlichen Etikett am Kleidungsstück angebracht. Bei der Frequenz entschieden sich die Projektbeteiligten für 13,56 MHz.

[21] Dies ist die Nummer, die – kodiert als EAN-13-Barcode – heutzutage auf einem Großteil der Produkte im Einzelhandel zu finden ist.

Erfassung des Warenausgangs beim Hersteller bzw. Logistikdienstleister

Im herkömmlichen Prozess ohne RFID kontrolliert Gerry Weber alle kommissionierten Lieferungen manuell auf Übereinstimmung mit der Bestellung: Vor der Auslieferung scannen Mitarbeiter die Barcodes auf den Etiketten an den Kleidungsstücken. Die Projektpartner wollten überprüfen, inwieweit dieser Arbeitsschritt automatisiert werden kann.

Bei der Durchführung des Tests wurde zwischen hängender und liegender Ware unterschieden. *Liegende Ware* wird in Kartons[22] verpackt, die u.a. auf einem Förderband transportiert werden. *Hängende Ware* wird in Folie verpackt. Die Warenausgangskontrolle findet hier vor der Verpackung statt. Durch den Verpackungsvorgang entstehen Transporteinheiten, die Mitarbeiter in der Regel mittels Hängeförderern im Distributionszentrum manuell fortbewegen.

Im Rahmen des Pilotprojekts setzten Kaufhof und Gerry Weber für die Mengenkontrolle in beiden Fällen stationäre RFID-Leser ein. Bei liegender Ware wurden die in einem Karton befindlichen Kleidungsstücke während des Transports auf dem Förderband erfasst. Bei hängender Ware las ein stationär angebrachter RFID-Leser die RFID-Tags an den Kleidungsstücken während des Transports auf dem Hängeförderer.

Erfassung des Wareneingangs im Verteillager

Bei der Wareneingangskontrolle im Kaufhof-Verteilzentrum führen Mitarbeiter im bisherigen Prozess manuell stichprobenartige Kontrollen durch, um die Liefergenauigkeit zu überprüfen. Kaufhof hat RFID hier eingesetzt, um 100%-Kontrollen auf Produktebene durchzuführen.

Anders als beim Hersteller werden Kartons mit liegender Ware nicht auf Förderbändern transportiert. Für Stichprobenprüfungen werden einzelne Kartons auf einen Tisch gestellt und ausgepackt. Im Pilotversuch wurde unterhalb dieses Tisches ein RFID-Leser angebracht, der automatisch die Kleidungsstücke identifizierte, die sich im Karton befinden.

Bei der Überprüfung hängender Ware war der Prozess ähnlich der Warenausgangskontrolle beim Hersteller. Allerdings wurden die RFID-Tags auf den Kleidungsstücken hier im verpackten Zustand gelesen.

Erfassung des Warenausgangs im Verteillager und des Wareneingangs in der Filiale (auf Ebene der logistischen Einheit)

Die Kontrolle des Warenausgangs im Verteillager und des Wareneingangs in der Filiale fand nur auf Ebene der logistischen Einheit statt. Hierzu brachten Mitarbeiter im Verteilzentrum RFID-Klebeetiketten an die Transportbehälter bzw. in Folie verpackten Kleidungsstücke an. Für den Piloten setzte Kaufhof die gleichen RFID-Transponder mit einer Frequenz von 13,56 MHz wie auch auf Einzelpro-

[22] Zum Zeitpunkt der Versuche verpackte Meyer & Meyer die Ware noch in Einwegpappkartons. Mehrwegbehälter wurden erst ab dem Kaufhof-Verteilzentrum genutzt. Mittlerweile setzen Kaufhof und Gerry Weber Mehrwegbehälter in der gesamten Logistikkette ab Lieferant ein.

duktebene ein. Für die Erfassung der Transporteinheiten wurden ein stationärer Leser am Warenausgang im Verteillager und ein mobiler Leser am Wareneingang in der Filiale verwendet. Dabei wurden bis zu acht logistische Einheiten (z.B. Mehrwegbehälter auf einer Palette) gleichzeitig durch das Leserfeld bewegt.

Inventur in der Filiale und Überprüfung der Produktverfügbarkeit auf der Verkaufsfläche

Kaufhof setzte für die Pilotversuche auf der Verkaufsfläche sowohl stationäre als auch mobile Leser ein. Die stationären Leser wurden in herkömmliche Regale integriert. So wurden Antennen z.B. unterhalb der Regalflächen positioniert. Mit Hilfe der stationären RFID-Leser konnte so der Bestand kontinuierlich überprüft werden. Beim zweiten Szenario gingen Mitarbeiter in bestimmten Zeitabständen mit mobilen Lesern über die Verkaufsfläche. Die Leser erfassten dabei die Kleidungsstücke, die sich innerhalb der Reichweite ihres Feldes auf der Verkaufsfläche befanden.

Diebstahlsicherung mit RFID (statt herkömmlicher EAS-Etiketten)

Bisher setzt Kaufhof EAS-Systeme mit einer Frequenz von 8,2 MHz ein. Diese können unter Umständen durch RFID ersetzt werden. Benchmark ist die mit derzeitigen Systemen erreichbare Erkennungsrate. Um zu überprüfen, ob entsprechende Leseraten mit RFID erreichbar sind, ließ Kaufhof RFID-Antennen an Rolltreppen installieren. In den Tests nahmen Mitarbeiter getaggte Gerry-Weber-Produkte und gingen mit diesen durch die Tore. Anschließend wurde kontrolliert, ob die RFID-Tags gelesen wurden.

RFID-basierte Produkterfassung an der Kasse

Sobald ein Kleidungsstück auf den Kassiertisch gelegt wurde, identifizierte der RFID-Leser das Kleidungsstück mit Hilfe des im RFID-Tag gespeicherten GTINs. Das Kassensystem konnte so den Preis des Produkts etc. sofort anzeigen, ohne dass der Mitarbeiter den Barcode scannen musste. Wie bereits erwähnt wurde das RFID-Etikett an der Kasse entfernt.

3.4 Ergebnisse des Pilotprojekts

Aus dem Pilotversuch konnten Kaufhof und Gerry Weber wesentliche Erkenntnisse für den Einsatz von RFID in der Bekleidungsindustrie ziehen. Diese beziehen sich zum einen auf Anforderungen an die RFID-Technologie, zum anderen auf die betriebswirtschaftlichen Potenziale. Insgesamt beurteilen Kaufhof und Gerry Weber die Ergebnisse des Pilotversuchs sehr positiv. In vielen Bereichen hat sich die Technologie als einsatzfähig herausgestellt. Dennoch gibt es in einigen Bereichen noch Entwicklungsbedarf. Diese Punkte sollen im Folgenden erläutert werden.

Leserate bei der Wareneingangskontrolle hängender Ware auf Produktebene

Ein wesentliches Kriterium für den möglichen Einsatz von RFID ist die erzielbare Leserate. Je nach Anwendung können die Anforderungen an die Leserate variieren. Kaufhof nennt eine Leserate von 99,9 % + x als Zielwert. Dieser Wert wurde in der Logistikkette beim Lesen von liegender Ware als auch beim Lesen von hängender Ware vor der Verpackung erreicht.

Probleme gab es in der Logistikkette bei hängender Ware nach der Verpackung. Hier konnte es – insbesondere bei dünnen Stoffen und Oberteilen – dazu kommen, dass die Etiketten sehr dicht aufeinander lagen und zudem durch die Verdichtung fast senkrecht zum Antennenfeld ausgerichtet waren. Die Leserraten reduzierten sich dadurch auf 80–90 %.

Die Leseraten bei verpackter Hängeware konnten aber auf nahezu 100 % erhöht werden, wenn die RFID-Etiketten an anderer Stelle angebracht wurden (z.B. bei Oberteilen am Ärmel statt im Nackenbereich), da die RFID-Etiketten dann frei hingen und sich bewegen konnten. Allerdings wäre eine solche Lösung aus Sicht von Kaufhof unvorteilhaft für Kunden, da diese sich dann häufig bücken müssten, um Preis und Größe eines Produkts zu erfahren. Dieses Problem ließe sich umgehen, wenn der Transponder nicht – wie bisher im Rahmen des Pilotprojekts – in das Warenetikett integriert wäre, sondern separat angebracht wird.

Bestandserfassung auf der Verkaufsfläche

Für die Bestandserfassung auf der Verkaufsfläche in der Filiale wurden sowohl stationäre als auch mobile Leser eingesetzt. Kaufhof geht davon aus, dass man im Prinzip alle Kleidungsstücke auf der Verkaufsfläche mittels stationärer RFID-Leser erfassen kann. Allerdings kann der Metallanteil in den derzeitigen Regalen (z.B. Kleiderstangen, Halterungen für Regalböden) und Konfektionsständern die Lesereichweite deutlich reduzieren. Hier ergeben sich zwei Optionen: Entweder wird stärker als bisher Kunststoff im Ladenbau verwendet, oder es wird eine hohe Anzahl von RFID-Antennen eingesetzt. Beide Optionen würden erhebliche Kosten nach sich ziehen. Eine weitere Schwierigkeit stellt die Stromversorgung stationärer Leser dar. Dies gilt insbesondere für Konfektionsständer, die in der Regel frei im Raum stehen und häufig umgestellt werden.

Mobile RFID-Leser wurden in zwei verschiedenen Ausführungen getestet. Tragbare RFID-Handlesegeräte eignen sich aus Sicht von Kaufhof primär für die gezielte Suche nach einem Kleidungsstück an einem bestimmten Ort (z.B. nach T-Shirts einer bestimmten Größe in einem Stapel). Bei den Versuchen betrug die Lesereichweite nur etwa 20–30 cm, sodass die Geräte derzeit aus Sicht von Kaufhof nicht für die Durchführung automatischer Inventuren geeignet sind.

Mit fahrbaren Lesern, bei denen Lesegerät und Antenne auf einem Rollwagen montiert sind, konnte Kaufhof deutlich bessere Ergebnisse erzielen. Ein wesentlicher Grund hierfür war die im Vergleich zu den Handlesern deutlich größere Fläche der Antenne. Allerdings ist bisher keine abschließende Bewertung möglich, inwieweit fahrbare Leser tatsächlich eine automatische Inventur ermöglichen. Bei dem getesteten Gerät handelte es sich um einen Prototypen, der sich für den Praxiseinsatz noch als zu unhandlich erwies.

Diebstahlsicherung

Als Diebstahlsicherung lieferten die RFID-Tags in den Tests schlechtere Ergebnisse als die bisher verwendeten EAS-Etiketten auf Basis von 8,2 MHz. Die erzielten Lesereichweiten waren zu gering für einen Einsatz z.B. an den Eingangstüren. An dieser Stelle sind Lesedistanzen von mehr als einem Meter erforderlich.

Kosten für RFID-Tags

Derzeit liegen die Preise für RFID-Tags noch um ein Mehrfaches über den 0,05 USD, die z.B. das Auto-ID Center als Ziel genannt hat [Sar01]. Legt man die in dem Projekt quantifizierten Nutzenpotenziale zugrunde, sollte die Verwendung eines RFID-Tags auf einem Kleidungsstück inklusive evtl. notwendigem zusätzlichem Aufwand für die Anbringung nicht mehr als 0,10–0,12 EUR kosten.

Wird das RFID-Tag nur ein Mal verwendet, sind die Tag-Kosten ein wesentlicher Kostentreiber. Wird das RFID-Tag hingegen mehrmals eingesetzt, sinkt die Bedeutung der Beschaffungskosten. Stattdessen rückt der Aufwand für die Rückführung und Wiederverwendung in den Vordergrund.

3.5 Betriebswirtschaftliche Potenziale

Häufig fokussiert sich die Diskussion um die Wirtschaftlichkeit von RFID auf die Kostenseite, insbesondere die Kosten für RFID-Tags und RFID-Leser. Auch wenn dies ein wesentlicher Aspekt ist, greift eine solche Diskussion zu kurz. Zunächst gilt es zu verstehen, welche Potenziale RFID bietet. Insbesondere Unternehmensberatungen haben bereits eine Reihe von Berichten veröffentlicht, die die generischen Nutzenpotenziale von RFID darstellen. Dennoch sind viele Unternehmen noch nicht in der Lage zu beurteilen, was das Thema RFID für sie konkret bedeutet. Fallbeispiele und Erfahrungsberichte aus der Praxis sind rar.

In der folgenden Übersicht soll am Beispiel von Kaufhof und Gerry Weber exemplarisch gezeigt werden, wie die Bekleidungsindustrie und der Handel von RFID profitieren können. Der Fokus liegt dabei auf den Potenzialen von RFID auf Produktebene. Es ist allerdings zu beachten, dass die Nutzenpotenziale nach den Erfahrungen der beiden Unternehmen je nach Hersteller und Händler variieren können.

Im Rahmen des Pilotprojekts konnten einige Nutzenpotenziale quantifiziert werden, bei anderen sind zum heutigen Stand nur qualitative Aussagen möglich. Bei den quantifizierten Potenzialen handelt es sich im Wesentlichen um Effizienzsteigerungen aufgrund von Einsparungen bei manuellen Tätigkeiten. Für Gerry Weber führt RFID zu einem geringeren Arbeitsaufwand bei Wareneingangs- und -ausgangskontrolle sowie im Kommissionierprozess. RFID ermöglicht eine automatische Mengenkontrolle und eine automatische Erfassung der kommissionierten Artikel. Bei Kaufhof verteilen sich die quantifizierbaren Potenziale etwa gleich auf Logistik und Filiale. In der Logistik sind es – vergleichbar mit Gerry Weber – Effizienzsteigerungen im Bereich des Wareneingangs und der Kommissionierung. In der Filiale wird mit Zeiteinsparungen an der Kasse und bei der vier Mal jährlich stattfinden Inventur gerechnet, da Bestände nun automatisch

erfasst werden können. Auf ein Kleidungsstück umgerechnet sind die quantifizierbaren Potenziale bei Gerry Weber höher als bei Kaufhof. Dies liegt unter anderem daran, dass Gerry Weber die Ware für Kaufhof kommissioniert.

Bei den qualitativen Nutzenpotenzialen handelt es sich primär um Qualitätsverbesserungen in den Prozessen und beim Kundenservice. Diese Potenziale für Gerry Weber und Kaufhof sind in Tabelle 1 dargestellt [BBQ04].

Die Wirtschaftlichkeitsbetrachtung beruht auf einer Reihe von Prämissen. So gehen die Unternehmen für ihre Berechnungen davon aus, dass 100% der Produkte und logistischen Einheiten mit RFID-Tags ausgerüstet sind und dass die Ware bereits beim Hersteller ausgezeichnet wird. Der Transponder wird dabei nicht in das Kleidungsstück integriert, sondern am Kleidungsstück angebracht.

Tabelle 1. Wirtschaftlichkeitsbetrachtung: Qualitativer Nutzen für Gerry Weber und Kaufhof auf Produktebene

Bereich	Qualitativer Nutzen
Gerry Weber	Vollkontrolle beim Warenausgang
	Fehlervermeidung durch Reduzierung manueller Tätigkeiten
	Weniger Falschlieferungen
	Verbesserte Kommunikationsmöglichkeiten zwischen allen Beteiligten entlang der Lieferkette
	Informationsmöglichkeiten über Produktakzeptanz beim Kunden
Kaufhof Logistik	Weniger Falschlieferungen
	Vollkontrolle beim Wareneingang
	Vollkontrolle beim Warenausgang
	Fehlervermeidung durch Reduzierung manueller Tätigkeiten
	Verbesserte Kommunikationsmöglichkeiten zwischen Lieferant, Kaufhof-Lager und Filialen
Kaufhof Filiale	Vollkontrolle am Wareneingang
	Vollkontrolle bei allen Arten des Filial-Warenausgangs
	Fehlervermeidung durch Reduzierung manueller Eingaben
	Weniger Bestandslücken
	Kürzere Schlangen an den Kassen durch beschleunigten Kassiervorgang
	Mehr Zeit für die Kunden
	Höhere Kundenzufriedenheit
	Höherer Umsatz aufgrund obiger Verbesserungen

Auf Produktebene ist eine Mehrweglösung angedacht, bei der das RFID-Tag in ein EAS-Etikett integriert wird. Wie bereits oben erwähnt, rechnen Kaufhof und

Gerry Weber damit, dass sich der Einsatz von RFID bei Kosten von nicht mehr als 0,10–0,12 EUR pro Umlauf (inklusive anteiliger Beschaffungskosten) für das RFID-Etikett rechnen wird. Es ist vorgesehen, dass der Lieferant die Anschaffungskosten der Transponder übernimmt, während Kaufhof die Umlaufkosten trägt. Auf Basis der vorliegenden Berechnungen würden bei einer solchen Aufteilung der Kosten sowohl Gerry Weber als auch Kaufhof vom Einsatz von RFID profitieren.

Auf logistischen Einheiten findet vermutlich keine Wiederverwendung der RFID-Tags statt. Aus heutiger Sicht rechnen die Unternehmen damit, dass RFID-Tags mit einer Frequenz von 13,56 MHz auf Produktebene und mit einer Frequenz von 868 MHz auf logistischen Einheiten zum Einsatz kommen.

3.6 Weiteres Vorgehen

Anfang Januar 2004 gab METRO bekannt, dass das Unternehmen im November 2004 mit der Einführung von RFID mit etwa 100 Lieferanten beginnen wird. Kaufhof ist eines der beteiligten METRO-Tochterunternehmen. Der Fokus liegt dabei auf der Verwendung von RFID auf Paletten und Transportverpackungen [Met04a]. In einem ersten Schritt sollen alle logistischen Einheiten, die über eine NVE (Nummer der Versandeinheit)[23] eindeutig identifizierbar sind, mit RFID-Tags ausgestattet werden. Bezüglich der Einführung von RFID auf Einzelproduktebene ab 2006 ist noch keine endgültige Entscheidung gefallen.

Für die Zukunft planen Kaufhof und Gerry Weber weitere Aktivitäten zum Einsatz von RFID auf einzelnen Kleidungsstücken. Die beiden Unternehmen möchten unter anderem ein konkretes Anwendungsszenario prototypisch umsetzen, bei dem RFID genutzt wird, um den Kundenberatungsprozess visuell zu unterstützen. Zudem treiben die beiden Projektpartner die Verbreitung von RFID in der gesamten Bekleidungsindustrie voran, wobei sich Kaufhof und Gerry Weber derzeit aktiv um die Einbindung weiterer Textileinzelhändler bzw. Bekleidungshersteller bemühen. Darüber hinaus sind die Unternehmen in diversen Initiativen und Arbeitskreisen von Industrieverbänden vertreten; mit der Centrale für Coorganisation (CCG) ist ein Arbeitskreis geplant, der sich mit Mehrweglösungen für RFID in der Bekleidungsbranche befassen soll.

Die Einführung von RFID in der geplanten Form wird nicht als eine isolierte Entscheidung einzelner Unternehmen gesehen, sondern als eine Initiative, die den gesamten Einzelhandel betrifft. Der Erfolg des Einsatzes von RFID hängt nicht zuletzt von der Anzahl der Einzelhändler und Konsumgüterhersteller ab, die die Einführung der Technologie vorantreiben. Um Händlern und Herstellern die Möglichkeit zu geben, Tests mit RFID durchzuführen, hat die METRO Group im Kaufhof-Verteilzentrum in Neuss-Norf ein RFID-Labor eingerichtet [Met04b]. In diesem METRO Group RFID Innovation Center sollen sowohl konkrete Anwendungsszenarien durchgespielt als auch Technologietests durchgeführt werden können.

[23] Die NVE wird in der Regel als EAN-128-Barcode kodiert.

4 Zusammenfassung und Schlussfolgerungen

Die Bekleidungsindustrie könnte eine der ersten Branchen sein, die RFID auf Produktebene einsetzt. Der vorliegende Beitrag hat einige der Einsatzmöglichkeiten von RFID beleuchtet. Die Erfahrungen aus dem beschriebenen Pilotversuch verdeutlichen die bestehenden Hindernisse, aber auch die Potenziale für den Einsatz von RFID.

Derzeit handelt es sich bei den meisten Anwendungsbeispielen noch um Pilotversuche. Viel wird davon abhängen, wie viele Unternehmen die Einführung von RFID aktiv vorantreiben werden. Offen ist zudem noch, wie die tatsächliche Einführung von RFID aussehen könnte. Auf absehbare Zeit wird es eine Koexistenz von Barcode und RFID geben. Hier müssen entsprechende Übergangsszenarien definiert werden.

Auf Einzelproduktebene ist noch nicht ganz klar, wie die RFID-Tags angebracht werden. So besteht die Möglichkeit, sie z.B. in Hängeetiketten, in EAS-Etiketten oder direkt in die Kleidung zu integrieren. Alle Verfahren haben gewisse Vor- und Nachteile und Implikationen (z.B. im Hinblick auf Wiederverwendbarkeit oder Nutzbarkeit des RFID-Tags über die Logistikkette hinaus). Hier wird sich erst noch herausstellen, wie die Prozesse und Geschäftspraktiken in Zukunft aussehen werden.

Die Erfahrungen aus dem Piloten lassen erkennen, dass eine Mehrweglösung sinnvoll, wirtschaftlich vorteilhaft und umsetzbar ist. Dieser Lösungsansatz wird von der CCG unterstützt, die gemeinsam mit Handel, Textilindustrie und Herstellern von Warensicherungssystemen ein Konzept für ein „Mehrweg-Taggingverfahren“ erarbeitet. Eine erste Pilotumsetzung entlang der gesamten Lieferkette wird in der zweiten Hälfte des Jahres 2005 erwartet.

Ein weiteres wichtiges Thema ist der Datenschutz. Die Akzeptanz der Technologie hängt unter anderem davon ab, dass es den Unternehmen gelingt, ihren Kunden zu vermitteln, welche Vorteile diese durch den Einsatz von RFID haben. Mit einer Mehrweglösung könnten die datenschutzrechtlichen Bedenken weitgehend ausgeräumt werden, da das RFID-Tag an der Kasse entfernt wird.

Ein Vorteil im Bekleidungseinzelhandel im Vergleich zu anderen Branchen liegt darin, dass viele Hersteller eigene Geschäfte betreiben und/oder mit Shop-in-Shop-Konzepten in Warenhäusern vertreten sind. Dies könnte die Einführung von RFID-Anwendungen in Verkaufsstellen vereinfachen. Die Problematik, dass in einer Übergangsphase nur ein Teilsortiment mit RFID-Tags ausgestattet ist, würde sich verringern, da in einem Geschäft bzw. einem bestimmten Bereich nur Produkte eines einzigen Herstellers verkauft werden.

Aus unserer Sicht deutet derzeit vieles darauf hin, dass sich RFID in der Bekleidungsindustrie durchsetzen wird.

Literatur

[Alb03] Albano S, Engels DW (2002) Auto-ID Center Field Trial – Phase I Summary. Auto-ID Center Technical Report, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TR-006.pdf

[BBQ04] Bentrup R, Büsing-Funke M, Quiede, U (2004) RFID in der Bekleidungsindustrie am Beispiel Gerry Weber. Präsentation auf dem RFID-Kongress für Partner der METRO Group, Köln, 14. Mai 2004

[Byr03] Byrnes, J (2003) Who Will Profit From Auto-ID? The Bottom Line, September 1, 2003, workingknowledge.hbs.edu/item.jhtml?id=3651&t=dispatch

[CCG02] Centrale für Coorganisation (2002), eBusiness in der Bekleidungswirtschaft – Managementleitfaden

[GWI03] Gerry Weber International AG (2003) Geschäftsbericht 2002/2003, www.gerryweber-ag.de/de/downloads/do45_gw_geschaefts_02-03.pdf

[IBM02] IBM Business Consulting Services (2002) Applying Auto-ID to Reduce Losses Associated with Shrink. Auto-ID Center Report, archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-003.pdf

[Lee02] Lee HL (2002) Aligning Supply Chain Strategies with Product Uncertainties. California Management Review 44(3): 105–119

[Met03] METRO Group (2003) Geschäftsbericht 2002, www.metro.de/servlet/PB/show/1005260/GB2002-dt.pdf

[Met04a] METRO Group (2004) METRO Group startet die unternehmensweite Einführung von RFID. METRO Group Presseerklärung, 12. Januar 2004, www.future-store.org/servlet/PB/menu/1002256/index.html

[Met04b] METRO Group (2004) Das METRO Group RFID Innovation Center in Neuss. METRO Group Hintergrund-Information, 7. Juli 2004, www.future-store.org/servlet/PB/show/1003381/RFIDnet-IC-Factsheet-dt-04-07-06.pdf

[Ott03] Otto A (2003) Supply Chain Event Management: Three Perspectives. International Journal of Logistics Management 14(2): 1–13

[Pri03] Privacy Rights Clearinghouse (2003) Position Statement on the Use of RFID on Consumer Products. November 20, 2003, www.privacyrights.org/ar/rfidposition.htm

[Rfi02] RFID Journal (2002) Learning from Prada. June 24, 2002, www.rfidjournal.com/article/view/272

[Rfi03] RFID Journal (2003) Behind the Benetton Brouhaha. April 14, 2003, www.rfidjournal.com/article/view/381

[Rfi04] RFID Journal (2004) Marks & Spencer Expands RFID Trial. February, 10, 2004, www.rfidjournal.com/article/view/791

[Sar01] Sarma S (2001) Towards the 5c Tag. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-006.pdf

[Red04] Reda S (2004) Prada's Pratfall: Chic Technology Stumbles. Stores, May 2004, www.stores.org/archives/2004/05/cover.asp

[TeI01] Texas Instruments (2001) The Gap Tests Texas Instruments RFID Smart Label Technology for Tracking Denim Clothing from the Factory to Store Shelves. Texas Instruments Press Release, November 13, 2001, www.ti.com/tiris/docs/news/news_releases/2001/rel11-13-01.shtml

Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie

Robin Koh
Auto-ID Lab, Massachusetts Institute of Technology

Thorsten Staake
Institut für Technologiemanagement, Universität St. Gallen

Kurzfassung. Gefälschte Arzneimittel stellen ein großes gesundheitliches Risiko für Patienten dar und verursachen einen erheblichen finanziellen Schaden bei den etablierten Unternehmen der pharmazeutischen Industrie. In diesem Beitrag wird ein dynamisches Tracking- und Tracing-Verfahren zur Sicherung der Supply Chain aller betroffenen Unternehmen vorgestellt. Es basiert auf der RFID-Technologie sowie einer geeigneten IT-Infrastruktur und ermöglicht eine effiziente Rückverfolgung und Lokalisierung von Arzneimitteln innerhalb der Lieferkette.

1 Einleitung

Durch die demografische Entwicklung und den Fortschritt in der Medizin sind Anzahl und Vielfalt der verkauften Medikamente enorm gestiegen. Immer größere Mengen an Rohstoffen und fertigen Produkten durchlaufen die Lieferkette der pharmazeutischen Industrie, die zunehmend der Supply Chain der Konsumgüterindustrie gleicht [Cot01]. Ein entscheidender Unterschied bleibt jedoch die erhöhte Sorgfaltspflicht, die Gesellschaft und Gesetzgeber von der Arzneimittelindustrie verlangen.

Übergeordnete Ziele des Gesundheitswesens sind das Wohl und die Sicherheit der Patienten. Um diese Ziele zu erreichen, erarbeiten zahlreiche Staaten Rechtsvorschriften, welche die Integrität von Medikamenten innerhalb der gesamten Lieferkette sicherstellen sollen. Diese Vorschriften fordern eine Dokumentation des gesamten Herstellungs- und Vertriebsprozesses, was bei den üblichen, papierbasierten Verfahren mit einem enormen Aufwand und hohen Kosten verbunden wäre [Mit98].

Die Dokumentation soll es Unternehmen ermöglichen, Medikamente während des gesamten Herstellungs- und Vertriebsprozesses zu lokalisieren (Tracking). Weiter muss die Historie jedes Medikamentes einschließlich seiner verwendeten Grundsubstanzen auch im Nachhinein nachvollziehbar sein (Tracing). Unter Historie versteht man zum Beispiel Informationen bezüglich Produktionsort, Fertigungseinheit, Zeit der Produktionsschritte sowie bisherige Eigentümer und Lagerorte.

Tracking und Tracing ermöglicht es Herstellern und Distributoren, Arzneimittelfälschung systematisch zu erkennen und zu bekämpfen und bildet so die Grundlage zur Verwirklichung eines hohen Sicherheitsstandards für Patienten. Bestehende Dokumentationssysteme sind jedoch wegen der manuellen Datenerfassung und der papierbasierten Datenhaltung für ein effizientes Tracking und Tracing ungeeignet. Daraus resultierend finden die Daten nur in Ausnahmefällen wie bei Rückrufaktionen oder in kleinzahligen Stichproben Verwendung, weshalb kein umfassender Schutz gewährleistet ist.

RFID-Technologien zur automatischen Identifikation und Lokalisierung physischer Objekte sowie Standards zur Datenübertragung und Integration der Informationen in Datenbanken stellen eine mögliche Lösung des Track- und Trace-Problems dar. Der vorliegende Beitrag setzt sich daher mit relevanten Aspekten von RFID-Systemen im Zusammenhang mit den Charakteristika der Lieferkette der pharmazeutischen Industrie auseinander.

2 Arzneimittelfälschung: Ein internationales Problem von signifikantem Ausmaß

Die World Health Organisation (WHO) definiert eine Fälschung im Zusammenhang mit Arzneimitteln als „die vorsätzliche und betrügerische Falschetikettierung hinsichtlich Identität, Zusammensetzung und/oder Herkunft eines Fertigprodukts oder eines Bestandteils von Arzneimitteln“ [WHO03].

Fälschungen führen zu einer Gefährdung der Sicherheit der Patienten sowie zu einem wirtschaftlichen Verlust für die etablierten Unternehmen der Pharmaindustrie. Nach Schätzungen der WHO lassen sich fünf bis acht Prozent des weltweiten Umsatzes von pharmazeutischen Produkten auf Fälschungen zurückführen [HDMA04]. Kenner der Industrie gehen davon aus, dass die Angaben der WHO auf konservativen Annahmen beruhen. Folgende Beiträge beschäftigen sich explizit mit dem Ausmaß der Fälschung von Arzneimitteln:

- WHO Counterfeit Drugs, Fact Sheet No. 275, November 2003: „In Niger starben vermutlich 2 500 Menschen wegen eines gefälschten Meningitis-Medikamentes.“ Weiter erwiesen sich in sieben untersuchten afrikanischen Ländern (Gabun, Ghana, Kenia, Mali, Mosambik, Sudan und Simbabwe) 23 % des günstigen Malariapräparates Chloroquin und 90 % der teureren Medikamente als Fälschungen.
- The Washington Post, 30. August 2002: „Im Jahr 2001 starben in China etwa 192 000 Menschen aufgrund der Einnahme von gefälschten Medikamenten. Bis zu 40 % der Medikamente in China sind Fälschungen.“
- The Lancet, 19. Juni 2001: „33 % der Anti-Malaria-Medikamente in Kambodscha, Laos, Burma, Thailand und Vietnam enthalten keine aktiven Inhaltsstoffe.“
- U.S. News & World Report, 11. Juni 2001: „Es wird angenommen, dass bis zu 40 % der Medikamente in Kolumbien gefälscht sind.“

- IFPW Focus, 13. Juni 2002: „Ungefähr 50 % der Arzneimittel, die in Nigeria verkauft werden, sind Fälschungen."
- U.S. News & World Report, 11. Juni 2001: „In einer zeitgleich an den internationalen Flughäfen in Dulles und Oakland durchgeführten Durchsuchungsaktion erwiesen sich 10 % der analysierten Medikamente als Fälschungen."

2.1 Ursachen und Entwicklung der Arzneimittelfälschung

Die potenzielle Gewinnspanne beim Handel mit gefälschten Pharmazeutika ist in den vergangenen Jahren durch die wachsende Anzahl teurer Medikamente erheblich gestiegen. Hohe Margen und geringe Risiken machen den Handel mit gefälschten Pharmazeutika attraktiv [FIP03]. Besonders beunruhigend ist in diesem Zusammenhang das Engagement von Gruppierungen aus dem Bereich der organisierten Drogenkriminalität, was den Umfang und die Signifikanz des Problems verdeutlicht.

In den USA begünstigen mehrere strukturelle Faktoren den Trend zur Arzneimittelfälschung [App03]. So existiert eine wachsende Anzahl an Großhändlern mit teilweise geringen Umsätzen, deren Preiskampf die Entwicklung eines „grauen Marktes" fördert. Zahlreiche Schnittstellen im Vertriebssystem von Medikamenten erleichtern das Einschleusen gefälschter Produkte in die Lieferkette. Leistungsfähige Computer und Farbdrucker ermöglichen die Nachahmung auch von aufwendigen Verpackungen.

Die Bemühungen verschiedener Länder, den Handel mit gefälschten Pharmazeutika einzuschränken, werden durch neue Freihandelsabkommen, Deregulierungsmaßnahmen und den nicht regulierten Verkauf von Lifestyle-Arzneimitteln über das Internet behindert. Das resultierende Umfeld begünstigt verstärkte Fälschungsaktivitäten [FIP03].

2.2 Reaktion des Gesetzgebers

Behörden zahlreicher Industrieländer haben den Handlungsbedarf bezüglich der mangelhaften Vorschriften zur lückenlosen Herkunftsdokumentation von Arzneimitteln erkannt und arbeiten bereits an Gesetzesvorlagen, die sich dieses Problems annehmen. Eine aus dem amerikanischen Bundesstaat Florida stammende Initiative sieht vor, einzelne Medikamente direkt mit folgenden Informationen zu verknüpfen [KSC03]:

1. Name des Medikamentes
2. Dosierung
3. Größe des Gebindes
4. Anzahl der Gebinde
5. Abfüllcharge oder Kontrollnummer
6. Name und Adresse aller an den bisherigen Transaktionen beteiligten Unternehmen, beginnend beim Hersteller
7. Zeitpunkt jeder Transaktion

Eine solche Auflage führt zu erheblichem, zusätzlichem Aufwand bei Herstellern und Distributoren. Dies wird umso deutlicher, wenn man bedenkt, dass ein typischer Händler bis zu 40 000 Medikamente auf Lager hält.

Ähnliche Anforderungen wie Florida stellt Italien mit dem so genannten Bollini-Gesetz an die Unternehmen. Bereits im Jahre 2000 verabschiedet, verpflichtet es alle Hersteller und Händler von Medikamenten zur eindeutigen Kennzeichnung jeder Verpackung mit Seriennummern und Barcodes. Diese mit europäischen Fördermitteln unterstützte Maßnahme soll die Rückverfolgbarkeit des Weges von Arzneimitteln durch die gesamte Wertschöpfungskette ermöglichen. Allerdings existieren für das enorme Datenaufkommen – allein in Italien durchwandern jährlich etwa 1,2 Milliarden zu kennzeichnende Produkte die Supply Chain – noch keine Datenbanken, die ein effizientes Tracking und Tracing ermöglichen. Aus diesem Grund wurde das Bollini-Gesetz bisher nicht vollständig umgesetzt. Ob Barcodes und herkömmliche Infrastrukturen zur Datenverarbeitung überhaupt zu einer befriedigenden Lösung führen, ist fraglich.

3 Ansätze zur Vermeidung von Arzneimittelfälschungen

Dem Druck der Behörden folgend und um wirtschaftlichen Schaden abzuwenden, geht die pharmazeutische Industrie mit verschiedenen Methoden gegen Fälscher vor. Allerdings hat sich bis heute kein Ansatz als wirklich effektiv erwiesen. Die meisten Verfahren beruhen auf manuell durchgeführten Kontrollen, bei denen Mitarbeiter einzelne Verpackungen auf auffällige Merkmale hin untersuchen. Ohne automatisierte Verfahren sind die Kontrollen jedoch zu teuer und zu zeitintensiv, sodass die Unternehmen meist auf eine kontinuierliche Untersuchung größerer Stichproben verzichten. Falls dennoch gefälschte Arzneimittel gefunden werden, reichen die vorliegenden Daten über das Ausmaß des Betrugs meist nicht aus, um eine angemessene Vorgehensweise abzuleiten.

3.1 Gängige Ansätze

Jüngste Bemühungen im Umgang mit gefälschten Pharmazeutika beruhen auf Verfahren der Informations- und Materialtechnologie oder dienen der Sensibilisierung der Beteiligten. Beispiele sind:

- **Chemische Verfahren.** Einige Hersteller versetzen ihre Medikamente mit charakteristischen, inerten chemischen Substanzen. Händler oder Endkunden können diese Stoffe mit Verfahren nachweisen, die vom Prinzip her einem Schwangerschaftstest aus der Apotheke gleichen.
- **Verpackungstechnik.** Aufwendige Verpackungen erschweren die Herstellung von Plagiaten. Maßnahmen reichen von der Verwendung komplizierter Packungsdesigns bis hin zum Anbringen von Hologrammen.
- **Aufklärung der Verbraucher.** Im US-amerikanischen Raum bemüht sich die Food and Drug Administration im Rahmen des Informationsprogramms Med-

watch[24] um eine Sensibilisierung der Endkunden. Medwatch meldet zudem Rückrufaktionen und warnt vor im Umlauf befindlichen gefälschten Produkten.

- **Aufklärung der Hersteller und Händler.** Sowohl die Healthcare Distribution Management Association (HDMA) Product Safety Task Force[25] als auch das amerikanische Institut für sicheren Umgang mit Arzneimitteln[26] informieren über verbesserte Verfahren zur Distribution von Arzneimitteln oder zur Gestaltung von Verpackung und Etikettierung.

Technische Verfahren zum Fälschungsschutz lassen sich in verdeckte und sichtbare sowie in chemische (Intra-Rezeptur) und verpackungsbasierte Herangehensweisen unterteilen [Mag02]. Tabelle 1 fasst die gängigsten Methoden zusammen und gibt eine Einschätzung hinsichtlich des Grades der Fälschungssicherheit.

Tabelle 1. Verfahren zum Schutz gegen Arzneimittelfälschungen

Fälschungsschutz	Verdeckt	Sichtbar	Wirksamkeit
Intra-Rezeptur			
Immuntest	✓		hoch
Einzelne Inhaltsstoffe		✓	hoch
Verpackungsebene			
Design		✓	gering
Wasserzeichen	✓	✓	gering
Digitale Wasserzeichen	✓	✓	hoch
Faser und Fäden	✓	✓	mittel
Reaktive Tinte	✓	✓	mittel
Hologramme, OVD	✓	✓	gering
Barcode		✓	gering

Die aufgeführten Verfahren sind statisch und bieten daher nur einen temporären Schutz gegen Fälschungen. Nach einiger Zeit sind die Betrüger meist in der Lage, die charakteristischen Merkmale nachzuahmen. Hersteller müssen daher anstreben, den Fälschern zu jeder Zeit einen Schritt voraus zu sein. Wie am Anfang des Beitrags erwähnt, verringert sich der zeitliche Vorsprung mit der Weiterentwicklung der PC- und Drucker-Technologie zunehmend. Außerdem steht der häufige Wechsel des Verpackungsdesigns dem Ziel einer beständigen Corporate Identity entgegen und sorgt zudem für Verwirrung bei den Konsumenten.

3.2 Schutz durch dynamische Verfahren

Die oben erwähnte Gesetzesinitiative aus Florida sieht eine kontinuierliche Aktualisierung der Stammbauminformationen bzw. der Historie eines Medikamentes vor. Darüber hinaus sind die beteiligten Unternehmen dazu angehalten, dynamische Daten wie Uhrzeit und Datum aller Transaktionen zu speichern. Ausgewählte Daten sollen dem Käufer zugänglich sein, der sie anhand einer eindeutigen

[24] www.fda.gov/medwatch/index.html
[25] www.healthcaredistribution.org
[26] www.ismp.org

Identifikationsnummer mit den Datenbanken des Verkäufers oder Herstellers abgleichen und so die Integrität der Angaben überprüfen kann.

Das folgende Beispiel illustriert den Informationsfluss in der Lieferkette der Pharmaindustrie über die Beschriftung der Verpackungen. Es verdeutlicht, dass ein dynamischer Ansatz mit der bisherigen Art der Etikettierung nur mit großem Aufwand möglich ist. Abbildung 1 zeigt, wie sich die Form der produzierten Güter innerhalb der Wertschöpfungskette der Pharmaindustrie verändert [KSC03]. Das Ergebnis jedes Arbeitsschrittes dient als Ausgangsprodukt des jeweils folgenden Prozesses. Wechselt ein Produkt den Besitzer oder wird es an einen anderen Standort verlagert, beschriftet der Absender das Transportbehältnis mit ausgewählten Informationen wie Name, Zusammensetzung, Losnummer und Verfallsdatum. Der Container selbst wird so zum Träger von Informationen. Diese Art der Informationsübermittlung ist nicht standardisiert und erschwert eine automatisierte Überprüfung der Daten beim Kunden erheblich. Weitere Probleme entstehen bei einer erneuten Verpackung und Beschriftung, z.B. durch eine zwischengeschaltete Spedition.

Dieses Problem der Etikettierung besteht in vergleichbarer Form in allen Schritten der Supply Chain, was ein effizientes Tracking und Tracing oder eine vollständige Verifikation der Integrität der Ausgangsstoffe erheblich erschwert. Im besten Falle sammeln Pharmaunternehmen ihre eigenen Daten in proprietären Datenbanken, zu einem Datenaustausch mit anderen Unternehmen kommt es nur selten. Rückrufaktionen werden so zu zeit- und kostenintensiven Prozessen, und Entscheidungen bezüglich des Umfangs der Aktionen basieren wegen der Unsicherheit der zugrunde liegenden Daten auf groben Schätzungen. Eine deutliche Verbesserung ist erst durch den Einsatz von RFID-Technologie möglich, womit sich der folgende Abschnitt beschäftigt.

4 RFID-Technologie: Schutz durch Informationen

Die RFID-Technologie eröffnet neue Wege sowohl im Kampf gegen den Arzneimittelbetrug als auch bei der Implementierung effizienter Tracking- und Tracing-Systeme. Wesentliche Vorteile gegenüber Barcode-Systemen ergeben sich aus der Möglichkeit, quasi zeitgleich Informationen von mehreren RFID-Tags ohne direkten Sichtkontakt zu einem Lesegerät zu erhalten (Pulkerfassung). Diese Eigenschaften vereinfachen den Aufbau eines Verfahrens zur automatischen Datenerfassung grundlegend. Werden RFID-Tags in einzelne Verpackungen integriert, so ermöglicht das System die Bestimmung des Inhaltes von ganzen Paletten, ohne diese zu öffnen.

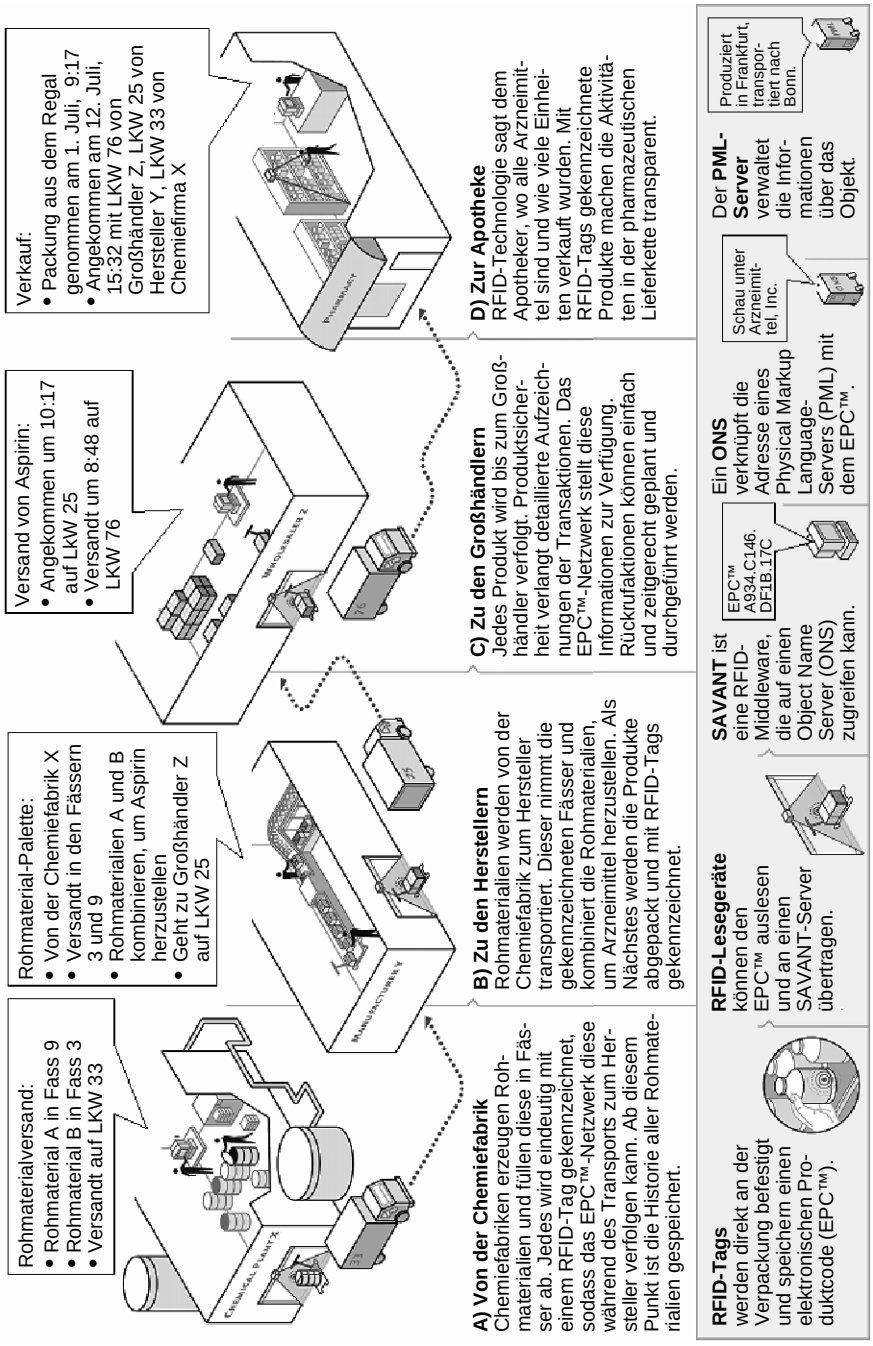


Abb. 1. Eine transparente Lieferkette: Historie von Arzneimitteln

Ein vollständig automatisiertes Verfahren zur Implementierung eines effektiven Tracking und Tracing einzelner Medikamente erfordert die Integration eines RFID-Chips auf der Ebene der Verpackungen, in der sie an den Endkunden abgegeben werden. Eine kostengünstige Lösung stellt die Verwendung einfacher ID-Tags dar, die lediglich eine eindeutige Identifikationsnummer übertragen können und keinen eigenen Speicher besitzen. Der oben genannte wesentliche Vorteil der automatisierbaren Datenerfassung bleibt weiter bestehen. Der fehlende Speicher wird durch eine Datenbank simuliert. Dabei verweist jeweils eine eindeutige Identifikationsnummer auf einen Datensatz in der zentralen Datenbank, in der die Stammbauminformationen verwaltet werden. Dies hat neben den geringeren Kosten auch den Vorteil einer einfachen Kommunikation zwischen RFID-Tags und Lesegerät, da die RFID-Tags von aufwendigen Schreibvorgängen entlastet werden. Die Anzahl der gleichzeitig erfassbaren Produkte steigt so erheblich.

Mit einer geeigneten IT-Infrastruktur, wie in „The Networked Physical World System“ [ESP02] vorgestellt, wird eine kontinuierliche Lokalisierung und Identifizierung von Medikamenten möglich. Die Historie eines Medikamentes kann so von allen an der Distribution beteiligten Unternehmen bis hin zum Endkunden nachvollzogen werden. Neben einem nachhaltigen Schutz vor Medikamentenfälschungen durch ein effizientes Tracking und Tracing können durch eine RFID-Lösung auch wertvolle Informationen für die Optimierung von Prozessen in der Supply Chain gesammelt werden.

Schwierigkeiten bei der Umsetzung der vorgeschlagenen Lösung resultieren aus dem großen, kontinuierlichen Datenstrom, der in einer zentralen Datenbank erfasst werden muss. Ein Ansatz zur Lösung dieses Problems ist in Abschnitt 5 dargestellt. Zuvor werden jedoch grundsätzliche Begriffe bezüglich der Datenstrukturen und des Informationsflusses in der Lieferkette eingeführt.

4.1 Datenhaltung: Aggregation und Vererbung

Auch wenn sich die Form der Produkte während des Herstellungsprozesses ändert, bleiben die Informationen über die verwendeten Ausgangsstoffe von Bedeutung. Dieser Zusammenhang kann als Vererbung spezieller Attribute betrachtet werden: Jedes Medikament, das von einem Endverbraucher erworben wird, hat eine bestimmte Losnummer und ein auf der Verpackung abgedrucktes Verfallsdatum. Mit der Losnummer sind Zulieferer und Händler verknüpft. Weiter besteht das Medikament aus verschiedenen Grundsubstanzen, die auch jeweils über die Losnummern identifiziert werden können. All diese Informationen werden als vererbte Attribute bezeichnet.

Um die gewaltige Menge an Datenbeziehungen zwischen Grundsubstanzen, Zwischenprodukten, Medikamenten und Verpackungen handhaben zu können, bedarf es der Anwendung folgender zwei Konzepte:

- **Aggregation von Daten.** Analog zur Aggregation von Komponenten in der Fertigung können Aussagen zu Produkten aus Informationen über deren Komponenten abgeleitet werden. Damit wird Tracking und Tracing möglich.
- **Vererbung von Daten.** Die Vererbung von Daten entspricht der Verknüpfung von Informationen über Ausgangsprodukte mit den Endprodukten durch El-

tern-Kind-Beziehungen. So umfasst die Historie eines Produktes auch die Historie der Ausgangsprodukte und ähnelt daher einem Stammbaum.

Aggregation und Vererbung reduzieren die erforderlichen Lesezugriffe an den kritischen Punkten der Supply Chain. Dadurch wird das Zusammenstellen der Informationen, welche für Tracking und Tracing oder die Überprüfung der Integrität der Produkte nötig sind, praktikabel. Mit Hilfe von Datenaggregation und Vererbung kann eine Palette durch das Lesen eines RFID-Tags eindeutig identifiziert und alle Informationen über jedes auf der Palette enthaltene Produkt sichtbar gemacht werden. Ohne Datenaggregation müsste für jedes Produkt ein separater Lesevorgang erfolgen, was den Prozess erheblich verteuern und verlangsamen würde.

Abbildung 2 veranschaulicht das Verfahren der Datenaggregation und Vererbung für den Informationsfluss zwischen zwei Parteien aus Abbildung 1 [KSC03]. In diesem Fall erfolgt der Informationsfluss parallel zum Fluss der Güter.

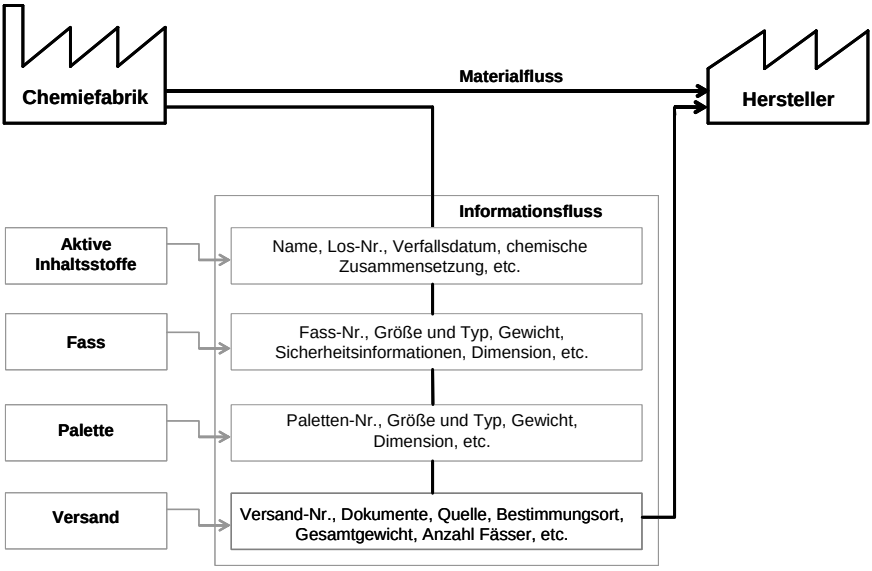


Abb. 2. Datenaggregation und Vererbung

Mehrere spezialisierte Veröffentlichungen setzen sich mit den technischen Details einer Lösung, wie sie von den Auto-ID Labs vorgeschlagen wurde, auseinander [FlK02, DiS03, Mil02a, Mil02b, CMF02]. In diesen wird auch näher auf das Zusammenspiel von Savant, Electronic Product Code (EPC), Physical Markup Language (PML) und Object Name Server (ONS) eingegangen.

4.2 Der Informationsfluss in der pharmazeutischen Lieferkette

Das der Logistik zugrunde liegende Prinzip beruht auf einem Fluss von Informationen für ein effektives Management. Insbesondere muss der Informationsfluss zwischen zwei Orten synchron zum parallelen Warenfluss ablaufen. Wichtige Konzepte zur Vereinfachung des Synchronisationsprozesses sind Vorpositionierungsregelungen oder die Verwendung eines zentralen Lagers innerhalb der Lieferkette [Mil02a, HMB03].

Anhand der Daten, die für einen Austausch von Waren zwischen zwei Unternehmen erforderlich sind, kann der Informationsfluss verdeutlicht werden. Fertige Produkte in der Konsumgüter- oder der Pharmaindustrie werden typischerweise in Kisten verpackt, welche wiederum auf Paletten zusammengefasst werden. Eine Lieferung besteht dann aus einer spezifischen Anzahl von Paletten. Jeder Lieferung sind eine Identifikationsnummer, ein Frachtbrief und eine Rechnungsnummer zugeordnet.

Jede Kiste ist durch einen RFID-Chip mit einer eindeutigen Identifikationsnummer ausgestattet. Ein Object Name Server (ONS) verknüpft die elektronische Identifikationsnummer, auch Electronic Product Code (EPC) genannt, mit dem dazugehörigen Eintrag in einer Datenbank. Dies kann über eine Internetverbindung oder ein firmeneigenes Netz geschehen [Mil02a, Mil02b]. Um den Fluss von Informationen mit dem Transport der Güter zu synchronisieren, stehen dem Absender drei Möglichkeiten zur Verfügung: 1. Synchronisierung durch vorheriges Senden einer Datei, welche alle Informationen bezüglich der zu empfangenden Lieferung enthält (thick file approach), 2. vorheriges Senden der Identifikationsnummern (thin file approach) oder 3. Übertragen ausgewählter Informationen an eine dritte Partei, welche dem Empfänger einen Zugriff ermöglicht.

Die Integrität der Lieferung kann bereits mit Option 2, also dem Senden der korrespondierenden Identifikationsnummern, überprüft werden. Tracking und Tracing wird jedoch erst durch den „thick file approach“ ermöglicht. Diese dynamischen Daten können folgende Informationen enthalten:

1. Absender
2. Ziel
3. Zeitangaben
4. Namen der beteiligten Unternehmen
5. Telemetrie-Informationen (z.B. Temperatur und Luftfeuchtigkeit)

Angaben zum Ort sind für Tracking und Tracing von besonderer Bedeutung, da sie Schlüsse auf den vorherigen Lagerort, die momentane Position und das geplante Ziel zulassen. Die Zeitangaben für jeden Ort erlauben die Berechnung der jeweiligen Verweildauer.

5 Realisierung des Informationssystems

Drei Faktoren tragen wesentlich zur Transparenz in der gesamten Lieferkette bei:

- Die elektronische Identifikationsnummer auf Ebene der einzelnen Produkte (Electronic Product Code, EPC), mit deren Hilfe sich die Granularität der Objektidentifikation verglichen mit herkömmlichen Barcode-Systemen erheblich erhöht [HMB03].
- Die Verfügbarkeit eines Produktdaten-Servers, der als Datenbank für Produktinformationen und zur Verwaltung der Stammbauminformationen dient.
- Eine gesicherte Internetverbindung, welche die Basis der Kommunikationsstruktur bildet.

Große Fortschritte innerhalb der letzten Jahre im Bereich der RFID-Tags und der Servertechnologie ermöglichen eine technische Umsetzung der vorgeschlagenen Lösung. Mehrere Hersteller von RFID-Tags, Lesegeräten und Produktdaten-Servern sind in der Lage, geeignete Komponenten in ausreichenden Mengen zu produzieren. Aufgrund von Skalen- und Lernkurveneffekten ist bei steigenden Stückzahlen mit einem deutlichen Rückgang der Preise zu rechnen. Ein umfassender Einsatz der RFID-Technologie in der Pharmaindustrie wird daher in naher Zukunft möglich sein.

Beschleunigt wird die Entwicklung von der US-amerikanischen Food and Drug Administration (FDA), welche in ihrem Bericht *Combating Counterfeit Drugs* ihre unterstützende Rolle bei der Einführung von RFID-Lösungen bekräftigt. Darüber hinaus plant die FDA, auch bei der Schaffung von Standards mitzuwirken. Einen groß angelegten Einsatz der RFID-Technologie erwartet die FDA bis zum Jahre 2007 [FDA04].

5.1 Datenbanken

Kernelemente der vorgeschlagenen Architektur sind drei Datenbanktypen. Für jede können den Beteiligten individuelle Zugriffsrechte eingeräumt werden.

Die *Herstellerdatenbank* beinhaltet Informationen zu den Medikamenten wie Zusammensetzung oder Gefahrenhinweise. Eine Teilmenge der Informationen ist für beteiligte Parteien über gesicherte Internetverbindungen zugänglich. Die zentrale *Repository-Datenbank* beinhaltet die gesamte Historie der Transaktionen eines Medikamentes in der Lieferkette. Auf diese Informationen können Berechtigte mit dem EPC als Schlüssel zugreifen. Die Repository-Datenbank kann von einer externen Organisation verwaltet werden und enthält lediglich Informationen, die zu einer Absicherung der Integrität der Arzneimittel benötigt werden. Die *lokalen Datenbanken* enthalten Informationen, die nur für den aktuellen Besitzer erforderlich sind. Dies können z.B. Angaben zum Aufbewahrungsort im Lager sein. Ein schematischer Überblick über die Datenbankstruktur ist in Abbildung 3 gegeben [KSC03].

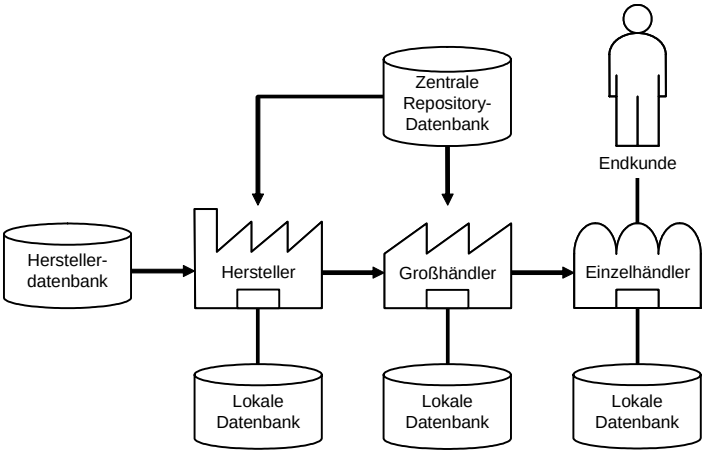


Abb. 3. Übersicht über die Datenbanken des Informationssystems

5.2 Anwendung zum Schutz vor Arzneimittelfälschung

Die vorgestellte Architektur ermöglicht sowohl effizientes, automatisiertes Tracking und Tracing als auch eine Überprüfung der Medikamente auf Echtheit. Im Folgenden sind analog zum Fluss eines Produktes durch die Lieferkette die Eintragungen in der zentralen Repository-Datenbank aufgeführt.

Tracking und Tracing. Abbildung 4 zeigt eine Darstellung der Lieferkette mit Produktdaten-Servern, welche die zentrale Repository-Datenbank realisieren [HMB03]. Die vier mit A, B, C und D bezeichneten Unternehmen entsprechen dem Chemikalien-Lieferant (A), dem Hersteller (B), dem Großhändler (C) und dem Händler (D) aus Abbildung 1. In diesem Szenario schreiben die Unternehmen die Informationen zur Aktualisierung des Stammbaums bei jeder Transaktion in die zentrale Repository-Datenbank. Die Konzepte der Vererbung und der Aggregation reduzieren den Kommunikationsaufwand auf die Übermittlung der Identifikationsnummern der entsprechenden Produkte bei Versand oder Einlagerung. Die Speicherung in einer zentralen Datenbank erleichtert den Zugang der Beteiligten und ermöglicht Suchanfragen in Echtzeit.

Überprüfung auf Echtheit. Ein erster Ansatz zur Überprüfung der Originalität von Medikamenten kommt ohne die Erstellung eines vollständigen Stammbaums aus. Die Pflege einer zentralen Datenbank entfällt, lediglich der über eine gesicherte Internetverbindung zugängliche Produktdaten-Server des Herstellers ist erforderlich. Mit der eindeutigen Identifikationsnummer eines Medikamentes kann der Käufer mittels elektronischer Anfrage feststellen, ob der Ursprung des Medikamentes mit den Angaben auf der Verpackung übereinstimmt. Der Ansatz entspricht dem weiter oben erwähnten „thin file approach“, bei dem Kunden lediglich EPCs übertragen und auf Vorhandensein in einer Liste gültiger Identifikationsnummern beim Hersteller überprüfen. Eventuell bestehende Diskrepanzen sind starke Indizien für Arzneimittelfälschungen [KSC03]. Dieses relativ einfache

Verfahren bietet einen weniger umfassenden Schutz vor Fälschungen als eine vollständige Tracking-und-Tracing-Lösung. Mit letzterer kann sich auch der Verkäufer als rechtmäßiger Besitzer ausweisen, jedoch beugt auch der erste Ansatz einem Betrug im großen Stile vor und kann als erster Schritt hin zur Implementierung einer vollständigen Tracking-und-Tracing-Lösung angesehen werden.

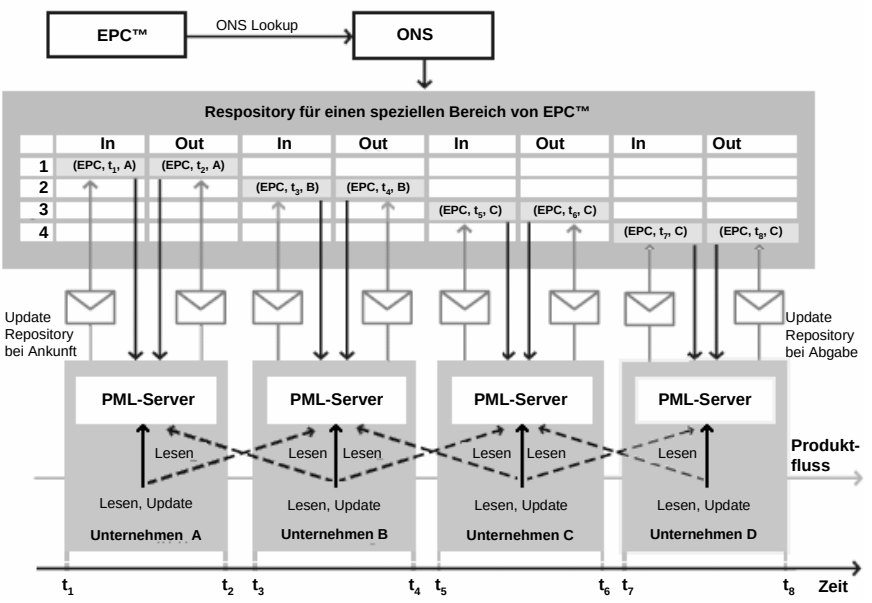


Abb. 4. Produktdaten-Server auf Ebene der einzelnen Wertschöpfungsstufen [KSC03]

Der Fälschungsschutz, den die beschriebene Tracking-und-Tracing-Lösung bietet, ist für die meisten Medikamente ausreichend. Ein höheres Maß an Fälschungssicherheit lässt sich mit RFID-Tags erreichen, welche in ihrer Funktionalität und Komplexität Smart Cards ähneln. Solche Tags stellen Funktionen für kryptografische Anwendungen zur Verfügung. Mit so genannten Challenge-Response-Ansätzen ist die Identifizierung von Tags anhand eines geheimen Schlüssels möglich, ohne diesen direkt zu übertragen. Der Schlüssel kann nicht ausgelesen werden, was die Duplizierung einzelner Transponder verhindert [StF04]. Eine Erweiterung der Infrastruktur um solche Verfahren ist möglich und stellt sicher, dass diese auch zukünftige Anforderungen erfüllt.

6 Zusammenfassung

Mit Hilfe moderner RFID-Technologie und geeigneten Informationssystem-Strukturen wird sowohl Tracking und Tracing als auch ein effektives Testen auf Echtheit von Arzneimitteln möglich.

Die vorgeschlagene Lösung setzt voraus, dass alle Hersteller, Spediteure, Großhändler und Händler mit Systemen zum Lesen von RFID-Tags ausgestattet sind und über das Internet mit externen Datenbanken kommunizieren können. Diese Voraussetzungen sind heute noch nicht gegeben. Die Mängel des bestehenden, auf Barcodes und herkömmlicher Etikettierung basierenden Ansatzes begünstigen jedoch den Einsatz von RFID-Technologie. Die Vorgaben der Gesetzgeber und die Empfehlungen einflussreicher Organisationen wie der amerikanischen Food and Drug Administration beschleunigen die Entwicklung weiter.

Tracking und Tracing kann darüber hinaus zukünftig als Basis weiterer Anwendungen dienen. Als Beispiel sei hier die stetig wachsende Zahl der Medikamente genannt, die in sehr geringen Stückzahlen auf einer „Make-to-order-Basis" hergestellt werden und deren effizienter Vertrieb eine große Herausforderung darstellt. RFID-Technologie legt auch hier die Grundlagen für eine effizientere und sicherere Gestaltung der Lieferkette der Pharmaindustrie.

Literatur

[App03] Appleby J (2003) Fake drugs show up in U.S. pharmacies: As prescription prices rise, counterfeiters chase profits. USA Today, March 15, 2003

[CMF02] Chang Y, McFarlane D, Koh R, Floerkemeier C, Putta L (2002) Methodologies for Integrating Auto-ID Data with Existing Manufacturing Business Information Systems. Auto-ID Center White Paper, www.autoidlabs.org/whitepapers/CAM-AUTOID-WH009.pdf

[Cot01] Cottril K (2001) Blockbuster Market. Traffic World 27: 17–19

[DiS03] Dinning M, Schuster EW (2003) Fighting Fiction. APICS – The Performance Advantage

[ESP02] Engels DW, Sarma SE, Putta L, Brock D (2002) The Networked Physical World System. In: Proceedings of the IADIS International Conference on WWW/Internet 2002

[FDA04] Food and Drug Administration (2004) Combating Counterfeit Drugs. Report, www.fda.gov/oc/initiatives/counterfeit/report02_04.html

[FIP03] International Pharmaceutical Federation (2003) FIP-Grundsatzerklärung zu gefälschten Arzneimitteln, www.fip.org/pdf/counterfeitmedicines2003DE.pdf

[FlK02] Floerkemeier C, Koh R (2002) Physical Mark-Up Language Update. Auto-ID Center Technical Memo, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-006.pdf

[HDMA04] Healthcare Distribution Management Association (2004) Pharmaceutical Product Tampering News Media Fact Sheet, www.healthcaredistribution.org/resources/pdf_news/Product%20Tampering%20edit.pdf

[HMB03] Harrison MG, Morgane HJ, Brusey JP, McFarlane DC (2003) PML Server Developments. Auto-ID Center White Paper, www. autoilabs.org/whitepapers/CAM-AUTOID-WH015.pdf

[KSC03] Koh R, Schuster EW, Chackrabarti I, Bellman A (2003) Securing the Pharmaceutical Supply Chain. Auto-ID Center White Paper, www.autoidlabs.org/whitepapers/MIT-AUTOID-WH021.pdf

[Mag02] Magali P (2002) Protecting Medicines & Pharmaceuticals – A Manual of Anti Counterfeiting Solutions. Reconnaissance International

[Mil02a] Milne TP (2002) Auto-ID Business Use-Case Framework (A-Biz) – Background. Auto-ID Center Technical Memo, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-009.pdf

[Mil02b] Milne TP (2002) Auto-ID Business Use-Case Framework (A-Biz): Despatch Advice Use-Case. Auto-ID Center Technical Memo, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TM-010.pdf

[Mit98] Mitchell P (1998) Documentation – an Essential Precursor to Drug Manufacturing. APICS – The Performance Advantage, September, 1998

[StF04] Staake T, Fleisch E (2004) The Potential of RFID in Anti-Counterfeiting. M-Lab Working Paper No. 26, Universität St. Gallen / ETH Zürich

[WHO03] WHO (2003) Counterfeit medicines – Frequently Asked Questions, www.who.int/medicines/organization/qsm/activities/qualityassuance/cft/counterfeit_faq.htm

Potenziale der RFID-Technologie für das Supply Chain Management in der Automobilindustrie

Martin Strassner
Institut für Technologiemanagement, Universität St. Gallen

Christian Plenge, Stefan Stroh
Booz Allen Hamilton GmbH, Düsseldorf und Frankfurt

Kurzfassung. RFID stellt nach dem Barcode die nächste evolutionäre Stufe der automatischen Identifikation (Auto-ID) dar. Diese Technologie ermöglicht die automatische Synchronisierung des Zustandes der physischen Ressourcen mit ihrer Abbildung in IT-Systemen. Dies führt zu Effizienzgewinnen durch die Vermeidung von Fehlern, die Einsparung manueller Tätigkeiten sowie die Beschleunigung von Abläufen. Mit diesen Eigenschaften besitzt die Technologie das Potenzial für zahlreiche Verbesserungen entlang von Wertschöpfungsketten. Der vorliegende Beitrag analysiert eine Reihe von Erfolg versprechenden Anwendungen im Bereich des Supply Chain Managements (SCM) in der Automobilindustrie. Hierbei zeigt der Beitrag, dass es in bestimmten Bereichen wie dem Behältermanagement oder in der Transportlogistik einen tatsächlichen Bedarf nach fortschrittlichen Auto-ID-Technologien gibt.

Schon heute nutzt die Automobilindustrie in verschiedenen Anwendungen die RFID-Technologie, beispielsweise zur Fahrzeugidentifikation, zur Qualitätskontrolle in der Produktion oder zum Management von Ladungsträgern. Weitere Effizienzsteigerungen ermöglicht der Einsatz standardisierter RFID-Systeme zur automatischen Identifikation von Einzelteilen und Produktionsmitteln (Assets). Bei vielen Anwendungen entsteht ein zusätzlicher Nutzen durch die Verknüpfung der Produktidentifikation mit weiteren Daten wie z.B. der Produkthistorie. Mögliche Anwendungen sind die Rückverfolgbarkeit von Teilen, die Verwaltung von Fahrzeugkonfigurationen, die Eindämmung der Produktpiraterie, die Umsetzung gesetzlicher Vorschriften (z.B. der Altautoverordnung) sowie das Asset Management.

Unternehmensübergreifende Szenarien erfordern hierbei eine ubiquitäre Auto-ID-Infrastruktur. Ebenso müssen die beteiligten Unternehmen Modelle für eine Verteilung von Kosten und Nutzen im Wertschöpfungsnetzwerk finden, sodass alle profitieren.

1 Einleitung

1.1 Motivation und Zielsetzung

Die Automobilindustrie sieht in der Optimierung der Lieferkette eine wichtige Maßnahme zur Steigerung der Wettbewerbsfähigkeit. Wesentliche Trends in diesem Bereich sind die Just-in-time-(JIT-) bzw. Just-in-sequence-(JIS)-Fertigung, die Dezentralisierung, die Massenindividualisierung (Mass Customization), die Null-Fehler-Strategie und die Verkürzung von Durchlaufzeiten.

Solche Konzepte sind nur durch weitere Effizienzsteigerungen in der Lieferkette zu verwirklichen. Nach Angaben von A.T. Kearney entfallen in der verarbeitenden Industrie bis zu 25 % der Betriebskosten auf das Supply Chain Management [May99]. Verglichen mit anderen Branchen gilt die Zulieferkette in der Automobilindustrie als vorbildlich – dies nicht zuletzt, weil die Unternehmen in den letzten Jahren einen großen Teil ihres IT-Budgets in die Verbesserung ihrer Supply-Chain-Management-Systeme investiert haben [Nav01].

Dennoch ist auch in der Automobilindustrie eine vollständige Transparenz in der Zulieferkette bisher noch eine Wunschvorstellung: Verspätete oder fehlgeleitete Lieferungen sowie falsche Informationen über Lagerbestände führen zu überhöhten Sicherheitsbeständen, langen Suchzeiten, Verzögerungen in der Produktion, Maschinenstillständen und teuren Eilbestellungen.

Einige Marktforschungsinstitute sehen RFID (Radiofrequenzidentifikation) als eine Schlüsseltechnologie zur Verbesserung von Lieferketten in Handel und Industrie[27]. RFID-Chips ermöglichen die automatische Identifikation (Auto-ID) ohne Sichtkontakt und im Pulk. Sie speichern mindestens eine Identifikationsnummer, lassen sich aber auch zur Speicherung von Datensätzen, z.B. der Produkthistorie oder warenbegleitender Informationen, verwenden [Fin02]. Booz Allen Hamilton und das Auto-ID Lab an der Universität St. Gallen haben im Rahmen einer Studie 24 Unternehmen aus der Automobil- und Logistikindustrie zu den Potenzialen der RFID-Technologie befragt [FRS04a, FRS04b]. 83 % gaben an, dass sie dieser Technologie eine strategische Bedeutung beimessen. Die Mehrzahl der befragten Unternehmen sieht sich als Innovator und sammelt bereits Erfahrungen mit operativen Anwendungen oder Pilotsystemen. Sowohl in der Automobilindustrie als auch bei den Logistikdienstleistern ist RFID derzeit ein wichtiges Thema auf Kongressen und Inhalt von mehreren Arbeitskreisen.

Dieser Beitrag untersucht, in welchen Bereichen RFID-Systeme Nutzen für die Automobilindustrie stiften können. Neben lokalen Anwendungen, wie beispielsweise dem Einsatz der RFID-Technologie zur Produktionskontrolle, befasst sich der Beitrag mit den Potenzialen, die in einer prozessübergreifenden Nutzung der Technologie liegen, und mit den Herausforderungen für die Einführung. Bei unternehmensübergreifenden Systemen betrifft dies alle Unternehmen, die zur Lieferkette der Automobilindustrie gehören.

Nachfolgend beschreibt der Beitrag anhand eines Modells der Wertschöpfungskette die Rollen der einzelnen Unternehmen bei der Nutzung von Auto-ID-

[27] Nach Allied Business Intelligence werden im Jahr 2007 46 % des RFID-Marktes auf Supply-Chain-Anwendungen entfallen [Rfi03b].

Systemen. Der zweite Abschnitt analysiert mögliche Anwendungsbereiche von RFID-Systemen und stellt jeweils das Nutzenpotenzial dar. Abschnitt 3 beschreibt basierend auf den Ergebnissen der Studie die Motivation für die Einführung von RFID-Lösungen, aber auch die Herausforderungen, mit denen die befragten Unternehmen hierbei konfrontiert sind. Abschließend fasst Abschnitt 4 die wesentlichen Erkenntnisse des Beitrags zusammen.

1.2 Die Wertschöpfungskette der Automobilindustrie

Entlang der Wertschöpfungskette (kurz Wertkette) der Automobilindustrie kooperieren unterschiedliche Unternehmen zur Erstellung des Endprodukts Automobil und komplementärer Services (siehe Abbildung 1). Zur Untersuchung der Auswirkungen des Einsatzes von RFID zur Produktkennzeichnung sind diejenigen Unternehmen relevant, die am physischen Warenfluss beteiligt sind: Hierzu gehören Zulieferunternehmen, Logistikdienstleister, die Fahrzeughersteller (Original Equipment Manufacturers, kurz OEMs), Händler und Werkstätten. Weitere Unternehmen, wie beispielsweise Informationsdienstleister oder Versicherungen, gehören ebenso zum Wertschöpfungsnetzwerk.

Ein Informationsaustausch zwischen den beteiligten Unternehmen kann die Effizienz der gesamten Wertkette erheblich steigern. Moderne Konzepte zur Effizienzsteigerung in der Lieferkette wie Collaborative Planning, Forecasting and Replenishment (CPFR), dezentral organisierte Zulieferparks, Vendor Managed Inventories (VMIs) oder JIT/JIS setzen Informationstransparenz entlang der Wertkette voraus. Beispielsweise beklagen die Zulieferer, dass die OEMs ihnen Daten über die tatsächlichen Bedarfe erst zu spät mitteilen, was zu Überproduktion oder teuren Sonderschichten führt.

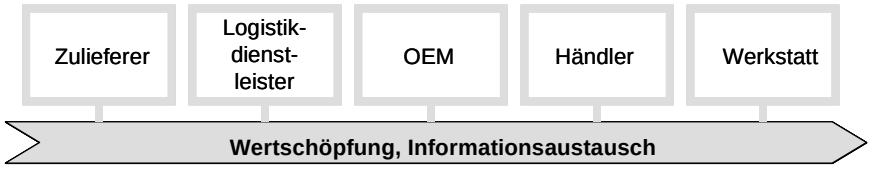


Abb. 1. Wertschöpfungskette der Automobilindustrie

Eine wesentliche Voraussetzung für einen effizienten Informationsaustausch zwischen den Wertschöpfungspartnern sind gemeinsame Daten- und Kommunikationsstandards. In der Praxis geben entweder die OEMs für die anderen Wertschöpfungspartner solche Standards vor oder sie kommen durch Vermittlung der Automobilverbände, z.B. AIAG (Automotive Industry Action Group), JAMA/JAPIA (Japan Automotive Manufacturers Association/Japan Auto Parts Industries Association) oder Odette[28], industrieweit zustande.

[28] Odette ist ein europäischer Automobilverband, der sich mit der Entwicklung von Standards in den Bereichen E-Business und Logistik befasst.

In der Vergangenheit ging die Initiative für Standards in der Logistikkette meistens von den OEMs aus, die derzeit am meisten Gewicht innerhalb der Wertschöpfungskette besitzen. Zunehmend spielen hierbei auch Technologieanbieter eine wichtige Rolle, die IT-Infrastrukturen zur Verfügung stellen, die einerseits vorhandene Standards unterstützen, andererseits aber auch neue Standards schaffen können.

Die Automobilhersteller waren in der Vergangenheit in der Lage, neue Standards rasch umzusetzen, wenn der Nutzen offensichtlich war. Ein Beispiel hierfür ist die Spezifikation von Versandetiketten gemäß GM 1724. Diesen Standard führte General Motors (GM) 1999 ein und seit 2001 ist er für alle Zulieferer von GM verpflichtend. Nach Schätzungen von GM spart das System mehr als 100 Millionen Dollar jährlich an Versand- und Fehlerkosten [Kil00]. Dieser Standard dient heute als Vorlage für einen gemeinsamen Standardisierungsvorschlag für die gesamte Automobilindustrie.

Beim Einsatz der RFID-Technologie vereinfachen Standards den Austausch von Informationen und senken, bezogen auf die gesamte Wertkette, die Kosten für die Einrichtung entsprechender Auto-ID-Systeme. Nachfolgendes Szenario, das von einer RFID-Kennzeichnung durch die Zulieferer ausgeht, soll dies verdeutlichen.

Angenommen, alle Bauteile eines Autos sollen mittels eines RFID-Chips eindeutig identifizierbar sein. Zu diesem Zweck müsste die Kennzeichnung schon während der Produktion durch den Zulieferer erfolgen. Dem Zulieferer entstehen zusätzliche Kosten für den Chip sowie für dessen Anbringung. Einen möglichen Nutzen können die Zulieferer durch ein effizienteres Lagermanagement (automatische Inventur) sowie in der Distribution generieren. Bei Kosten von ca. 0,50 EUR pro RFID-Chip wird sich jedoch die Verwendung zur Produktkennzeichnung für die meisten Produkte wirtschaftlich nicht rechtfertigen lassen.[29] Allerdings können die OEMs durch Anwendungen in den Bereichen Lagermanagement, Diebstahlschutz, Echtheitsnachweis, Produktionsmanagement, Distribution und Recycling Verbesserungen erzielen.

Händler und Werkstätten können die automatische Identifikation in den Bereichen Distribution, Diebstahlkontrolle, Echtheitsnachweis sowie Wartung nutzen. Die wesentlichen Kostenblöcke und Nutzenpotenziale für die einzelnen Unternehmen sind in Tabelle 1 dargestellt.

Es stellen sich die Fragen, wie einerseits ein derartiges System mit möglichst geringen Kosten realisiert werden kann und andererseits die Kosten so aufgeteilt werden können, dass alle Beteiligten profitieren. Für die im folgenden Abschnitt beschriebenen Anwendungen zeigt der Beitrag, wie RFID zu Verbesserungen führen kann, inwieweit Standards dafür eine Voraussetzung darstellen und durch welchen Nutzen sich die Einführung wirtschaftlich rechtfertigen lässt.

[29] Derzeit liegen die Preise für passive RFID-Chips bei ca. 0,50 EUR. Durch steigende Nachfrage könnte in einigen Jahren ein Preis von nur noch 0,05 EUR möglich sein [Sar01].

Tabelle 1. Kosten- und Nutzenverteilung bei der RFID-Einzelteilekennzeichnung

	Zulieferer	OEM	Händler	Werkstatt
Kosten	• RFID-Kennzeichnung • Anpassung des Produktionsprozesses • Erfassungsgeräte • Infrastruktur	• Erfassungsgeräte • Infrastruktur • Integration in die bestehende IT-Infrastruktur	• Erfassungsgeräte • Infrastruktur	• Erfassungsgeräte • Infrastruktur
Nutzen	• Lagermanagement • Distribution • Diebstahlkontrolle	• Lagermanagement • Diebstahlkontrolle • Echtheitsnachweis • Produktion • Distribution • Rückrufe • Recycling	• Distribution • Diebstahlkontrolle • Echtheitsnachweis	• Wartung • Echtheitsnachweis

2 Anwendungen und Nutzenpotenziale

Nutzenpotenziale der RFID-Technologie bestehen in verschiedenen Anwendungsbereichen des Supply Chain Managements der Automobilindustrie. Dieser Beitrag ordnet die Anwendungen zwei Einsatzgebieten zu, dem Tracking von Einzelteilen und dem Asset Management (siehe Abbildung 2). Nachfolgende Abschnitte beschreiben zu jedem der Einsatzgebiete, auf welche Weise die RFID-Technologie Nutzen stiften kann und nennt Anwendungsbeispiele.

Das Tracking[30] von Einzelteilen ermöglicht Verbesserungen in den Bereichen Lagermanagement, Distribution, Echtheitsnachweis, Diebstahlschutz, Produktion, Rückruf, Wartung und Recycling. Zu diesem Zweck ist eine Kennzeichnung notwendig. Heute übliche Methoden zur Kennzeichnung von Einzelteilen sind nicht standardisierte Beschriftungen (als Label oder Gravur), OCR-Beschriftungen, einzeilige Barcodes, 2-D-Barcodes, Matrixcodes sowie RFID-Chips. Nur die Abwicklung über eine gemeinsame Auto-ID-Infrastruktur ermöglicht ein effizientes Tracking von Einzelteilen über die gesamte Wertschöpfungskette hinweg.

[30] Unter Tracking wird hier die Ortsverfolgung sowie die Statusüberwachung verstanden.

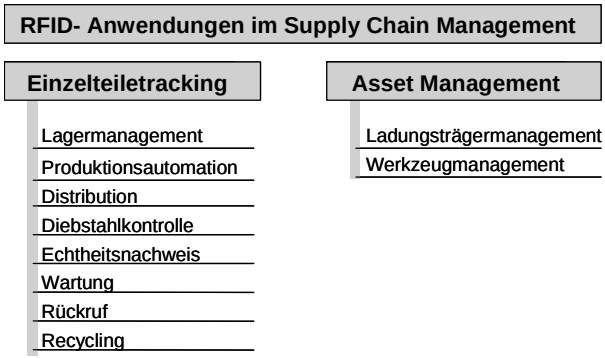


Abb. 2. RFID-Anwendungsbereiche im SCM der Automobilindustrie

2.1 Tracking von Einzelteilen

Lagermanagement

Die Aufgabe des Lagermanagements ist die Bereitstellung eines Puffers zur Deckung des Bedarfs nachgelagerter Stufen in der Wertkette. Mangelnde Kenntnis über Lagerbestände und Kundennachfrage der nachgelagerten Stufen sind eine Ursache für den „Bullwhip-Effekt“ (Peitscheneffekt) [LPW97]. Dieser Effekt führt aus Lieferantensicht zu nicht vorhersehbaren Schwankungen in der Kundennachfrage. Um die Lieferfähigkeit sicherzustellen, legen die Lieferanten Sicherheitsbestände an, die mit entsprechenden Lagerhaltungskosten verbunden sind.

Neben Schwankungen auf der Nachfrageseite können Sicherheitsbestände auch aufgrund mangelnder Zuverlässigkeit der Versorgungsseite notwendig sein. Bei langen Bestellzeiten oder häufigen Abweichungen von vereinbarten Lieferterminen, z.B. bedingt durch Maschinenausfälle, die Wahl eines unzuverlässigen Transportmittels, Lieferungen an den falschen Ort, müssen die Unternehmen auch Sicherheitsbestände halten. Andernfalls steigt das Risiko teurer Eilbestellungen oder Produktionsstillstände.

Klassische Zentrallager ersetzen die Automobilwerke zunehmend durch kleine produktionsnahe Lager. Die Anlieferung von ca. 30 % aller Teile erfolgt nach dem Just-in-time-Verfahren. Die dezentralen Lager sind meist nicht automatisiert und erfordern manuelle Koordination. Aus diesem Grund kommt es häufiger vor, dass eine Ladung auf dem Werksgelände an den falschen Ort gelangt.

Das Tracking der Teilelieferungen kann die Transparenz in der Lieferkette erhöhen. Beim Tracking erfasst das Informationssystem Teilelieferungen entweder an bestimmten Kontrollpunkten in der Lieferkette (z.B. Lagerausgang) oder fortlaufend. Bei Verwendung traditioneller Identifikationstechnologien (z.B. Barcode) ist eine zuverlässige Kontrolle nur mit großem Aufwand machbar. Die RFID-Technologie bietet die Möglichkeit, die Kontrollen nach Art und Menge der Teile automatisch, d.h. ohne manuelle Tätigkeiten, und weitgehend fehlerfrei durchzuführen.

Zur Realisierung eines solchen Systems gibt es verschiedene Möglichkeiten der Kennzeichnung:

- Kennzeichnung jedes Einzelteils
- Kennzeichnung der Verpackungseinheit
- Kennzeichnung des Ladungsträgers

Falls jedes Einzelteil gekennzeichnet ist, kann prinzipiell an jedem Kontrollpunkt eine Überprüfung auf Identität und Menge der Teile erfolgen[31]. Zu diesem Zweck müssten sich Leseschleusen mit Anbindung an das IT-System an den Kontrollpunkten befinden. Unter Zuhilfenahme zusätzlich im System verfügbarer Informationen (z.B. über den Bestimmungsort, Liefertermin, Rückrufe) lassen sich vor Ort Entscheidungen über die weitere Behandlung der Lieferung (z.B. Wahl des Transportmittels, Bestimmung des Lagerplatzes oder Retouren) treffen.

In den meisten Fällen ist eine Unterscheidung einzelner Teile einer Teileart nicht notwendig. Eine Kennzeichnung der Verpackungseinheit ist in diesem Fall ausreichend. Wenn jedoch in der Transportkette eine Vereinzelung der Verpackungseinheit erfolgt, z.B. durch Umverpackung, ist eine Kennzeichnung der Verpackungseinheit eventuell nicht sinnvoll.

Auch durch Kennzeichnung des Ladungsträgers (Behälter, Container, Palette) ist ein Tracking der Lieferung möglich. Diese Anwendung wird oft als „Soft Tracking“ bezeichnet. Die Informationen über die Lieferung (Inhalt des Ladungsträgers) sind hierbei in einer Datenbank gespeichert. Bei der Beladung bzw. Entladung muss eine Aktualisierung dieser Daten erfolgen. Dieser Vorgang stellt eine potenzielle Fehlerquelle dar. Aufgrund der Wiederverwendbarkeit der Ladungsträger ist hierfür auch der Einsatz teurerer aktiver Transponder mit großer Erfassungsreichweite sinnvoll. Diese Chips lassen sich leicht mit einem Datenspeicher kombinieren, sodass sich warenbegeleitende Informationen (z.B. der Lieferschein) auf dem Ladungsträger speichern lassen.

Die Auswahl des passenden Systems hängt wesentlich von der Art der Lieferung ab. Bei häufig in sehr großen Stückzahlen gelieferten B- und C-Teilen erscheint z.B. eine Einzelteilidentifikation weder notwendig noch aus wirtschaftlichen Gründen sinnvoll. Nachfolgendes Beispiel beschreibt, mit welcher Lösung der Automobilhersteller Ford an einigen Standorten die Teileversorgung sicherstellt.

Beispiel „Teileversorgung bei Ford“. Ford setzt an einigen Standorten ein Kanban-System ein, das die RFID-Technologie zur Ermittlung der Bedarfe sowie zum werksinternen Tracking des Nachschubs verwendet. An den betreffenden Standorten existiert ein Netzwerk von Lesestationen mit Antennen, die eine Erfassung der verwendeten Transponder innerhalb der Werke ermöglichen. Das Signal eines Transponders wird jeweils von mehreren Antennen empfangen. Ein zentrales Lokalisierungsgerät berechnet aus diesen Daten mittels Triangulation die Position des Transponders bzw. des Objekts, welches der Transponder kennzeichnet.

[31] Im praktischen Einsatz existieren technische Beschränkungen bei der Verwendung der RFID-Technologie in metallischem Umfeld. In diesem Fall wird die Erfassungsreichweite reduziert bzw. eine zuverlässige Erfassung ist nicht immer möglich.

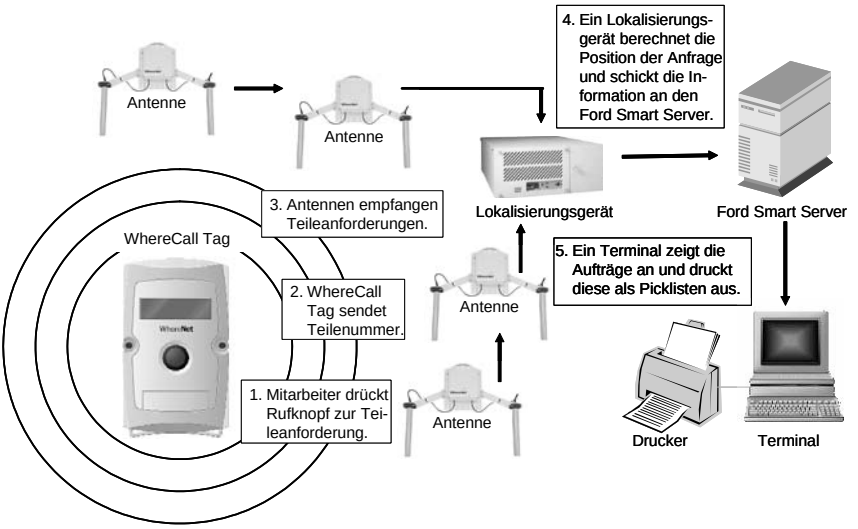


Abb. 3. Architektur des WhereCall-Systems zur Teileversorgung

Zur Anforderung von Teilen verwenden die Monteure „elektronische Bestellkarten“. Hierbei handelt es sich um mobile Geräte (WhereCall Tags), die mit einem Transponder ausgestattet sind, und denen eine Teilenummer zugeordnet ist. Diese Geräte lassen sich einfach am Bedarfsort anbringen. Wenn der Monteur Nachschub benötigt, drückt er auf einen Knopf am Gerät. Der Transponder sendet dann die Teilenummer an das Nachschubsystem. Das Lokalisierungsgerät bestimmt hierbei zusätzlich den Ort der Bestellung (siehe Abbildung 3).

Die Rollcontainer, die auf dem Gelände zum Transport von Teilen eingesetzt werden, sind ebenfalls mit Transpondern ausgestattet. Bei der Befüllung wird in einer Datenbank die auf dem Chip gespeicherte Containernummer der entsprechenden Teilenummer zugeordnet. Auf diese Weise bestimmt das Nachschubsystem den nächsten verfügbaren Teilevorrat und generiert einen Transportauftrag für die Werkslogistik. Mit diesem System hat Ford die Zuverlässigkeit der Teileversorgung erhöhen können [Nav00].

Echtheitsnachweis und Diebstahlschutz

Nach Angaben eines Automobilherstellers handelt es sich bei 10 % aller als Originalersatzteile vertriebenen Teile in Wirklichkeit um Fälschungen. Dies würde entgangene Umsätze in Höhe von 12 Milliarden Euro pro Jahr für das Ersatzteilgeschäft der gesamten Automobilindustrie bedeuten [SLA02].

Hierbei lassen sich zwei Arten von „Fälschungen“ unterscheiden. Erstens existieren nachgeahmte Produkte (Plagiate), deren Herkunft sich schwer ermitteln lässt. Die Qualität dieser Produkte kann sehr unterschiedlich sein. Falls der Kunde davon ausgeht, ein Originalersatzteil gekauft zu haben und unzufrieden mit dem Produkt ist, kann dies dem Ansehen des OEMs schaden.

Zweitens rechnen die OEMs auch solche Teile zu den „Fälschungen“, die zwar von einem offiziellen Vertragspartner gefertigt wurden, jedoch nicht über einen bestimmten Vertriebsweg auf den Markt gelangt sind. An diesen Teilen, die als Originalteile verkauft werden, verdient der OEM nicht mit. Dennoch ist er von einer möglichen Produkthaftung betroffen. Das Risiko, wegen eines solchen Teils verklagt zu werden, ist neben den Umsatzeinbußen und möglichen Imageschäden ein weiterer Grund, gegen „Fälschungen“ vorzugehen.

Diebstahl ist in der Automobilindustrie genauso wie in Lieferketten anderer Industriebereiche ein Problem. Teile verschwinden sowohl während des Transports vom Zulieferer zum Werk (externer Diebstahl) als auch im Werk selbst (interner Diebstahl). Besonders vom Diebstahl betroffen sind Elektronikteile. Ein Lösungsansatz zur Reduktion des externen Diebstahls besteht in der Versiegelung der Transportbehälter.

Die Verwendung der RFID-Technologie zur Teilekennzeichnung kann dazu beitragen, Fälschungen sowie Diebstähle aufzudecken. Wenn jedes Teil eine individuelle Seriennummer besitzt, lässt sich in Verbindung mit der zugehörigen Produkthistorie jederzeit nachweisen, ob es sich um eine Fälschung bzw. ein gestohlenes Teil handelt. Diese Anwendung setzt eine entsprechende Infrastruktur von Kontrollstellen voraus, an denen die Identitätsprüfung erfolgt. Der Zugriff auf die Produkthistorien (z.B. aus einem Produktdatenmanagement-System) muss gewährleistet sein. Aufgrund der Menge der zu überprüfenden Teile sind vollständige Kontrollen nur dann wirtschaftlich sinnvoll, wenn sie automatisch, wie etwa durch RFID-Technologie, möglich sind.

Auch mit einer solchen Anwendung von RFID-Chips wäre es nicht möglich, jeden Diebstahl bzw. jede Fälschung sofort zu entdecken. Allerdings lassen sich Stationen in der Lieferkette, die stark von Schwund betroffen sind, besser identifizieren. Eine wichtige Kontrollstelle in diesem System könnte der Handel einnehmen und auf diese Weise die Verbreitung von Fälschungen und gestohlener Ware eindämmen. Da RFID-Kennzeichnungen schwer fälschbar sind, ließen sich gefälschte und gestohlene Teile noch lange nach dem Verkauf eindeutig identifizieren, z.B. wenn ein Rechtsstreit dies erfordert.

Produktionsautomation und Massenindividualisierung

Automobile sind in der heutigen Zeit mehr und mehr Einzelanfertigungen gemäß Kundenwunsch.[32] Dies stellt eine Herausforderung für das Produktionsmanagement dar. Durch eine laufende Qualitätskontrolle wird sichergestellt, dass die Monteure die Teile eindeutig den Bestellungen zuordnen können und die Fahrzeuge entsprechend den Bestellungen richtig zusammenbauen.

Die Identifikation des halbfertigen Fahrzeugs durch Barcode oder RFID-Chip ist in der Produktion üblich. Mittels dieser Kennzeichnung erkennt das Produktionssteuerungssystem das Fahrzeug an den einzelnen Arbeitsstationen und schlägt die zu verrichtenden Arbeitsschritte vor. Bei RFID-Systemen ist der Chip meist nicht am Fahrzeug direkt, sondern am Träger des Transportsystems angebracht.

[32] Würden alle Ausstattungsvarianten eines Golf IV gleich häufig gebaut, dann würden im Jahr höchstens zwei Fahrzeuge mit der gleichen Konfiguration hergestellt werden.

Dadurch ist eine Wiederverwendung möglich. Problematisch ist diese Vorgehensweise allerdings, wenn der Träger gewechselt wird, wie z.B. vor der Lackierung.

Neben der Identifikationsfunktionalität, welche die Massenindividualisierung unterstützt, ermöglichen solche Systeme auch die ständige Überwachung des Produktionsfortschritts. Auf diese Weise lässt sich der Auslieferungszeitpunkt genauer bestimmen und „Problemfahrzeuge“, die z.B. zu lange an einer Arbeitsstation stehen, kann die Produktionsleitung schneller identifizieren. Einige Systeme ermöglichen auch die Speicherung von Datensätzen zur Qualitätssicherung auf dem Chip. Ein solches System ist beispielsweise bei der Motorenfertigung von Ford im Einsatz.

Beispiel „Qualitätskontrolle in der Motorenfertigung bei Ford“. Die Montageträger des Motorenwerks von Ford in Essex besitzen RFID-Chips mit Datenspeichern. Je nach Bedarf legt die Produktionsplanung die Fertigungsreihenfolge der einzelnen Motorentypen fest. Sämtliche für die Produktion relevanten Daten eines Motors speichert das Produktionssystem dann auf dem Datenspeicher am Montageträger.

Jede Arbeitsstation liest die auszuführenden Arbeitsschritte aus dem Datenspeicher und quittiert die Ausführung. Den aktuellen Produktionsfortschritt übermittelt die Arbeitsstation an das Produktions-, Planungs- und Steuerungs-System (PPS-System). Die Dokumentation der Durchführung von Qualitätskontrollen erfolgt auf die gleiche Weise. Nach Abschluss der Fertigung lassen sich die teilweise äußerlich nicht unterscheidbaren Motoren mittels des Chips leicht identifizieren. Die gespeicherten Daten ermöglichen vor der Auslieferung die Sicherstellung der durchgeführten Qualitätskontrollen.

Die in der Anwendung verwendeten RFID-Chips sind ebenso wie der Montageträger wieder verwendbar. Die Schnittstelle zur Anbindung an das PPS-System musste Ford individuell erstellen. Ein wichtiger Grund für die Speicherung aller produktionsrelevanten Daten auf dem Chip ist, dass die Daten unabhängig von einem Zugriff auf das PPS-System verfügbar sein sollen. Die Produktion ist somit unabhängig von kurzzeitigen Ausfällen des Netzwerkes [EMS98].

Bisher setzen die Fahrzeughersteller RFID nur in wenigen Fällen für die automatische Identifikation von Einzelteilen ein. Vereinzelt gibt es Anwendungen in der Produktion, bei denen Einzelteile mit RFID-Chips gekennzeichnet sind. Bei diesen Teilen führt der falsche Einbau zu hohen Folgekosten, wie z.B. bei Kabelbäumen, oder die Dokumentation des Einbaus ist gesetzlich vorgeschrieben, wie z.B. bei Prallschutzelementen.

Distribution

In der Automobilindustrie organisieren Zulieferer, OEMs und Händler die Distribution von Teilen und fertigen Fahrzeugen. Die Distribution umfasst die Kommissionierung, die Verpackung und den Versand. Eine Warenausgangskontrolle soll sicherstellen, dass der Versand der Güter in der richtigen Menge und Qualität an die nächste Stufe der Wertkette bzw. an den Kunden erfolgt.

Bei der Kommissionierung kann die Produktkennzeichnung durch RFID dazu beitragen, dass schon während der Zusammenstellung der Lieferung ein automati-

scher Abgleich mit den Bestelldaten erfolgt. Insbesondere dort, wo eine hohe Anzahl an Produkten und Produktvarianten an verschiedene Empfänger zu senden ist, treten häufig Fehler auf. Diese hohe Komplexität trifft z.B. für die Ersatzteildistribution der OEMs zu. Das zentrale Ersatzteillager von Volkswagen in Kassel verwaltet beispielsweise mehr als 200 000 verschiedene Teilesorten, für die der Hersteller eine europaweite Auslieferung binnen 48 Stunden anbietet. Bestimmte elektronische Bauteile (z.B. Airbag-Steuerungen) erfordern vor der Auslieferung eine kundenindividuelle Konfiguration [TeS02].

Eine Kontrolle auf Richtigkeit der Lieferung erfolgt im Rahmen einer Warenausgangskontrolle. Mittels RFID-Technologie kann diese automatisiert durch Abgleich mit den Bestelldaten erfolgen. Weitere Informationen, die sich entweder auf dem Chip speichern lassen oder die aus einer Datenbank abgerufen werden können, sind beispielsweise die Konfiguration, die Qualitätsstufe sowie Anweisungen zu Verpackung und Transport.

Beim Versandhandel gibt es vergleichbare RFID-Anwendungen. Hierbei besitzen die zur Kommissionierung verwendeten Behälter eine RFID-Kennzeichnung. Vor der Zusammenstellung der Lieferung erfolgt mittels dieser Kennzeichnung die Zuordnung von Kommissionierbehältern zu einzelnen Bestellungen [Rfi03a]. Bei der anschließenden Erfassung der einsortierten Artikel verwendet der Versandhändler allerdings den Barcode.

Beispiel „Identifikation auszuliefernder Fahrzeuge bei Volkswagen". Ein Beispiel für den Einsatz der RFID-Technologie ist das System, das Volkswagen zur Identifikation der auszuliefernden Fahrzeuge in der Autostadt in Wolfsburg einsetzt. Bevor ein Fahrzeug auf den für die Auslieferung vorgesehen Parkplatz gelangt, bringt ein Mitarbeiter am Rückspiegel einen aktiven Transponder, der eine rote Signallampe besitzt, an. Wenn der Kunde ein bestimmtes Fahrzeug abholen möchte, fährt ein mit einem Lesegerät ausgerüstetes Suchfahrzeug über den Parkplatz und erkennt das richtige Fahrzeug anhand der blinkenden Signallampe [Ide00].

Rückruf

Die Anzahl an Rückrufen ist in der Automobilindustrie in den vergangenen Jahren stetig angestiegen. Öffentliche Rückrufaktionen sind teuer und schaden dem Ansehen des Herstellers[33]. Häufig sind die Hersteller verpflichtet, ganze Produktserien zurückzurufen, obwohl nur wenige Exemplare eines Bauteils von einem Fehler betroffen sein könnten. Würden exakte Daten über die Konfiguration jedes Autos vorliegen, wie es beispielsweise bei Flugzeugtriebwerken der Fall ist, könnten Rückrufaktionen viel gezielter, unauffälliger und billiger durchgeführt werden.

Ein bekanntes Beispiel ist der Rückruf von 14,4 Millionen Reifen der Firma Firestone durch Ford im Jahr 2000. Der Rückruf erfolgte in mehreren Staffeln, wobei Ford den Kreis der betroffenen Fahrzeuge jedes Mal weiter ausdehnte. Den

[33] Beispielsweise wurden im Jahr 2000 nach Angaben des ADAC 94 Rückrufaktionen in Deutschland durchgeführt.

durch die Rückrufaktion entstandenen Schaden beziffert Ford auf 2,6 Milliarden Dollar.

Beispiel „Standardisierung für das Reifen-Tracking". Ab 2006 schreibt in den USA der TREAD-(Transportation Recall Enhancement, Accountability, and Documentation-)Act den Herstellern vor, die Zuordnung von Fahrzeuggestellnummern und Seriennummern der verwendeten Reifen in einer Datenbank zu speichern.

Im Jahr 2002 definierte die AIAG (Automotive Industry Action Group) den Standard B-11, der zwei Möglichkeiten zur Kennzeichnung von Reifen spezifiziert. Eine Spezifikation verwendet 2-D-Barcodes, die andere basiert auf RFID-Chips. Dabei handelt es sich um den ersten Standard der Automobilindustrie, der eine RFID-Kennzeichnung auf Einzelteilebene spezifiziert. Hierbei hat der Reifenhersteller den Chip auf der Außenseite des Reifens zu befestigen. Die Datenstruktur der RFID-Lösung umfasst Angaben über den Hersteller, Werk, Datum, Reifengröße, eine eindeutige Seriennummer, die Fahrzeugnummer sowie einen frei verfügbaren Bereich.

Der VDA (Verband der Automobilindustrie) arbeitet ebenfalls an einem Standard für die Kennzeichnung von Reifen. Die Motivation liegt in möglichen Verbesserungen in der Reifenlogistik aber auch der Einhaltung des TREAD-Acts für Exportreifen. Die Variantenvielfalt von Reifen verlangt eine zuverlässige Kennzeichnung. Bei der Bereifung von Neufahrzeugen müssen die Hersteller neue Reifen verwenden und somit auf das Herstelldatum achten.

Die Form eines Reifens erschwert die Verwendung von Barcodes, da sich keine exakte Stelle für die Anbringung definieren lässt. RFID bietet hier die Möglichkeit einer unkomplizierten Identifikation, ohne erst die Position der Kennzeichnung finden zu müssen.

Wartung und Recycling

Eindeutig identifizierbare Bauteile können im After-Sales-Bereich außer bei Rückrufaktionen auch bei der Wartung sowie beim Recycling hilfreich sein. Bei der Wartung von Fahrzeugen spielt heute die Kenntnis der genauen Fahrzeugkonfiguration, insbesondere der elektronischen Bauteile, eine wichtige Rolle. Einige dieser Teile sind programmierbar. Durch unterschiedliche Softwareversionen zusammenwirkender Teile kann es zu Funktionsfehlern kommen. Die Information über die Fahrzeugkonfiguration kann der Hersteller entweder zentral, z.B. in einem Produktdatenmanagement-System, verwalten oder auf einem Datenspeicher am Fahrzeug selbst verfügbar machen. In beiden Fällen ist nach jedem Wartungseingriff eine Aktualisierung der Daten notwendig.

Schon heute fragt das Fahrzeugsystem einige Zustandsinformationen permanent ab (z.B. Funktionsfähigkeit der Airbags, Temperatur oder Beschleunigung der Räder). RFID-Chips, ggf. in Kombination mit Sensoren, könnten noch mehr Informationen über Einzelteile an ein fahrzeuginternes Überwachungssystem senden. Beispielsweise verwenden einige Reifendruck-Messsysteme RFID-Chips, um die vier Räder zu unterscheiden. Aufgrund des Alters von Verschleißteilen könnte das Fahrzeugsystem einen vorsorglichen Austausch empfehlen. Ein sol-

ches System könnte sogar sicherstellen, dass das Fahrzeug nur dann fährt, wenn keine unlizenzierten sicherheitsrelevanten Teile (z.B. Plagiate) enthalten sind.

Gemäß EU-Richtlinie 2000/53/EG müssen die Hersteller ab dem Jahr 2006 für Altautos eine Verwertungsquote von 85 % sicherstellen, ab dem Jahr 2015 sind es 95 %. Hierzu sind die Hersteller auch verpflichtet, den Verwertungsbetrieben demontagerelevante Informationen zu jedem Fahrzeug zur Verfügung zu stellen und wieder verwendbare bzw. verwertbare Bauteile und Werkstoffe zu kennzeichnen.

Der Einsatz der RFID-Technologie als Datenträger für demontagerelevante Informationen könnte vor allem bei größeren Bauteilen, die sich evtl. für eine Wiederverwendung eignen, sinnvoll sein. Durch Kenntnis der Produkthistorie einzelner Teile lässt sich der Wert leichter einschätzen. Die Demontage und Wiederverwendung spielt vor allem bei relativ neuen Unfallwagen eine wichtige Rolle. Altautos hingegen zerlegen die Verwertungsbetriebe nach der Trockenlegung nur grob und führen sie dem Shredder zu. Die für 2006 geforderte Verwertungsquote von 85 % erreichen die europäischen Verwertungsbetriebe schon heute.

2.2 Asset Management

Assets wie etwa Ladungsträger oder Werkzeuge sind Beispiele für Objekte, für die sich häufig geschlossene Kreisläufe identifizieren lassen. Beim Einsatz der RFID-Technologie ist hierbei eine Wiederverwendbarkeit der Chips möglich. Dies wiederum erhöht die Wirtschaftlichkeit der Anwendungen. Deshalb existieren in diesem Bereich derzeit schon einige Anwendungsbeispiele. Nachfolgende Abschnitte stellen Anwendungen sowie den möglichen Nutzen beim Behältermanagement und beim Werkzeugmanagement dar.

Behältermanagement

Ohne die passenden Behälter ist ein Transport von Teilen in der Automobilindustrie nicht möglich. Hierzu gehören zahlreiche standardisierte Behälter, z.B. Paletten, Gitterboxen oder VDA-Kleinladungsträger (KLTs), aber auch Spezialbehälter wie z.B. Motorengestelle oder Bremsteilebehälter. Der Anteil an Mehrwegverpackungen liegt mittlerweile bei ca. 80 % [Che03].

Die Verfügbarkeit der Behälter ist die Voraussetzung für die Teileversorgung der Produktion. Um die Verfügbarkeit von Behältern zu gewährleisten, halten die Unternehmen der Automobilindustrie Sicherheitsbestände. Dem systematischen Management dieser Behälter, etwa durch ein Behältermanagementsystem, haben die meisten Unternehmen bisher wenig Beachtung beigemessen.

Behältermanagementsysteme sollen sicherstellen, dass jederzeit die benötigten Behälter in gutem Zustand zur Verfügung stehen, gleichzeitig der Bestand an Behältern so gering wie möglich ist. Zu diesem Zweck optimiert das System auch die Umlaufzeiten. Das bedeutet z.B., dass das System die Behälter nach jedem Einsatz sofort wieder zur weiteren Verwendung zur Verfügung stellt oder bei Bedarf die Reinigung oder Wartung veranlasst.

Behälter-Tracking kann helfen, dieses Ziel zu erreichen. Durch die Verfolgung der Bewegungen lassen sich Verzögerungen im Umlauf aufdecken und nicht mehr benötigte Behälter zur weiteren Verwendung freigeben. Durch Protokollierung jeder Verwendung lassen sich nutzungsabhängige Wartungen durchführen und regelmäßige Reinigungen sicherstellen. Eine Überwachung der Verfügbarkeit von Behältern über einen längeren Zeitraum ermöglicht die Ermittlung eines effizienten Bestands an Behältern.

Die Möglichkeit, Behälter eindeutig zu identifizieren, erleichtert die Bereitstellung der richtigen Behälter. Diese Funktionalität ist vor allem bei gemischten Behälterpools wichtig. Ebenso erleichtert dies die Rückführung in den richtigen Behälterpool. Nachfolgendes Beispiel beschreibt, wie Volkswagen die RFID-Technologie zum Tracking von Spezialladungsträgern verwendet.

Beispiel „Tracking von Spezialladungsträgern bei Volkswagen". In einem Pilotversuch hat Volkswagen einige hundert Spezialladungsträger mit aktiven RFID-Chips ausgestattet. Jeder dieser Ladungsträger hat einen Wert von mehr als 1 000 Euro. Wenn einmal kein Ladungsträger verfügbar ist, kann dies zu Maschinenstillständen und Verzögerungen in der Produktion führen.

Mit der selbst entwickelten Software „VisuM" kann Volkswagen die Behälter in den Werken Brüssel, Mosel und Wolfsburg lokalisieren. Hierzu teilt die Anwendung die Werkshallen in Zonen ein. Erfassungsgeräte befinden sich an den Zugängen zu diesen Zonen. Auf diese Weise kann VisuM für jeden Spezialladungsträger ermitteln, in welcher Zone sich dieser befindet.

Mit den so gewonnenen Daten kann die Werkslogistik bei Bedarf den räumlich nächstgelegenen Ladungsträger verwenden. Positive Effekte des Systems sind die Reduktion der Umlauftage um 5 %, die Reduktion des Verlusts an Ladungsträgern um 3 %, die Verringerung des Suchaufwandes um 75 % sowie die Verringerung von Maschinenstillständen um 35 % [Pel03].

Werkzeugmanagement

Neben Behältern gehören auch die zur Montage bzw. bei Wartung und Reparatur verwendeten Werkzeuge zu den beweglichen Assets. Ohne Ordnungssystem müssen Mitarbeiter die Werkzeuge häufig suchen, was zu Verzögerungen bei der auszuführenden Tätigkeit führt.

Falls mehrere Mitarbeiter die gleichen Werkzeuge verwenden, ist die Anwendung eines Ausleihsystems sinnvoll. Ein solches System verwaltet, welcher Mitarbeiter welche Werkzeuge entliehen hat und erinnert diesen ggf. an die Rückgabe. Das System trackt die Verwendung der Werkzeuge. Mit den Nutzungsdaten kann das System bestimmen, wann Werkzeuge vor dem Verschleiß zu ersetzen sind und so den Bestand an Werkzeugen optimieren. Ebenso kann das Tracking der Werkzeuge Diebstählen vorbeugen.

Für die Verwendung der RFID-Technologie bei dieser Anwendung spricht die Robustheit der Markierung gegen äußere Einflüsse sowie die unkomplizierte Verwendung in Verbindung mit Selbstbedienungssystemen. Bei kleinen Werkzeugen, vor allem wenn diese aus Metall sind, funktioniert die RFID-Technologie allerdings aus physikalischen Gründen nur mit sehr eingeschränkter Erfassungsreichweite.

3 Kriterien für die Einführung der RFID-Technologie

In der Automobilindustrie steht die Einführung der RFID-Technologie noch am Anfang. Die meisten Anwendungen, die im Bereich der Lieferkette eingesetzt werden, befinden sich im Pilotstadium. Die folgenden beiden Abschnitte stellen basierend auf den Ergebnissen einer Studie zu den Potenzialen der RFID-Technologie dar, aus welchen Gründen und für welche Einsatzgebiete Unternehmen in der Automobilindustrie die Einführung der RFID-Technologie verfolgen und welche Herausforderungen sie bei der Einführung sehen [FRS04a].

3.1 Motivation für die Einführung

Die wichtigsten *Vorteile der RFID-Technologie gegenüber dem Barcode* sind die Möglichkeit der Erfassung von Objekten ohne Sichtkontakt und der gleichzeitigen Erfassung mehrerer Objekte (Pulkerfassung), die Widerstandsfähigkeit des Chips gegen äußere Einflüsse (Hitze, Staub, Wasser) sowie die Möglichkeit, Daten auf dem Chip zu speichern. Diese Eigenschaften machen viele Anwendungen erst möglich, z.B. die automatische Wareneingangskontrolle bzw. die Speicherung warenbegleitender Informationen am Packstück. Ein zusätzlicher Vorteil aktiver RFID-Systeme ist die gegenüber passiven Systemen größere Reichweite. Hiermit lassen sich auch die in der Logistik häufig anzutreffenden *ungeführten Prozesse direkt in IT-Systemen abbilden*. Beispielsweise existieren für die Bewegungen von Ladungsträgern im Werk selten exakt vorgegebene Routen.

Als wichtigsten Treiber für die Verwendung der RFID-Technologie bewerten Unternehmen der Automobilindustrie das Potenzial zur Effizienzsteigerung in der Lieferkette [FRS04a]. Zwar ist die Mehrheit der befragten Unternehmen mit der Prozessqualität zufrieden, erkauft diese jedoch mit aufwendigen Qualitätssicherungsmaßnahmen. Beispielsweise gibt ein Hersteller von Achsen an, dass ihm durch manuelle Sortierung entsprechend der Sequenzvorgaben des OEMs Kosten in Höhe von 20 Euro pro Achse entstehen. Beim Versand von Teilen nach Übersee führt ein Logistikdienstleister nach erfolgter Verladung von Packstücken in die Container Qualitätskontrollen durch, deren Aufwand ein Drittel des gesamten Arbeitsaufwands der Verladung entspricht. Automatisierte Erfassungsvorgänge mittels RFID können dazu beitragen, die Prozessqualität effizienter zu sichern.

Die in der Studie befragten Unternehmen bewerten die Potenziale der RFID-Technologie für verschiedene Einsatzbereiche unterschiedlich (siehe Abbildung 4 [FRS04a]). Die Mehrheit strebt beim Einsatz der RFID-Technologie *prozessübergreifende Tracking&Tracing-Anwendungen* an. Genauere Daten über den Status von Lieferungen sollen dazu beitragen, dass die Unternehmen früher auf unerwartete Ereignisse, z.B. Verspätungen von Lieferungen, reagieren können. Dadurch erhoffen sie sich Einsparungen bei der Bearbeitung solcher Ereignisse und bei den Fehlerfolgekosten. So können beispielsweise die Werke ihre Produktionspläne noch rechtzeitig anpassen oder auf anderem Weg Nachschub beschaffen. Auch die Zulieferer profitieren von genauen Daten über den Lieferstatus. Eine automatische Mitteilung über den erfolgten Wareneingang beim Kunden ermöglicht es ihnen, die Rechnungsstellung ebenso automatisch folgen zu lassen.

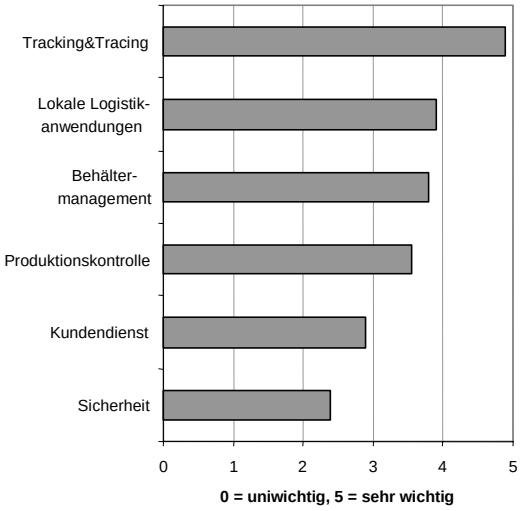


Abb. 4. Priorisierung von RFID-Anwendungen

Der Einsatz von RFID für lokale *Anwendungen zur Verbesserung von Lieferkette und Produktion* spielt für die meisten der befragten Unternehmen eine ebenso wichtige Rolle wie das Tracking&Tracing. Sie erwarten vor allem Effizienzsteigerungen beim Wareneingang, beim Lagermanagement und in der Distribution. Zur Kennzeichnung von Warenlieferungen verwendet die Automobilindustrie standardisierte Warenanhänger aus Papier. In der Regel müssen die Mitarbeiter am Wareneingang eintreffende Lieferungen nur dem zuvor per EDI (Electronic Data Interchange) eingetroffenen Lieferschein zuordnen. Eine exakte Qualitätskontrolle führen sie nur in seltenen Fällen durch. Die Folge ist, dass Fehler erst im Rahmen der Lagerbestandskontrolle bzw. beim Lagerabruf auffallen. Eine mittels RFID automatisierte Vollständigkeitskontrolle, zumindest auf Behälter- oder Packstückebene, würde die Wareneingangsbuchung beschleunigen und Bestandsabweichungen im Lagermanagement vermeiden helfen.

In der Produktion, die heute bereits einen sehr hohen Automatisierungsgrad besitzt, sehen die befragten Unternehmen das Potenzial der RFID-Technologie vor allem in einer Verbesserung des Konfigurationsmanagements und zur Durchführung von Qualitätskontrollen während des Zusammenbaus. Eine Verbesserung des Konfigurationsmanagements lässt sich durch eine Automation der Dokumentation erreichen. Insbesondere bei sicherheitsrelevanten Teilen, wie z.B. Airbags und Prallschutzelementen, ist ein korrekter Einbau wichtig. Sind die entsprechenden Teile mit RFID-Chips gekennzeichnet, können an den Arbeitsstationen montierte Lesegeräte den Einbau erfassen. Zur Sicherstellung der Rückverfolgbarkeit und für den Fall eines Rückrufs ist es vor allem bei sicherheitsrelevanten Teilen hilfreich, wenn Informationen über Seriennummern bzw. Chargennummern der verbauten Teile fahrzeugbezogen vorliegen.

Viele Unternehmen planen den Einsatz der RFID-Technologie zur Verbesserung des *Asset Managements* oder besitzen bereits operative Anwendungen in die-

sem Bereich. Die Automobilindustrie setzt für die meisten Transportprozesse Mehrwegbehälter ein. Sowohl bei den teuren Spezialbehältern als auch bei den standardisierten Gitterboxen und den Kleinladungsträgern tritt ein Schwund von 5–8 % pro Jahr auf. Bei den hochwertigeren Behältern, etwa ab einem Preis von 100 Euro, entstehen einem Automobilwerk jährlich Kosten für Ersatzinvestitionen aufgrund verschwundener Behälter in Höhe von mehren Millionen Euro. Als weiteren Grund für das Tracking der Transportbehälter mittels RFID bezeichnen viele der befragten Unternehmen die Möglichkeit, auf diese Weise auch indirekt den Inhalt der Behälter tracken zu können.

Zahlreiche Anwendungen der RFID-Technologie sind auch im Bereich der After Sales Services, z.B. in der Wartung oder beim Recycling, und bei Sicherheitsanwendungen, z.B. zur Produktauthentifikation, denkbar. Einige Unternehmen sehen zwar auch in diesen Bereichen ein Verbesserungspotenzial, mehrheitlich stufen sie solche Projekte im Vergleich zu den oben genannten Anwendungen derzeit aber als weniger wichtig ein. Häufig sind in diesem Bereich mögliche Anwendungsszenarien weniger bekannt und der zusätzliche Nutzen von RFID im Vergleich zu anderen Technologien oder organisatorischen Maßnahmen unklar.

3.2 Herausforderungen bei der Einführung

Die in der Automobilindustrie bereits operativen Anwendungen zeigen nur ansatzweise das Potenzial, das die RFID-Technologie für die Wertkette der Automobilindustrie bietet. Eine breite Durchdringung hat in vielen Bereichen noch nicht stattgefunden. Beispielsweise handelt es sich bei den oben genannten Anwendungen in Produktion oder Asset Management um *Insellösungen*. Darüber hinaus existieren relativ wenige öffentlich bekannte Anwendungsbeispiele.

Obwohl die Automobilindustrie die Potenziale der Technologie erkannt hat, schreitet die Umsetzung operativer Anwendungen eher langsam voran. Die in der Studie befragten Unternehmen nennen hierfür mehrere Gründe (siehe Abbildung 5 [FRS04a]). An erster Stelle nennen sie den *fehlenden Nachweis der Wirtschaftlichkeit* solcher Lösungen. Dies trifft insbesondere für offene RFID-Systeme zu, bei denen RFID-Tags nicht mehrfach verwendet werden. Für viele dieser Anwendungen liefert RFID einerseits keinen nennenswerten Vorteil gegenüber dem Barcode, andererseits ist der *Preis für RFID-Chips noch zu hoch.* Anwendungen rechnen sich häufig nur dann, wenn mehrere Partner der Wertschöpfungskette RFID verwenden. Für diesen Fall müssen sich die beteiligten Unternehmen auf *Modelle zur Kosten- und Nutzenverteilung* einigen. Beispielsweise fallen die Kosten für das Tagging eines Bauteils zunächst beim Hersteller an. Nachgelagerte Partner in der Wertschöpfungskette benötigen nur Infrastrukturinvestitionen, um von RFID zu profitieren.

Kooperative Prozesse wie die unternehmensübergreifende Logistik lassen sich dann effizient mit IT gestalten, wenn es Standards zum Datenaustausch oder sogar eine gemeinsame Infrastruktur gibt. Da beispielsweise der Einsatz von RFID in der Teileverfolgung die gesamte Wertschöpfungskette betrifft, ist hierbei die Definition gemeinsamer Standards notwendig. *Fehlende Standards* sind ein wesentlicher Grund, warum die Verwendung von RFID in der Automobilindustrie (wie auch in anderen Industriebereichen) noch nicht weiter verbreitet ist. Dass regional

unterschiedliche Frequenzbänder für die Nutzung von RFID zur Verfügung stehen, kommt erschwerend hinzu. Bezüglich der Datenhaltung ist zu klären, inwieweit es sinnvoll ist, Daten dezentral am Objekt zu speichern oder über eine gemeinsame Infrastruktur zur Verfügung zu stellen.

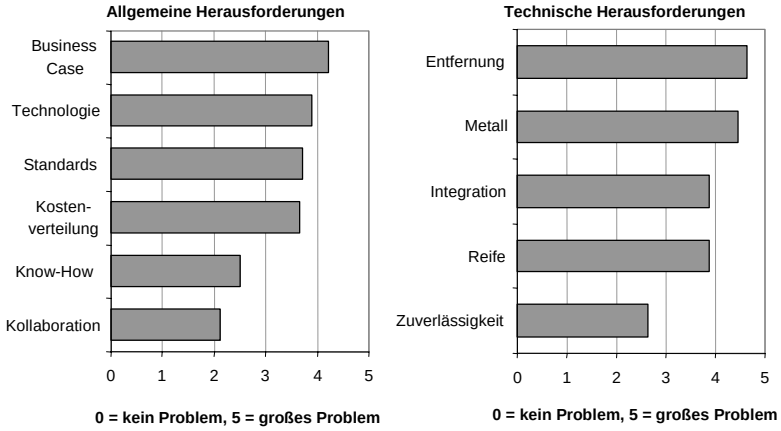


Abb. 5. Herausforderungen bei der Umsetzung von RFID-Systemen

Heute sind RFID-Projekte meist *von einzelnen lokalen Organisationseinheiten getrieben*, die sich nicht untereinander abstimmen. Dies behindert die Umsetzung offener und prozessübergreifender RFID-Lösungen, die z.B. Logistik, Produktion, Distribution und das Ersatzteilwesen gleichzeitig betreffen. Sinnvoll wäre die Schaffung einer zentralen Organisation oder zumindest die Koordination durch ein RFID-Rahmenprogramm, wie es einige Fahrzeughersteller derzeit planen.

Viele RFID-Projekte scheitern auch wegen *technologischer Probleme*, weil entweder die RFID-Technologie generell oder das im konkreten Fall ausgewählte System nicht den Anforderungen gerecht wird. Die befragten Unternehmen, die bereits Pilotinstallationen durchgeführt haben, geben an, dass sie mit der erzielten *Lesereichweite*, insbesondere bei *metallischem Umfeld*, mit *dem Integrationsaufwand* in die bestehende Systemlandschaft und mit der *technologischen Reife* der verwendeten RFID-Systeme nicht zufrieden sind. Insbesondere für die Einzelteileidentifikation besitzen RFID-Chips keine Optimaleigenschaften. Sie sind entweder zu groß oder erreichen nicht die gewünschte Reichweite. Durch Erfahrung im Umgang mit der Technologie und die Berücksichtigung von Standards können Anwender solche Probleme vermeiden. Die Integration in die bestehende IT-Infrastruktur, die Anwender heute selbst leisten müssen, wollen Softwareanbieter zukünftig mittels Standardsoftware erleichtern. Beispielsweise bietet SAP die so genannte „SAP Auto-ID-Infrastructure“ zur Integration der RFID-Technologie in bestehende SAP-Anwendungen an.

4 Fazit

Eine wachsende Anzahl von Unternehmen der Automobilindustrie ist der Meinung, dass die RFID-Technologie ein bedeutendes Potenzial zur Verbesserung des Supply Chain Managements besitzt. Ein Handlungsbedarf entsteht aus wachsendem Rationalisierungsdruck, dem Trend zur Massenindividualisierung und steigenden Anforderungen an Qualität und Rückverfolgbarkeit.

Als wichtigsten Vorteil sehen die Unternehmen mögliche Effizienzsteigerungen in der Lieferkette. Hingegen liegt der Schwerpunkt heutiger operativer Anwendungen in der Produktionsautomation, insbesondere beim Tracking des Fertigungsfortschritts und beim Behältermanagement. Diese lokalen Anwendungen sind auch ohne Standards zur Kennzeichnung sowie zum Datenmanagement wirtschaftlich rentabel.

Sobald es sich um offene Anwendungen handelt, wie z.B. beim Tracking von Kleinladungsträgern oder Einzelteilen, entsteht die Notwendigkeit von Standards, die positive Auswirkungen auf die Zuverlässigkeit, den Preis und die Möglichkeit zu kooperativen Anwendungsszenarien bieten. Solche Anwendungen lassen sich nur durch Betrachtung der gesamten Wertkette wirtschaftlich rechtfertigen. Hierbei stehen den Kosten für die Kennzeichnung und die Infrastruktur die Nutzenpotenziale bei verschiedenen Anwendungen, z.B. Verbesserungen in den Bereichen Lagermanagement, Produktion, Distribution, Diebstahlschutz, Echtheitskontrolle sowie Rückrufe, Wartung und Recycling, gegenüber.

Ein großes Nutzenpotenzial der RFID-Technologie kann die Automobilindustrie bereits durch das Tracking der zum Transport eingesetzten Ladungsträger erschließen. Über die Aufgaben des Behältermanagements hinaus, wie z.B. die Verfügbarkeitskontrolle, die Auslastungssteuerung und die Vermeidung von Schwund, lassen sich in Verbindung mit dem Behälter auch die transportierten Güter tracken. Da wegen mehrfacher Verwendung der Behälter nur ein einziger RFID-Chip pro Ladungsträger notwendig ist, kann das System aufgrund geringerer Hardwarekosten leichter die Wirtschaftlichkeit erreichen.

Die Automobilindustrie hat in der Vergangenheit die Einführung neuer Technologien zur Effizienzsteigerung von Logistik und Produktion sehr gut gemeistert. Eine leistungsfähige IT-Infrastruktur ist vorhanden und bildet eine Basis für den Einsatz der RFID-Technologie.

Literatur

[Che2003] Chep (2003) Branchenübersicht Kraftfahrzeuge, www.chep.com/chepdoc/de/docs/industries/automotive.pdf

[EMS98] EMS (1998) Ford's "Quality is Job 1" = Radio Frequency Identification (RFID) from Escort Memory Systems. www.ems-rfid.com/apps/fordcase.html

[FRS04a] Fleisch E, Ringbeck J, Stroh S, Plenge C, Strassner M (2004) From Operations to Strategy – The Potential of RFID for the Automotive Industry. M-Lab Working Paper No. 23, Universität St. Gallen / ETH Zürich

[FRS04b] Fleisch E, Ringbeck J, Stroh S, Plenge C, Dittmann, L, Strassner M (2004) RFID – The Opportunity for Logistics Service Providers. M-Lab Working Paper No. 24, Universität St. Gallen / ETH Zürich

[Fin02] Finkenzeller K (2002) RFID-Handbuch. Hanser, München

[Ide00] Identec Solutions (2000) Identec Solutions Customer Success Story – Volkswagen Autostadt, www.identecsolutions.com/pdf/success_story_Volkswagen.pdf

[Kil00] Kilbane D (2000) Technology test drives the automotive supply chain. Frontline Solutions 9: 20–26

[LPW97] Lee HL, Padmanabhan V, Whang S (1997) The Bullwhip Effect in Supply Chains. Sloan Management Review 38(3): 93–102

[May99] Mayer S (1999) Erfolgsfaktoren für das Supply Chain Management nach der Jahrtausendwende. In: Pfohl HC (Hrsg) Logistik 2000plus – Visionen-Märkte-Ressourcen. Schmidt, S 1–20

[Nav00] Navas D (2000) Automotive on the Cutting Edge. Supply Chain Systems Magazine 6, www.scs-mag.com/reader/2000_06/index.htm

[Nav01] Navas D (2001) Automotive Revs Up For Lean Times. Supply Chain Systems Magazine 20(6), www.scs-mag.com/reader/2001/2001_06/index.htm

[Pel03] Pelich C (2003) RFID bei Volkswagen AG. Vortrag M-Lab Workshop, Wolfsburg, 25. April 2003

[Rfi03a] RFID-Journal (2003) RFID Helps to Perfect Order Picking. RFID Journal, April 2, 2003, www.rfidjournal.com/article/view/366

[Rfi03b] RFID Journal (2003) ABI – RFID Market Poised for Growth. RFID Journal, July 18, 2003, www.rfidjournal.com/article/view/506

[SLA02] SLA (2002) Authentication and Counterfeiting Protection Conference Review. Smart Labels Analyst 13: 1–3

[Sar01] Sarma S (2001) Towards the 5c Tag. Auto-ID Center White Paper, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-006.pdf

[StF03] Strassner M, Fleisch E (2003) The Promise of Auto-ID in the Automotive Industry. Auto-ID Center Report, archive.epcglobalinc.org/publishedresearch/MLB-AUTOID-BC001.pdf

[TeS02] Tellkamp C, Schoch T (2002) Wirtschaftlichkeitsbetrachtung zum Einsatz von Transpondern im FIB-Zentrum bei VW. Interner Projektbericht, M-Lab, Universität St. Gallen / ETH Zürich

RFID-Anwendungen bei der Volkswagen AG – Herausforderungen einer modernen Ersatzteillogistik

Antonio Cocca
Volkswagen AG, Baunatal

Thomas Schoch
Institut für Pervasive Computing, ETH Zürich

Kurzfassung. Nach einer kurzen Darstellung, wie sich der Bereich „Vertrieb Original Teile“ im Volkswagen-Konzern einbettet und wie sich die zunehmende Elektronifizierung der Automobile auf ihn auswirkt, werden vier RFID-Projekte innerhalb des Volkswagen-Konzerns beschrieben. Aufbauend auf den dabei gewonnenen Erfahrungen untersucht der vorliegende Beitrag, wie sich die Erkenntnisse auf das Ersatzteilgeschäft übertragen lassen. Die in diesem Rahmen entstandenen Projektvorschläge werden zunächst beschrieben, bevor das durchgeführte Projekt im „Zentrum für fahrzeugintelligente Bauteile“ näher betrachtet wird. Diese Darstellung enthält eine Istanalyse der Prozesse, die durch RFID optimierten Sollprozesse sowie eine Beschreibung eines vor Ort durchgeführten RFID-Tests mit Ersatzteilen.

1 Der Volkswagen-Konzern

Die Volkswagen AG ist mit ihren beiden Markengruppen VW und Audi momentan der viertgrößte Automobilhersteller der Welt, der jährlich über 5 Millionen Fahrzeuge an Kunden ausliefert.

Die Volkswagen-Gruppe ist ein weltweit agierendes und produzierendes Unternehmen, das in 11 Ländern und 44 Produktionsstätten hochwertige Automobile und Nutzfahrzeuge herstellt und in mehr als 150 Ländern vertreibt. Momentan hält der Gesamtkonzern einen Weltmarktanteil von 12,1 % im Automobilsektor. Im konsolidierten Umsatz von 86,9 Milliarden EUR für das Jahr 2002 ist auch der Finanzsektor des Konzerns, die Financial Services, enthalten.

In diesem Umfeld eingebettet agiert der „Vertrieb Original Teile“ (VO), der für die Konzernmarkengruppen VW, AUDI und Nutzfahrzeuge das weltweite Teilegeschäft verantwortet (siehe Abbildung 1) und als eigenständiger Bereich dem Vertrieb der Markengruppe Volkswagen zugeordnet ist. Der Bereich VO hat seine Zentrale im Werk Baunatal in Nordhessen, wo eines der größten Lager Europas betrieben wird.

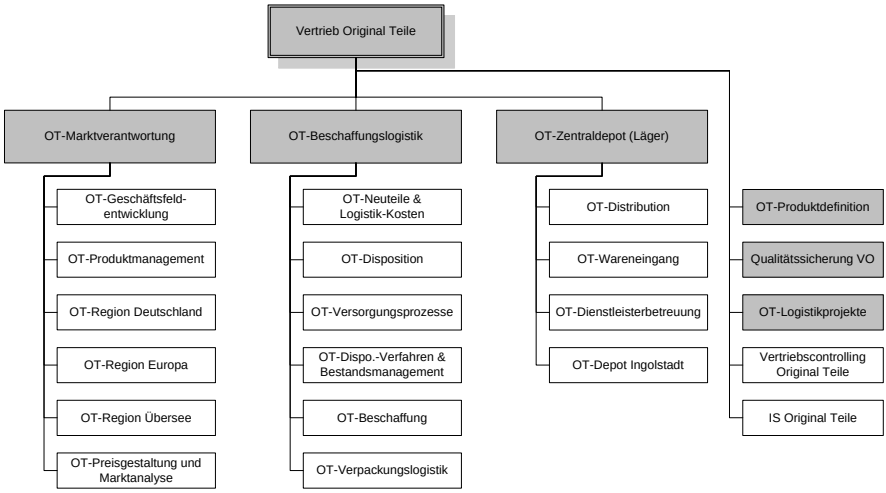


Abb. 1. Organisation des Bereichs VO

Einige Kennzahlen, die in Tabelle 1 dargestellt sind, verdeutlichen die Größenordnungen, in denen sich der Bereich VO bewegt.

Tabelle 1. Kennzahlen des Bereichs VO

Kennzahl	Wert
Mitarbeiter	3 000
Lagerfläche	800 000 m^2
Sortimentsumfang	280 000 verschiedene Positionen
Auftragspositionen	60 000 pro Tag (16 Mio. pro Jahr)
Tägliche Liefermenge	1 540 t
Service	24h-Lieferung innerhalb Europas, 2-mal täglich innerhalb Deutschlands
Umsatz	4 Mrd. EUR

2 Veränderungen im After-Sales-Markt

Die Situation des After-Sales-Marktes, den der Bereich VO bearbeitet, wird momentan durch drei einschneidende Veränderungen geprägt:

- die Novellierung der Gruppenfreistellungsverordnung (GVO), welche es Vertragshändlern ermöglicht, auch andere Marken anzubieten, und die damit verbundene Neuausrichtung der Vertriebsstrategie,
- eine starke Konzentrationsbewegung in den Vertriebskanälen, insbesondere auf Handelsebene, aber auch auf Ebene der First-Tier-Lieferanten, welche eigene Handelsorganisationen aufbauen, und
- eine steigende Preissensibilität des Endkunden nach dem Motto: „Mobilität zu günstigen Preisen“.

Neben diesen Veränderungen ist eine zunehmende Virtualisierung der Vermarktung, wie es z.B. die Plattformen TecCom oder Parts.Com mit großem Erfolg zeigen, festzustellen. Hier werden ganze Supply-Chain-Prozessketten des Ersatzteilgeschäfts via Internet oder Intranet abgewickelt. Um die steigende Komplexität der Logistik-Netzwerke steuern zu können, werden bei Volkswagen zunehmend Technologien wie virtuelle Warenhäuser, Telematik-Systeme, einheitliche IT-Systeme und die Transpondertechnologie eingesetzt.

Letztendlich sind auch die Kundenanforderungen in den letzten Jahren stetig gestiegen, denn Kunden sind heutzutage oft nicht mehr bereit, wegen einer Problemlösung mehrere Dienstleister zu konsultieren, sondern erwarten stattdessen eine Komplettlösung. Des Weiteren ist die Kundenerwartung hinsichtlich der Lösungsgeschwindigkeit weiter gestiegen, was bei einer zunehmenden Fahrzeugkomplexität und bei größeren Teilesortimenten nur durch eine ausgeklügelte Technik und Logistik zu kompensieren ist. Die Kundenbindung im Allgemeinen wird durch spezielle Methoden und Befragungen intensiviert, die letztendlich in ein Customer-Relationship-Management münden und einer systemseitigen Unterstützung bedürfen.

3 Elektronikstrategie

Neben den genannten Trends im After-Sales-Bereich ist in den letzten Jahren ein bedeutender Trend in der Automobilwirtschaft im Allgemeinen zu erkennen: die Zunahme der Elektronik im Fahrzeug. In modernen Oberklassefahrzeugen werden Funktionen von der Abstandsmessung über Keyless-Entry bis hin zur Zentralverriegelung elektronisch gesteuert. Kontinuierlich werden diese technischen Errungenschaften auch in den unteren Fahrzeugklassen zum Standard, wie z.B. der Golf V mit bis zu 40 verschiedenen Steuergeräten zeigt.

Dieser Trend erhöht auch die Anforderungen an die Ersatzteilversorgung, in der nun zwei unterschiedliche Lebenszyklen bei einem Fahrzeug aufeinander treffen. Der automobile Lebenszyklus dauert bei Volkswagen bis zu 22 Jahren, der sich aus 7 Jahren Fahrzeugproduktion und 15 Jahren Ersatzteilversorgung zusammensetzt, da Volkswagen nach Produktionsende eines Fahrzeugs eine 15-jährige Ersatzteilversorgung garantiert. Der Lebenszyklus elektronischer Bauteile hingegen ist wesentlich kürzer und beträgt zwischen 2 und 4 Jahren. Dieser neue und wesentlich kürzere Lebenszyklus stellt neue Herausforderungen an die Prozesse des traditionellen Ersatzteilgeschäfts. Erschwert wird das Ersatzteilgeschäft zusätzlich noch durch die steigende Komplexität der Teile und durch die verschärften Anforderungen an Beschaffung, Lagerung und Distribution dieser Teile.

Hier setzt das Team „Elektronikstrategie“ des Bereichs VO an: In einer Querschnittsfunktion werden neue Lösungen für die Herausforderungen der Elektronifizierung gesucht und umgesetzt. Zusammen mit dem M-Lab untersucht dieses Team die zuvor genannten neuen Herausforderungen an die Ersatzteillogistik und schlägt Lösungen vor, die auf der Transpondertechnologie beruhen und im Nachfolgenden besprochen werden.

4 RFID-Projekte bei der Volkswagen AG

Schon seit mehreren Jahren beschäftigt sich die Volkswagen AG mit den Möglichkeiten der Transpondertechnologie [Fin02]. Daraus entstanden mehrere Ansätze, die in operative Projekte übergingen. Vier dieser Projekte werden im Folgenden vorgestellt.

4.1 VisuM

VisuM steht als Abkürzung für *Visu*alisierung und *M*ap-Matching. In diesem System werden Informationen über Ort, Zeit und Zustand von Objekten, die mit aktiven Transpondern ausgestattet sind, in einer Datenbank gespeichert. Für jedes Objekt, welches einen Transponder trägt, wird im VisuM-System ein Schlüsselpaar abgelegt. Dieses Schlüsselpaar bildet den Bezug zwischen der eindeutigen Transponder-ID und dem Objekt, an dem der Transponder angebracht ist. Je nach Objekt kann es sich dabei um eine VW-Inventarnummer, einen Behälter-Typ, ein Kfz-Kennzeichen oder eine Fahrgestellnummer handeln. Mit Hilfe einer grafischen Benutzeroberfläche kann sich ein Anwender die Daten zu den überwachten Objekten aus der VisuM-Datenbank anzeigen lassen (siehe Abbildung 2). Neben der Visualisierung können auch andere Programme mit Hilfe der Schlüsselpaare auf die VisuM-Datenbank zugreifen.

Mit dieser Funktionalität präsentiert sich VisuM als Middleware-Schicht zwischen diversen Transpondersystemen und Legacy-Systemen, die transponderbezogene Informationen verarbeiten. Ein Vorteil der Middleware besteht in der Abstraktion von dem zugrunde liegenden Transpondersystem, sodass Anwendungen nicht auf das Transpondersystem hin angepasst werden müssen. Falls ein neues Transpondersystem unterstützt werden soll, muss lediglich eine Anbindung an das VisuM-System entwickelt werden.

4.2 Fahrzeug Finish Center (FFC)

Im FFC werden in manufakturähnlichen Bearbeitungsstationen abschließende Umbauten an produzierten Fahrzeugen durchgeführt. Die Kapazitätsplanung und Ablaufverfolgung war bislang ein hochgradig manueller und fehleranfälliger Prozess, der durch den Einsatz von aktiver Transpondertechnologie wesentlich verbessert wurde, u.a. wurden bei den Wartezeiten vor Prozessbeginn als auch im Prozess und beim Durchsatz von Fahrzeugen signifikante Verbesserungen erzielt. Dazu einige Kennzahlen des Aufbaus:

- 50 stationäre Gates
- 150 Antennen
- 2 500 Transponder

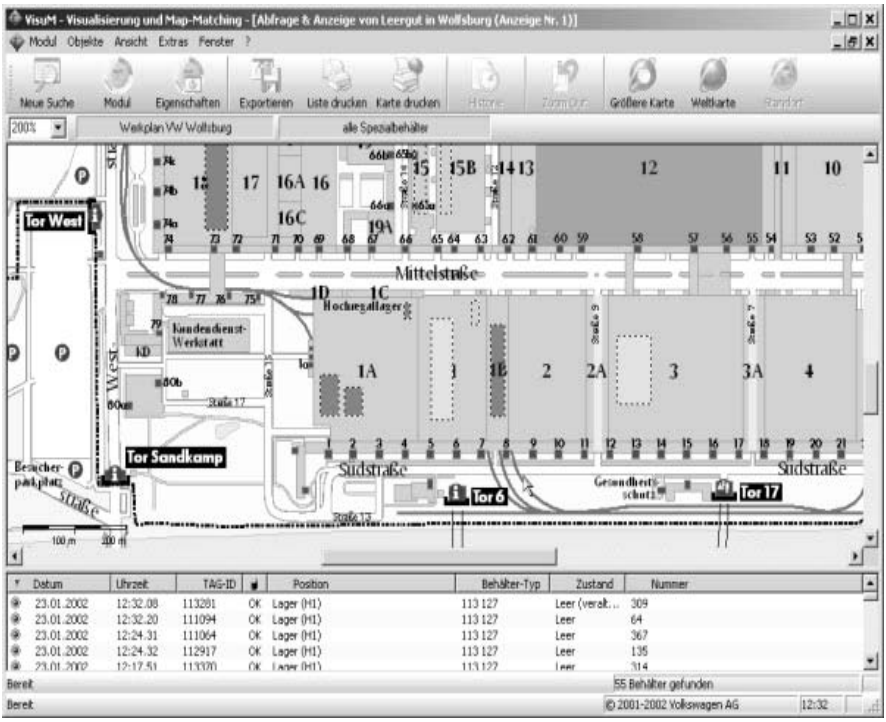


Abb. 2. Grafische Benutzeroberfläche für Endanwender des VisuM-Systems

4.3 Prozesssteuerung AUTOSTADT

Mit der AUTOSTADT wurde in Wolfsburg ein neuartiges, herstellergebundenes Auslieferzentrum für Neufahrzeuge eröffnet. Aus den beiden Glastürmen der AUTOSTADT, die als Lager für abholbereite Fahrzeuge dienen, können an einem Werktag bis zu 1 000 Fahrzeuge an Kunden übergeben werden. Dazu mussten zunächst neue Prozesse eingeführt werden, die eine pünktliche Vorbereitung des Fahrzeugs ermöglichen. Zur Vorbereitung eines Fahrzeugs zählen Aufgaben wie die Endreinigung oder das Anbringen von Nummernschildern, die zum Teil von Fremdfirmen ausgeführt werden, welche ebenfalls in die neuen Prozesse zu integrieren waren.

Zur Steuerung dieses komplexen Prozesses von der Fertigstellung des Fahrzeugs bis zur Kundenübergabe entschied sich Volkswagen für aktive Transponder, die im Fahrzeug angebracht sind und die jedes Fahrzeug eindeutig identifizieren. Durch den Einsatz der Transpondertechnologie wurde der Gesamtprozess transparenter; das Accounting für Dienstleister erfolgt seitdem automatisch und letztlich können vereinbarte Kundentermine eingehalten werden. Die Kennzahlen zu diesem Projekt lauten wie folgt:

- 60 stationäre Gates
- 180 Antennen
- 10 000 Transponder

4.4 Behältermanagement für Golf-Blechteile

Im Prozess für die logistische Bereitstellung von Blechteilen werden spezielle Behälter eingesetzt, die die Beschädigung der transportierten Blechteile auf ein Minimum reduzieren sollen. Diese Spezialbehälter sind kapitalintensiv und besitzen zudem eine teilespezifische Ausprägung. Im hier betrachteten Anwendungsfall kommt hinzu, dass diese Spezialbehälter drei Produktionsstandorte in Europa durchlaufen müssen. In einem Pilotprojekt wurden Spezialbehälter für Golf-Blechteile mit aktiven Transpondern ausgestattet und an allen drei Standorten verfolgt. Die dabei erzielten Optimierungen sind in Tabelle 2 dargestellt.

Tabelle 2. Optimierungen beim Behältermanagement

Art der Optimierung	Höhe der Optimierung
Reduktion Umlauftage	5 %
Reduktion Fehlbestand bei Erstlieferung	1 %
Reduktion Verlust im Betrieb	2 %
Verringerung Suchaufwand	75 %
Reduktion falscher Lieferungen	90 %
Reduktion Maschinenstillstand	35 %

Die Lösung umfasst in Summe

- 20 stationäre Gates,
- 80 Antennen sowie
- 1500 Transponder

an drei verschiedenen Standorten (Wolfsburg, Mosel, Brüssel). Das Projekt wurde erfolgreich während der Laufzeit der Serienfertigung des Golf IV eingesetzt und ist daher von Beginn an in die Fertigung des Golf V integriert.

5 RFID für die Ersatzteillogistik

Volkswagen erkannte recht früh den Nutzen, den RFID in der Automobilbranche stiften kann, wie die im vorherigen Abschnitt beschriebenen Projekte belegen. Dementsprechend war es für Volkswagen ein logischer Schritt, zusammen mit dem M-Lab zu evaluieren, wie entsprechende Technologien die Ersatzteillogistik optimieren können.

5.1 Projektvorschläge

Im Rahmen der Kooperation wurden zunächst sechs Projektvorschläge, die in verschiedenen Bereichen der Ersatzteillogistik neue und effiziente Ansätze für die dortigen Herausforderungen bieten, erarbeitet:

- Optimierungen der Lieferkette. Wie können Lieferkettenprozesse mit Hilfe der Transpondertechnologie optimiert werden?
- Smarte elektronische Ersatzteile. Wie können Bauteile mit diversen Software-Versionen kooperieren?
- Verpackung. Wie können Verpackungen effizient verwendet werden?
- Fälschungssicherheit. Wie kann sichergestellt werden, dass nur lizenzierte Originalteile in den Handel kommen?
- Automatische Inventur. Wie kann eine Inventur automatisiert werden, sodass diese jederzeit möglich ist?
- Ein „smartes Warehouse". Wie können die internen Logistikprozesse mit Hilfe der Transpondertechnologie optimiert werden?

Zwei Kriterien waren für die Auswahl des Projektvorschlags „smartes Warehouse" wesentlich: Es wurde geprüft, ob sich die Notwendigkeit von Infrastrukturmaßnahmen in Grenzen hält und ob die Fokussierung auf Kernprozesse gegeben ist. Für diesen Vorschlag sprachen ebenfalls bereits existierende Bestrebungen seitens Volkswagen.

5.2 RFID-Einsatz im Zentrum für fahrzeugintelligente Bauteile

Zusammen mit dem Volkswagen-Projektteam „Transpondereinsatz im Vertrieb Original Teile" galt es die Frage zu klären, wie ein Einsatz der RFID-Technologie im Bereich VO aussehen könnte und wie dieser die dort angesiedelten Prozesse verändert. Um das Ganze überschaubar zu halten, wurde ein sowohl räumlich als auch organisatorisch abgegrenzter Teilbereich des Bereichs VO, das „Zentrum für fahrzeugintelligente Bauteile" (FIB-Zentrum), für die Untersuchungen herangezogen. Das FIB-Zentrum ist für diejenigen Teile verantwortlich, die im Fahrzeug Steuerungsfunktionen übernehmen und dazu größtenteils fahrzeugspezifisch individualisiert werden. Des Weiteren werden im FIB-Zentrum sicherheitsrelevante Teile wie Schlüssel gelagert, die dort gefräst sowie programmiert werden.

Um im FIB-Zentrum Optimierungen mit Hilfe der RFID-Technologie auszuloten, wurde die folgende Methodik angewendet: Eine Istanalyse lieferte zunächst ein Bild über die relevanten Prozesse. Darauf aufbauend fand eine Schwachstellenanalyse statt, um Optimierungspotenziale zu bestimmen. Für jedes dieser Optimierungspotenziale wurde analysiert, ob eine Lösung mit Hilfe der RFID-Technologie Abhilfe versprach. In Sollprozessen wurden schließlich die Optimierungen erfasst. Die Erstellung eines Business Cases musste schließlich zeigen, ob dieser neue Sollprozess wirtschaftlich wäre. Auf technischer Seite mussten erste prototypische Tests zeigen, ob die Sollprozesse prinzipiell mit der vorhandenen RFID-Technologie umsetzbar sind.

Die Analyse der Prozesse im FIB-Zentrum ergab vereinfacht das folgende Bild: Beim Wareneingangsprozess, einer der zentralen Prozesse im FIB-Zentrum, werden die Originalteile in einem Metallcontainer am Wareneingang des FIB-Zentrums zusammen mit einem Einlagerungsbeleg in Empfang genommen. Die Ware wird zunächst gesichtet und mit Hilfe des Einlagerungsbelegs in das eingesetzte SAP-System eingebucht, welches daraufhin einen Einlagerungsort innerhalb des Lagers vorschlägt. Bevor die Ware dann eingelagert wird, kann stichprobenartig eine manuelle Kontrolle auf Qualität und Quantität erfolgen. Nachdem der Metallcontainer mit den Waren eingelagert wurde, wird dieser Sachverhalt im SAP-System quittiert, welches daraufhin die Ware für Kundenaufträge freigibt.

Die Bearbeitung eines Kundenauftrags stellt den zweiten zentralen Prozess im FIB-Zentrum dar. Das SAP-System gibt in definierten Intervallen die Kundenaufträge in Form so genannter „Pickets“ heraus. Mitarbeiter nehmen sich diese Pickets, um den darauf vermerkten Auftrag zu bearbeiten. Hauptsächlich handelt es sich dabei um das Greifen verschiedener Teile. Im Falle eines Steuergerätes ist noch zusätzlich auf dem Picket vermerkt, welche Parametrierung aufgespielt werden muss, und im Fall eines Schlüssels, wie dieser gefräst werden muss. Nachdem das Teil geholt und ggf. bearbeitet wurde, muss es noch mit den anderen Teilen eines Kundenauftrags zusammengeführt werden. Dazu werden die Teile in eine für jeden Kundenauftrag vorgesehene Kundenbox gelegt und mit Hilfe eines Barcodescanners wird das Teil mit der Box – beide besitzen einen Barcode – für die weitere Verarbeitung und für den Transport verknüpft. Ist ein Kundenauftrag vollständig abgearbeitet, wird die Kundenbox am Warenausgang zum Abtransport bereitgestellt.

Obwohl Volkswagen die Prozesse mit der bisherigen Technologie schon effizient gestaltet hat, bietet RFID die Möglichkeit, diese noch weiter zu optimieren. Dementsprechend konnten aufbauend auf der Istanalyse einige Potenziale zur Prozessoptimierung ausgemacht werden:

- Die Überprüfung der ankommenden Lieferungen erfolgt nur stichprobenartig, sodass nicht überprüfte Lieferungen potenziell dazu beitragen, dass ein ungenaues Abbild im SAP-System erzeugt wird, was später zu manuellen Korrekturen führt. Insofern fallen Mehr- oder Minderlieferungen oft nicht auf und können nicht mit dem Lieferanten verrechnet werden. Da das Einbuchen der ankommenden Lieferungen per Hand erfolgt, ergeben sich dabei unter Umständen fehlerhafte Eingaben und lange Bearbeitungszeiten.
- Die Durchführung einer Inventur ist analog zum Einbuchen fehleranfällig und langwierig. Des Weiteren können Situationen auftreten, in denen dem SAP-System zufolge noch Originalteile vorhanden sein müssten, diese aber in Wirklichkeit aufgebraucht sind. Umgekehrt kann der Fall auftreten, dass nach dem SAP-System Teile aufgebraucht sein müssten, diese tatsächlich aber noch vorrätig sind. Beide Fälle führen zu einer unnötigen Unter- oder Überdeckung und zu einem zusätzlichen Korrekturaufwand.
- Etliche Arbeitsschritte müssen im SAP-System manuell quittiert werden. Auch hier gilt wie für alle manuellen Eingaben, dass diese zu höheren Fehlerraten und zu niedrigen Ausführungsgeschwindigkeiten führen. Ob ein Container mit Originalteilen wirklich an dem Ort abgestellt wurde, wie es das SAP-System

vorschlägt, kann nicht überprüft werden. Falls nun ein Container falsch eingelagert wurde, kann dies erst später im Prozess festgestellt werden, was dann zu erhöhtem Aufwand führt, um den Fehler zu korrigieren.

- Bedingt durch den hohen Umschlag an Teilen sowie die vielfache manuelle Interaktion ist es nicht möglich, Qualitätsdaten und dergleichen auf Ebene des einzelnen Ersatzteils zu erfassen. Die Auswertung dieser Daten würde bei Prozessverbesserungen, der Entlohnung, den Nachweispflichten oder einer ISO-9000-Zertifizierung helfen.
- Bei Kundenaufträgen, die Steuergeräte oder Schlüssel umfassen, erfolgt die Auswahl des Steuergeräteprogramms oder des Fräsprogramms manuell, sodass hier wieder die Nachteile manueller Tätigkeiten zum Tragen kommen. Entsprechende Nachteile ergeben sich beim Zusammenführen der Teile eines Kundenauftrags in eine Kundenbox.

Die Verbesserungspotenziale legen nahe, dass eine Prozessoptimierung mittels Transpondertechnologie hauptsächlich darauf abzielen sollte, bisherige Aufgaben, die entweder manuell oder überhaupt nicht erfolgen, durch eine automatisierte Lösung zu ersetzen. Diese Lösung muss zum einen die auftretenden Mengen an Originalteilen im Prozess in angemessener Zeit und zum anderen mit einer vernachlässigbar geringen Fehlerquote verarbeiten können. Bei der Entwicklung dieser Lösung muss sowohl eine Kosten-Nutzen-Analyse deren Vorteilhaftigkeit zeigen als auch eine technische Evaluierung darlegen, dass diese auch tatsächlich umsetzbar ist.

In der erarbeiteten Lösung werden alle Metallcontainer, Kundenboxen und alle Originalteile mit einem passiven RFID-Tag versehen. Des Weiteren werden RFID-Leser am Wareneingang sowie -ausgang und an den Bearbeitungsplätzen zur Programmierung der Steuergeräte bzw. zum Fräsen von Schlüsseln installiert. Zusätzlich werden noch RFID-Leser an jedem Einlagerungsort vorgesehen. Mit dieser Konfiguration ist es möglich, die zuvor beschriebenen Potenziale zur Prozessoptimierung voll umzusetzen. Der RFID-Leser am Wareneingang kann nun jede ankommende Lieferung auf Vollständigkeit überprüfen und die erkannten Originalteile automatisch in das SAP-System einbuchen. Das System kann dann mit Hilfe der RFID-Leser an den Einlagerungsorten automatisch überprüfen, ob die Metallcontainer am richtigen Ort eingelagert wurden und ebenfalls die Einlagerung automatisch im SAP-System quittieren. Bei der Bearbeitung von Kundenaufträgen kann durch die Erkennung eines Ersatzteils automatisch das passende Steuerungsprogramm eingespielt bzw. der passende Fräsvorgang durchgeführt werden. Das Verknüpfen mit der Kundenbox kann hier ebenfalls automatisch erfolgen. In der Summe ergibt sich, dass alle wesentlichen Aufgaben der Prozesse im FIB-Zentrum, bei denen eine Interaktion des Benutzers mit dem System notwendig war, automatisiert werden können sowie Kontrollen nun lückenlos erfolgen können.

Die auf dieser Lösung durchgeführte Kosten-Nutzen-Analyse macht plausible Annahmen. Die Kosten umfassen zum einen Posten wie die Hardware-Infrastruktur, Schulung des Personals und dergleichen und zum anderen Kosten für den laufenden Betrieb wie beispielsweise RFID-Tags oder die Wartung. Bei einer diskontierten Zahlungsreihe ergab sich aufgrund der gemachten Annahmen, dass sich die Investition nach 1,9 Jahren amortisieren würde. Eine darauf aufbau-

ende Sensitivitätsanalyse ergab, dass außer in einem konkreten Worst-Case-Szenario eine Variation der maßgeblichen Parameter der Annahmen immer innerhalb der ersten fünf Jahre zu einer Amortisation führt. Risiken bei der Einführung befinden sich aufseiten des Early Adopters, da es noch keine ausreichenden Erfahrungen gibt. Aber auch fehlende Standards in der Automobilbranche erschweren langfristige Wirtschaftlichkeitsbetrachtungen.

Nachdem die Kosten-Nutzen-Analyse die vorgeschlagene Lösung als vorteilhaft einstufte, musste eine technische Evaluierung noch zeigen, ob die Lösung mit der gegenwärtig verfügbaren Technik überhaupt zu realisieren ist. Um den Aufwand der Evaluierung zu minimieren, wurde zunächst ein RFID-Szenario entwickelt, welches die höchsten Anforderungen an die Technik stellt. Dieses Szenario bezieht sich auf die Erkennung aller Originalteile einer eintreffenden Lieferung am Wareneingang. Die hohen Anforderungen liegen sowohl in der gleichzeitigen Erkennung von bis zu 500 Teilen als auch in der metallischen Umgebung begründet. Beide Anforderungen stellen noch eine große Herausforderung für die momentan verfügbare RFID-Technologie dar. Für den Test wurden u.a. 500 Fensterhebermotoren mit RFID-Tags in der Größe von Kreditkarten bestückt und schichtweise in einen der Metallcontainer gelegt (siehe Abbildung 3).

Aufseiten der RFID-Hardware wurden nur Standardkomponenten verwendet, die nicht auf die spezielle Situation des Wareneingangs bei Volkswagen optimiert waren. Insofern war eine typische Erkennungsrate von 83 % aller Teile (siehe Tabelle 3) zwar so nicht ausreichend für eine einsatzfähige Lösung, lässt aber vermuten, dass sich mit einer speziell auf die Gegebenheiten vor Ort abgestimmten Hardware weit bessere Resultate erzielen lassen. Weitere Tests mit Teilen, die weniger Metall aufwiesen und in geringeren Stückzahlen vorhanden waren, ergaben hingegen Erkennungsquoten von 100 %.

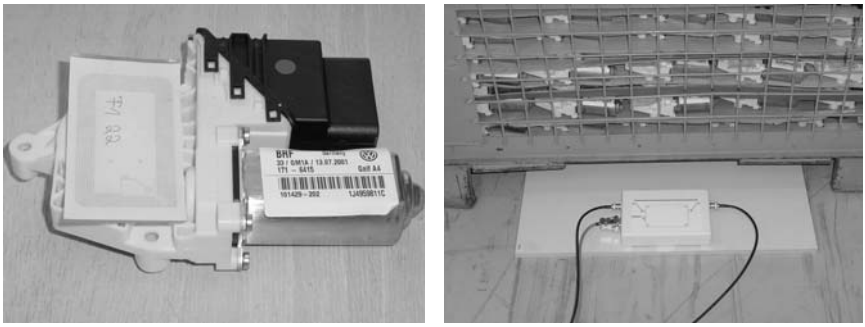


Abb. 3. Fensterhebermotor mit RFID-Tag und Metallcontainer mit Leseantenne

Generell kann festgestellt werden, dass die erarbeitete Lösung zwar wirtschaftlich sinnvoll, aber die in der Evaluation eingesetzte Technik nur bedingt tauglich für die Erkennung von großen Mengen an Teilen in einer metallischen Umgebung ist. Erst weitere Tests können abschließend zeigen, ob eine speziell auf die Umgebungsbedingungen abgestimmte Hardware die notwendigen Anforderungen erfüllen kann.

Tabelle 3. Auswertung des Versuchs mit 500 Fensterhebermotoren

Zustand des Tags	Anteil
erkannt	83 %
verdeckt (nicht erkannt)	11 %
Randlage (nicht erkannt)	4 %
teilweise verdeckt (nicht erkannt)	1 %
unklar (nicht erkannt)	1 %
fehlerhaft (nicht erkannt)	0 %

5.3 „Smart Warehouse“

Aufbauend auf den Ergebnissen des Projekts im FIB-Zentrum soll nun ein konkretes Einsatzszenario geprüft werden. Dabei bietet sich der automatische Wareneingang an, da er einfach auf entsprechende Vorgänge außerhalb des FIB-Zentrums zu übertragen ist. Bevor dieser flächendeckend im Bereich VO eingesetzt wird, soll er jedoch zunächst in einem Piloten im FIB-Zentrum realisiert werden.

Neben der Auswahl der geeigneten Hardware, die die beiden zuvor genannten schwierigen Anforderungen erfüllt, muss auch die Software-Integration in einem Piloten betrachtet werden. Hier bietet es sich an, das zuvor beschriebene VisuM-System einzusetzen, welches nur für die Gegebenheiten vor Ort konfiguriert sowie mit dem SAP-System gekoppelt werden muss. Möglich wäre auch die direkte Kopplung mit dem SAP-System über eine Middleware-Komponente wie die Auto-ID Infrastructure [Kub03] von SAP.

Bevor mit den Arbeiten zur Software-Anbindung begonnen werden kann, müssen zunächst die Resultate, die die Hardware-Evaluierung liefert, abgewartet werden. Es wurde dazu mit über vierzig RFID-Herstellern sowie RFID-Systemintegratoren Kontakt aufgenommen und vereinzelt Tests durchgeführt. Hierbei zeigte sich recht schnell, dass nur eine Hand voll Anbieter prinzipiell eine Lösung in diesem schwierigen metallischen Umfeld anbieten kann. Ein Test vor Ort mit Metallcontainern, die beispielsweise mehrere hundert Fensterhebermotoren enthalten, muss letztlich zeigen, ob eine geeignete RFID-Hardware für einen Piloten existiert. Falls die Evaluation erfolgreich abgeschlossen wird, ist im nächsten Schritt die Software-Anbindung zum SAP-System zu realisieren. Gleichzeitig werden dann auch die so genannten Key Performance Indicators (KPI) bestimmt, die dazu dienen, den Piloten aus betriebswirtschaftlicher Sicht zu bewerten. Schließlich wird der Pilot dann parallel zum laufenden Betrieb aufgesetzt und kontinuierlich die KPIs gemessen.

Die „Smart Warehouse“-Applikation wäre eine erste Umsetzung von teilebezogener Transpondernutzung bei der Volkswagen AG. Damit wäre die Voraussetzung geschaffen, weitere RFID-basierende Applikationen zu entwickeln bzw. weitere Prozesse einer entsprechenden Optimierung zu unterziehen. Dies könnte zum einen interne Prozesse, wie Umlagerungen, Nachschubversorgung oder Warenausgang, und zum anderen extern wirksame Prozesse, wie Wareneingang beim Kunden oder Tracking und Tracing, betreffen.

Literatur

[Fin02] Finkenzeller K (2002) RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3., aktualisierte und erweiterte Auflage. Carl Hanser Verlag

[Kub03] Kubach U (2003) Integration von Smart Items in Enterprise-Software-Systeme. HMD – Praxis der Wirtschaftsinformatik 229: 56–67

Tracking von Ladungsträgern in der Logistik – Pilotinstallation bei einem Güterverladeterminal

Martin Strassner
Institut für Technologiemanagement, Universität St. Gallen

Stephan Eisen
Intellion AG, St. Gallen

Kurzfassung. Das systematische Management von Ladungsträgern für den Gütertransport kann einen wesentlichen Beitrag zur Steigerung der Effizienz von Logistikketten leisten. Transpondersysteme ermöglichen eine automatische Erfassung von Ladungsträgern an Kontrollpunkten und steigern die Transparenz von Transportprozessen. Die gewonnenen Daten tragen zur Verbesserung der Auslastung, der Umlaufzeit und der Verfügbarkeit bei. Weitere Anwendungspotenziale bestehen beispielsweise in der Einführung nutzungsabhängiger Abrechnungsmodelle, im Outsourcing von Ladungsträgerpools oder im indirekten Tracking der beförderten Güter. Der vorliegende Beitrag zeigt anhand einer Pilotinstallation, wie die Transpondertechnologie automatisch Bewegungsdaten misst und wie sich durch weitere Aufbereitung aus diesen Daten relevante Kenngrößen für die Steuerung der Prozesseffizienz bestimmen lassen.

1 Einleitung und Problemstellung

Die Verfügbarkeit von Ladungsträgern (z.B. Container, Paletten, Behälter, Gestelle) ist eine Voraussetzung für den Transport von Gütern und damit auch für die industrielle Produktion. Trotzdem ist dieser Bereich bisher gering automatisiert [Abe04]. Die Folge sind ineffiziente Prozesse durch lange Umlaufzeiten, schlechte Auslastung, unnötig hohe Bestände an Ladungsträgern und mangelnde Kenntnis über deren physischen Zustand.

Zur Verbesserung der Verfügbarkeit tragen Pool-Systeme bei (siehe Abbildung 1). Diese sammeln alle verfügbaren Ladungsträger an einer zentralen Stelle. Lieferanten rufen bei Bedarf Ladungsträger ab, um ihre Kunden zu beliefern. Der Kunde ist für die Rückführung in den Pool verantwortlich.

Hierbei entstehen lange Umlaufzeiten z.B. dann, wenn bei der Rückführung von Leergut für den Belieferten kein ausreichender Anreiz besteht, den nicht mehr benötigten Ladungsträger sofort zurückzugeben. Einen solchen Anreiz könnte ein nutzungsabhängiges Abrechnungsmodell schaffen. Zum Beispiel können Mietsysteme, bei denen eine Tagesmiete zu entrichten ist, die Rücklaufquote verbes-

sern. Die Berechnung von zusätzlichen Gebühren bei Überschreitung einer vereinbarten Leihfrist kann die Rückführung ebenfalls beschleunigen.

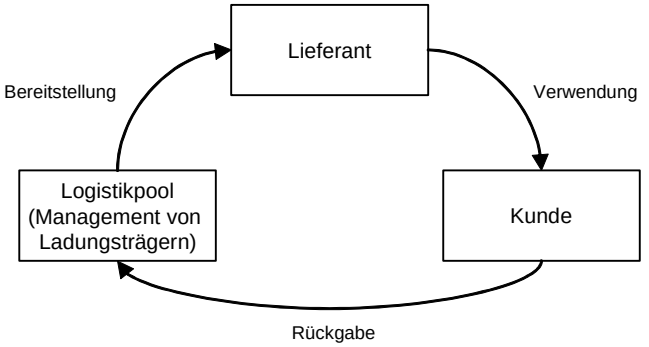


Abb. 1. Container-Kreisläufe beim Pool-System

Um Störungen bei der Verfügbarkeit zu vermeiden, halten Unternehmen typischerweise mehr Ladungsträger vorrätig, als eigentlich für den Betrieb notwendig wären. Diese stellen unnötigerweise gebundenes Anlagevermögen dar. Neben den genormten Standardladungsträgern, z.B. Europaletten, ISO-Container oder VDA-KLTs (Verband der Automobilindustrie-Kleinladungsträger), die meist durch Logistikdienstleister verwaltet werden, trifft dies insbesondere für zahlreiche Spezialladungsträger zu. Beispielsweise benötigen in der Automobilindustrie verschiedene Bauteile, wie etwa Motoren, Getriebe oder Türen, jeweils spezielle Ladungsträger. Diese kosten häufig mehr als 1 000 Euro pro Stück.

Eine weitere mögliche Ursache für Probleme stellt der physische Zustand der Ladungsträger dar. Wird ein Schaden erst während der Nutzung bemerkt, kann es zu Verzögerungen von Lieferungen oder zu Unfällen kommen. Für Gefahrguttransporte gelten deshalb gesetzliche Vorschriften, die eine regelmäßige Überprüfung der eingesetzten Ladungsträger verlangen [Bam03].

Asset-Management-Systeme bieten eine Möglichkeit zur IT-gestützten Verwaltung von Ladungsträgerpools. Allerdings verwalten solche Systeme häufig nur die Gesamtanzahl an vorhandenen Behältern einer Sorte. Eine Ursache hierfür ist der große manuelle Aufwand, der zur Erfassung jedes einzelnen Behälters bei Verwendung traditioneller Identifikationsmethoden wie etwa Nummerierung oder Barcodes notwendig wäre. Bei der manuellen Erfassung der Poolzugänge und -abgänge unterlaufen Mitarbeitern immer wieder Fehler, sodass die im System gespeicherten Werte selten hinreichend genau mit der Realität übereinstimmen.

Aus diesem Grund setzen einige Unternehmen für das Ladungsträgermanagement die Transpondertechnologie ein. Diese Technologie, zu der auch die Radio-Frequency-Identification-(RFID-)Technologie gehört, ermöglicht eine automatische Erfassung entsprechend ausgerüsteter Gegenstände ohne manuelle Tätigkeiten und ohne direkte Sichtverbindung zum Erfassungsgerät [Fin02].

Ein Beispiel für eine solche Anwendung bietet die Firma Container And Pallet Services[34] (CAPS) aus den USA, die wieder verwendbare Ladungsträger an Kun-

[34] www.usecaps.com.

den aus der Industrie verleiht. Die Kunden von CAPS erwarten, dass stets die gewünschte Menge an Ladungsträgern verfügbar ist und dass diese sich in einem einwandfreien Zustand befinden. In der Vergangenheit hatte CAPS nicht exakt protokolliert, welche Ladungsträger die Firma an welche Kunden verliehen hatte. Dies hatte dazu geführt, dass sich Leergut beim Kunden angesammelt hat, während eine Verknappung an abrufbereiten Ladungsträgern im Pool auftrat. Wegen ungenauer Daten über die Bestände im Pool konnte CAPS den Kunden keine sofortigen, verbindlichen Zusagen für Abrufe erteilen.

Heute nutzt CAPS für einen Teil der Behälter ein selbst entwickeltes Behältermanagementsystem. Dieses System verwendet in einem Pilotversuch die RFID-Technologie zur eindeutigen automatischen Identifikation. Bei der Auslieferung der Ladungsträger an den Kunden sowie bei der Rücknahme erfassen Mitarbeiter von CAPS diese mit einem mobilen Lesegerät. Die Lesegeräte übertragen die Daten automatisch an das System, das somit stets den aktuellen Bestand an Behältern zur Verfügung stellen kann. Außerdem erfasst das System, welche Behälter ein Kunde für welchen Zeitraum ausgeliehen hat. Diese Informationen bilden die Grundlage für ein neues Abrechnungsmodell. Statt einer Pauschalgebühr pro ausgeliehenem Behälter bestimmt die tatsächliche Leihzeit die fällige Gebühr. Ebenfalls auf den Nutzungsdaten basierend führt CAPS nun eine planmäßige nutzungsabhängige Wartung der Ladungsträger durch. Das System hat dem Unternehmen geholfen, den Behälterkreislauf transparent zu machen und die Verwaltung des Bestandes zu automatisieren.

Ein weiteres Beispiel für den Einsatz der Transpondertechnologie für das Behältermanagement stammt aus der Brauindustrie. Brauereien verzeichnen einen regelmäßigen Schwund der zur Auslieferung an Gaststätten verwendeten Aluminium-Bierfässer. In der englischen Brauindustrie bewegt sich der Schwund in einer Größenordnung von 3–5 % pro Jahr. Der hierdurch entstandene Schaden wird auf ca. 21 Millionen Euro pro Jahr geschätzt [Sac99]. Die Brauereien vermuten, dass Diebe die Bierfässer wegen des hohen Aluminiumwertes einschmelzen.

Ebenso besteht für die Kunden kein Anreiz, die Bierfässer möglichst schnell wieder an den Hersteller zurückzugeben. Die Kunden bezahlen lediglich nach Anzahl bezogener Fässer. Eine systematische Dokumentation über den Verleih von Bierfässern führen die meisten Brauereien nicht durch.

Die Brauerei Scottish Courage führte aus diesem Grund ein RFID-basiertes Tracking-System ein. Das Unternehmen ließ alle 1,8 Millionen Bierfässer mit Transpondern ausstatten. Beim Warenausgang erfassen Mitarbeiter die Fässer mittels eines Handlesegerätes und ordnen sie im System dem Kunden zu. Das Transpondersystem ermöglicht hierbei die eindeutige und zuverlässige Identifikation der Bierfässer mit geringem manuellem Aufwand. Die Schwundquote sank nach der Einführung des Systems auf 1,9 % und die Umlaufzeit pro Fass verkürzte sich im Durchschnitt um vier Tage. Durch geringere Anschaffungskosten für neue Bierfässer erhöhten sich die Erträge der Brauerei aus dem Verkauf an Gaststätten um 3 % [FTi03].

In einem weiteren Schritt hat die Brauerei den Pool von Bierfässern an die Firma Trenstar ausgelagert [Tre02]. Hierbei bietet die automatische Identifikation die Grundlage für ein zuverlässiges Abrechnungssystem. Lesegeräte im Bereich der Füllanlage ermöglichen ein Abrechnungsmodell in Abhängigkeit von der An-

zahl der Befüllungen. Mit diesem Schritt hat Scottish Courage das Risiko, Bierfässer zu verlieren, ausgelagert.

Weitere Beispiele für Pilotinstallationen von Behältermanagementsystemen mit Hilfe der RFID-Technologie gibt es in der Automobilindustrie[35]. Beispielsweise hat Volkswagen Spezialgestelle mit Transpondern ausgestattet und trackt diese. Mittels einer selbst entwickelten Software kann Volkswagen jederzeit den Standort der getrackten Behälter bestimmen[36].

Die beschriebenen Anwendungen beziehen sich auf das Management von lokalen Behälterpools. Es handelt sich typischerweise um Anwendungen mit geschlossenen Kreisläufen („closed loop"), und die verwendeten Systeme sind proprietär. Trotzdem ermöglichen die gewonnenen Daten einige nützliche Anwendungen. Die anhand geschlossener Kreisläufe gewonnenen Erkenntnisse sind ein erster Schritt in Richtung des Aufbaus solcher Anwendungen bei globalen Lieferketten und formulieren Rahmenbedingungen für die damit verbundene notwendige Standardisierung.

Nachfolgende Abschnitte beschreiben anhand einer Pilotinstallation zum Fuhrparkmanagement von LKW-Aufliegern, wie ein solches System aufgebaut wurde und welchen Nutzen die durch das System gewonnenen Daten ermöglichen.

2 Pilotsystem zum Tracking von LKW-Aufliegern

Die nachfolgend beschriebene Pilotinstallation[37] wurde bei einem Güterverladeterminal in der Nähe von Graz in Österreich durchgeführt. Das Terminal lagert Container, die per Bahn ankommen, zwischen und liefert sie bei Abruf an die in der Region ansässige Automobilindustrie aus. Folgende Abschnitte stellen zunächst den allgemeinen Prozess des Containerkreislaufes zwischen dem Güterterminal und einem Automobilwerk dar. Danach folgen die Beschreibungen der Zielvorstellungen, der technischen Funktionsweise sowie der gewonnenen Daten. Der letzte Abschnitt beschreibt die hieraus abgeleiteten Erkenntnisse für den Nutzen eines solchen Systems und die Kosten.

2.1 Prozess des Containerumlaufs

Dieser Abschnitt beschreibt die wesentlichen Prozessschritte der im Rahmen der Pilotanwendung betrachteten Lieferkette sowie die Containerbewegungen (siehe Abbildung 2). Die Container stammen aus Nordamerika und gelangen auf dem Seeweg nach Europa. Anschließend erfolgt der Bahntransport bis zum Terminal.

[35] Die Aktionen der deutschen Automobilindustrie werden über den Arbeitskreis „Behälterstandardisierung" des VDA koordiniert [VDA03].

[36] Siehe Beitrag zu RFID in der Automobilindustrie in diesem Buch.

[37] An dem durch das österreichische Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) geförderten Projekt beteiligt waren das Cargo Center Graz, die Identec Solutions AG, die Intellion AG und das Institut für Wirtschaftsinformatik der Universität St. Gallen [StF02].

Bei Bedarf bringen LKWs die Container zum Automobilwerk und holen gleichzeitig leere Container wieder zum Terminal zurück. Da alle Container auf diese Weise wieder zum Terminal zurückkommen, besteht zwischen dem Terminal und dem Automobilwerk ein geschlossener Kreislauf. Das Güterterminal führt die gesammelten leeren Container an Pools der Reedereien zurück.

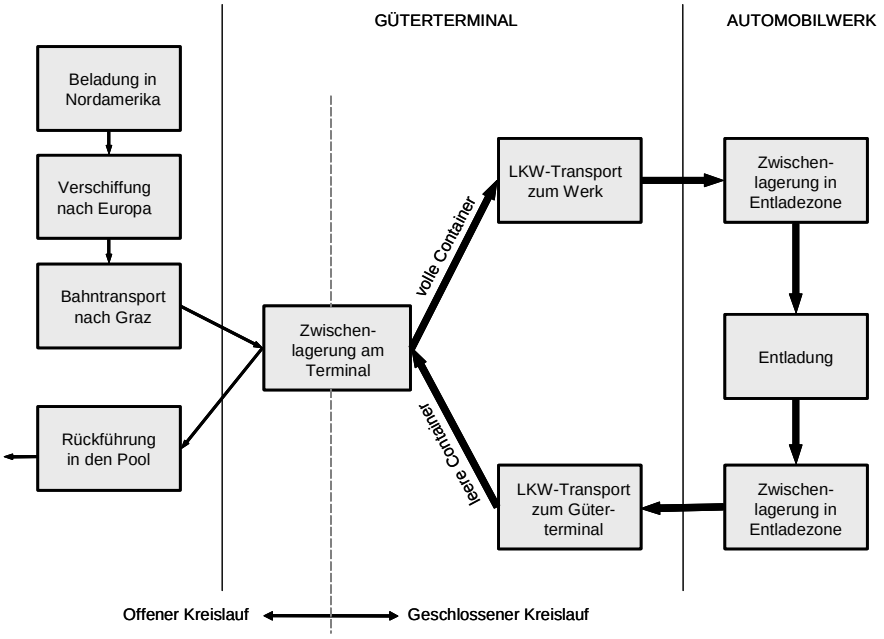


Abb. 2. Containerkreislauf

Die Lieferkette umfasst die folgenden Schritte:

- **Beladung und Transport in Nordamerika.** Nach erfolgter Auslieferung bestätigen die Zulieferer dies über ein EDI-System. Die Versandbestätigung liegt dem Automobilwerk spätestens mit einer Verzögerung von 30 Minuten vor. In einem der drei nachgeschalteten Konsolidierungszentren erfolgt eine Umverpackung in ISO-Standardcontainer für die Verschiffung. Von hier transportieren Speditionen die Container weiter zu einem von sechs Häfen. Einige Hersteller verschiffen ihre Lieferungen direkt ohne den Umweg über ein Konsolidierungszentrum.
- **Verschiffung nach Europa.** Während der Verschiffung liefert ein Tracking-System regelmäßig aktualisierte Positionsangaben. Beispielsweise wegen Wetterbedingungen oder Verzögerungen am Zoll ist eine genaue Vorhersage der Fahrtdauer nicht möglich. Durchschnittlich treten Abweichungen von ca. zwei Tagen auf.
- **Bahntransport nach Graz.** Nach der Ankunft im europäischen Hafen erfolgt die Verladung auf die Bahn. Die aktuelle Materialbedarfsreihenfolgeplanung bestimmt die Zugzusammensetzung. Während des Bahntransports liefern die

Deutsche Bahn (DB) sowie die Österreichische Bundesbahn (ÖBB) bei der Ankunft an bestimmten Bahnhöfen aktualisierte Positionsdaten. Beim Güterverkehr sind Abweichungen bei der Streckenführung möglich, einen genauen Fahrplan gibt es nicht. Endbahnhof ist das Containerterminal in Graz. Beim Eintreffen erhält das Automobilwerk auf elektronischem Weg eine Ankunftsbestätigung. Pro Tag treffen durchschnittlich drei Züge mit je 40–50 Containern ein.

- **Zwischenlagerung und Vorsortierung am Containerterminal.** Die Reihenfolge des Eintreffens bestimmt auch die Reihenfolge der Einlagerung. Dabei stapeln Kranfahrer bis zu vier Container übereinander. Welche Container auszuliefern sind, teilt das Automobilwerk bis 15 Uhr des Vortages per Fax mit. Mit dieser Information führen die Lagermitarbeiter eine Vorsortierung (Kommissionierung) durch, um die Abholung am nächsten Tag nicht zu verzögern. Würden die Container schon beim Eintreffen in der Reihenfolge des Abrufs eingelagert, könnte dieser Sortierschritt entfallen. Pro Tag fordert das Automobilwerk im Durchschnitt 140 Container an. Die durchschnittliche Zwischenlagerungszeit beträgt drei bis fünf Tage. Diese ist als Puffer notwendig, da die Transportzeiten aus Nordamerika nicht genau vorhersagbar sind.
- **LKW-Transport zum Automobilwerk.** Für den Transport zum Automobilwerk verladen Kranfahrer die vorsortierten Container auf Sattelauflieger. Insgesamt stehen bis zu 125 Sattelauflieger zur Verfügung. LKWs bringen die Sattelauflieger mit den Containern direkt bis zur Entladezone innerhalb des Werkes. Der Transport dauert mindestens 30 Minuten. Von der Entladezone befördern Transportfahrzeuge die beladenen Sattelauflieger zu den Docks der Werkshalle.
- **Entladung beim Automobilwerk.** An den Docks führen Mitarbeiter des Automobilwerks die Wareneingangskontrolle durch. Hierzu erfassen sie mit Strichcode-Scannern die gelieferten Teile manuell und vergleichen die Daten mit den Bestellmengen. In seltenen Fällen kommt es vor, dass die Lieferung zu wenig Teile enthält bzw. Teile beschädigt sind. In diesem Fall fordern sie sofort telefonisch Nachschub beim Güterterminal an. Das Güterterminal kann fehlende Teile in der Regel innerhalb einer Stunde nachliefern.
- **Rücktransport zum Güterterminal und Rückführung der Container.** Transportfahrzeuge bringen die leeren Container samt Auflieger zurück in die Entladezone. Dort nimmt jeweils ein LKW, der gerade einen vollen Container gebracht hat, einen leeren zurück. Das Containerterminal sammelt die leeren Container in einem Zwischenlager und leitet sie dann an einen von den Reedereien genehmigten Pool weiter.

2.2 Ziele des Pilotsystems

Das Ziel bei der Entwicklung der Pilotinstallation war die Verbesserung des Managements von Aufliegern (oder vergleichbarer Ladungsträger in der Logistik) durch die automatische Identifikation mittels aktiver Transponder. Das Pilotsystem sollte einerseits die technische Machbarkeit im Umfeld der Containerlogistik

zeigen und andererseits helfen, Nutzen stiftende Anwendungen mit den gewonnenen Daten im Bereich des Güterterminals zu identifizieren.

Das Tracking von Aufliegern ermöglicht die Verbesserung der Prozesseffizienz und -qualität des Fuhrparkmanagements. In diesem Zusammenhang ist die Untersuchung der für das Ladungsträgermanagement wichtigen Kennzahlen Umlaufzeit, Auslastung und Verfügbarkeit relevant:

- **Auslastung.** Die Überwachung der Auslastung ermöglicht die Einhaltung nutzungsabhängiger Wartungszyklen oder die Steuerung einer gleichmäßigen Abnutzung der Ladungsträger. Die Anzahl der Fahrten pro Auflieger ist eine Messgröße zur Bestimmung der Auslastung.
- **Verfügbarkeit.** Eine für den Betrieb angemessene Anzahl an Aufliegern bewirkt eine Verbesserung der Effizienz des Fuhrparks. Falls permanent eine große Anzahl Auflieger im Terminal stehen, signalisiert dies einen unangemessen hohen Bestand. Wenn hingegen der Bestand zu knapp bemessen ist, kann dies zu Verzögerungen bei der Auslieferung führen. Um solche Situationen zu vermeiden, setzen Logistiker häufig mehr Ladungsträger als notwendig ein. Ob die Anzahl Auflieger angemessen ist, lässt sich durch die Beobachtung der an einer Reihe von aufeinander folgenden Tagen jeweils minimalen bzw. maximalen Anzahl im Terminal verfügbarer Auflieger bestimmen. Falls häufig sehr viele Auflieger verfügbar sind, deutet dies auf einen ineffizient hohen Bestand hin.
- **Umlaufzeit.** Die Umlaufzeit setzt sich aus den Transport-, Be- und Entladungs- sowie Standzeiten zusammen. Zur Messung können die Zeiten herangezogen werden, die sich Auflieger jeweils inner- bzw. außerhalb des Terminals befinden.

2.3 Aufbau des Pilotsystems

Eine Pilotinstallation zur automatischen Ein- und Ausfahrtskontrolle an einem Güterterminal sollte zeigen, ob die Transpondertechnologie einen Beitrag zur Effizienzsteigerung im Güterumschlag leisten kann. Die hierbei eingesetzte Transpondertechnologie funktioniert nach folgendem Prinzip (siehe Abbildung 3):

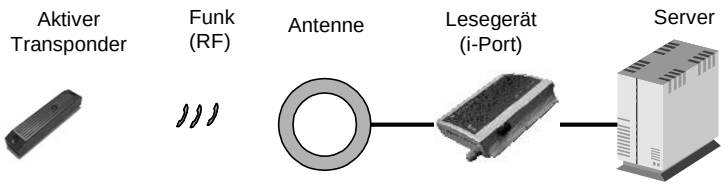


Abb. 3. Prinzipielle Funktionsweise des RFID-Systems

Ein an den Ladungsträgern angebrachter Transponder ermöglicht die automatische Identifikation mittels UHF (Ultrahochfrequenz), ohne dass hierfür ein Sichtkontakt notwendig ist. Nach Aktivierung durch ein von einer Antenne erzeugtes elektromagnetisches Feld übermittelt der Transponder eine Identifikationsnummer. Ein Lesegerät interpretiert die von der Antenne empfangenen Signale und leitet die Daten in digitaler Form an einen Server zur Verarbeitung weiter.

Zur Realisierung des Pilotsystems kam die aktive ILR (Intelligent Long Range)-Technologie der Firma Identec Solutions[38] zum Einstz. Diese besteht aus aktiven Transpondern, mobilen und stationären Schreib-Lesestationen (i-Ports) mit Ethernet- bzw. Funk-LAN-Anbindung sowie Software-Modulen für die Anbindung an übergeordnete IT-Systeme. Der Erfassungsradius beträgt im freien Feld bis zu 100 m.

Abb. 4. Position des Tags am Auflieger

Insgesamt verwendete die Pilotinstallation 26 Transponder, zwei Gate-Antennen, ein i-Port-Lesegerät sowie einen PC mit Modemanschluss. Die Anbringung der Tags erfolgte bei 26 zufällig ausgewählten Aufliegern jeweils an der Oberkante der hinteren Stoßstange (vgl. Abbildung 4). Da das Gelände über nur einen zentralen Ein- und Ausgang mit einer Breite von ca. 15 m verfügt, waren zwei Gate-Antennen für die Ein- und Ausfahrtskontrolle ausreichend (vgl. Abbildung 5).

Abb. 5. Hofeinfahrt des Güterterminals

[38] www.identecsolutions.at

Die Installation der Gate-Antennen erfolgte einige Meter versetzt, um die Richtung der Bewegung (Ein- oder Ausfahrt) erfassen zu können (vgl. Abbildung 6). Auf diese Weise gelangte ein Auflieger (Transponder) immer zuerst in das Lesefeld der einen Antenne und erst mit einer Verzögerung in das der zweiten Antenne. Ein i-Port-Lesegerät wertete die Daten aus und speicherte sie in Form eines tabellarischen Protokolls. Die Firma Intellion rief dann die Daten regelmäßig per Funkmodem (GSM) ab und verwendete die eigens entwickelte Software Object-Control zur weiteren Aufbereitung der Daten[39].

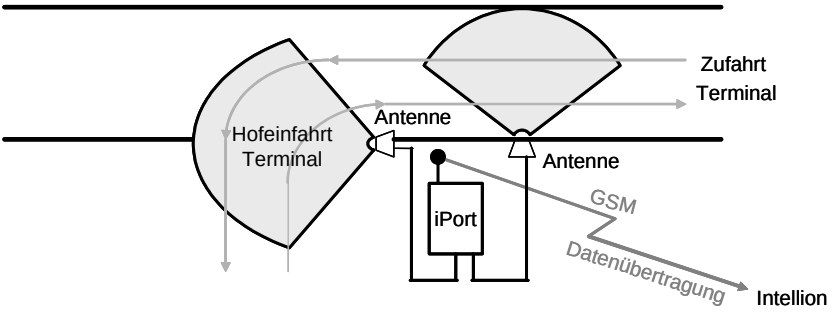


Abb. 6. Aufbau des Pilotsystems

2.4 Messergebnisse des Pilotsystems

Die nachfolgend beschriebenen Messwerte beziehen sich auf einen Zeitraum von sechs Wochen. Das Pilotsystem erfasste die Ein- und Ausfahrten der 26 getrackten Auflieger über diesen Zeitraum. Hierzu lieferte das System 2 516 Einzelmessungen. Die Auswertung untersucht die Anzahl der Fahrten, die Aufliegerverfügbarkeit sowie die Prozessgeschwindigkeit.

Anzahl der Fahrten. Die Anzahl der Fahrten liefert Hinweise für den Bedarf an Aufliegern und ermöglicht, die Auslastung einzelner Auflieger zu ermitteln. Insgesamt ergab die Messung im Beobachtungszeitraum 1 162 Fahrten, was im Durchschnitt ca. 40 Fahrten pro Auflieger entspricht.

Die Auslastung der einzelnen Auflieger, nach Aufliegernummern ausgewertet, ist allerdings unregelmäßig. Die Fahrtenzahlen liegen in einem Schwankungsspektrum von 15–71 Fahrten (Abbildung 7).

[39] www.intellion.com

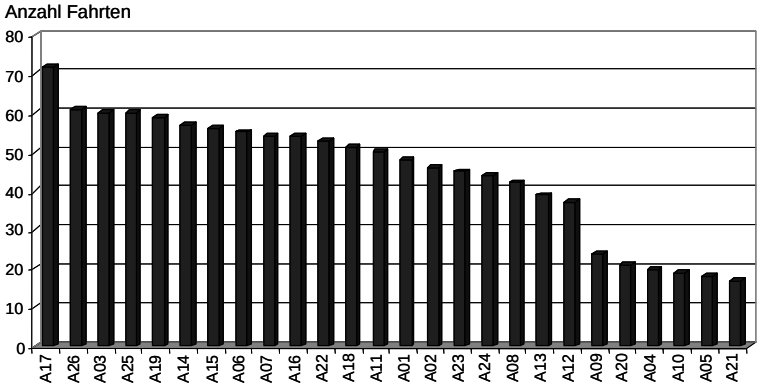


Abb. 7. Anzahl Fahrten im Beobachtungszeitrum nach Auflieger

Verfügbarkeit. Eine aussagekräftige Überwachung der verfügbaren Auflieger setzt eine Untersuchung des Gesamtbestands über einen längeren Zeitraum voraus. Um das Prinzip der Verfügbarkeitsmessung zu zeigen, stellt Abbildung 8 den minimal bzw. maximal verfügbaren Bestand der im Rahmen des Prototypen untersuchten Auflieger pro Tag über den Beobachtungszeitraum dar. Jede Ein- und Ausfahrt aktualisierte automatisch eine durch das System geführte Bestandsgröße. Das Minimum bzw. Maximum dieser Bestandsgröße an einem Tag entsprach der minimalen bzw. maximalen Anzahl an verfügbaren Aufliegern an diesem Tag. Die Messung ergab, dass zu bestimmten Zeiten tatsächlich keine Auflieger zur Verfügung standen[40]. Auf der anderen Seite war zu keiner Zeit mehr als die Hälfte des erfassten Bestandes im Terminal, was auf einen zu hohen Bestand hätte schließen lassen.

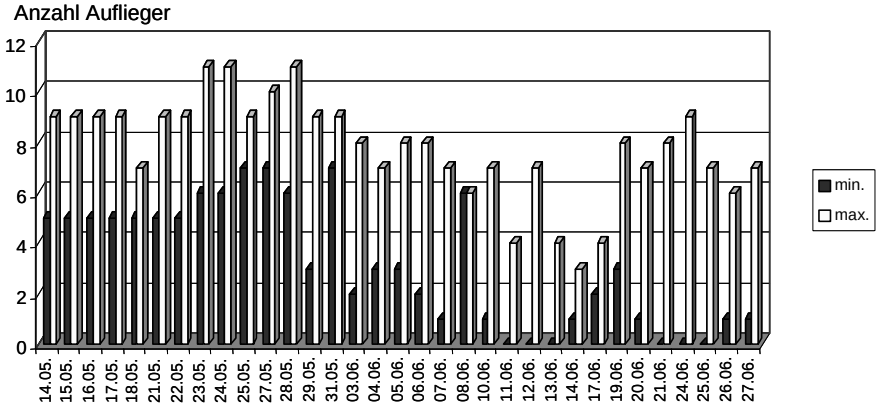


Abb. 8. Minimale und maximale Verfügbarkeit

[40] Diese Aussage gilt nur für die 26 der insgesamt ca. 125 Auflieger, die im Rahmen des Prototypen erfasst wurden.

Prozessgeschwindigkeit. Die Analyse der Zeiten, in denen sich ein Auflieger innerhalb oder außerhalb des Terminals befand, lieferte Informationen über die Prozessgeschwindigkeit: Die Zeit innerhalb des Terminals wurde von der Standzeit, der Wartezeit sowie der Beladezeit bestimmt. Die Standzeit umfasste Zeiten, in denen ein Auflieger sich nicht im Einsatz befand, z.B. weil er sich im Pool oder in der Reparatur befand. Die Wartezeit gab an, wie lange der Fahrer warten musste, nachdem er im Terminal angekommen war, bis die Beladung des Aufliegers begann.

Zeit innerhalb des Terminals = Standzeit+Wartezeit+Beladezeit

Falls sich ein Auflieger mehr als 3 Stunden auf dem Terminal befand, ging diese Untersuchung von einer Standzeit aus. Dementsprechend stellte die restliche Zeit eine Schätzung der Warte- und Beladezeit dar. Das Ergebnis zeigte mit wenigen Abweichungen eine durchschnittliche Warte- und Beladezeit von 15–25 Minuten, während die Standzeiten sehr unterschiedlich ausfielen (siehe Abbildung 9).

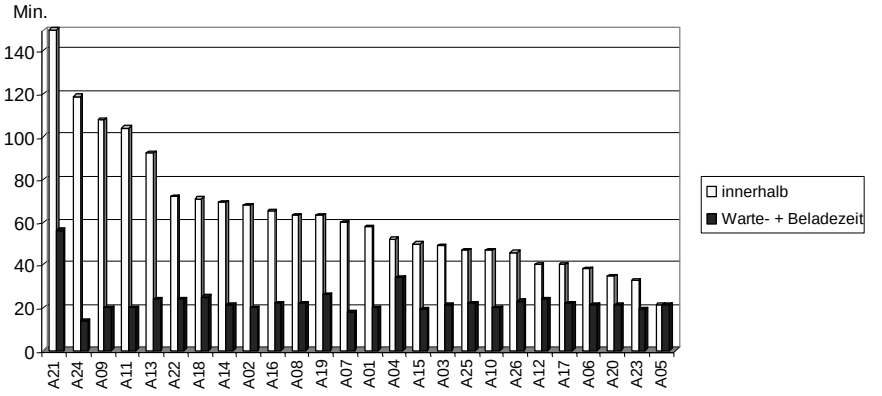


Abb. 9. Durchschnittliche Zeiten innerhalb des Terminals

Die Zeit, die sich ein Auflieger außerhalb des Terminals befand, setzte sich aus der Fahrzeit (ca. 40 Minuten) sowie der Entlade-, Warte- und Standzeit beim Automobilwerk zusammen. Als durchschnittliche Zeit außerhalb des Terminals ergab die Auswertung 8–10 Stunden, wobei einzelne starke Abweichungen auffielen. Dies könnte darauf hinweisen, dass einige Auflieger unnötig lange Standzeiten außerhalb des Terminals aufgewiesen haben (siehe Abbildung 10). In Anbetracht dessen, dass die Betreiber des Terminals auch die durchschnittliche Zeit außerhalb des Terminals von 8–10 Stunden als ungewöhnlich lange empfanden, könnten die mittels der Pilotinstallation gewonnenen Ergebnisse einen Anlass zur genaueren Untersuchung der Abläufe im Automobilwerk geben.

Zeit außerhalb des Terminals = Fahrzeit+Wartezeit+Entladezeit+Standzeit

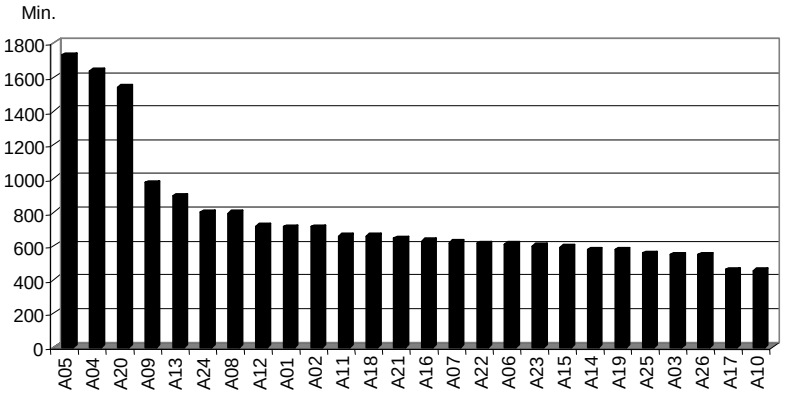


Abb. 10. Durchschnittliche Zeiten außerhalb des Terminals

2.5 Kosten- und Nutzenbetrachtung

Aus der Interpretation der Ergebnisse des Vorangehenden leitet dieser Abschnitt Handlungsempfehlungen für eine Verbesserung des Aufliegertrackings am Güterterminal ab. Zuvor folgt eine Übersicht der notwendigen technischen Komponenten für ein der Pilotinstallation entsprechendes System zum Tracking aller 125 im Einsatz befindlichen Auflieger sowie über dessen Kosten (Angaben gerundet):

- Zwei Gate-Antennen mit i-Port-Lesegerät und Installation: EUR 10 000
- 125 aktive Tags inklusive Installation: EUR 8 750 (EUR 70 pro Transponder)
- Kosten für die Anbindung an ERP-Systeme: EUR 10 000–20 000
- Wartung: EUR 500–1 000 pro Jahr

Bei einem Abschreibungszeitraum von fünf Jahren bedeutet dies insgesamt jährliche Aufwendungen in Höhe von ca. EUR 8 000. Folgende Verbesserungspotenziale haben sich durch die Pilotinstallation gezeigt:

Die *Auslastung der Auflieger* hat sich als sehr ungleichmäßig erwiesen. Die mittels der Anwendung gewonnenen Daten könnten zur Steuerung der Auslastung eingesetzt werden und um nutzungsabhängige Wartungszyklen einzuführen. Im Voraus planbare Wartungen ermöglichen die Auslastungssteuerung des Wartungsbetriebes und minimieren das Risiko des unerwarteten Ausfalls von Ladungsträgern.

Bezüglich der *Verfügbarkeit von Aufliegern* hat sich ergeben, dass zu bestimmten Zeiten keiner der getaggten Auflieger am Terminal verfügbar war. Da über die anderen Auflieger keine Informationen vorliegen, kann im konkreten Fall keine Handlungsempfehlung abgeleitet werden. Hätte sich das gleiche Ergebnis bei der Überwachung aller Auflieger ergeben, wäre dies ein Indiz, den Bestand an Aufliegern zu erhöhen.

Bei der Messung der *Umlaufzeit* hat sich die Vermutung bestätigt, dass der Aufliegerumlauf unnötig lange gedauert hat. Während bezüglich der Warte- und Beladezeiten innerhalb des Terminals (durchschnittlich ca. 15–20 Minuten) kein Handlungsbedarf besteht, waren die langen Standzeiten der Auflieger beim belieferten Automobilwerk (durchschnittlich 9–10 Stunden inklusive Nachtstandzeiten) auffällig. Hier sollte der Terminalbetreiber die Ursachen der langen Standzeiten überprüfen, zu denen er momentan keine Informationen besitzt. Ggf. ist eine schnellere Rückführung der Auflieger möglich. In diesem Fall würde sich die Verfügbarkeit von Aufliegern verbessern, sodass die Terminalbetreiber evtl. auf eine Bestandserhöhung verzichten bzw. den Bestand kostensenkend verkleinern könnten.

Ein Gesamtnutzen ließe sich nur mit Kenntnis der tatsächlichen Anzahl der einzusparenden Auflieger berechnen. Die Berechnung dieser Zahl setzt die Bewegungsdaten aller Auflieger sowie die tatsächlich mögliche Verkürzung der Umlaufzeit voraus. Angenommen ein Auflieger verursacht jährliche Abschreibungen von EUR 400. Dann würde der Nutzen des Systems die Kosten ab einer Reduktion des Aufliegerbestands um 21 übersteigen. Die Quantifizierung weiterer Nutzenpotenziale, die sich aus der Verbesserung der Verfügbarkeit sowie der Wartung ergeben könnten, setzt allerdings zusätzliche Daten voraus, z.B. die Folgekosten aus mangelnder Verfügbarkeit von Aufliegern.

3 Fazit und Ausblick

Wie Anwendungsbeispiele aus der Logistik zeigen, ermöglicht die Transpondertechnologie ein automatisiertes Management von mobilen Ressourcen. Die in diesem Beitrag beschriebene Pilotinstallation an einem Güterterminal in Graz demonstriert beispielhaft, welche Potenziale die Integration physischer Ressourcen mit Systemen der Datenverarbeitung besitzt. Dieses abschließende Kapitel beurteilt die Relevanz der Ergebnisse des Pilotversuchs, zeigt Potenziale der Transpondertechnologie für das Ladungsträgermanagement auf und beschreibt Kriterien für die Einführung der Technologie.

Die im Rahmen des Pilotsystems gewonnenen Erkenntnisse gelten für die in der Untersuchung erfassten 26 Auflieger, die nicht notwendigerweise repräsentativ für den Gesamtbestand sind. Voraussetzung für wirksames Fuhrparkmanagement wäre die Überwachung des Gesamtbestandes an Aufliegern. Einzelne Abweichungen, die bei den Messungen aufgetreten sind, wie z.B. deutlich überdurchschnittlich hohe Standzeiten bestimmter Auflieger, erfordern eine zusätzliche Analyse der Messdaten bzw. Zusatzinformationen, z.B. über Werkstattaufenthalte der Auflieger. Es ist also eine Analyse und Interpretation der gewonnenen Daten notwendig, um konkrete Handlungsempfehlungen abzuleiten. Allerdings sind die durch den Prototyp aufgedeckten Schwächen, wie etwa un-

gleichmäßige Auslastung, fehlende Verfügbarkeit sowie ineffiziente Zirkulationszeiten, typisch für den Einsatz von Transportbehältern in der Logistik[41].

Die durch Erfassung der Ladungsträgerbewegungen entstehende Prozesstransparenz ermöglicht die Überwachung und Steuerung des Ladungsträgerbestandes mit den Zielen, die Auslastung effizient zu gestalten, die Verfügbarkeit sicherzustellen und die Umlaufgeschwindigkeit zu maximieren. Auf diese Weise helfen die mittels Transpondertechnologie gewonnenen Erkenntnisse, die Prozesse am Terminal zu optimieren.

Neben der Optimierung des Fuhrparkmanagements und der Prozessgeschwindigkeit können durch den Einsatz von Transpondern an allen Aufliegern noch weitere Vorteile entstehen. Ein effizientes Management und die zuverlässige Erfassung der Nutzung von betrieblichen Ressourcen unterstützen beispielsweise das Outsourcing an Logistikdienstleister, wie das Beispiel der Firma Trenstar zeigt. Diese können durch Spezialisierung und das Management großer Pools zu einer steigenden Effizienz im Ladungsträgermanagement beitragen.

Die Transportprozesse in der Logistik sind in der Regel weniger geführt als Prozesse in der Produktion. Aus diesem Grund sind traditionelle Identifikationsmethoden, die eine geringe Erfassungsreichweite besitzen und daher manuelle Tätigkeiten erfordern, weniger geeignet. Die aktive Transpondertechnologie erschließt zahlreiche bisher nicht mit IT-Systemen erfassbare Prozesse für eine systematische Überwachung und Steuerung.

Da der Transport von Gütern in der Logistik meist in Verbindung mit Ladungsträgern erfolgt, ermöglicht das Tracking der Ladungsträger indirekt auch das Tracking der Güter. Bei diesem so genannten „Soft-Tracking“ verwaltet entweder ein IT-System die Verknüpfung zwischen Ladung und Träger oder der Transponder speichert die Daten über die Güter, die der Ladungsträger transportiert. Potenziale zur Verbesserung der Prozessteuerung und -kontrolle bestehen durch die Kommunikation dieser Informationen an Kontrollpunkten in der Lieferkette (z.B. am Wareneingang eines Lagerhauses). Vordefinierte und automatisch ausgelöste Aktionen (z.B. Steuerung der Einlagerung oder Versendung eines Belegs) unterstützen die Automation und damit die Prozesseffizienz.

Da bei dieser Lösung nur der wieder verwendbare Ladungsträger einen Transponder besitzt, sind die Kosten geringer als bei der Kennzeichnung der Güter. Den niedrigeren Kosten stehen die höhere Komplexität sowie Störanfälligkeit solcher Systeme gegenüber. Der kritische Prozess bei einem Soft-Tracking-System ist die „Verheiratung“ des Ladungsträgers mit dem Inhalt. Hierbei können prinzipiell die gleichen Fehler passieren, wie sie für die manuelle Datenerfassung charakteristisch sind.

Die Kennzeichnung von Ladungsträgern mittels Transpondertechnologie ist schon heute eine weit verbreitete Anwendung, insbesondere wenn folgende Voraussetzungen erfüllt sind:

- hoher Wert des Ladungsträgers
- hoher Wert, Verderblichkeit oder Gefährlichkeit der Güter

[41] In Pilotinstallationen verschiedener Bereiche hat die Firma Identec Solutions ein Einsparungspotenzial zwischen 5 % und 20 % beim Bestand an Transportbehältern festgestellt.

- hohe Folgekosten, falls die Lieferung nicht rechtzeitig eintrifft
- Verleihmodelle
- geschlossene Kreisläufe
- ungeführte Prozesse

Richtungsweisend für eine weitere Verbreitung sind Ankündigungen einiger bedeutender Unternehmen, welche den Einsatz von Transpondern auf Ladungsträgern in ihren Zulieferketten fordern. Beispielsweise verlangt das weltgrößte Handelsunternehmen Wal-Mart bis zum Jahr 2005 den Einsatz von Transpondern auf Paletten [Rfi03]. In der Automobilindustrie gibt es Bemühungen des VDA zur Standardisierung von Transpondersystemen zur Behälteridentifikation.

Entscheidend für die rasche Einführung ist in diesem Zusammenhang auch, inwieweit Softwarehersteller die RFID-Technologie in ihre Produkte integrieren. Integration bedeutet hierbei nicht nur die Verwendung des Transponders als Ersatz für den Barcode, sondern auch, dass die Anwendungssysteme darüber hinausgehende Funktionen wie die Verwaltung von objektbezogenen Daten (z.B. Produkthistorien, physische Zustände und Beziehungen) unterstützen. Ebenso entsteht ein nennenswerter wirtschaftlicher Nutzen nur dann, wenn die Anwendungen die Potenziale, welche die zusätzlichen Daten zur Steigerung der Prozesseffizienz bieten, auch nutzen. Die Schaffung von Transparenz, wie sie die oben dargestellte Pilotinstallation verfolgt, ist dabei nur der erste Schritt. Erst die Implementierung von regelbasierten Aktionen, welche z.B. die Verwendung von Ladungsträgern automatisiert steuern, trägt wesentlich zur Steigerung der Prozesseffizienz bei.

Literatur

[Abe04] Aberdeen Group (2004) RFID-Enabled Logistics Asset Management, Improving Capital Utilization, Increasing Availability, and Lowering Total Operational Costs.

[Bam03] BAM (2003) Rechtliche Grundlagen für die Tätigkeit der BAM – Bundesanstalt für Materialforschung und -prüfung, www.bam.de/pdf/ueber_uns/rechtsgrundlagen/rechtsgrundlagen_april_03.pdf

[Fin02] Finkenzeller K (2002) RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3., aktualisierte und erweiterte Auflage. Carl Hanser Verlag

[FTi03] Financial Times (2003) Alien concept coming to a store near you. March 5, 2003, www.equitekcapital.com/newsalien.htm

[Rfi03] RFID Journal (2003) Wal-Mart Draws Line in the Sand. June 11, 2003, www.rfidjournal.com/article/view/462

[Sac99] SACO (1999) Advanced RFID Systems in Practical Use. Extract from paper by Graham DN Miller, Project Director, Scottish Courage Brewing Limited, www.saco.co.za/appinst.html

[StF02] Strassner M, Fleisch E (2002) SmartLogistics – Prozesspotenziale und Anwendungsfelder von neuen Identifikationstechnologien in der Logistik. M-Lab Arbeitsbericht Nr. 17, Universität St. Gallen / ETH Zürich

[Tre02] TrenStar (2002). TrenStar Selected by Leading U.K. Brewer to Acquire its Keg Fleet and Provide Management Services. TrenStar Press Release, April 29, 2002, www.trenstar.com/news_events/scotco.asp

[VDA03] VDA (2003) Aufgaben und Ziele der Logistik-Arbeitskreise, www.vda.de/de/vda/intern/organisation/abteilungen/logistic_02_2.html

Automatische Produktidentifikation in der Supply Chain des Einzelhandels

Christian Tellkamp
Institut für Technologiemanagement, Universität St. Gallen

Stephan Haller
SAP Research, Karlsruhe, SAP AG

Kurzfassung. Der Einzelhandel steht unter großem Wettbewerbs- und Kostendruck. Neben der Entwicklung neuer Konzepte in der Verkaufsanbahnung und im Verkaufsabschluss streben Händler und Hersteller von Konsumgütern danach, die Prozesse in der Supply Chain weiter zu verbessern. Bisher noch nicht befriedigend gelöste Themen umfassen mangelhafte Produktverfügbarkeit, Produktverfall, Diebstahl sowie administrative Probleme wie fehlerhafte Lieferungen. Ein weiterer wesentlicher Aspekt ist der Verbraucherschutz. Technologien zur automatischen Produktidentifikation wie RFID bieten hier neue Lösungsmöglichkeiten. Der vorliegende Beitrag zeigt die Nutzenpotenziale von RFID in der Lieferkette des Einzelhandels auf, beschreibt den Status quo der Einführung und diskutiert einige häufig genannte Hindernisse für die weitere Verbreitung.

1 Einleitung

Der Einzelhandel steht unter hohem Wettbewerbs- und Kostendruck. Große Einzelhandelsketten erreichen in der Regel nur Umsatzrenditen im unteren einstelligen Prozentbereich. In Deutschland stagnieren die Umsätze im Einzelhandel seit 10 Jahren weitgehend. Einzelhändler stehen vor der Herausforderung, sich von ihren Mitbewerbern zu differenzieren und weiter Kosten zu senken. Was passiert, wenn dies nicht gelingt, zeigt sich im Lebensmittelbereich in Deutschland. Dort beträgt der Marktanteil von Discountern mittlerweile fast 40 % [Wen04].

In den letzten Jahren gab es eine Vielzahl von Publikationen zum Thema Supply Chain Management im Einzelhandel. Diese befassten sich beispielsweise mit der Frage, wie die Lieferkette gestaltet werden kann, um z.B. den „Bullwhip-Effekt“ zu reduzieren [LPW97] und schnell auf Kundenbedürfnisse reagieren zu können [Fis94]. Eine viel diskutierte Strategie ist es, Informationen über die Endkundennachfrage und Lagerbestände allen Partnern in der Supply Chain zur Verfügung zu stellen. Hierzu sind Prozesse notwendig, die qualitativ hochwertige Daten liefern. Wie Raman et al. [RDT01] in zwei Fallstudien aufzeigen, gibt es bei operativen Prozessen zum Teil noch erhebliche Verbesserungspotenziale. So sind die Informationen zum Lagerbestand nicht immer akkurat. Bei einem Einzel-

händler wich der Lagerbestand im Informationssystem für 65 % aller Produkte vom tatsächlichen Lagerbestand ab. Die Abweichung des Lagerbestands betrug im Durchschnitt 35 % des vorgesehenen Bestands. In einem anderen Fall waren 16 % der Produkte, bei deren Suche der Kunde einen Mitarbeiter im Supermarkt um Hilfe bat, verfügbar, allerdings nicht am eigentlichen Verkaufsort, sondern im Lager oder in einem falschen Regal. Neben dem Bullwhip-Effekt ist dies ein weiterer Grund dafür, dass im Einzelhandel schätzungsweise drei bis vier Prozent der Produkte nicht im Regal verfügbar sind [IBM02b, RDT01].

Im Lebensmittelbereich liegt der Anteil unverkäuflicher Produkte, z.B. aufgrund von Beschädigungen oder abgelaufenem Haltbarkeitsdatum, nach Industrieangaben in den USA bei ungefähr einem Prozent des Umsatzes [Lig02]. Unverkäufliche Produkte sind auch in anderen Segmenten ein Problem; im Kleidungsbereich gilt es beispielsweise, den Anteil unverkäuflicher saisonaler Artikel zu minimieren.

Eine weitere operative Herausforderung ist die Vermeidung von Schwund aufgrund von Diebstahl durch Mitarbeiter und Kunden, administrative Fehler oder Betrug durch Lieferanten. Der Schwund im Einzelhandel beträgt nach Umfragen in den USA im Durchschnitt 1,8 % des Umsatzes, in einigen Segmenten sogar fast 3 % [HoD01].

Ein wesentliches Thema im Lebensmittelbereich ist ferner der Verbraucherschutz. Gefragt ist hier vor allem eine sorgfältige Dokumentation der Herkunft der Produkte. Anfang 2005 trat eine EU-Verordnung [EuU02b] in Kraft, die die Rückverfolgbarkeit von Lebensmitteln durch alle Produktions-, Verarbeitungs- und Vertriebsstufen fordert. Verantwortlich für die Einführung dieses Systems sind Lebensmittelunternehmer, worunter sowohl Hersteller als auch Einzelhändler, die Lebensmittel verkaufen, fallen.

2 Einsatz automatischer Identifikationstechnologien

2.1 Schwachpunkte Barcode-basierter Anwendungen

Ungenaue Informationen über Produktverfügbarkeit oder Haltbarkeit, fehlerhafte Lieferungen sowie Schwund und mangelhafte Rückverfolgbarkeit sind Problembereiche, bei denen automatische Identifikationstechnologien (Auto-ID-Technologien) helfen können, Produkte eindeutig und weitgehend ohne manuelle Intervention zu identifizieren.

Bisherige Barcode-basierte Anwendungen (z.B. Einsatz von Barcode-Scannern in der Lagerhaltung oder an Supermarktkassen) können dies nur bedingt leisten. Barcodes haben in diesem Zusammenhang zwei wesentliche Schwächen:

- Mit dem Lesen von Barcodes ist im Allgemeinen ein gewisser manueller Aufwand verbunden, um eine Sichtverbindung zwischen Barcode-Leser und Barcode herzustellen. Dazu müssen häufig der Barcode-Leser, das Produkt oder sogar Leser und Produkt bewegt werden (z.B. wenn mehrere Kartons auf einer Palette gestapelt sind und diese einzeln gelesen werden sollen). Dieser Aufwand führt dazu, dass Barcodes nur an einigen dezidierten Punkten in der Lie-

ferkette gelesen werden. Beim Wareneingang im Supermarkt wird in der Regel nur ein Barcode gelesen, der zur Identifikation der Lieferung dient. Ob in der Lieferung selbst Produkte fehlen oder falsche Produkte enthalten sind, kann so nicht festgestellt werden. Ein etwaiger Schwund ist ebenfalls nicht feststellbar. Auch Diebstahl von Produkten aus dem Lager durch Mitarbeiter oder im Laden durch Kunden ist mit solchen Barcode-Lösungen nicht zu entdecken. Diese Faktoren wirken sich negativ auf die Produktverfügbarkeit aus. Im Laden selbst ist zudem nur über manuelle Kontrollen feststellbar, ob sich ein Produkt tatsächlich im Regal befindet. Die Informationen im Bestandswirtschaftssystem sind, wie oben dargestellt wurde, nicht immer verlässlich, und auch Kassensysteme erlauben hier nur eine näherungsweise Abschätzung (z.B. durch die Überprüfung, ob ein bestimmtes Produkt über einen längeren Zeitraum nicht verkauft wurde).

- Die derzeit im Einzelhandel auf Produktebene eingesetzten Barcodes sind identisch für alle Instanzen eines Produktes. Dies verhindert die eindeutige Identifizierung eines einzelnen Produktes. Eine Überprüfung der Haltbarkeit oder die Rückverfolgung eines einzelnen Produktes auf Basis der derzeit verwendeten Barcodes ist dadurch nicht möglich.

2.2 Nutzenpotenziale automatischer Identifikationstechnologien

Die derzeit wohl am intensivsten diskutierte Technologie zur automatischen Produktidentifikation ist die Radio-Frequency-Identification-(RFID-)Technologie. Die oben angesprochenen Probleme können dadurch sicherlich nicht komplett beseitigt werden, aber gewisse Verbesserungspotenziale erscheinen plausibel. Darüber hinaus kann RFID-Technologie zu Effizienzsteigerungen beitragen, z.B. bei der Erfassung von Wareneingängen und -ausgängen oder bei der Kommissionierung, und so zu einer Verringerung des im Lager gebundenen Kapitals führen.

Zu den spezifischen Nutzenpotenzialen von RFID in der Supply Chain im Einzelhandel gibt es eine Reihe von Veröffentlichungen, z.B. von Accenture [Acc02] und IBM Business Consulting Services [IBM02a] im Rahmen des Auto-ID Centers sowie eine Untersuchung im Rahmen der Future Store Initiative [Fut04]. Eine allgemeine Beschreibung der Nutzenpotenziale von RFID in der Supply Chain liefern McFarlane and Sheffi [MFS03].

Der vorliegende Beitrag beschäftigt sich mit Anwendungen der RFID-Technologie in Verteilzentren und Einzelhandelsgeschäften. Der Fokus liegt auf RFID-Anwendungen in der Lieferkette für verpackte Konsumgüter vom Hersteller bis in den Supermarkt. Die Aussagen lassen sich jedoch auf andere Einzelhandelsbereiche übertragen. In den Ausführungen zu den einzelnen Nutzenpotenzialen soll zwischen dem Einsatz von RFID-Tags auf Kartons und Paletten einerseits sowie dem Einsatz auf einzelnen Produkten andererseits unterschieden werden. Folgende Nutzenpotenziale werden untersucht:

- Erhöhung der Effizienz und Fehlervermeidung beim Wareneingang und -ausgang
- Erhöhung der Effizienz und Fehlervermeidung bei der Kommissionierung
- Verringerung des Lagerbestandes

- Erhöhung der Produktverfügbarkeit
- Vermeidung von Diebstahl
- Verringerung des Anteils unverkäuflicher Waren
- Selbst-Check-out in Supermärkten
- Rückverfolgbarkeit von Produkten

Die skizzierten Anwendungen können nur beispielhaft sein und reflektieren derzeit diskutierte Lösungsmöglichkeiten. Auch allgemein gültige Aussagen zur Höhe der Nutzenpotenziale entlang der Supply Chain sind kaum möglich. Die Angaben in Tabelle 1 können daher nur grobe Anhaltspunkte geben, welche Nutzenpotenziale von RFID an welchen Punkten in der Supply Chain relevant sind und auf welcher Ebene RFID-Tags sinnvoll zum Einsatz kommen. Die Angaben in der Tabelle beruhen auf der Annahme, dass der Hersteller in seinem Lager nur Vollpaletten lagert.

Tabelle 1. Anhaltspunkte für Nutzenpotenziale von RFID in der Supply Chain

Nutzenpotenzial	Herstellerlager			Distributions-zentrum			Filiale		
	P	K	E	P	K	E	P	K	E
Effizienz und Fehlervermeidung beim Wareneingang und -ausgang sowie bei der Kommissionierung	X	X		X	X		X	X	
Verringerung des Lagerbestandes	X			X	X			X	X
Erhöhung der Produktverfügbarkeit	X			X	X			X	X
Vermeidung von Diebstahl		X	X		X	X		X	X
Verringerung des Anteils unverkäuflicher Waren	X			X	X			X	X
Selbst-Check-out in Supermärkten		–			–				X
Rückverfolgbarkeit von Produkten	X	X	X	X	X		X	X	X

Legende: Einsatz von RFID auf P = Paletten-, K = Karton-, E = Einzelproduktebene; Kreuze (X) deuten an, auf welcher Ebene RFID zum Einsatz kommen kann; ein Strich (–) steht für ein nicht relevantes Potenzial

Vor der Diskussion der einzelnen Nutzenpotenziale soll noch der Aspekt der Aggregation angesprochen werden, der wesentlich für das Verständnis des Einsatzes von RFID in der Supply Chain ist.

2.3 Aggregation und RFID in der Supply Chain

Auch beim Einsatz von RFID-Tags auf Produktebene werden RFID-Tags auf Transporteinheiten nicht zwangsläufig überflüssig. Dies gilt insbesondere bei Produkten, die Flüssigkeiten enthalten oder deren Verpackungen zum Teil aus Metall bestehen. Kritisch sind ebenfalls Anwendungsfälle, in denen eine große Anzahl von Tags in kurzer Zeit oder über größere Distanzen gelesen werden muss. Will man z.B. komplette Lieferungen überprüfen, ist die Leserate (d.h. der Anteil der RFID-Tags, die richtig erkannt werden) auf Produktebene unter Umständen zu gering. Selbst wenn die Leserate für jedes RFID-Tag 99,95 % beträgt, bedeutet dies bei 100 Produkten, dass mit einer Wahrscheinlichkeit von knapp 5 % mindestens eines nicht erkannt wird.

Als Lösungsmöglichkeit bietet sich eine Aggregation von Produkten an. Dabei werden die Produkte einzeln gelesen und der nächsthöheren Aggregationsstufe (in der Regel einem Karton) zugeordnet. Entsprechendes gilt auch für die Aggregation von Kartons zu Paletten. Wird das RFID-Tag auf dem Karton bzw. der Palette dann gelesen, z.B. beim Wareneingang, kann damit automatisch erfasst werden, was sich in dem Karton bzw. auf der Palette befindet. In diesem Zusammenhang spricht man manchmal von „Soft-Tracking“. Es ist in solchen Fällen nicht einmal zwingend notwendig, auf der höheren Ebene (z.B. der Palette) RFID-Tags einzusetzen. Es reicht im Prinzip aus, wenn z.B. ein Karton auf einer Palette erkannt wird, da damit auf die Palette und somit den Rest der Lieferung geschlossen werden kann. Der beschriebene Aggregationsmechanismus reduziert das Problem von Fehllesungen, hat jedoch auch gewisse Nachteile. So entfällt z.B. die Möglichkeit zu überprüfen, ob sich auf einer Palette tatsächlich die angegebenen Produkte befinden. Fehllieferungen, bei denen die Information zur Lieferung nicht mit der tatsächlichen Lieferung übereinstimmt, oder Schwund können so nicht mehr aufgedeckt werden.

2.4 Nutzenpotenziale von RFID-Tags auf Kartons und Paletten

Da es sich bei den relevanten Transporteinheiten bis zum Übergang auf die Verkaufsfläche in der Regel um Kartons oder sogar Paletten handelt, sind viele der Potenziale von RFID bereits bei der Nutzung von RFID auf diesen Ebenen realisierbar. Wir betrachten hier nur einen Ausschnitt der Lieferkette, nämlich die Stufe des Verteilzentrums und des Supermarkts. Die Aussagen für Verteilzentren gelten in ähnlicher Form auch für andere vorgelagerte Distributionsstufen bis hin zum Lager beim Hersteller. Bei den vorgelagerten Stufen ist anzunehmen, dass Paletten als die relevante Transporteinheit anzusehen sind.

Wareneingang und -ausgang

Automatische Produktidentifikation mittels RFID-Tags ermöglicht eine *effizientere Erfassung von Wareneingängen und -ausgängen*. Dazu werden im Verteilzentrum an den Wareneingängen und -ausgängen RFID-Leser installiert. Diese erfassen die Tags, die auf den eingehenden bzw. ausgehenden Kartons oder Paletten

angebracht sind. Mit den auf den Tags gespeicherten Nummern kann die Lieferung eindeutig identifiziert werden; eine manuelle Erfassung entfällt. Besteht eine Lieferung aus mehreren mit RFID-Tags ausgestatteten Einheiten (z.B. Kartons), kann die *Vollständigkeit und Korrektheit der Lieferung überprüft* werden – vorausgesetzt, auf den Kartons befinden sich RFID-Tags und die Tags sind fehlerfrei lesbar. In diesem Fall kann zudem eine manuelle Erfassung der Entnahmen bei der Kommissionierung entfallen. Die Entnahme kann automatisch, z.B. bei der Zusammenführung der Lieferung, verbucht werden.

Im Supermarkt geht es um die Erfassung und Überprüfung von Anlieferungen sowie darum, festzustellen, wann Ware vom Lager auf die Verkaufsfläche übergeht. Mit RFID besteht die Möglichkeit zur Trennung des Bestands in einen Teil, der sich auf der Verkaufsfläche befindet, und einen Teil, der sich im Lager befindet. Diese Information war bislang vielfach nicht vorhanden, was eine Ursache für mangelhafte Produktverfügbarkeit im Regal ist.

Lagerbestand und Produktverfügbarkeit

Automatische Produktidentifikation kann zudem dabei helfen, den *Lagerbestand zu reduzieren* und gleichzeitig die *Produktverfügbarkeit zu erhöhen*. Einzelne Fallstudien im Handel haben gezeigt, dass der tatsächliche Lagerbestand häufig nicht mit dem Bestand im Informationssystem übereinstimmt [RDT01]. Da die Informationen ungenau sind, werden höhere Lagerbestände gehalten, um die Verfügbarkeit sicherzustellen. Dies gelingt aber nur eingeschränkt. In einer Untersuchung konnte gezeigt werden, dass tendenziell die Supermärkte mit einem niedrigen Lagerbestand eine höhere Produktverfügbarkeit aufwiesen [BGC02]. Die beiden Ziele stehen also nicht notwendig im Konflikt zueinander. Genauere Informationen zum tatsächlichen Lagerbestand sind eine Möglichkeit, Verbesserungen bei der Verfügbarkeit bei gleichzeitiger Verringerung der Kapitalbindung zu erreichen.

Für das Entstehen von Lagerungenauigkeiten gibt es eine Reihe von Gründen: Lieferungen enthalten die falschen Produkte oder sind unvollständig, der Lagerbestand dezimiert sich durch Diebstahl oder andere Arten von Schwund, Eingänge und Ausgänge von Waren werden falsch erfasst, oder Waren werden am falschen Ort gelagert und sind nicht auffindbar. Um diese Ungenauigkeiten zu reduzieren, gibt es verschiedene Lösungsalternativen: Zum einen kann die Genauigkeit durch die automatische Erfassung von Wareneingängen und -ausgängen erhöht werden. Dies entspricht der oben beschriebenen Anwendung zur Überprüfung der Vollständigkeit und Korrektheit einer Lieferung. Ungenauigkeiten, die durch Diebstahl im Lager oder Lagerung am falschen Ort entstehen, lassen sich allerdings so nicht aufdecken. Zum anderen können RFID-Leser an Lagerorten installiert werden, die ständig erfassen, welche Kartons oder Paletten sich tatsächlich dort befinden. Dies erfordert allerdings eine große Anzahl an Lesern und setzt bei einer Erfassung auf Kartonebene voraus, dass eine hinreichend hohe Leserate erzielt werden kann. Mit einer solchen Lösung ist praktisch jederzeit eine Inventur möglich, bei der Lagerungenauigkeiten – zumindest bis auf Ebene einzelner Kartons – sofort entdeckt werden. Alternativ zu stationären Lesern können Unternehmen mobile Leser, z.B. an Gabelstaplern und sonstigen Geräten, oder aber auch Hand-

leser einsetzen. Mit Hilfe von zusätzlichen RFID-Tags, die an Lagerorten angebracht sind, ist eine näherungsweise Lokalisierung der Ware möglich. Bei dieser Variante kann jedoch immer nur der Bestand an einzelnen Lagerplätzen aktualisiert werden, z.B. denjenigen, aus denen Mitarbeiter gerade Ware entnehmen.

In der Verkaufsstelle kann RFID auf Kartonebene dabei helfen, eine Trennung zwischen Bestand auf der Verkaufsfläche und Bestand im Lager zu realisieren. Obwohl Einzelhändler bestrebt sind, die Bestände im Lager der Verkaufsstelle möglichst klein zu halten, gibt es immer noch bestimmte Produkte, die dort zwischengelagert werden wie Aktionsware oder Schnelldreher, für die nicht genug Regalfläche vorhanden ist (z.B. Toilettenpapier, Getränke). In Verbindung mit Point-of-Sale-(POS-)Daten kann das Bestandsführungssystem eine rechtzeitige Nachbefüllung des Regals aus dem Lager anstoßen, was bisher nicht möglich war.

Diebstahl

Die *Vermeidung von Diebstahl* lässt sich mit Hilfe von RFID-Tags auf zwei grundsätzliche Arten realisieren. Diese seien hier mit direkter und indirekter Vermeidung bezeichnet. Bei der direkten Vermeidung wird ein Alarm o.Ä. ausgelöst, wenn der Verdacht besteht, dass Produkte gestohlen werden. Bei der indirekten Vermeidung zielt die Verwendung darauf, die Quellen für Diebstahl zu identifizieren (z.B. durch die Feststellung von Schwund an bestimmten Orten), um entsprechende Gegenmaßnahmen vornehmen zu können. Die Wirksamkeit von RFID zum Diebstahlschutz auf der Ebene von Kartons und Paletten ist eingeschränkt. Der Diebstahl von einzelnen Produkten lässt sich so nicht erfassen. Es ist zu vermuten, dass RFID in diesen Fällen im Wesentlichen zur indirekten Vermeidung von Diebstahl eingesetzt wird.

Unverkäufliche Produkte

Automatische Identifikationstechnologien können auch helfen, den *Anteil unverkäuflicher Produkte zu reduzieren*. Es gibt verschiedene Gründe, warum Waren unverkäuflich werden. Dazu gehören Beschädigungen der Verpackung oder des Inhalts, Ablauf des Haltbarkeitsdatums, Auslaufmodelle, spezielle nur kurzzeitig verfügbare Angebote oder saisonale Produkte. RFID-Technologie kann dabei helfen, die Produkte zu identifizieren, bei denen die Gefahr besteht, dass sie nicht mehr verkauft werden können. Hierzu sind in der Regel zusätzliche Informationen zum Produkt notwendig wie der Termin, bis zu dem Produkte verkauft werden können (z.B. Mindesthaltbarkeitsdatum, Gültigkeitsdauer eines Angebots). Sind Bestand und weitere Produktinformationen wie Haltbarkeitsdatum etc. bekannt, können auf Basis dieser Informationen geeignete Aktivitäten angestoßen werden, um den Verderb oder Wertverlust zu verhindern. So ist es denkbar, dass bei einem Überbestand Rabatte eingeräumt werden. Um Beschädigungen der Verpackung oder des Inhalts aufzudecken oder sogar zu verhindern, können Sensoren eingesetzt werden, die z.B. die Lagertemperatur aufzeichnen und evtl. alarmieren, wenn die Temperatur einen bestimmten Grenzwert überschreitet. Befinden sich nur gleichartige Produkte in einem Karton oder auf einer Palette, reicht eine Identifi-

kation auf dieser Ebene aus, um die Potenziale realisieren zu können, solange die Verpackungseinheit intakt ist.

Rückverfolgbarkeit

Automatische Identifikationstechnologien können ferner auch bei der *Rückverfolgung* von Produkten helfen. Zum Teil gibt es gesetzliche Auflagen, die Hersteller und Händler zur Rückverfolgung verpflichten. So hat die EU eine Verordnung erlassen, die Lebensmittelunternehmen dazu verpflichtet, bis 2005 entsprechende Systeme und Verfahren zu installieren. Die Unternehmen müssen festhalten, von welchen Unternehmen sie Erzeugnisse bezogen und an welche sie ihre Ware geliefert haben [EuU02b]. Mit RFID-Tags auf Kartons oder Paletten lässt sich erfassen, welche Produkte oder Produktchargen in die Produktion eingeflossen sind bzw. an welche Kunden sie ausgeliefert wurden. Eine Verfolgung einzelner Produkte ist bis zu dem Punkt möglich, an dem der Karton oder die Palette aufgebrochen wird. Dazu muss allerdings gewährleistet sein, dass die Identität der einzelnen Produkte bei der Aggregation zu Kartons bzw. Kartons zu Paletten erfasst wird. Dies setzt nicht notwendigerweise voraus, dass das Produkt selbst mit einem RFID-Tag ausgerüstet ist.

2.5 Nutzenpotenziale von RFID-Tags auf Produktebene

Auf Produktebene ergeben sich weitere Vorteile durch den Einsatz von RFID-Tags. Im Folgenden soll dargestellt werden, was dies für die Nutzenpotenziale bedeutet. Hierbei betrachten wir die Nutzenpotenziale einzeln und diskutieren die Veränderungen gegenüber einem Einsatz von RFID auf Kartons und Paletten. Für eine Realisierung der Nutzenpotenziale nach Anbruch der Verpackungseinheit, wie es häufig geschieht, wenn ein Produkt auf die Verkaufsfläche kommt, ist in der Regel der Einsatz auf Produktebene notwendig. Dabei ist natürlich zu beachten, dass die Gesamtkosten für RFID-Tags stark ansteigen, wenn statt Paletten und Kartons einzelne Produkte damit ausgestattet werden.

Wie bereits diskutiert, reichen RFID-Tags auf Produkten alleine jedoch in einer Reihe von Fällen nicht aus, um die Nutzenpotenziale von RFID in Distributionszentren und im Lager von Supermärkten zu realisieren. Dies liegt vor allem an der zu geringen Leserate auf Produktebene, wenn eine Vielzahl von Produkten auf einmal erfasst werden soll. Hier ist die Aggregation von einzelnen Produkten zu Kartons und von Kartons zu Paletten eine geeignete Lösung. Auf bestimmte Beschränkungen bei der Realisierung der Nutzenpotenziale bei der Aggregation (z.B. Erkennung von Fehllieferungen und Diebstahl) wurde bereits hingewiesen. In bestimmten Anwendungen ist dies aufgrund technischer Beschränkungen aber kaum zu verhindern.

Wareneingang und -ausgang

Für eine *effizientere Erfassung von Wareneingängen- und -ausgängen* ist eine Auszeichnung auf Produktebene in der Regel nicht erforderlich. Befindet sich z.B.

ein RFID-Tag an der Palette, reicht es aus, dieses zu lesen, um die entsprechende Buchung im Warenwirtschaftssystem vorzunehmen. Eine *Überprüfung von Vollständigkeit und Korrektheit von Lieferungen auf Produktebene* ist so allerdings nicht möglich. Eine solche Überprüfung setzt voraus, dass ein RFID-Leser sämtliche mit RFID-Tags ausgestatteten Produkte erfassen kann, die sich z.B. auf einer Palette befinden. Für manche Produkte ist dies nur schwer bis gar nicht realisierbar, für andere, z.B. Kleidungsstücke, ist dies realistischer. Auf Produktebene sind die Vorteile von RFID deshalb in vielen Fällen vermutlich gering. Dies gilt insbesondere für Verteilzentren, in denen häufig Kartons mit gleichartigen Produkten oder sogar ganze Paletten die relevanten Transporteinheiten darstellen. Gegenüber dem Einsatz auf Kartons könnte z.B. festgestellt werden, ob einzelne Produkte in einem Karton fehlen oder dort nicht hineingehören. Im Einzelhandelsgeschäft können RFID-Tags auf Produktebene von Vorteil sein, wenn z.B. angebrochene Kartons aus dem Lager auf die Verkaufsfläche oder von der Verkaufsfläche ins Lager transportiert werden, z.B. weil nicht die komplette Anlieferung ins Regal passt.

Lagerbestand und Produktverfügbarkeit

Der Einsatz von RFID-Tags auf Produktebene kann auch darauf abzielen, *Lagerbestände zu reduzieren* und die *Produktverfügbarkeit zu erhöhen*. Die Überlegungen sind analog zum Einsatz von RFID auf Kartons und Paletten. Ebenso wie bei der Überprüfung von Lieferungen sind die zusätzlichen Nutzenpotenziale in den dem Supermarkt vorgelagerten Distributionsstufen allerdings in vielen Fällen vermutlich eher gering.

Etwas anders sieht es in der Verkaufsstelle aus: Eine Studie hat gezeigt, dass in knapp drei Viertel der Fälle Probleme beim Einzelhändler die Ursache waren, dass Produkte nicht im Regal verfügbar waren [BGC02]. RFID-Technologie kann zur Ermittlung der genauen Bestände auf der Verkaufsfläche eingesetzt werden, was einige der Ursachen für mangelhafte Produktverfügbarkeit zumindest teilweise beseitigt. Um die Regalbestände zu erfassen, ist es notwendig, die betreffenden Regale mit RFID-Lesern und Antennen auszustatten oder mobile Leser einzusetzen. Durch die genaue Abbildung des Bestandes im Laden lassen sich Überbestände in Regalen aufdecken, Nachbestellungen erfolgen auf Basis des konkreten Bestands, und Fehlplatzierungen von Produkten im Laden können aufgedeckt werden.

Diebstahl

Mit RFID-Tags auf Produkten können *Diebstähle* vermieden bzw. aufgedeckt werden. Dies gilt sowohl im Lager als auch im Laden, z.B. wenn ein RFID-Tag an der Supermarkt-Kasse gelesen wird, der zu einem nicht bezahlten Produkt gehört (direkte Diebstahlvermeidung). Die Anwendung von RFID-Tags ist in diesem Fall sehr ähnlich zu herkömmlichen Diebstahlschutzetiketten. Wird der Warenbestand im Regal erfasst, lässt sich zudem im Abgleich mit dem Point-of-Sale-System Schwund feststellen. Durch Analyse solcher Daten lassen sich unter Umständen Prozessverbesserungen realisieren, die mittelfristig zu geringeren

Diebstahlquoten führen. Darüber hinaus kann bei einer eindeutigen Produktidentifizierbarkeit festgestellt werden, ob ein bestimmtes Produkt möglicherweise gestohlen wurde. Dies erschwert den Weiterverkauf oder Umtausch gestohlener Waren (indirekte Diebstahlvermeidung).

Unverkäufliche Ware

Die Aussagen zur *Vermeidung unverkäuflicher Ware* sind analog zu denen beim Einsatz von RFID-Tags auf Kartons und Paletten. Der Vorteil von RFID-Tags auf Produktebene ist wiederum, dass eine Überprüfung auch noch nach Aufbrechen der Transporteinheit möglich ist, wie z.B. bei der Überprüfung der Haltbarkeitsdaten von Produkten im Kühlregal. Für den Einsatz auf der Verkaufsfläche im Supermarkt ist dies relevant; das zusätzliche Nutzenpotenzial beim Einsatz im Lager wie auch im Distributionszentrum wird in vielen Fällen allerdings vermutlich gering sein.

Kassiervorgang

Automatische Produktidentifikation kann helfen, den Bezahlvorgang an der Kasse effizienter zu gestalten. *Selbst-Check-out-Systeme* lassen sich sowohl mittels Barcode als auch RFID-Tags realisieren. Der Vorteil von Selbst-Check-out-Systemen ist zum einen, dass der Kundenservice verbessert werden kann, z.B. weil der Kunde nicht mehr an der Kasse anstehen muss, zum anderen kann der Einzelhändler Personalkosten an der Kasse einsparen. Barcode-basierte Systeme sind bereits seit mehreren Jahren erhältlich und werden in kleinerem Rahmen eingesetzt, sind jedoch noch nicht flächendeckend verfügbar. Bei Barcode-basierten Systemen erfasst der Kunde die gekauften Produkte selbst, indem er den Barcode einliest, z.B. bevor er ein Produkt in den Einkaufswagen legt. Mit Hilfe von Stichproben soll Diebstahl verhindert werden. Häufig sind diese Systeme nur für Kunden nutzbar, die sich z.B. über Kundenkarten identifiziert haben.

Bei RFID-basierten Systemen kann die Produkterfassung automatisch geschehen, d.h., die Erfassung erfolgt ohne Intervention des Käufers direkt, wenn dieser das Produkt in den Einkaufswagen legt oder den Einkaufswagen durch die Kasse schiebt. Erstere Lösung hat den Vorteil, dass weniger Probleme mit der Leserate auftreten sollten, da keine Pulkerfassung notwendig ist. Zudem kann der Kunde z.B. über ein akustisches oder optisches Signal am Einkaufswagen darüber informiert werden, ob der Einkaufswagen das Produkt auch tatsächlich erkannt hat.

Selbst-Check-out-Systeme auf Basis von RFID werden vermutlich erst zum Einsatz kommen, wenn der überwiegende Teil des Produktsortiments mit RFID-Tags ausgestattet ist. Problematisch ist unter Umständen die Verhinderung von Diebstahl, da der Kunde auf mögliche Lesefehler verweisen kann, wenn nicht erfasste Produkte bei ihm entdeckt werden bzw. Lesefehler sich relativ leicht provozieren lassen. Durch den zusätzlichen Einsatz von Waagen, wie dies bereits bei Barcode-basierten Systemen der Fall ist, lässt sich dieses Problem allerdings reduzieren.

Rückverfolgbarkeit

RFID-Tags können ferner dabei helfen, die *Rückverfolgbarkeit von Produkten zu verbessern*. Mit RFID-Tags auf Produkten kann eine Rückverfolgung über die Supply Chain hinaus bis zum Endkunden erfolgen. RFID-Tags auf Produkten können z.B. eingesetzt werden, um für jeden Endkunden, der über eine Kundenkarte verfügt, eindeutig festzuhalten, welches Produkt er gekauft hat bzw. zu welcher Produktcharge dieses gehört. Damit könnten Kunden z.B. bei Rückrufaktionen direkt angesprochen werden. Dies kann als *vorwärts gerichtete Rückverfolgung* bezeichnet werden. Derzeit beginnt man, solche Systeme für den Einzelhandel zu diskutieren. Eine *rückwärts gerichtete Verfolgbarkeit* auf Produktebene kann ebenfalls mit RFID realisiert werden. Jedes Produkt, das an einen Endkunden verkauft wurde, ließe sich so über die verschiedenen Stufen der Lieferkette verfolgen, z.B. um die Ursache von Qualitätsproblemen zu identifizieren. Bei dieser rückwärts gerichteten Produktverfolgung sind die Vorteile von RFID gegenüber nichtautomatisch auslesbaren eindeutigen Produkt- oder Chargenbezeichnungen (z.B. Serien- oder Chargennummern) nicht notwendigerweise gegeben, solange nicht große Produktstückzahlen individuell überprüft werden müssen. (Sofern die Produkte zu einer größeren Transporteinheit gehören, reicht es aufgrund der Möglichkeit zur Aggregation aus, die in der Hierarchie höhere Aggregationsstufe zu identifizieren.) Es ist zu beachten, dass eine rückwärts gerichtete Verfolgbarkeit auf Basis des RFID-Tags nicht mehr möglich ist, wenn das Tag beim Verkauf an den Endkunden permanent deaktiviert wird, da das Produkt dann nicht mehr eindeutig identifiziert werden kann.

2.6 Anforderungen an die Leserinfrastruktur

Um die diskutierten Nutzenpotenziale realisieren zu können, ist es notwendig, eine Infrastruktur von RFID-Lesern aufzubauen. Die folgenden Ausführungen beschränken sich im Wesentlichen auf die Anzahl der benötigten Leser. Andere relevante Aspekte wie Middleware oder notwendige Anpassungen der Unternehmenssoftware beim Einsatz von RFID werden in den abschließenden Abschnitten dieses Beitrags kurz angesprochen.

Die Anzahl und Platzierung der Leser hängt unter anderem vom angestrebten Nutzenpotenzial, dem Anwendungsfall und der Ebene der Produktverfolgung ab. Für den betrachteten Einsatz von RFID in der Lieferkette im Einzelhandel erscheint es sinnvoll, zwischen ereignisbasierten und statusbasierten Anwendungsfällen zu unterscheiden. Als *ereignisbasiert* sei ein Anwendungsfall bezeichnet, bei dem es darum geht, das RFID-Tag einmalig zu erfassen. Der Lesevorgang kann hier beispielsweise durch ein physisches Ereignis eingeleitet werden, z.B. wenn sich ein RFID-Tag durch das Feld eines Lesers bewegt. Ereignisbasierte Anwendungsfälle sind z.B. die Wareneingangskontrolle oder Produktrückverfolgung in der oben beschriebenen Form. Bei *statusbasierten Anwendungsfällen* geht es darum, dass Tags in der Regel mehrmals über einen längeren Zeitraum gelesen werden, z.B. um den Bestand von Produkten in einem Regal zu überprüfen.

Die Zuordnung von Nutzenpotenzial zu Anwendungsfällen ist nicht eindeutig. Für einige Nutzenpotenziale gibt es sowohl ereignis- als auch statusbasierte An-

wendungsfälle, z.B. bei der Erfassung und Vermeidung von Schwund; Erfassung von Schwund beim Wareneingang ist ein ereignisbasierter Anwendungsfall, während die Erfassung von Schwund im Regal sowohl ein status- als auch ein ereignisbasierter Anwendungsfall sein kann.

Zum Teil lassen sich ursprünglich statusbasierte in ereignisbasierte Anwendungsfälle umwandeln (und umgekehrt). So können statt stationärer Leser zur Überwachung der Produktverfügbarkeit in Regalen auch mobile Leser eingesetzt werden. Die hierdurch erreichbare Genauigkeit ist jedoch limitiert und hängt stark von der Häufigkeit der Überprüfung ab. Darüber hinaus spielt die Leserate der mobilen Leser eine Rolle. Bei mobilen Lesern kann diese durch einen größeren Abstand oder eine ungünstige Positionierung beeinträchtigt werden. Zudem ist die Anzahl bzw. Dauer der Lesevorgänge geringer als bei stationären Lesern. Je häufiger bzw. je länger gelesen wird, desto größer die Wahrscheinlichkeit, dass ein RFID-Tag erkannt wird.

Was hat die Unterscheidung in ereignisbasierte und statusbasierte Anwendungsfälle für Implikationen bezüglich der Anwendungen von RFID in der Lieferkette? Unsere bisherigen Erfahrungen in Projekten lassen vermuten, dass für ereignisbasierte Anwendungen in der Regel eine geringere Anzahl von Lesern notwendig ist. Dies liegt darin begründet, dass die Anzahl von Lokationen, an denen ereignisbasierte Erfassungen von RFID-Tags durchgeführt werden, geringer ist als die Anzahl der Lokationen für statusbasierte Erfassungen. Für eine Wareneingangskontrolle reicht es z.B. aus, wenn an den jeweiligen Toren, durch die die Lieferungen auf dem Weg ins Lager geschoben werden, RFID-Leser angebracht werden. Für eine direkte Diebstahlvermeidung im Laden sind RFID-Leser an Kassen sowie an weiteren Eingängen und Ausgängen notwendig. Für statusbasierte Anwendungsfälle ist es hingegen notwendig, RFID-Leser an allen Orten anzubringen, an denen Objekte erfasst werden sollen. Soll z.B. in einem Supermarkt ständig überprüft werden, ob die einzelnen Produkte tatsächlich am richtigen Ort in den Regalen vorhanden sind, sind sämtliche infrage kommenden Regale mit RFID-Lesern und Antennen auszustatten. (Alternativ können, wie oben beschrieben, auch mobile Leser – unter Berücksichtigung der beschriebenen Konsequenzen – eingesetzt werden.)

Die Anforderungen an die Leserinfrastruktur hängen auch von der Ebene ab, auf der RFID-Tags eingesetzt werden. Soll z.B. die Korrektheit einer Lieferung auf der Ebene von Kartons überprüft werden, ist dies in der Regel einfacher zu realisieren, als wenn die Korrektheit auf Produktebene überprüft werden soll.

2.7 Übersicht der Nutzenpotenziale

Aufgrund der Vielzahl von Produkten, die im Einzelhandel zu finden sind, und diversen alternativen Gestaltungsmöglichkeiten für Anwendungen ist es schwierig, allgemein gültige Aussagen zu machen, welche Nutzenpotenziale abhängig von der Ebene, auf der die Produktverfolgung stattfindet, und der Leserinfrastruktur realisiert werden können. Tabelle 2 gibt auf Basis der obigen Beschreibung eine Übersicht über die Nutzenpotenziale der RFID-Technologie beispielhaft für Distributionszentren. Aufgezeigt werden unter anderem die Vor- und Nachteile

eines Einsatzes von RFID auf der Produktebene gegenüber dem Einsatz auf Karton- und Palettenebene.

Es lässt sich festhalten, dass ein Einsatz auf Produktebene in der Regel nur dann sinnvoll ist, wenn auch tatsächlich eine Handhabung auf Einzelproduktebene stattfindet. Dies ist in Verteilzentren eher selten der Fall. Der Einsatz auf Produktebene kann dann sinnvoll sein, wenn gemischte Kartons an- oder ausgeliefert werden und wenn Schwund auf der Ebene individueller Produkte auftritt.

Auf eine ähnlich ausführliche Aufstellung der Nutzenpotenziale im Supermarkt haben wir aus Platzgründen verzichtet. Diese kann aber aus der obigen Aufstellung und den Ausführungen abgeleitet werden. Es gibt allerdings einen wesentlichen Unterschied: Erst durch den Einsatz von RFID auf Produktebene wird man in vielen Fällen einen Mehrwert erzielen können, der den Einsatz von RFID auch über das Lager hinaus auf der Verkaufsfläche rechtfertigt. Anwendungen wie Selbst-Check-out-Systeme basierend auf RFID können so überhaupt erst realisiert werden. Zu beachten ist hier, dass dadurch die Zahl der notwendigen RFID-Leser unter Umständen um ein Vielfaches steigt (z.B. wenn Regale mit RFID-Lesern ausgestattet werden). Im Gegensatz dazu ist anzunehmen, dass die Anzahl an Lesern im Distributionszentrum im Vergleich zu einer Anwendung auf Karton- oder Palettenebene in vielen Fällen weitgehend konstant bleibt – vorausgesetzt, eine hinreichend hohe Leserate auf Produktebene ist gewährleistet.

Von einer Abschätzung bezüglich der Höhe der Nutzenpotenziale haben wir abgesehen. Dies dürfte sehr stark von den Umständen z.B. der Produktkategorie abhängen. Überlegungen zu den Potenzialen von RFID bei der Verringerung von Schwund und unverkäuflichen Produkten für verschiedene Produktkategorien finden sich in diversen Veröffentlichungen (siehe z.B. [IBM02a].

2.8 Weitere Anwendungsmöglichkeiten

Die Nutzenpotenziale automatischer Produktidentifikation sind mit den oben genannten Anwendungen in der Supply Chain noch nicht ausgeschöpft. Weitere Anwendungsmöglichkeiten liegen z.B. in der Verbesserung der Kundeninteraktion oder des Customer Relationship Management (z.B. durch Bereitstellung von Produktinformationen für Kunden oder personalisierten Angeboten [Rfi02a]). Auch im Produktlebenszyklus-Management ergeben sich potenzielle Anwendungsmöglichkeiten, z.B. bei Elektro- und Elektronikgeräten, für die in der EU Rücknahmeverpflichtungen und bestimme Wiederverwendungs- und Recyclingquoten eingeführt werden [EuU02a]. Auch im eigentlichen Produktionsprozess, z.B. bei der Aufzucht von Rindern[42], setzen Unternehmen bereits seit Jahren RFID-Technologie ein. Zudem lassen sich Produkte schwerer fälschen, wenn Unternehmen sie durch die gesamte Wertschöpfungskette verfolgen können oder die RFID-Tags verschlüsselte Informationen enthalten. Auch Anwendungen, die RFID mit Sensoren kombinieren, z.B. zur Überprüfung der Haltbarkeit unabhängig vom aufgedruckten Haltbarkeitsdatum, sind nicht auf die Lieferkette beschränkt.

[42] www.ti.com/tiris/docs/solutions/cowid.shtml

Tabelle 2. Nutzenpotenziale von RFID am Beispiel von Distributionszentren

	Objektverfolgung auf Karton- und Palettenebene				Objektverfolgung auf Produktebene		
Nutzenpotenzial	Anforderung an Leserinfrastruktur	Potenzielle technische Limitationen	Anwendungsfall und mögliche Aggregationsstufe	Vor- und Nachteile einer Objektverfolgung auf Produktebene	Anforderung an Leserinfrastrukur	Potenzielle technische Limitationen	Anwendungsfall und mögliche Aggregationsstufe
Erhöhung der Effizienz bei Wareneingang, Warenausgang und bei der Kommissionierung	Moderat (hoch bei stationären Lesern an Lagerorten): stationäre Leser an Wareneingang- und -ausgang, stationäre oder mobile Leser für Kommissionierung	Leserate bei Aggregation von Produkten zu Kartons und Kartons zu Paletten	Ereignisbasierter Anwendungsfall; Aggregation von Kartons zu Paletten	– Kosten für RFID-Tags	Moderat (hoch bei stationären Lesern an Lagerorten): wie vorne	Leserate bei Aggregation von Produkten zu Kartons und Kartons zu Paletten	Ereignisbasierter Anwendungsfall; Aggregation von Produkten zu Kartons und Kartons zu Paletten
Fehlervermeidung bei Wareneingang, Warenausgang und bei der Kommissionierung	Moderat (hoch bei stationären Lesern an Lagerorten): stationäre Leser an Wareneingang- und -ausgang, stationäre oder mobile Leser für Kommissionierung	Leserate beim Lesen von Kartons auf Paletten	Ereignisbasierter Anwendungsfall	+ Kontrolle bis aufs einzelne Produkt – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Moderat (hoch bei stationären Lesern an Lagerorten): siehe vorne, allerdings höhere Anforderungen wg. Identifikation auf Produktebene	Leserate beim Lesen von Produkten auf Paletten	Ereignisbasierter Anwendungsfall

Tabelle 2. (Fortsetzung)

Erhöhung der Produktverfügbarkeit und Verringerung des Lagerbestands	Moderat (hoch bei stationären Lesern an Lagerorten): stationäre Leser an Wareneinund -ausgang, stationäre oder mobile Leser für Bestandserfassung	Leserate beim Lesen von Kartons auf Paletten, wenn Paletten aufgebrochen werden	Ereignisbasierter Anwendungsfall; bei stationären Lesern an Lagerorten auch statusbasierter Anwendungsfall; Aggregation von Kartons zu Paletten solange Paletten nicht aufgebrochen werden	+ Genauigkeit bis aufs einzelne Produkt, wenn Kartons aufgebrochen werden – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Moderat (hoch bei stationären Lesern an Lagerorten): siehe vorne, allerdings höhere Anforderungen wg. Identifikation auf Produktebene	Leserate beim Lesen von Produkten auf Paletten, wenn Kartons aufgebrochen werden	Ereignisbasierter Anwendungsfall; bei stationären Lesern an Lagerorten auch statusbasierter Anwendungsfall; Aggregation von Produkten zu Kartons, solange Kartons nicht aufgebrochen werden
Direkte Vermeidung von Diebstahl	Gering: stationäre Leser an Ein- und Ausgängen zur Kontrolle	Vorsätzliche Behinderung des Lesens	Ereignisbasierter Anwendungsfall	+ Kontrolle bis aufs einzelne Produkt – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Gering: wie vorne	Vorsätzliche Behinderung des Lesens	Ereignisbasierter Anwendungsfall
Indirekte Vermeidung von Diebstahl	Moderat (hoch bei stationären Lesern an Lagerorten): stationäre oder mobile Leser für Bestandserfassung	Leserate beim Lesen von Kartons auf Paletten	Statusbasierter Anwendungsfall; bei mobilen Lesern an Lagerorten ereignisbasierter Anwendungsfall	+ Kontrolle bis aufs einzelne Produkt – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Moderat (hoch bei stationären Lesern an Lagerorten): siehe vorne, allerdings höhere Anforderungen wg. Identifikation auf Produktebene	Leserate beim Lesen von Produkten auf Paletten	Statusbasierter Anwendungsfall; bei mobilen Lesern an Lagerorten ereignisbasierter Anwendungsfall

Tabelle 2. (Fortsetzung)

Verringerung des Anteils unverkäuflicher Waren	Moderat (hoch bei stationären Lesern an Lagerorten): stationäre oder mobile Leser für Bestandserfassung	Leserate beim Lesen von Kartons auf Paletten, wenn Paletten aufgebrochen werden	Statusbasierter Anwendungsfall; bei mobilen Lesern an Lagerorten ereignisbasierter Anwendungsfall; Aggregation von Kartons zu Paletten, solange Paletten nicht aufgebrochen werden	+ Genauigkeit bis aufs einzelne Produkt bei ungleichartigen Produkten oder wenn Kartons aufgebrochen werden – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Moderat (hoch bei stationären Lesern an Lagerorten): siehe vorne, allerdings höhere Anforderungen wg. Identifikation auf Produktebene	Leserate beim Lesen von Produkten auf Paletten, wenn Kartons aufgebrochen werden	Statusbasierter Anwendungsfall; bei mobilen Lesern an Lagerorten statusbasierter Anwendungsfall; Aggregation von Produkten zu Kartons, solange Kartons nicht aufgebrochen werden
Produktrückverfolgbarkeit	Gering: stationäre Leser an Wareneinund -ausgang	Leserate beim Lesen von Kartons auf Paletten, wenn Paletten aufgebrochen werden	Ereignisbasierter Anwendungsfall; Aggregation von Kartons zu Paletten, solange Paletten nicht aufgebrochen werden	+ Genauigkeit bis aufs einzelne Produkt bei ungleichartigen Produkten oder wenn Kartons aufgebrochen werden – tatsächlich erreichbare Leserate – Kosten für RFID-Tags	Gering: siehe vorne	Leserate beim Lesen von Produkten auf Paletten, wenn Kartons aufgebrochen werden	Ereignisbasierter Anwendungsfall; Aggregation von Produkten zu Kartons, solange Kartons nicht aufgebrochen werden

3 Status quo der Einführung

3.1 Anwendungsbeispiele

Es gibt bereits eine Vielzahl von Anwendungen von RFID in der Lieferkette. Diese aufzuzählen ist nicht Ziel dieses Artikels. Für eine Übersicht zu betriebswirtschaftlichen Anwendungen sei auf den Beitrag von Elgar Fleisch in diesem Band verwiesen.

Einsatz auf Transportbehältnissen

Auch im Einzelhandel werden RFID-Anwendungen seit Jahren diskutiert. Ende der 90er-Jahre hat Sainsbury einen Pilotversuch mit wieder verwendbaren Transportbehältnissen durchgeführt [Kär02]. Marks & Spencer hat begonnen, RFID-Tags auf wieder verwendbaren Transportbehältnissen für Kühlkost einzusetzen. Der Roll-out sieht vor, dass insgesamt 3,5 Millionen Behältnisse mit RFID-Tags ausgestattet werden [MahoJ].

Einsatz auf Karton- und Palettenebene

Mittlerweile hat eine Reihe von Einzelhändlern bekannt gegeben, dass sie RFID-Tags nicht nur auf wieder verwendbaren Transportbehältnissen, sondern auf Karton- und Palettenebene zur Warenerfassung einsetzen wollen. Abbildung 1 gibt eine Übersicht über einige wesentliche Unternehmensmeldungen und Termine bezüglich der Einführung von RFID auf Paletten-, Karton- und Produktebene im Einzelhandel. Wal-Mart kündigte an, ab Januar 2005 mit seinen Top-100-Lieferanten RFID auf Karton- und Palettenebene einzusetzen [Wal04]. Die Einführung beginnt in Texas und soll bis Ende 2006 für die USA abgeschlossen sein [Rfi03]. Im April 2003 eröffnete Metro den so genannten „Future Store“. In diesem wird auf Pilotbasis das gesamte Trockensortiment auf Karton- und Palettenebene mit RFID-Tags ausgestattet. Die RFID-Tags werden im Metro-eigenen Distributionszentrum angebracht. Auf einzelnen Produkten (z.B. Gillette Rasierklingen, Kraft Frischkäse) befinden sich zusätzlich RFID-Tags auf Produktebene, um den Bestand auch im Regal erfassen zu können. Bei Frischkäse wird zudem das Haltbarkeitsdatum überprüft [Wol03]. Im November 2004 hat Metro mit der Einführung von RFID auf Karton- und Palettenebene begonnen. In einem ersten Schritt statten 20 Lieferanten Paletten mit RFID-Tags aus [Met04]. Tesco fokussiert sich auf den Einsatz von RFID auf Kartonebene. Im Rahmen der Secure-Supply-Chain-Initiative werden seit November 2004 unternehmensintern Behälter mit RFID-Tags für den Transport hochwertiger Konsumgüter wie Kosmetika und Rasierklingen eingesetzt. Im zweiten Quartal 2005 startet der RFID-Roll-out auf Kartonebene mit Lieferanten [Tes04].

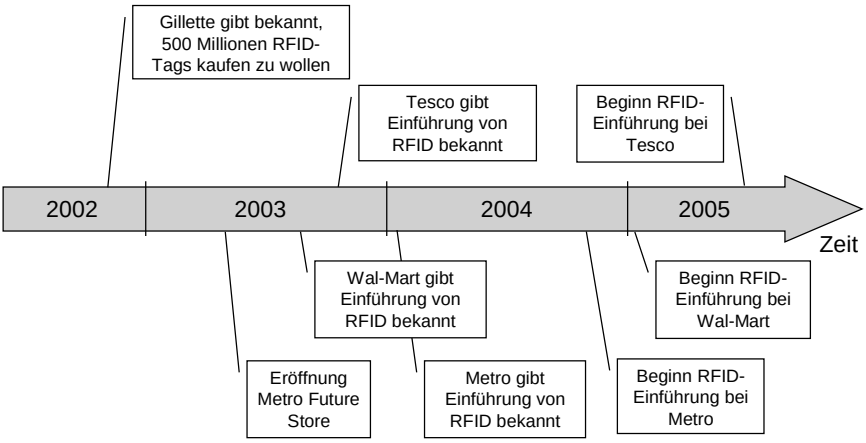


Abb. 1. Meilensteine bei der Einführung von RFID im Einzelhandel

Einsatz auf Produktebene

Auf Produktebene haben diverse Unternehmen aus der Textilindustrie bereits Pilotanwendungen durchgeführt (z.B. The Gap [TeI01], Kaufhof und Gerry Weber [Kau03]). Durch RFID-Tags in Kleidungsstücken ist es möglich, diese durch die Supply Chain zu verfolgen. Damit soll die Prozesseffizienz gesteigert und der Bestand im Laden sowohl auf der Verkaufsfläche als auch im Lager genauer erfasst werden. Der Beitrag von Tellkamp und Quiede in diesem Buch befasst sich eingehender mit dem Einsatz von RFID in der Textilindustrie und speziell den Erkenntnissen aus dem Pilotprojekt von Kaufhof und Gerry Weber.

Philips hatte im März 2003 angekündigt, dass Benetton RFID-Technologie einsetzen und jährlich mehrere Millionen Kleidungsstücke der Marke Sisley mit RFID-Tags ausstatten will. Benetton erhoffe sich dadurch eine bessere Überprüfung von Lieferungen und wolle manuelle Handhabungskosten in der Supply Chain reduzieren. In Zukunft sollten auch komplette Läden mit RFID-Lesern ausgestattet werden, um den genauen Bestand jederzeit erfassen und z.B. Kleidungsstücke, die Kunden an einen anderen als den ursprünglichen Ort zurückgehängt haben, wieder auffinden zu können. Philips rechnete mit einem Absatz von jährlich etwa 15 Millionen RFID-Tags [Phi03]. Allerdings kam knapp einen Monat nach der Ankündigung die Meldung, dass eine Entscheidung über den Einsatz von RFID-Tags bei Benetton noch nicht gefallen sei. In der Pressemitteilung von Benetton wird das Thema Datenschutz als ein kritischer Punkt genannt [Ben03].

Gillette strebt an, mit Hilfe von „Smart Shelves“ in Supermärkten die Verfügbarkeit ihrer Produkte zu erhöhen und Kundendiebstahl zu reduzieren. Dazu werden RFID-Tags auf Produktebene eingesetzt. Gleichzeitig sollen die RFID-Tags auch dazu dienen, Schwund in der Lieferkette zu vermeiden und die Prozesseffizienz zu verbessern. Gillette hat einen Vertrag über die Lieferung von 500 Millionen RFID-Tags unterzeichnet [Rfi02b]. Das Unternehmen arbeitet hier unter anderem mit Wal-Mart und Tesco zusammen. Wal-Mart hat allerdings im Juli 2003

angekündigt, keine Smart Shelves in Supermärkten einzusetzen und sich vorerst auf die Nutzenpotenziale von RFID bei der Verfolgung von Paletten und Kartons in der Supply Chain zu fokussieren. Die vorgesehenen Anwendungen sowohl bei Wal-Mart als auch bei Tesco sind auf Kritik bei einzelnen Verbraucherschützern gestoßen [Lin03, Gua03]. Für weitere Ausführungen zum Thema Datenschutz sei auf die Beiträge von Langheinrich und Thiesse verwiesen.

In den zuletzt genannten Beispielen werden RFID-Tags auf Produktebene eingesetzt. Hierfür können zwei Gründe angeführt werden:

- Bei einigen Anwendungsfällen (Diebstahlschutz bei Rasierklingen bzw. Bestandserfassung von Kleidungsstücken im Laden) ist es notwendig, dass sich die RFID-Tags am Produkt befinden.
- Die Kosten für ein RFID-Tag scheinen relativ gering im Vergleich zum erwarteten Nutzen. Dies hängt von verschiedenen Faktoren ab, unter anderem – aber nicht nur – vom Wert des Produkts. So sind Rasierklingen nicht nur verhältnismäßig teuer, sondern gehören auch zu den meistgestohlenen Produkten überhaupt [Sma03].

3.2 Hindernisse für die weitere Verbreitung

Bislang wird die RFID-Technolgie in der Supply Chain im Einzelhandel erst vereinzelt eingesetzt. Es gibt bereits einige Anwendungen, bei denen – insbesondere wieder verwendbare – Transportverpackungen mit RFID-Tags ausgestattet werden, um den Warenfluss durch die Supply Chain verfolgen zu können. Anwendungen, bei denen einzelne Produkte mittels RFID-Tags identifziert werden können, stecken noch in den Anfängen. Gründe hierfür sind unter anderem fehlende Standards, die Notwendigkeit der Koordination in der Lieferkette und fehlende Komplettlösungen. Auf der Kostenseite werden häufig die noch zu hohen Preise für RFID-Tags und -Leser genannt. Datenschutzbedenken spielen eine Rolle, falls die RFID-Tags auch nach dem Verkauf noch weiter genutzt werden könnten oder dazu dienen könnten, das Kundenverhalten im Laden zu überwachen. Diese Hindernisse sollen nachfolgend im Einzelnen behandelt werden. Auf technische Limitationen hinsichtlich der erreichbaren Leserate oder Interferenz mit anderen Systemen wollen wir hier nicht weiter eingehen.

Fehlende Standards

Bisher wird RFID-Technologie häufig in relativ isolierten Anwendungen bei einzelnen Unternehmen oder in Zusammenarbeit mit wenigen Partnern eingesetzt. Bei solchen Anwendungen spielen Standards eine geringere Rolle. Dies ändert sich allerdings, wenn RFID-Tags von einer Vielzahl verschiedener Produzenten von Konsumgütern eingesetzt werden und in der gesamten Lieferkette verwendet werden. Von 1999 bis Oktober 2003 arbeitete das Auto-ID Center in Zusammenarbeit mit Einzelhandelsunternehmen wie Metro und Wal-Mart, Herstellern von Konsumgütern wie Gillette, Nestlé und Procter & Gamble, RFID-Technologieanbietern wie Philips und Alien Technology sowie IT-Unternehmen wie SAP und Sun Microsystems an der Definition der notwendigen Standards [AsS03]. Seit

November 2003 hat EPCglobal, ein Joint Venture von EAN International und UCC, die Standardisierungsaktivitäten übernommen [EPC03]. Einen Überblick über die Technologiestandards von EPCglobal gibt der Beitrag von Flörkemeier.

Herausforderung Zusammenarbeit in der Lieferkette

Das RFID-Tag wird sinnvollerweise direkt im Herstellungsprozess in das Produkt integriert, die Nutzung ist jedoch in der gesamten Lieferkette möglich. Ohne weitere Regelung würde dies bedeuten, dass diese Kosten einseitig vom Hersteller getragen werden. Da er aber nur einen Teil der Nutzenpotenziale realisieren kann, wäre die Integration eines RFID-Tags für ihn alleine betrachtet unter Umständen nicht rentabel. Dies kann die Einführung von RFID-Tags verhindern, obwohl die realisierbaren Nutzenpotenziale für die gesamte Lieferkette größer als die erwarteten Kosten sind. Eine Zusammenarbeit der verschiedenen Partner in der Lieferkette erscheint in solchen Fällen notwendig. Darüber hinaus müssen sich die Partner auf gewisse Prozesse, Datenformate und Ähnliches einigen. Es ist anzunehmen, dass sich Anwendungen schneller durchsetzen werden, bei denen nur wenige Partner involviert sind.

Einzelhändlern mit einer starken Marktstellung wie Wal-Mart in den USA kommt eine wichtige Rolle zu. Das Verhalten dieser Unternehmen entscheidet vermutlich, ob sich die Technologie durchsetzen wird. Aufgrund ihrer Position können sie die Einführung von RFID auch bei ihren Lieferanten forcieren.

Nichtverfügbarkeit von Lösungspaketen

Bislang gibt es noch keine Komplettlösungen im Bereich RFID. Dies bezieht sich auf verschiedene Ebenen wie Leserinfrastruktur, Middleware und Anpassung von Unternehmenssoftware. Bisher ist der Aufbau einer RFID-Infrastruktur noch mit hohem individuellem Installations- und Testaufwand verbunden, z.B. hinsichtlich Anbringung von Lesern in Regalen oder beim Wareneingang. Beispielhaft verdeutlicht dies der Bericht von Albano und Engels [AlE02], der die ersten Ergebnisse eines Pilotversuchs zusammenfasst und die aufgetretenen Probleme sowie Lösungsansätze beschreibt.

Im Bereich Middleware besteht derzeit noch keine Übereinkunft, welche Anforderungen diese im Einzelnen erfüllen müssen, wie der Beitrag von Schoch in diesem Band verdeutlicht. Unter Middleware seien hier Anwendungen verstanden, die Schnittstellen für die Anbindung von Lesern und für die Integration in Unternehmenssoftware bereitstellen sowie bestimmte Aufgaben der Filterung, Aggregation, Verarbeitung und Verteilung der gelesenen Daten übernehmen. Mittlerweile bieten einige Unternehmen Middleware-Komponenten an, z.B. SAP [SAP04] und Infineon [Gil04].

In einigen Szenarien werden RFID-Tags im Wesentlichen als Ersatz für Barcodes verwendet, ohne dass zusätzliche Daten gesammelt werden (z.B. wenn beim Wareneingang statt eines Barcodes auf der Palette ein RFID-Tag gelesen wird). Dies wird in der Regel nur geringe Anpassungen der Unternehmenssoftware erfordern. Andere Anwendungen, z.B. solche, bei denen Daten zu individuellen Produkten erfasst und verwaltet werden, unterstützen gängige Unternehmenssoft-

warelösungen im Einzelhandel bislang erst unvollständig. In diesem Bereich besteht noch Entwicklungsbedarf. Wie diese Lösungen genau aussehen werden, ist derzeit noch nicht klar erkennbar.

Unklare Kosten-Nutzen-Relation

Die Kosten für RFID-Tags sind derzeit für die Integration in einzelne Produkte vielfach noch zu hoch. Auf Karton- oder Palettenebene spielen diese Kosten eine geringere Rolle. Dies gilt auch für wieder verwendbare Transportbehälter, bei denen die RFID-Tags mehrmals verwendet werden können. Ziel des Auto-ID Centers ist das RFID-Tag für 0,05 USD [Sar01]. Die Kosten für RFID-Tags hängen wesentlich vom Produktionsvolumen und den Funktionalitäten ab. Die oben erwähnten 0,05 USD gelten für „einfache“ passive RFID-Tags, die keine weitere Information außer einem eindeutigen Produktbezeichner tragen und in Stückzahlen von mehreren hundert Millionen pro Jahr hergestellt werden. „Aufwendigere“ Tags (z.B. mit mehr Informationen, größerer Reichweite, Sensoren u.Ä.) oder Tags, die in kleineren Stückzahlen produziert werden (z.B. aufgrund kundenspezifischer Anforderungen), werden preislich darüber liegen.

Aber auch 0,05 USD sind für viele Produkte im Supermarkt zu teuer, so z.B. für den in der Presse viel zitierten Joghurtbecher. Ein Tagging solcher Produkte ist deshalb wohl erst zu erwarten, wenn Technologien wie die Polymertechnologie entsprechend ausgereift sind. Bei der Polymertechnologie bestehen die Chips nicht mehr aus Silizium, sondern aus Kunststoff. Die Produktionskosten solcher Chips sind erheblich niedriger, da sie in einem Druckverfahren hergestellt werden können. In Zukunft sollte es sogar möglich sein, Polymer-Tags ähnlich wie heute Barcodes direkt auf das Produkt zu drucken. Allerdings wird es noch einige Jahre dauern, bis die Technik so weit ist, auch wenn einzelne Hersteller schon bedeutende Fortschritte gemacht haben [Inf02a, Inf02b].

Die Kosten für einen RFID-Leser spielen insbesondere dort eine Rolle, wo eine große Anzahl von Lesern benötigt wird, z.B. in stationären Anwendungsfällen, bei denen Regale oder Lagerplätze überwacht werden. Ebenso wie bei RFID-Tags ist bei RFID-Lesern mit deutlich fallenden Preisen zu rechnen. Zudem wird daran gearbeitet, die Anzahl der Antennen pro Leser zu erhöhen, wodurch die notwendige Anzahl an Lesern gesenkt werden könnte.

Datenschutz

Werden RFID-Tags nicht nur eingesetzt, um Produkte in der Lieferkette zu verfolgen, sondern auch darüber hinaus, stellt sich die Frage des Datenschutzes. Zumindest bei dem obigen Beispiel von Benetton kann man vermuten, dass Bedenken von Kunden und Verbraucherschützern eine wesentliche Rolle spielen. Aufklärung und ein Dialog mit den involvierten Parteien über die realen Möglichkeiten der Technologie und ihre Beschränkungen sowie über mögliche Folgen sind wichtig. Teilweise erscheinen die geäußerten Bedenken wenig begründet. Sollen RFID-Tags tatsächlich über die Lieferkette hinaus funktionsfähig bleiben und nicht spätestens beim Kauf automatisch zerstört werden, könnte Konsumenten gegebenenfalls ein Wahlrecht eingeräumt werden, ob sie damit einverstanden

sind, dass das Tag funktionsfähig bleibt. Dies gibt allen Verbrauchern, die Datenschutzbedenken haben, die Möglichkeit, sich vor realen oder vermeintlichen Eingriffen in ihre Privatsphäre zu schützen. Erfahrungen mit verschiedenen anderen Technologien haben gezeigt, dass dies die Kundenakzeptanz fördern kann [Can02]. Die Beiträge von Langheinrich und Thiesse in diesem Buch befassen sich ausführlich mit dem Thema Datenschutz und RFID.

4 Zusammenfassung und Schlussfolgerungen

Automatische Produktidentifikation mittels RFID-Technologie bietet diverse Potenziale zur Verbesserung der Supply-Chain-Prozesse im Einzelhandel. Neben Effizienzgewinnen (z.B. bei der Erfassung von Lieferungen und beim Check-out an der Kasse) bietet RFID-Technologie im Vergleich zum etablierten Barcode weitere Vorteile bei der Kontrolle von Lieferungen (z.B. Überprüfung der Korrektheit) oder Lagerbeständen (z.B. Überprüfung der Verfügbarkeit oder der Haltbarkeit) sowie bei der Vermeidung von Diebstahl. Darüber hinaus kann mittels RFID-Tags eine bessere Rückverfolgbarkeit von Produkten oder Produktchargen realisiert werden. Doch RFID kann nicht nur in der Lieferkette eingesetzt werden, sondern z.B. auch zur Produktionssteuerung oder zur Verbesserung des Customer Relationship Management.

Für eine zumindest teilweise Realisierung vieler Potenziale reicht es aus, RFID-Tags auf der Ebene von Paletten und Kartons einzusetzen, da dies in der Regel bis hin zum Supermarkt die relevanten Verpackungseinheiten im Einzelhandel sind. Ein Aufbrechen von Kartons findet häufig erst statt, wenn die Produkte auf die Verkaufsfläche transportiert werden. Um auch nach der Vereinzelung der Produkte noch von der RFID-Technologie profitieren zu können, wird es vielfach notwendig, RFID-Tags auf Produktebene zu verwenden. Für einzelne Produktkategorien kann der Einsatz von RFID-Tags auf Produktebene sinnvoll sein, vor allem bei relativ teuren Produkten wie Kleidungsstücken oder bei Produkten mit hohem Diebstahlrisiko wie Rasierklingen.

Nicht alle Potenziale sind technisch ohne Weiteres realisierbar. Insbesondere die Erreichbarkeit einer hinreichend hohen Leserate ist in einigen Fällen kritisch zu sehen. Hier spielen zum einen physikalische Eigenschaften des Produktes eine Rolle, zum anderen aber auch das Anwendungsszenario. Problematisch sind häufig Anwendungen wie z.B. die Überprüfung einer Lieferung, bei der praktisch ausnahmslos alle Kartons, die sich auf einer Palette befinden, korrekt gelesen werden müssen.

Wie anhand einiger Beispiele aufgezeigt wurde, gibt es bereits eine Reihe von RFID-basierten Anwendungen und Pilotversuche im Einzelhandel. Diese beschränken sich derzeit hauptsächlich auf die Ebene von – häufig wieder verwendbaren – Transportverpackungen. Anwendungen auf Produktebene befinden sich im Einzelhandel noch in der Testphase.

Auch wenn die Bedenken von Verbraucherschützern nicht immer begründet erscheinen, verzögern diese die Einführung von Anwendungen zumindest auf Produktebene. Weitere Hindernisse sind fehlende Standards, die Notwendigkeit zur Zusammenarbeit in der Lieferkette, fehlende Komplettlösungen sowie die

Preise für RFID-Tags und -Leser im Vergleich zum erwarteten Nutzen. In diesen Bereichen ist allerdings derzeit sehr viel in Bewegung. Die Problemfelder sind bekannt, und die Marktteilnehmer arbeiten an deren Beseitigung.

Noch ist nicht klar, ob sich RFID-Technologie in der Supply Chain im Einzelhandel durchsetzen wird. Unter anderem aufgrund der Aktivitäten des Auto-ID Centers bzw. EPCglobal scheint eine industrieweite Einführung – ähnlich wie vor etwa 25 Jahren beim Barcode – aber am ehesten in dieser Branche gegeben. Vermutlich wird die weitere Entwicklung von zwei Seiten getrieben: zum einen durch Verwendung von RFID-Tags auf Kartons und Paletten für eine Vielzahl von Gütern, zum anderen durch den selektiven Einsatz von RFID-Tags auf Produktebene für ausgewählte Produkte. Auf absehbare Zeit werden Barcode und RFID-Technologie sicherlich nebeneinander existieren.

Literatur

[AsS03] Ashton K, Sarma S (2003) Introducing The EPC Network. Vortrag EPC Symposium, Chicago, USA, September 16, 2003

[Acc02] Accenture (2002) Auto-ID Across the Value Chain – From Dramatic Potential to Greater Efficiency & Profit. Auto-ID Center Report, archive.epcglobalinc.org/publishedresearch/ACN-AUTOID-BC-001.pdf

[AlE02] Albano S, Engels DW (2002) Auto-ID Center Field Trial – Phase I Summary. Auto-ID Center Technical Report, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TR-006.pdf

[Ben03] Benetton (2003) No microchips present in garments on sale. Benetton Press Release, April 4, 2003, www.benetton.com/press/sito/_media/press_releases/rfiding.pdf

[BGC02] Bharadwaj S, Gruen TW, Corsten DS (2002) Retail Out of Stocks – A Worldwide Examination of Extent, Causes, and Consumer Responses. Grocery Manufacturers of America, Food Marketing Institute and CIES – The Food Business Forum

[Can02] Cantwell B (2002) Why Technical Breakthroughs Fail – A History of Public Concern with Emerging Technologies. Auto-ID Center White Paper, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-016.pdf

[EPC03] EPCglobal, Inc. (2003) EAN International and Uniform Code Council Introduce New Joint Venture and Identity for AutoID, Inc. EPC Global, Inc. Press Release, September 16, 2003, www.epcglobalinc.org/news/pr_09162003.html

[EuU02a] Europäische Union (2002) Richtlinie 2002/96/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 über Elektro- und Elektronik-Altgeräte – Gemeinsame Erklärung des Europäischen Parlaments

[EuU02b] Europäische Union (2002) Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit

[Fis94] Fisher ML, Hammond JH, Obermeyer WR, Raman A (1994) Making Supply Meet Demand in an Uncertain World. Harvard Business Review 82(5): 83–93

[Fut04] METRO Group Future Store Initiative (2004) RFID: Uncovering the value – Applying RFID within the Retail and Consumer Package Goods Value Chain. Report

SAP, Intel with Retail Forward and M-Lab, www.future-store.org/servlet/PB/show/1002180/RFID_METRO_Broschure.pdf

[Gil04] Gillert F (2004) Infineon Technologies AG – mit „Ident Solutions“ als Generalunternehmer für RFID-Systemlösungen am Markt aktiv. Jahrbuch ident 2004, ident Verlag und Service

[Gua03] The Guardian (2003) Tesco tests spy chip technology, July 19, 2003, www.guardian.co.uk/uk_news/story/0,3604,1001211,00.html

[HoD01] Hollinger RC, Davis JL (2001) National Retail Security Survey. Department of Sociology and the Center for Studies in Criminology and Law, University of Florida

[IBM02a] IBM Business Consulting Services (2002) Applying Auto-ID to Reduce Losses Associated with Shrink. Auto-ID Center Report, archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-003.pdf

[IBM02b] IBM Business Consulting Services (2002) Focus on Retail – Applying Auto-ID to Improve Product Availability at the Retail Shelf. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-001.pdf

[Inf02a] Infineon (2002) Infineon Technologies has developed polymer chips with excellent electrical characteristics and optimised them for cost-effective manufacturing. Infineon Press Release, November 12, 2002, www.infineon.com/cgi/ecrm.dll/jsp/shownewsarchive.do

[Inf02b] Infineon (2002) Infineon First to Integrate Plastic Chips on Commercially Available Packaging Film. Infineon Press Release, November 12, 2002, www.infineon.com/cgi/ecrm.dll/jsp/shownewsarchive.do

[Kau03] Kaufhof (2003) Kaufhof AG startet RFID-Pilotprojekt mit Gerry Weber. Kaufhof Pressemitteilung, 26. Juni 2003, www.galeria-kaufhof.de/sales/coco/co_presse_011_mit_030626_log.asp

[Kär02] Kärkkäinen M (2002) RFID in the grocery supply chain – a remedy for logistics problems or mere hype? Working Paper. ECR Student Award

[Lig02] Lightburn A (2002) Unsaleables Benchmark Report. Joint Industry Unsaleables Steering Committee, Food Distributors International, Food Marketing Institute and Grocery Manufacturers of America

[Lin03] Line56.com (2003) Wal-Mart Cancels RFID Trial, July 14, 2003, www.line56.com/articles/default.asp?ArticleID=4816

[LPW97] Lee HL, Padmanabhan V, Whang S (1997) The Bullwhip Effect in Supply Chains. Sloan Management Review 38(3): 93–102

[MahoJ] Mahoney K (o.J.) Opportunities for RFID in the Supply Chain – A Marks & Spencer Case Study. www.intellident.co.uk/Solutions/SupplyChainDistribution/MSRollOut

[Met04] METRO Group (2004) METRO Group startet Einsatz von RFID in der Logistik. METRO Group Pressemitteilung, 29. Oktober 2004, www.future-store.org/servlet/PB/menu/1003975_l1/index.html

[MFS03] McFarlane D, Sheffi Y (2003) The Impact of Automatic Identification on Supply Chain Operations. International Journal of Logistics Management 13(1): 1–18

[Phi03] Royal Philips Electronics (2003) Benetton Selects Philips to Introduce Smart Labels across 5 000 Worldwide Stores. Philips Press Release, March 11, 2003, www.prdomain.com/companies/p/philips/news_releases/200303mar/pr_20030311.htm

[RDT01] Raman A, DeHoratius N, Ton Z (2001) Execution – The Missing Link in Retail Operations. California Management Review 43(3): 136–152

[Rfi02a] RFID Journal (2002) Learning from Prada. June 24, 2002, www.rfidjournal.com/article/view/272

[Rfi02b] RFID Journal (2002) Gillette to Buy 500 Million EPC Tags. November 15, 2002, www.rfidjournal.com/article/view/115

[Rfi03] RFID Journal (2003) Wal-Mart Lays Out RFID Roadmap. November 10, 2003, www.rfidjournal.com/article/view/647

[Sar01] Sarma S (2001) Towards the 5c Tag. Auto-ID Center White Paper, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-006.pdf

[SAP04] SAP AG (2004) SAP Launches First RFID Solution to Help Customers Automate RFID-Enabled Business Processes. SAP Press Release, January 12, 2004, www.sap.com/company/press/press.asp?pressID=2609

[Sma03] Smart Labels Analyst (2003) Smart Labels USA 2003. Conference Review, April 27, 2003, www.idtechex.com/slaapr03.pdf

[TeI01] Texas Instruments (2001) The Gap Tests Texas Instruments RFID Smart Label Technology for Tracking Denim Clothing from the Factory to Store Shelves. Texas Instruments Press Release, November 13, 2001, www.ti.com/tiris/docs/news/news_releases/2001/rel11-13-01.shtml

[Tes04] Update on the Use of Radio Barcodes within Tesco. Tesco Press Release, November 3, 2004, www.tesco.com/radiobarcodes/press_3.htm

[Wal04] Wal-Mart Begins Roll-Out Of Electronic Product Codes in Dallas/Fort Worth Area. Wal-Mart Press Release, April 30, 2004, www.walmartstores.com/wmstore/wmstores/Mainnews.jsp?pagetype=news&template=NewsArticle.jsp&categoryOID=-8300&contentOID=13794&catID=-8248&prevPage=NewsShelf.jsp&year=2004

[Wen04] Wenzel H (2004) Auswirkungen der Discountwelle auf die Handelslandschaft oder der Einzelhandel in den Zeiten der Cholera. Vortrag Münsteraner Führungsgespräche, Köln, 6. Februar 2004, www.einzelhandel.de/servlet/PB/show/1025420/Weitz_Discountwelle_Meffert.doc

[Wol03] Wolfram G (2003) METRO Group Future Store Initiative – RFID in the Supply Chain. Vortrag EPC Symposium, Chicago, USA, September 15, 2003, www.future-store.org/servlet/PB/show/1001568/RFID_Metro_Wolfram_Short.pdf

Nutzenpotenziale smarter Maschinen am Beispiel von Verkaufsautomaten

Christian Tellkamp
Institut für Technologiemanagement, Universität St. Gallen

Uwe Kubach
SAP Research, Karlsruhe, SAP AG

Kurzfassung. Maschinen werden „smart", wenn sie in die Lage versetzt werden, Betriebsparameter und Kontextinformationen aus ihrer Umgebung aufzunehmen, Daten zu versenden und zu empfangen sowie auf Basis dieser Daten Aktivitäten anzustoßen. Ausgehend von allgemeinen Potenzialen smarter Maschinen beleuchtet der Beitrag spezifisch die Potenziale für den Einsatz bei Verkaufsautomaten, wobei der Fokus auf den Vorteilen für den Betreiber liegt. Er beschreibt eine Pilotlösung, in der Daten von Verkaufsautomaten in ein ERP-System integriert werden. Das Beispiel eines Automatenbetreibers verdeutlicht, wie bestimmte Potenziale realisiert werden können. Auf Basis dieses Beispiels erfolgt eine Abschätzung, in welchen Bereichen smarte Verkaufsautomaten bzw. smarte Maschinen voraussichtlich gewinnbringend eingesetzt werden können.

1 Einleitung

„Smarte" Maschinen verfügen über Sensoren und Aktuatoren und können mit ihrer Umgebung kommunizieren. Anwendungen smarter Maschinen sind häufig Machine-to-Machine-(M2M-)Applikationen, d.h., die Kommunikation erfolgt direkt zwischen der smarten Maschine und einer zentralen Applikation. Menschliche Aktivitäten, z.B. für die Erfassung von Daten, können dadurch entfallen. Die Datenerfassung erfolgt mittels Sensoren, die häufig schon in den Maschinen eingebaut sind. Eine Übermittlung der Daten kann entweder zu ganz bestimmten Zeitpunkten oder ereignisbasiert erfolgen, z.B. wenn eine Fehlfunktion vorliegt.

Für die Datenübertragung kommen in Abhängigkeit von der Anwendung verschiedene Technologien infrage. Bei stationären Maschinen, z.B. in der Produktion, kommt eine Anbindung über das Festnetz infrage. Alternativ können aber auch drahtlose Übertragungstechnologien genutzt werden, wenn z.B. eine drahtgebundene Anbindung zu aufwendig wäre. Für kurze Entfernungen stehen dabei Technologien wie Infrarot, Bluetooth, DECT oder WLAN zur Verfügung. Bei größeren Entfernungen und an Stellen, an denen eine Anbindung an das Festnetz nicht gegeben ist, ist eine Übertragung von Daten über das Mobilfunknetz möglich, ebenso bei mobilen Maschinen (z.B. bei Flottenmanagement-Lösungen).

Die Daten fließen in der Regel in eine zentrale Anwendung, z.B. in ein Enterprise-Resource-Planning-(ERP-)System, in der sie aufbereitet und verarbeitet werden. Dieses zentrale System kann selbst Aktivitäten initiieren. Wie oben bereits angesprochen, werden diese Anwendungen häufig als M2M-Applikationen bezeichnet, da menschliche Aktivitäten bei der Datenerfassung und -übertragung sowie bei bestimmten standardisierten Schritten der Datenaufbereitung und -auswertung nicht mehr notwendig sind. Dies bedeutet allerdings nicht, dass die Anwendungen in jedem Fall vollautomatisch funktionieren. Bei bestimmten Aktivitäten ist der Mensch nicht zu ersetzen. Dies gilt zum einen für die Durchführung bestimmter physischer Tätigkeiten z.B. bei Wartung und Reparatur, aber auch für nichtroutinemäßige Datenauswertungen.

Die Idee smarter Maschinen, wie hier beschrieben, ist prinzipiell nicht neu. In der Produktion gibt es darauf beruhende Anwendungen bereits seit den 60er-Jahren [Kvi02]. Im Maschinen- und Anlagenbau spricht man in diesem Zusammenhang häufig von Teleservice. Bisher galt: Je komplexer die produzierende Maschine, desto höher der Anteil an Herstellern, die Teleservice anbieten [Bor02].

Die zugrunde liegenden Technologien sind mittlerweile allerdings so weit ausgereift und kostengünstig, dass sie in einer Vielzahl von Maschinen eingesetzt werden können. Dadurch dürfte die Zahl der Anwendungen in den nächsten Jahren deutlich steigen. Ein Indiz hierfür ist die Tatsache, dass – wie im Beispiel unten aufgezeigt wird – Anbieter von Standardunternehmenssoftware an Projekten arbeiten, die die Potenziale einer Integration der Maschinendaten in ihre Softwareprodukte demonstrieren. Zudem forcieren Technologieanbieter wie Nokia das Thema. Das Unternehmen bietet GSM-Kommunikationsmodule an und unterstützt Anwender bei der Realisierung von Projekten[43]. Nokia sieht typische M2M-Anwendungsfelder in den Bereichen Service & Wartung, automatische Steuerung der Haus- und Gebäudetechnik, Infotainment, nutzungsorientierte Abrechnung („pay-per-use“) sowie Transport & Logistik [Nok04]. Marktforschungs- und Beratungsunternehmen wie Gartner erwarten eine weitere Verbreitung von M2M-Anwendungen, in denen Mobilfunktechnologie zur Kommunikation mit den Geräten eingesetzt wird [Gar02].

Einige beispielhafte Anwendungen existieren bereits: Canon bietet für seine Kopierer ein so genanntes „Remote Diagnostics System“ an, das den Hersteller über aufgetretene Störungen sofort informiert und automatisch Tonerbestellungen initiieren kann. Zudem werden die Zählerstände der Geräte automatisch übermittelt; die bisherige manuelle Zählerstandsermittlung entfällt. Die Kunden der Firma können über einen Browser direkt auf Statusinformationen zu allen am System angeschlossenen Kopierern zugreifen[44].

In einem Pilotversuch haben Miele und IBM gezeigt, wie Nutzungsszenarien „intelligenter Waschmaschinen“ in Mehrfamilienhäusern aussehen können, in denen sich mehrere Parteien einige Waschmaschinen teilen. Die Lösung erlaubt es Mietern, Waschzeiten über Mobiltelefon, PC oder Telefon zu buchen, wodurch sich die Nutzung der Maschine besser koordinieren lässt. Per SMS informiert sie das System über den aktuellen Status des Waschvorgangs. Darüber hinaus führen

[43] www.nokia.com/nokia/0,8764,49424,00.html

[44] www.canon.de/support/serviceangebote/serviceangebote_cbs/e_maintenace/index.asp

die Maschinen eine elektronische Selbstdiagnose durch und melden Störungen oder Wartungsbedarf unverzüglich per SMS an den Hausmeister sowie den Hersteller. Die Pilotanwendung sieht vor, dass Miele dann entscheidet, ob der Hausmeister den Service direkt vor Ort durchführen kann oder ob hierfür ein Miele-Fachhändler notwendig ist [IBM01].

Autoversicherer wie Norwich Union[45] und Progressive Insurance führen Pilotversuche durch, bei denen sich der Versicherungstarif für ein Auto auf Basis verschiedener Nutzungsparameter berechnet [Lit02]. Die notwendigen Daten werden mit Hilfe von GPS-Sensoren erfasst und per Mobilfunknetz übertragen.

2 Nutzenpotenziale smarter Maschinen

Smarte Maschinen bieten eine Reihe von Nutzenpotenzialen. Wie die oben genannten Beispiele bereits andeuten, können sie bei der Reduzierung operativer Kosten helfen, in dem sie z.B. ereignisbasierte Service- und Wartungsleistungen ermöglichen. Die Produkthistorie einer Maschine lässt sich weitgehend ohne manuelles Sammeln und Eingeben von Daten erfassen. Anpassungen, z.B. an der Steuerungssoftware, können zentral durchgeführt werden. Für bestimmte Maschinen kann auch das Risiko für Diebstahl oder Vandalismus reduziert werden, weil dies gegebenenfalls einen Alarm auslösen würde. Missbrauch kann darüber hinaus reduziert werden, indem die Benutzung einer Maschine nur möglich ist, nachdem diese entsprechend zentral freigeschaltet wurde.

Durch direkte Benachrichtigung eines Technikers bei Fehlfunktionen können Zeiten, in denen die Maschine nicht verfügbar ist, reduziert werden. Dem Techniker – aber auch dem Benutzer – können zudem relevante Informationen (z.B. Wartungshistorie, Nutzungsdaten, Reparatur- oder Bedienungshinweise) zur Verfügung gestellt werden. Nutzungsdaten können zudem Aufschlüsse hinsichtlich möglicher Prozess- oder Produktverbesserungen liefern. Ein Hersteller kann so z.B. ermitteln, wo sein Produkt Schwachstellen hat oder welche Funktionalitäten häufiger verwendet werden als andere. Neue Abrechnungsmodelle sind möglich, wenn Maschinen nicht mehr wie bisher gekauft oder zu festen Konditionen geleast werden, sondern nur für die tatsächliche Verwendung bezahlt wird.

3 Der Markt für Verkaufsautomaten

Ein Beispiel für eine Maschine, die mit Hilfe von Technologie smart werden kann, ist ein Verkaufsautomat. Dieser verkauft bestimmte Produkte oder Dienstleistungen gegen Entgelt ohne persönliche Anwesenheit eines Verkäufers. Es gibt eine Vielzahl von Produkten, die in Verkaufsautomaten angeboten werden. In den meisten Automaten werden Heiß- und Kaltgetränke, Nahrungsmittel, Zigaretten oder Tickets verkauft. Es gibt aber auch Automaten, in denen Karten zum Wiederaufladen des Guthabens bei Prepaid-Mobiltelefonen, CDs und DVDs, Blumen,

[45] www.norwichunion.com/pay_as_you_drive

Lotterielose etc. verkauft werden. Auch Geldautomaten können als Verkaufsautomaten betrachtet werden.

In Europa waren im Jahr 2001 etwa 2,8 Millionen Verkaufsautomaten für Nahrungsmittel und Getränke im Einsatz. Hinzu kommen noch einmal ca. 1,2 Millionen Zigarettenautomaten sowie zusätzlich Ticket- und andere Automaten. Der Umsatz bei Nahrungsmitteln und Getränken wird auf 25 Milliarden Euro geschätzt. In Deutschland kommt ein Nahrungsmittel- und Getränkeautomat auf etwa 220 Personen. In Österreich ist die Automatendichte fast doppelt so hoch. Die Automatendichte ist in einigen Ländern noch deutlich höher: In den USA kommen auf einen Automaten 40 Einwohner, in Japan sogar nur 20 Einwohner (wobei hier allerdings Zigarettenautomaten mitgerechnet sind). Der Betreibermarkt ist fragmentiert, es gibt nur wenige große Betreiber. Die durchschnittliche Betriebsgröße liegt in der EU bei fünf Mitarbeitern.

Die Branche steht gegenwärtig diversen Herausforderungen gegenüber. Diese sind zum einen legislativer Natur. So gibt es in der EU z.B. neue Hygienevorschriften im Nahrungsmittel- und Getränkebereich sowie strengere Umweltschutzbestimmungen (wie die EU-Richtlinie 2002/96/EG über Elektro- und Elektronik-Altgeräte). Auf der Marketingseite kämpfen die Betreiber mit dem Problem, dass Kunden Produkten aus dem Automat eine niedrige Qualität beimessen und dafür keinen hohen Preis bezahlen wollen. Getränkeautomatenbetreiber spüren auch die Konkurrenz von Kaffeeläden. Auf der technischen Seite werden Technologien wie die Fernüberwachung und -diagnose von Automaten sowie die Auswirkungen elektronischer Bezahlverfahren wie Zahlungen per Mobiltelefon diskutiert[46].

4 Nutzenpotenziale smarter Verkaufsautomaten

Viele der in Abschnitt 2 skizzierten allgemeinen Vorteile smarter Maschinen gelten entsprechend auch für Verkaufsautomaten. Darüber hinaus gibt es allerdings auch einige Potenziale, die spezifisch für Verkaufsautomaten sind. Tabelle 1 gibt eine Übersicht und kurze Beschreibung der identifizierten Potenziale.

Welche der Potenziale im Einzelfall tatsächlich realisiert werden können, hängt von diversen Umständen ab, z.B. von den Produkteigenschaften und den bestehenden Prozessen und Systemen. Hierauf wird weiter unten eingegangen. Zunächst soll aber anhand eines konkreten Projekts beschrieben werden, wie eine systemtechnische Umsetzung einer solchen Lösung für Verkaufsautomaten aussehen kann.

[46] www.eva.be

Tabelle 1. Nutzenpotenziale smarter Verkaufsautomaten

Kategorie	Nutzenpotenzial
Steigerung der Effizienz von Befüllung und Betrieb	Erhöhung der Produktverfügbarkeit und Verringerung der Anzahl der Befüllungen durch ereignisbasierte Befüllung auf Basis zeitnaher Bestands- und Verkaufsdaten
	Beschleunigung des Befüllvorgangs durch Wegfall manueller Datenerfassung (z.B. Füllstand)
	Minderung des Warenbestands in Automaten und in Servicefahrzeugen
	Verringerung des Aufwands für Durchführung von Preisänderungen durch Fernübermittlung von Preisdaten
	Verringerung des Aufwands für Software-Aktualisierung durch Fernübermittlung der Änderungen
Vermeidung unverkäuflicher Ware	Vermeidung von zu langer Lagerung von Ware im Automaten
	Vermeidung des Entstehens unverkäuflicher Ware aufgrund von Funktionsstörungen (z.B. Kühlung)
Erhöhung der Sicherheit	Abschreckung gegen Aufbruch von Automaten und Vandalismus
	Abschreckung gegen Diebstahl kompletter Automaten
Steigerung der Wartungseffizienz	Verringerung des Inspektionsaufwands durch ereignisbasierte Wartung
	Erhöhung der Automatenverfügbarkeit durch sofortige Übermittlung von Funktionsstörungen
Standortoptimierung	Optimierung der Automatenstandorte aufgrund von Verkaufszahlen etc.
Sortimentsoptimierung	Optimierung des Sortiments in Automaten aufgrund von Verkaufszahlen etc.
Gewinnung von Marketinginformationen	Rückschlüsse über Kundenverhalten durch Erfassung der Kundeninteraktion am Automaten
	Beurteilung des Erfolgs von Marketinginitiativen, z.B. über Erfassung von Verkaufszahlen
	Interaktive Werbung am Automaten
Verbesserung der Kassenhaltung	Reduzierung des Aufwands für physische Verarbeitung des Geldes (z.B. Entnahme, Transport, Zählen) bei Nutzung elektronischer Zahlungsmittel (z.B. Geldkarte, EC- und Kreditkarte, Mobiltelefon)
	Verringerung der Kapitalbindung durch zeitnahe Übermittlung von elektronisch getätigten Käufen mit Geldkarte

5 Systemtechnische Umsetzung

Aufgrund sehr kleiner Gewinnmargen in der Automatenbranche sowie der starken Fragmentierung des Marktes stehen die meisten Betreiber größeren Investitionen in die Aufrüstung ihres Automatenparks zunächst skeptisch gegenüber. Um die Vorteile smarter Verkaufsautomaten zu demonstrieren, hat SAP Research mit dem Smart Vending Center (SVC) eine Testplattform geschaffen, die es den Partnern im SVC ermöglicht, mit minimalen Investitionen Evaluierungen ihrer Business Cases durchzuführen, bevor sie sich endgültig für eine Investition in entsprechende Technologien entscheiden.

Die gegenwärtigen Partner im SVC decken bereits alle konzeptionellen Schichten einer integrierten Smart-Vending-Lösung, vom Automatenhersteller bis zur Applikation, ab (siehe Abbildung 1).

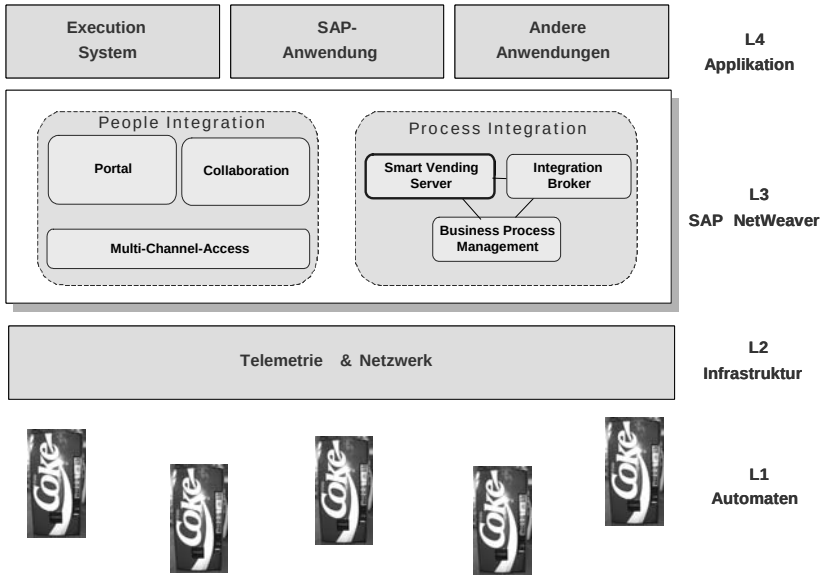


Abb. 1. Konzeptionelle Schichten einer integrierten Smart-Vending-Lösung

Kern des Smart Vending Centers ist der Smart Vending Server, ein Prototyp einer Softwarekomponente, die Daten verschiedenster Automaten unterschiedlicher Hersteller entgegennehmen kann und in SAP NetWeaver, die Integrationsplattform der SAP, integriert. Umgekehrt kann der Smart Vending Server auch Daten, z.B. Softwareupgrades, Steuerungsdaten oder Preisinformationen, an Automaten versenden.

Die Kommunikation zwischen den Automaten und dem Smart Vending Server kann wahlweise über das GSM-Netz (SMS oder GPRS) oder ein LAN erfolgen. Kommunikationsendpunkte in den Automaten sind Telemetriemodule, die neben der Kommunikation mit dem SVC für die Datenerfassung und -pufferung im Automaten zuständig sind.

Diese M2M-Kommunikation stellt für Mobilfunknetzbetreiber eine große Chance und zugleich eine interessante Herausforderung dar, da gegenwärtig noch keine für M2M-Anwendungen attraktiven Tarifmodelle verfügbar sind. Eine Lösung könnten transaktionsbasierte Modelle sein, bei denen nach Anzahl der übermittelten Transaktionen und nicht nach übertragenem Datenvolumen oder Verbindungszeit abgerechnet wird.

Aus technischer Sicht ist eine Lösung, wie sie im SVC realisiert ist, offen für Daten von ganz unterschiedlichen smarten Maschinen. Vorausgesetzt die entsprechenden Sensoren etc. sind vorhanden, ist die einzige weitere Randbedingung, dass sich eine entsprechende Telemetriekomponente in die Maschine einbauen lässt, um sie auch tatsächlich „smart“ zu machen.

6 Realisierung der Potenziale in einem konkreten Anwendungsfall

Im Folgenden soll die mögliche Realisierung einiger Nutzenpotenziale smarter Verkaufsautomaten an einem konkreten Anwendungsfall diskutiert werden. Bei der untersuchten Firma handelt es sich um einen Betreiber von Zigarettenautomaten im südwestdeutschen Raum.

6.1 Erhöhung der Produktverfügbarkeit

Für die Befüllung der ca. 10 000 Automaten, die das Unternehmen betreibt, sind rund 30 Mitarbeiter zuständig. Jeder Mitarbeiter hat feste Touren, die er in einem bestimmten Rhythmus abfährt. Pro Tag befüllt er ca. 40–50 Automaten. Die Befüllintervalle betragen zwischen vier Tagen, wöchentlich, zweiwöchentlich und vierwöchentlich. Jeder Mitarbeiter erhält am Morgen ein mobiles Datenerfassungsgerät. Auf dem Gerät ist die vom Mitarbeiter zu fahrende Tour für den Tag in der Reihenfolge der abzufahrenden Automaten hinterlegt sowie die Befüllung der einzelnen Automatenschächte. Am Automaten angekommen, liest der Mitarbeiter die Verkaufsdaten aus (sowie ggf. den mit Geldkarte bezahlten Betrag), befüllt den Automaten, entnimmt das Geld und kontrolliert die Funktionsfähigkeit des Automaten. Die Daten werden am Ende des Tages an das Informationssystem des Unternehmens übertragen.

Die Verkaufszahlen der einzelnen Automaten fließen in eine eigene Software, die den Sollbestand der einzelnen Produkte je Automat berechnet. Diese berücksichtigt bisher Daten zur kurzfristigen Nachfrage, aber auch Durchschnittswerte über einen längeren Zeitraum. Um den Füllstand in den Automaten bei Schwankungen in der Nachfrage (z.B. aufgrund von Sommerbeginn, Ferien oder Feiertagen) auszugleichen, sind zum Teil beträchtliche manuelle Korrekturen an den automatisch bestimmten Sollbeständen erforderlich.

Zeitnahe Informationen smarter Verkaufsautomaten ermöglichen die variable Bestimmung geeigneter Befüllzeitpunkte auf Basis aktueller Verkaufszahlen und Bestände. Prinzipiell kann hierdurch die Produktverfügbarkeit erhöht werden,

ohne die Bestände zu erhöhen; aufgrund der genaueren Bestandsinformationen ist es sogar denkbar, dass diese gesenkt werden können. Um das Nutzenpotenzial tatsächlich realisieren zu können, ist allerdings eine dynamische Tourenplanung erforderlich, die – in Abhängigkeit von der Tour des Befüllers – festlegt, welche Automaten er zusätzlich befüllen soll. Eine dynamische Befüllung kommt dabei nur für solche Automaten infrage, bei denen der erwartete Nutzen die Zusatzkosten übersteigt.

6.2 Erhöhung der Automatenverfügbarkeit

Bei der Instandhaltung der Automaten kann grundsätzlich unterschieden werden zwischen Inspektion, Wartung und Instandsetzung. Inspektion und Wartung finden im betrachteten Anwendungsfall praktisch bei jeder Befüllung des Automaten statt. Dazu gehören kleinere Arbeiten wie die Reinigung der Solarzellen, das Entfernen verklemmter Münzen oder der Austausch leerer Akkus. Gesonderte Inspektionen durch Servicetechniker gibt es nicht. Viele der anfallenden Wartungsarbeiten, z.B. Software-Updates, können ebenfalls vom Befüller durchgeführt werden. Bei schwerwiegenderen Funktionsstörungen benachrichtigt der Mitarbeiter, der für die Befüllung zuständig ist, einen Servicetechniker. Ein größeres Einsparungspotenzial erwartet das Unternehmen bezüglich Inspektion und Wartung daher nicht.

Meldungen über Störungen, die eine Instandsetzung erfordern, erhält das Unternehmen über zwei Kanäle: Entweder wird die Störung von einem Mitarbeiter, der den Automaten bestücken will, entdeckt. In solchen Fällen benachrichtigt der Mitarbeiter den Servicetechniker in der Regel direkt, wenn er die Störung nicht selber beheben kann. In anderen Fällen meldet ein Kunde eine Störung, z.B. weil sein Geld im Automaten stecken geblieben ist. (Jeder Automat hat für Störfälle eine aufgedruckte Telefonnummer.) Dann benachrichtigt die Zentrale einen Techniker. Jeder der sechs Servicetechniker bearbeitet im Schnitt 10–15 Störungen pro Tag. Angestrebt wird eine Reparatur am selben Tag, an dem die Störung gemeldet wird. Zu jedem bearbeiteten Störfall wird ein Bericht ausgefüllt, der in der Zentrale manuell erfasst wird. Für jeden Automaten kann so die komplette Wartungshistorie abgerufen werden.

Typische Störungen (die teilweise auch vom Befüller selbst behoben werden können) sind verschmutzte Solarzellen, Vandalismus und ein verstopfter Münzkanal. Störungen können verschiedene Konsequenzen haben. Viele Störungen beeinträchtigen die Funktionsfähigkeit des Automaten nur wenig (z.B. verschmutzte Solarzellen) und werden für den Nutzer überhaupt nicht sichtbar. Bei anderen sind einzelne Funktionen (z.B. die Ausgabe von Produkten aus bestimmten Schächten) am Automaten gestört. Nur in seltenen Fällen kommt es dazu, dass ein kompletter Automat nicht mehr funktionstüchtig ist.

Ein smarter Verkaufsautomat kann sofort melden, wenn Störungen auftreten und um welche Störungen es sich handelt. Heutige Automaten verfügen bereits über eine Vielzahl eingebauter Sensoren, die diverse Parameter überwachen. Abhängig von der Schwere der Störung könnte dann entschieden werden, einen Servicetechniker loszuschicken oder aber zu warten, bis der Befüller das nächste Mal

vor Ort ist. Die Automatenverfügbarkeit kann so ohne größere organisatorische Veränderungen erhöht werden.

6.3 Verringerung der Kapitalbindung

Dem Unternehmen steht das Geld aus einem Automaten erst nach dessen Leerung zur Verfügung. Dies gilt sowohl für Barzahlungen als auch für Zahlungen mit Geldkarte und führt zu einer hohen Kapitalbindung in den Automaten.

Wird ein Automat smart, ergeben sich daraus zwei Konsequenzen: Zum einen ist eine elektronische Anbindung des Automaten notwendig, damit bestimmte Zahlverfahren (z.B. Bezahlung per Mobiltelefon) überhaupt genutzt werden können. Zum anderen kann der mit Geldkarte (oder anderen bargeldlosen Zahlungsmitteln) bezahlte Betrag zeitnah abgerufen werden. Hieraus ergibt sich eine Reduktion des notwendigen Betriebskapitals. Das resultierende Potenzial dürfte in den nächsten Jahren steigen, da mit einer weiteren Verbreitung bargeldloser Zahlungsmittel gerechnet wird und immer mehr Automaten mit Geldkartenfunktionalität ausgerüstet werden.

7 Zusammenfassung und Schlussfolgerungen

Wenn Maschinen smart werden, bietet dies eine Reihe von Vorteilen für den Betreiber. Mittels smarter Maschinen können Betriebs- und Wartungskosten gesenkt und die Verfügbarkeit verbessert werden. Zusätzlich können die gesammelten Informationen, wie z.B. Betriebsdaten, für Analysen genutzt werden, um das Leistungsangebot nachhaltig zu verbessern.

Der Fokus des vorliegenden Beitrags lag auf den konkreten Nutzenpotenzialen für Verkaufsautomaten. Anhand eines Pilotprojekts wurde demonstriert, wie eine systemtechnische Umsetzung in einem ERP-System aussehen kann. Für einen Automatenbetreiber haben wir exemplarisch einige der möglichen Nutzenpotenziale aufgezeigt. Inwieweit diese tatsächlich realisierbar sind, hängt unter anderem von den bestehenden Prozessen und den vorhandenen Informationssystemen ab.

Ausgehend von unserem Beispiel sehen wir wesentliche Anwendungsmöglichkeiten smarter Verkaufsautomaten vor allem in Bereichen, bei denen Produkt- oder Automatenverfügbarkeit kritisch sind und bei denen die Voraussetzungen gegeben sind, ereignisbasiert Serviceleistungen zu erbringen. Wie in dem Beispiel dargestellt, sind viele der Informationen mit einem gewissen Zeitverzug bereits lokal verfügbar. Die Einführung einer Lösung unter Verwendung smarter Technologien ist gerade für solche Unternehmen interessant, die diese Daten bislang noch nicht nutzen.

Für smarte Maschinen im Allgemeinen gelten grundsätzlich die gleichen Aussagen. Bei gewissen Maschinen, z.B. in der Produktion, sind solche Anwendungen bereits seit Längerem im Einsatz. Interessant wird das Thema jetzt aber auch für kleinere und weniger aufwendige Maschinen, bei denen solche Lösungen bislang nicht möglich waren, etwa aus Kostengründen. Für Kleingeräte, z.B. elektrische Werkzeuge, spielt in Zukunft unter Umständen die Verhinderung von Miss-

brauch, Diebstahl sowie die Möglichkeit zur Lokalisierung der Geräte eine entscheidende Rolle.

In der Softwareindustrie gibt es Überlegungen, existierende Standardsoftware um Funktionalitäten für das Management smarter Maschinen zu erweitern. Hierdurch sinkt der Aufwand zur Einführung einer solchen Lösung. Da gleichzeitig auch die Kosten für Sensoren und Datenübertragung weiter sinken werden, ist mit einer weiteren Verbreitung smarter Maschinen in den nächsten Jahren zu rechnen.

Literatur

[Bor02] Borgmeier, A (2002) Teleservice im Maschinen- und Anlagenbau: Anwendung und Gestaltungsempfehlungen. Deutscher Universitäts-Verlag

[Gar02] Gartner, Inc. (2002) The M2M Market Explained. Gartner Research Note, May 14, 2002

[Kvi02] Kviselius NZ (2002) Swedish M2M Industry Case Study. Conference Proceedings M-Business – International Conference on Mobile Business

[IBM01] IBM Deutschland (2001) Mieles intelligente Waschmaschine: mobiles e-business fürs Alltägliche. IBM Deutschland Hintergrundinformation, www-5.ibm.com/de/pressroom/presseinfos/2001/010208_1.html

[Lit02] Litman TA (2002) Implementing Pay-As-You-Drive Vehicle Insurance: Policy Options. Report, The Institute of Public Policy Research

[Nok04] Nokia Corporation (2004) Machine-to-Machine: Let your machines talk. White Paper

Werkzeugmanagement in der Flugzeugwartung – Entwicklung eines Demonstrators mit ERP-Anbindung

Martin Strassner
Institut für Technologiemanagement, Universität St. Gallen

Matthias Lampe
Institut für Pervasive Computing, ETH Zürich

Udo Leutbecher
SAP Systems Integration AG, München

Kurzfassung. Ungeplante Verzögerungen in der Flugzeugwartung verursachen hohe Folgekosten. Ineffizientes Werkzeugmanagement ist eine mögliche Ursache für derartige Verzögerungen. Hohe Sicherheitsbestimmungen verlangen regelmäßige Kontrollen des Werkzeugbestands, um zu verhindern, dass Mechaniker Werkzeuge versehentlich in der Maschine vergessen. Auch die Anforderungen an die Funktionsfähigkeit der Werkzeuge sind hoch, und Werkzeuge, die Mechaniker gemeinsam nutzen, müssen diese häufig vor dem Gebrauch suchen.

Dieser Beitrag beschreibt Lösungen, die dazu beitragen, das Werkzeugmanagement zu automatisieren: Die smarte Werkzeugkiste erkennt, welche Werkzeuge sich in ihr befinden, protokolliert ihren Zustand und warnt den Mechaniker bei Unvollständigkeit oder falls Werkzeuge falsch einsortiert wurden. Bei der Werkzeugausleihe ist stets bekannt, welcher Mechaniker welche Werkzeuge entliehen hat. Außerdem protokolliert das System die Nutzungshäufigkeit der Werkzeuge und liefert damit Hinweise auf deren Verschleiß. Diese Lösungen verwenden die RFID-Technologie zur automatischen Identifikation von Werkzeugen und zeigen eine Möglichkeit zur Integration mit einem ERP-System. Die hier beschriebenen Lösungen sind leicht auf andere Unternehmen der Branche übertragbar, da das Werkzeugmanagement in der Flugzeugwartung ein hoch standardisierter Prozess ist.

1 Das Werkzeugproblem der Flugzeug AG

1.1 Einleitung[47]

Die Flugzeug AG[48] entwickelt und fertigt Kleinflugzeuge und ist im MRO-(Maintenance, Repair und Overhaul-)Geschäft tätig. Regelmäßige Wartungen sind gesetzlich vorgeschrieben. Die genauen Wartungszyklen legen die Hersteller fest. Je nach Flugzeugtyp sind bei Passagierflugzeugen so genannte A-Checks alle 350–600 Flugstunden fällig.

Die Flugzeugwartung ist sehr teuer, insbesondere wenn ungeplante Reparaturen notwendig werden. Die Wartungskosten betragen ca. 12 % der Betriebskosten eines Flugzeugs, ferner entstehen bei der Wartung von gewerblich genutzten Passagierflugzeugen hohe Opportunitätskosten. Bei ungeplanten Wartungsereignissen liegen diese Kosten bei ca. 23 000 EUR pro Stunde [Bro03]. Deshalb ist die effiziente Gestaltung des MRO-Prozesses wichtig für die Wettbewerbsfähigkeit von Wartungsunternehmen. Ein Teilbereich, der wesentlich zur Steigerung der Effizienz des Prozesses beitragen kann, ist das Werkzeugmanagement. Dieser Bereich verursacht aus verschiedenen Gründen Verzögerungen:

- Sicherheitsbestimmungen verlangen, dass die Werkzeugbestände regelmäßig kontrolliert und protokolliert werden. Diesen zeitaufwendigen Vorgang führen die Mechaniker manuell durch.
- Falls die Mechaniker ein Werkzeug vermissen, müssen aus Sicherheitsgründen alle Maschinen in der Werkstatt bleiben, bis der Verbleib aufgeklärt ist.
- Häufig befinden sich Werkzeuge nicht an ihrem Platz, und die Mechaniker müssen sie vor dem Gebrauch suchen.
- Die Anforderungen an die Funktionsfähigkeit von Werkzeugen in der Flugzeugwartung sind hoch. Die Messung des Verschleißes erfolgt durch Sichtkontrolle. Dieses Verfahren ist ungenau. Stellt ein Mechaniker den Verschleiß erst während der Wartung fest, kann sich die Wartung verzögern.

In Zusammenarbeit mit der Firma SAP SI AG hat das M-Lab die Prozesse des Werkzeugmanagements bei der Flugzeug AG analysiert und gezeigt, wie Technologien zur automatischen Identifikation eine Effizienzsteigerung ermöglichen. Ziel des gemeinsamen Projekts war es, ein System zu entwickeln, um die Verwaltung von Werkzeugen weitgehend zu automatisieren. Zur automatischen Erfassung und Verwaltung der Werkzeugbestände verwendet die Lösung RFID-Technologie in Verbindung mit einem SAP-System.

Die folgenden beiden Abschnitte beschreiben den MRO-Prozess der Flugzeug AG sowie die bestehenden Probleme im Werkzeugmanagement. Anschließend stellt Kapitel zwei die im Rahmen des Projekts entwickelten RFID-basierten Lösungen, den smarten Werkzeugkasten sowie die smarte Werkzeugausgabe vor und beschreibt die Integration der Lösung mit einem SAP-System unter Verwendung

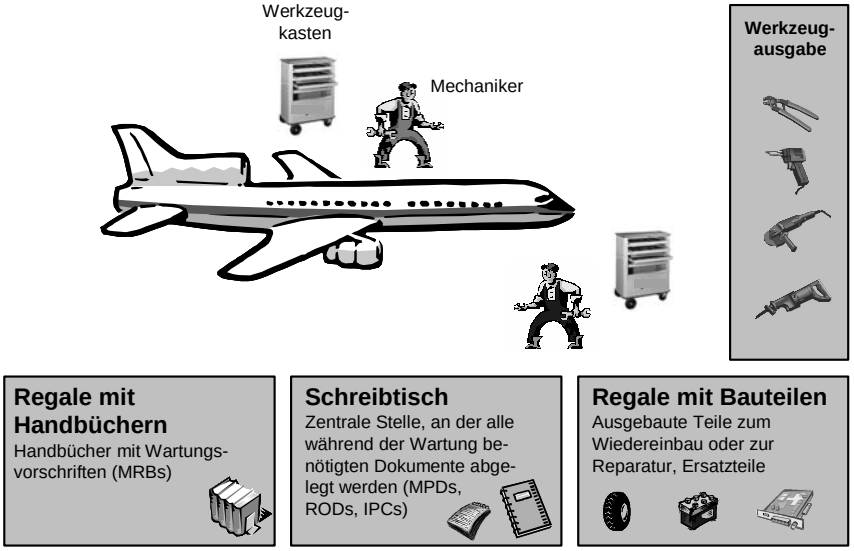
[47] Dieser Beitrag basiert in wesentlichen Teilen auf [SFL04].

[48] Der Name der Firma wurde geändert. Die prozessspezifischen Informationen, die in diesem Artikel beschrieben werden, wurden durch Interviews mit Mitarbeitern des Unternehmens sowie durch Betrachtung vor Ort gewonnen.

des SAP Business Connectors. Kapitel drei betrachtet Kosten- und Nutzenaspekte der Lösung. Abschließend fasst das letzte Kapitel die gewonnenen Erkenntnisse über die Möglichkeiten zur Verbesserung des Werkzeugmanagements durch RFID zusammen, beschreibt aber auch die Grenzen der technischen Umsetzung.

1.2 Der MRO-Prozess

Der MRO-Prozess wird in einem Hangar durchgeführt (siehe Abbildung 1). Hierbei benötigen die Mechaniker Zugriff auf verschiedene Dokumente. Alle Dokumentationen, die während der Durchführung zu erstellen sind, bewahren die Mechaniker auf einem zentralen Schreibtisch auf. In der Nähe befinden sich weitere Regale, auf denen die ausgebauten Bauteile sowie Ersatzteile liegen. Ebenfalls an einer zentralen Stelle im Hangar befinden sich die Handbücher der Hersteller (MRBs[49]), die Wartungsvorschriften für die einzelnen Komponenten enthalten. Während der Wartung sind meistens mehrere Mechaniker gleichzeitig an einem Flugzeug tätig. Jeder Mechaniker besitzt einen persönlichen Werkzeugkasten, der häufig benötigte Werkzeuge enthält. Zusätzlich besteht die Möglichkeit, Spezialwerkzeuge bei einer Werkzeugausgabe auszuleihen.



MRB: Maintenance Review Board, MPD: Maintenance Planning Document,
ROD: Discrepance Report, IPC: Illustrated Parts Catalogue

Abb. 1. Layout des Wartungsarbeitsplatzes

[49] Maintenance Review Boards

Für den MRO-Prozess existieren strenge, größtenteils gesetzlich geregelte Auflagen an Qualität, Sicherheit und Nachweispflicht. Die Prozesse sind in der Branche weitgehend standardisiert.[50] Grob umfasst der Prozess der Flugzeugwartung bei der Flugzeug AG folgende Schritte:

- **Kundenauftrag und Planung.** Ein MRO-Prozess wird durch einen Kundenauftrag initiiert. Zu einem vereinbarten Termin bringt der Kunde das Flugzeug in den Hangar und übergibt die relevanten Dokumente (Logbücher) dem Service Center. Die Logbücher enthalten Informationen über Flugstunden, Betriebsstunden, Anzahl der Starts und Landungen, Gesamtzustand des Flugzeugs und seiner Bauteile sowie festgestellte Probleme. Mit diesen Informationen planen die Mechaniker die MRO-Tätigkeiten. Einige der verwendeten Daten liegen in elektronischer Form vor, z.B. die Anzahl der Flugstunden, andere Angaben stammen von Piloten oder Eigentümern des Flugzeugs, z.B. Anzahl der Starts und Landungen sowie aufgetretene Probleme. Diese Daten können fehlerhaft sein, falls sie auf Schätzungen beruhen oder versehentliche Falschangaben enthalten. Die Planung halten die Mechaniker im so genannten „Maintenance Planning Document“[51] (MPD), das die durchzuführenden Aufgaben und die zugehörigen Aktivitäten beschreibt, fest.
- **Beschaffung von Bauteilen und Werkzeugen.** Gemäß den Angaben im MPD bestimmen die Mechaniker die zu beschaffenden Teile und Werkzeuge. Fehlende Bauteile können sie bei der Beschaffungsstelle mittels des Bauteilekatalogs (IPC) bestellen. Spezialwerkzeuge können sie bei der Werkzeugausgabe bestellen und ausleihen. Fehlende Teile, lange Lieferzeiten oder verlegte Werkzeuge verursachen Verzögerungen des MRO-Prozesses.
- **Durchführung der MRO-Aktivitäten.** Die MRO-Aktivitäten führen die Mechaniker gemäß der Reihenfolgeplanung des MPD durch. Fehler, die sie erst bei der Durchführung erkennen, können eine Erweiterung des MPDs oder die Beschaffung weiterer Ersatzteile und Werkzeuge erforderlich machen. Die Mechaniker nehmen alle Aktivitäten, die sie ausführen, in den so genannten „Discrepancies Report“ (ROD) auf. Jedes Bauteil, das sie während der Wartung inspizieren, ersetzen oder reparieren, müssen sie eindeutig anhand seiner Seriennummer identifizieren und den Status des Teils beschreiben. Gesetzliche Vorschriften verlangen, dass die Mechaniker vor der Durchführung von Wartungen an einem Bauteil in den Handbüchern der Hersteller nachsehen. Manchmal vernachlässigen die Mechaniker jedoch diesen zeitintensiven Vorgang.
- **Kontrolle und Auslieferung.** Nach der Durchführung aller Wartungsaktivitäten kontrolliert ein Inspektor das Ergebnis. Der Inspektor stellt ein so genanntes „Aircraft Certificate of Release to Service and Maintenance Statement“ aus, das alle ausgeführten Wartungsaufgaben und Reparaturen sowie alle reparierten bzw. ersetzten Bauteile beschreibt. Abschließend kann der Kunde das Flugzeug abholen.

[50] Vgl. z.B. [ATA03].

[51] In diesem Beitrag werden englische Fachbegriffe verwendet, wenn keine gängigen deutschen Übersetzungen existieren.

Einige Schwächen des MRO-Prozesses können sich auf die Qualität des Ergebnisses oder den Zeitpunkt der Auslieferung auswirken: Es wird geschätzt, dass Mechaniker durchschnittlich 15–20 % ihrer Zeit mit der Suche nach Dokumenten oder Werkzeugen verbringen [Mec99]. Manuell zu erstellende Dokumente sind für den Mechaniker eine aufwendige Arbeit, die ihn von der Durchführung von Wartungsaktivitäten abhält. Hierbei aufgetretene Fehler können bei der Planung nachfolgender MRO-Aufgaben zu Problemen führen. Falls die Mechaniker vergessen, die Handbücher der Hersteller auf aktuelle Änderungen zu überprüfen, kann dies ebenso zu qualitativen Mängeln bei der Wartung führen. Der folgende Abschnitt beschreibt die Schwächen des Werkzeugmanagements, das wesentliche Auswirkungen auf die Effizienz des gesamten MRO-Prozesses besitzt.

1.3 Werkzeugmanagement

Jeder Mechaniker besitzt einen persönlichen Werkzeugkasten mit den wichtigsten zur Durchführung des MRO-Prozesses benötigten Werkzeugen. Darüber hinaus können die Mechaniker Spezialwerkzeuge bei der Werkzeugausgabe ausleihen. Bei dem Werkzeugkasten handelt es sich um einen rollbaren Metallcontainer mit mehreren Schubladen, in denen sich die Werkzeuge befinden. Um die visuelle Vollständigkeitskontrolle zu erleichtern, existieren für die einzelnen Werkzeugtypen angepasste Schaumstoffaussparungen (siehe Abbildung 2).

Abb. 2. Der Werkzeugkasten

Jeder Mechaniker ist für seine Werkzeuge verantwortlich. Er muss sie bei Verlust ersetzen, und falls er ein Werkzeug im Flugzeug liegen lässt, muss er mit Sanktionen rechnen. Die folgenden vier Aufgaben müssen die Mechaniker bezüglich des Werkzeugkastens manuell ausführen:

- **Markierung.** Um die Werkzeuge einem Mechaniker eindeutig zuordnen zu können, ist auf jedem Werkzeug eine Personalnummer eingraviert. Die Gravur nehmen die Mechaniker selbst vor. Für einen Werkzeugkasten dauert das ca. zwei Tage.

- **Routinemäßige Vollständigkeitskontrolle.** Nach jeder Reparatur ist der Mechaniker verpflichtet, den Werkzeugkasten auf Vollständigkeit zu überprüfen, damit keine Werkzeuge im Flugzeug zurückbleiben.
- **Gründliche Vollständigkeitskontrolle.** Einmal pro Woche muss jeder Mechaniker mit einem Kollegen nach dem Vier-Augen-Prinzip neben der Vollständigkeit auch überprüfen, ob die richtigen Werkzeuge enthalten sind. Der Vorgang ist auf einem Kontrollblatt zu dokumentieren und dauert ca. eine Stunde pro Werkzeugkasten.
- **Werkzeugsuche.** Falls nach der Reparatur ein Werkzeug in einem Werkzeugkasten fehlt, müssen es die Mechaniker sofort suchen. Bis zur Auffindung müssen alle Flugzeuge, an denen der entsprechende Mechaniker gearbeitet hat, im Hangar bleiben.

Die Werkzeugausgabe wird durch einen Werkzeugmeister bedient. Die Werkzeuge befinden sich in eindeutig zugeordneten Fächern in Regalen (siehe Abbildung 3). Der Werkzeugmeister verwendet eine Excel-Tabelle zur Verwaltung der Werkzeugdaten. Drei Aufgaben lassen sich im Zusammenhang mit der Werkzeugausgabe identifizieren:

- **Ausleihe.** Ein Mechaniker darf maximal 10 Werkzeuge gleichzeitig ausgeliehen haben. Zu diesem Zweck besitzt er 10 mit seiner Personalnummer versehene Metallmünzen, die er im Austausch gegen Werkzeuge abgibt. Der Werkzeugmeister legt die Metallmünzen in die Aufbewahrungsfächer der ausgeliehenen Werkzeuge.
- **Rückgabe.** Der Mechaniker gibt die Werkzeuge dem Werkzeugmeister im Austausch gegen seine Münzen zurück. Dieser kontrolliert manuell den Zustand der Werkzeuge und entscheidet, ob er die Werkzeuge warten oder ersetzen muss.
- **Werkzeugsuche.** Manchmal wollen Mechaniker wissen, welche Werkzeuge sie ausgeliehen haben. Für die Suche nach Münzen des betreffenden Mechanikers in den Regalen benötigt der Werkzeugmeister bis zu drei Stunden

Abb. 3. Die Werkzeugausgabe

Die Schwachstellen dieser Prozesse lassen sich zusammenfassend durch fehlende Dokumentationen und menschliche Fehler begründen. Dies führt zu Suchaktionen, falsch abgelegten Werkzeugen oder Metallmünzen, vertauschten Werkzeugen und vergessenen Kontrollen.

2 Smarte Lösungen mit RFID

Die RFID-Technologie ermöglicht es, Werkzeuge eindeutig zu kennzeichnen und automatisch zu erfassen. Die folgenden Abschnitte beschreiben ein Anwendungsszenario, das eine RFID-basierte Lösung für das Werkzeugmanagement zusammen mit weiteren Technologien des Ubiquitous Computings zur Unterstützung des MRO-Prozesses verwendet, sowie die von den Autoren implementierten Demonstratoren „smarter Werkzeugkasten“ und „smarte Werkzeugausgabe“.

2.1 Anwendungsszenario

Das folgende Szenario verbindet die Anwendung der RFID-Technologie mit weiteren Technologien des Ubquitous Computing und mit der Anwendung klassischer IT-Systeme. Bei diesem Szenario besitzt jeder Mechaniker einen persönlichen tragbaren Computer, das so genannte „Pervasive Device“ (PD), welches für den Mechaniker als Benutzerschnittstelle zu allen Applikationen dient, die er zur Durchführung der MRO-Aufgaben benötigt. Hierbei könnte es sich beispielsweise um einen persönlichen digitalen Assistenten (PDA) handeln, der mit Spracherkennung, Auto-ID-Funktionalität und Mobilkommunikation ausgestattet ist.

Zu Beginn des MRO-Prozesses informiert das PD den Mechaniker über die auszuführenden Aufgaben und die benötigten Teile und Werkzeuge. Nachdem der Mechaniker die Anweisungen geprüft und die Annahme des Auftrags bestätigt hat, holt er sich die benötigten Spezialwerkzeuge aus der Werkzeugausgabe. Da das System die Werkzeuge schon automatisch reserviert hat, braucht der Mechaniker diese nur noch abzuholen, wobei ihn sein PD identifiziert. Danach holt er die auf den Regalen bereitliegenden Teile. Durch Vorbeiführen des PD an den Teilen kann der Mechaniker diese eindeutig identifizieren, und das System stellt sicher, dass er die richtigen Teile nimmt.

Bei der Durchführung von Wartungsaufgaben führt ihn sein PD durch den Prozess, indem es alle notwendigen Aktivitäten auflistet. Ebenso zeigt es die benötigten Kapitel der Wartungshandbücher an. Um zu überprüfen, ob der Mechaniker die Informationen tatsächlich liest, verlangt das PD eine Bestätigung entweder durch das Drücken eines Knopfes oder mittels Sprachkommando. Bei jeder Aktivität verwendet der Mechaniker das PD zur Identifikation der entsprechenden Bauteile und kann Wartungshistorien oder Statusreports abrufen. Die Aktualisierung der Wartungshistorie erfolgt automatisch gemäß den durchgeführten Aktivitäten bzw. kann vom Mechaniker durch Spracheingaben ergänzt werden. Diese Informationen werden auch zeitgleich in den ROD aufgenommen.

Nach Erledigung eines MRO-Auftrags bestätigt der Mechaniker dies mit dem PD, wodurch der Inspektor automatisch eine Nachricht erhält. Anhand des RODs

kontrolliert er das Ergebnis. Nachdem er die ordnungsgemäße Ausführung aller Wartungsaufgaben bestätigt hat, wird durch das System das "Aircraft Certificate of Release to Service and Maintenance Statement" erstellt und mit der digitalen Signatur des Inspektors versehen. Das PD erinnert den Mechaniker daran, alle Werkzeuge in den Werkzeugkasten zurückzulegen bzw. bei der Werkzeugausgabe abzugeben. Falls ein Mechaniker ein falsches Werkzeug in seinen Werkzeugkasten legt, weist ihn sein PD automatisch auf den Irrtum hin.

Die für das Wartungsszenario vorgeschlagene Lösungsarchitektur (siehe Abbildung 4) unterscheidet zwischen Komponenten der realen Welt, zu denen die smarten Objekte und Geräte gehören, und den IT-Systemen der digitalen Welt, bei der die Architektur drei Schichten verwendet: die Ubiquitous-Computing-Infrastruktur, ERP-Systeme und MRO-Applikationen. Diese drei Schichten nutzen eine zentrale Datenbank. Die wesentliche Leistung der Architektur ist die Integration der IT-Anwendungen mit den physischen Objekten.

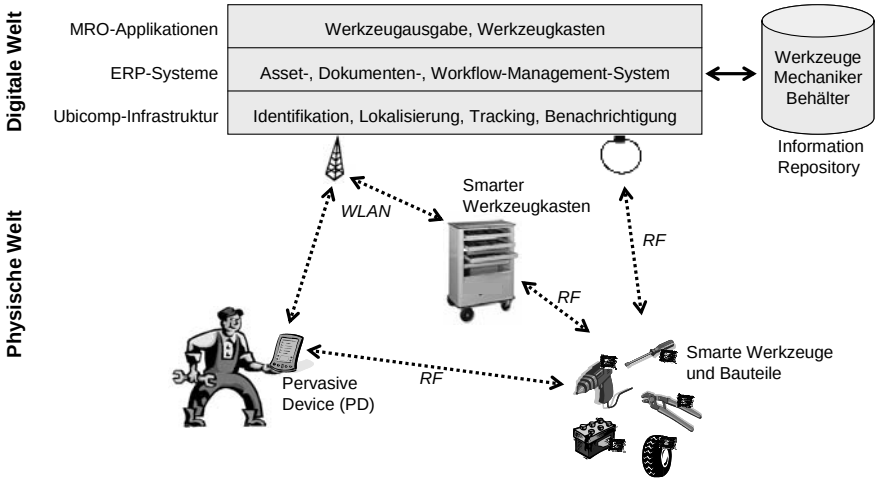


Abb. 4. Anwendungsarchitektur für MRO in der Flugzeugwartung

Durch die Verwendung von Technologien zur automatischen Identifikation, zur mobilen Kommunikation sowie Sensorik und Datenspeicherung können beliebige physische Objekte smart werden [GSB00]. Solche *smarten Objekte* sind in der Lage, untereinander zu kommunizieren bzw. können über eine Infrastruktur mit verschiedenen Anwendungssystemen kommunizieren. Werkzeuge, Bauteile und Werkzeugkästen sind im oben dargestellten Anwendungsszenario Beispiele für smarte Objekte. Der smarte Werkzeugkasten ist z.B. in der Lage, automatisch seinen Inhalt zu ermitteln und seinen Zustand dem Mechaniker mitzuteilen.

Der Mechaniker integriert sich durch seinen persönlichen tragbaren Computer, das PD, in die IT-Umgebung. Es erlaubt ihm, mit den smarten Objekten zu kommunizieren, auf die Datenbank zuzugreifen, z.B. um Handbücher einzusehen, und weitere Applikationen zu nutzen. Derartige Applikationen ermöglichen ihm beispielsweise die Reservierung von Werkzeugen bei der Werkzeugausgabe oder die Anforderung von Unterstützung bei der Durchführung von Aktivitäten. Außerdem

kann er sich durch das System über für ihn relevante Ereignisse informieren lassen.

Das PD kann ein beliebiger tragbarer Computer sein, der die folgenden Voraussetzungen erfüllt: (a) Das PD muss eine drahtlose Verbindung zur Ubiquitous-Computing-Infrastruktur herstellen können, (b) es benötigt ein gewisses Maß an Rechenkapazität, um eigenständig Anwendungen ausführen zu können, (c) es muss eine Benutzerschnittstelle besitzen, die es erlaubt, dem Mechaniker Informationen mitzuteilen, und es muss als Eingabemedium verwendbar sein.

Die *Ubiquitous-Computing-Infrastruktur* bildet den Kern der Lösungsarchitektur, der die Verbindung zwischen digitaler und physischer Welt ermöglicht. Sie stellt mehrere Dienste für darüberliegende Anwendungen zur Verfügung: (a) Identifikation, (b) Tracking, (c) Lokalisierung, (d) Benachrichtigungen der Mechaniker über ihre PDs. RFID-Chips an den Werkzeugen und Bauteilen ermöglichen die Dienste (a) bis (c). Der Zustand eines smarten Objekts wird in der Ubiquitous-Computing-Infrastruktur gespeichert und bei Bedarf an das Asset-Management-System weitergeleitet. Die Infrastruktur übernimmt außerdem die Kommunikation zwischen smarten Objekten und Mechanikern oder Anwendungen, d.h., die Kommunikation geht nicht vom smarten Objekt aus, sondern die Ubiquitous-Computing-Infrastruktur initiiert sie anhand von vordefinierten Geschäftsregeln. Um den Dienst (d) sicherzustellen, ist eine drahtlose Kommunikationsinfrastruktur wie z.B. Wireless LAN (WLAN) nötig. Beispiele für den Aufbau von Ubiquitous-Computing-Infrastrukturen, die auch in obigem Beispiel eingesetzt werden könnten, beschreiben u.a. Goyal [Goy03], Römer et al. [RSM04] und Kubach [Kub03].

2.2 Der smarte Werkzeugkasten

Der smarte Werkzeugkasten übernimmt die Aufgabe der Vollständigkeitskontrolle und benachrichtigt den Mechaniker, falls Werkzeuge fehlen, sich an der falschen Stelle befinden oder wenn der Mechaniker sie austauschen oder warten sollte. Die Applikation arbeitet weitgehend autonom, kann aber auch mit der Ubiquitous-Computing-Infrastruktur mittels WLAN kommunizieren, z.B. um Reports über Kontrollen oder den Status von Werkzeugen zu senden. Zur automatischen Überwachung des Inhalts sind alle Werkzeuge mit RFID-Chips gekennzeichnet. Außerdem protokolliert die Applikation die Nutzungshäufigkeit der Werkzeuge anhand der Häufigkeiten, mit denen die Mechaniker Werkzeuge entnehmen und zurücklegen. Das Werkzeugmanagementsystem empfängt diese Daten über die Ubiquitous-Computing-Infrastruktur und wertet sie aus.

Der smarte Werkzeugkasten integriert sich nahtlos in den MRO-Prozess. Das heißt, die Art und Weise, wie der Mechaniker den Werkzeugkasten bzw. die Werkzeuge verwendet, ändert sich nicht. Die Applikation entlastet den Mechaniker von aufwendigen Kontrollen und benachrichtigt ihn nur beim Auftreten von Fehlern. Im Rahmen des Projekts bei der Flugzeug AG haben die Autoren den smarten Werkzeugkasten prototypisch implementiert. Kleine kostengünstige passive RFID-Chips auf den Werkzeugen ermöglichten eine für die Identifikation innerhalb des Werkzeugkastens ausreichende Reichweite. Die Identifikations-

nummer auf den RFID-Chips setzte sich aus der Seriennummer des betreffenden Werkzeugs und der Seriennummer des zugehörigen Werkzeugkastens zusammen.

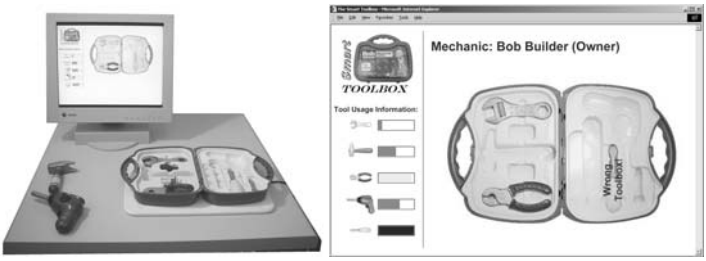


Abb. 5. Aufbau und Screenshot des Demonstrators zum smarten Werkzeugkasten

Der in Abbildung 5 dargestellte Demonstrator visualisiert den Status des Werkzeugkastens. Auf der Anzeige weist eine Markierung auf falsch einsortierte Werkzeuge hin. Bei der Implementierung haben die Autoren verschiedene Probleme identifiziert: (a) Da die meisten Werkzeuge aus Metall sind, benötigt die Lösung spezielle RFID-Systemkomponenten (z.B. ferritbeschichtete RFID-Chips, niedrige Übertragungsfrequenz). (b) Da der Werkzeugkasten aus Metall ist, ermöglichen nur innerhalb des Werkzeugkastens montierte Antennen eine zuverlässige automatische Identifikation. (c) Einige Werkzeuge sind so klein, dass ein zusätzlich angebrachter RFID-Chip bei der Verwendung der Werkzeuge stören würde.

2.3 Die smarte Werkzeugausleihe

Ähnlich wie beim smarten Werkzeugkasten verwendet die Werkzeugausgabe die RFID-Technologie. Jedes Werkzeug erhält zur eindeutigen Kennzeichnung einen RFID-Chip. RFID-Lesegeräte an der Ausgabe ermöglichen die automatische Erfassung der Werkzeuge. Alternativ wäre eine Kennzeichnung mittels eines Barcodes bzw. 2-D-Codes denkbar.

Zur Anforderung der Werkzeuge verwendet der Mechaniker sein PD, anhand dessen ihn auch die smarte Werkzeugausleihe identifiziert. Während der Mechaniker die ausgeliehenen Werkzeuge über die Theke schiebt, dokumentiert die Werkzeugausleihe den Vorgang automatisch. Ebenso erfasst diese die Werkzeuge bei der Rückgabe. Die Suche nach Werkzeugen ist bei dieser Applikation nicht mehr notwendig. Der Mechaniker kann den Ausleihstatus von Werkzeugen mittels seines PDs abfragen. Die smarte Werkzeugausgabe verwendet die Ubiquitous-Computing-Infrastruktur, um Mechaniker und Werkzeuge zu identifizieren, Anfragen nach Werkzeugen entgegenzunehmen und Nachrichten an Mechaniker zu schicken.

Der Demonstrator der smarten Werkzeugausgabe ist ein erster Schritt zu einer vollständig automatisierten Lösung. Die Bedienung durch den Werkzeugmeister ist dabei weiterhin notwendig. Ein RFID-Lesegerät mit einer Antenne befindet sich am Ausgabeschalter (siehe Nr. 1 in Abbildung 6), um die Werkzeuge, welche

die Mechaniker über die Theke schieben, eindeutig zu identifizieren. Die weiteren Verarbeitungsschritte veranlasst das System. Es überprüft für jedes Werkzeug den Ausleihstatus. Bei ausgeliehenen Werkzeugen initiiert es den Rückgabeprozess, andernfalls den Ausleihprozess. Die Aktionen des Systems visualisiert ein Bildschirm (siehe Nr. 2 in Abbildung 6).

Abb. 6. Smarte Werkzeugausgabe mit RFID-Antenne (Nr. 1) und Bildschirm (Nr. 2)

Die Anwendung besteht aus drei Teilen: (a) der Auto-ID-Infrastruktur, welche die Identifikation von Mechanikern und Werkzeugen ermöglicht, (b) der Client-Applikation, welche die Identifikationsereignisse verarbeitet und die Ausleihe bzw. Rückgabe steuert, sowie (c) der Web-Applikation, die den Status von Werkzeugen bereitstellt. Die Client-Applikation ist über das Internet mit dem Werkzeugmanagementsystem verbunden. Das Werkzeugmanagementsystem ist auf einem SAP Web Application Server implementiert, und die Verbindung stellt, wie im nächsten Abschnitt beschrieben, der SAP Business Connector her.

2.4 Integration mit SAP

Der Demonstrator für den smarten Werkzeugkasten ist ein Beispiel für ein eigenständiges RFID-System, das auch ohne Infrastruktur oder Backend-Systeme funktioniert. Für viele Anwendungen existieren jedoch schon IT-Systeme mit etabliertem Funktionsumfang, z.B. ERP-Systeme zur Abwicklung von Kundenaufträgen, zur Bestellung von Material und zur Verwaltung von Assets. In diesem Fall ist es sinnvoll, diese Systeme um die Möglichkeiten der RFID-Technologie zu erweitern, statt ein zusätzliches System zu installieren. Die RFID-Technologie, bzw. eine Middleware, übernimmt hierbei die Aufgabe der automatischen Identifikation von Objekten. Die Geschäftslogik stellt das ERP-System zur Verfügung.

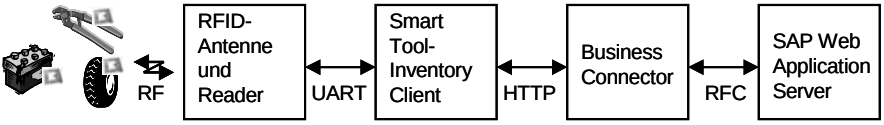


Abb. 7. Integration der smarten Werkzeugausleihe mit SAP

Die Flugzeug AG plante zur Zeit der Entwicklung der hier vorgestellten Lösungen auch die Einführung von SAP R/3 im Wartungsbetrieb. Aus diesem Grund stellte die Flugzeug AG die Anforderung, dass eine Integration der smarten Lösungen mit dem SAP-System möglich sein muss. Der Demonstrator zur smarten Werkzeugausleihe berücksichtigt diese Anforderung und unterstützt die Integration mit einem SAP-System.

Die Anwendung befindet sich auf einem SAP Web Application Server. Dieser verwaltet auch die Benutzer- und Werkzeugstammdaten sowie die Ausleih- und Wartungsdaten. Die Anwendung unterstützt Funktionen zum Einpflegen, Ändern oder Löschen von Werkzeugen oder Benutzern sowie zum Ausleihen, zur Rückgabe und zur Abfrage nach ausgeliehenen Werkzeugen sowie zur Durchführung der Wartung. Diese Funktionen stellt der Web Application Server per RFC (Remote Function Call) auch anderen Anwendungen zur Verfügung.

```
<?xml version="1.0" ?>
  <inventory inventoryID="INV1">
     <mechanic mechID="D019200" />
     <action>A</action>
     <items>
       <item toolid="888-AA" />
       <item toolid="926-AA" />
       <item toolid="111-BB" />
      </items>
  </inventory>
```

Abb. 8. XML-File zur Übergabe an den Business Connector

Der im obigen Abschnitt beschriebene Client, der diese Funktionen an der Werkzeugausgabe den Mechanikern zur Verfügung stellt, kommuniziert mittels XML-Daten, die er per HTTP an die Anwendung schickt. Zur Übersetzung der Daten verwendet die Lösung den SAP Business Connector, der XML-Anfragen in RFC-Aufrufe übersetzt und die Antwort im XML-Format zurück an den Client schickt (siehe Abbildung 7). Eine grafische Benutzeroberfläche erleichtert die Konfiguration des Business Connectors. Hierbei lassen sich die Funktionsargumente der Anwendung Bezeichnern zuordnen, die das XML-Dokument zur Bezeichnung der entsprechenden Objekte verwenden. Abbildung 8 stellt ein Beispiel eines XML-Dokuments dar, das die smarte Werkzeugausleihe veranlasst, die Ausleihe der drei Werkzeuge mit den Signaturen 888-AA, 926-AA und 111-BB aus der Werkzeugausleihe mit der Nummer INV1 an den Mechaniker mit der Personalnummer D019200 vorzunehmen.

3 Wirtschaftlicher Nutzen

Das in Abschnitt 2.1 dargestellte Anwendungsszenario beschreibt einen im Vergleich zur Ausgangssituation wesentlich effizienteren MRO-Prozess. Ein wirtschaftlicher Nutzen kann für die Flugzeug AG aus folgenden Vorteilen resultieren:

- **Vermeidung von Verzögerungen.** Sorgfältige Planung unter Berücksichtigung der verfügbaren Ressourcen trägt dazu bei, Verzögerungen während des MRO-Prozesses zu vermeiden. Suchaktionen können entfallen. Durch eine regelmäßige Wartung von Werkzeugen lassen sich Schäden durch schadhafte Werkzeuge vermeiden. Insgesamt reduziert dies das Risiko für ungeplante Wartungszeiten.
- **Vermeidung von durch Menschen verursachten Fehlern.** Die Anleitung des Mechanikers mittels PD trägt dazu bei, durch Menschen verursachte Fehler zu vermeiden. Das Gerät stellt sicher, dass die Mechaniker die richtigen Aktivitäten ausführen, die richtigen Bauteile und Werkzeuge verwenden, sowie keine Werkzeuge an die falsche Stelle legen. Insgesamt führt dies zu einer höheren Qualität und Sicherheit des MRO-Prozesses.
- **Automatisierte Dokumentation.** Einzelne Arbeitsschritte, die Verwendung von Werkzeugen sowie Vollständigkeitskontrollen dokumentiert das System automatisch. Dies stellt die Korrektheit und Vollständigkeit der Dokumentation und damit auch die Einhaltung der gesetzlichen Vorschriften sicher und hilft, zeitaufwendige manuelle Tätigkeiten zu vermeiden. Zusätzlich dient die Dokumentation als zuverlässige Planungsgrundlage folgender MRO-Tätigkeiten:
- **Effizienter Einsatz von Ressourcen.** Der Einsatz von Mitarbeitern, Bauteilen und Werkzeugen erfolgt geplant und überwacht. Dies trägt zur Minimierung unproduktiver Tätigkeiten wie Suchaktionen und Wartezeiten bei. Die unmittelbare Rückgabe der Werkzeuge an die Werkzeugausgabe nach dem Gebrauch hilft, den Werkzeugbestand zu optimieren und führt zu Einsparungen an selten genutzten Werkzeugen.
- **Benutzerfreundlichkeit.** Das eingesetzte Anwendungssystem unterstützt den MRO-Prozess im Hintergrund. Das heißt, der Mechaniker kann sich auf die MRO-Tätigkeiten konzentrieren, während verschiedene Systeme zusammenarbeiten, um Aufgaben wie die Dokumentation, das Werkzeugmanagement oder die Teilebeschaffung zu erleichtern. Das PD ist ein intuitiv zu bedienendes multifunktionales Gerät, das der Mechaniker immer bei sich hat, und das ihn bei allen Tätigkeiten unterstützt.

Zur monetären Bestimmung des wirtschaftlichen Nutzens des smarten Werkzeugkastens und der smarten Werkzeugausgabe stellen nachfolgende Abschnitte die quantifizierbaren Nutzenpotenziale den Kosten für Implementierung und Betrieb gegenüber.

3.1 Kosten-Nutzen-Analyse des smarten Werkzeugkastens

Wesentliche Nutzenpotenziale des smarten Werkzeugkastens bestehen in der Beschleunigung und Sicherstellung der Kontrollen, in der Vermeidung von Suchaktionen nach Werkzeugen, die sich nach Abschluss einer Reparatur nicht im Werkzeugkasten befinden, sowie in der Einsparung der manuellen Markierung. Diese Nutzenpotenziale lassen sich mit Hilfe von plausiblen Annahmen quantifizieren:

- Die Arbeitsstunde eines Mechanikers kostet 70 EUR.
- Die Mechaniker müssen die Werkzeugkästen und deren Inhalt einmal bei Neuanschaffung und dann alle 1,5 Jahre markieren. Die Lebensdauer eines Werkzeugkastens beträgt 6 Jahre. Die Markierung dauert 2 Manntage (16 Stunden), das entspricht bei 60 Werkzeugkästen einem Arbeitsaufwand von ca. 640 Stunden (44 800 EUR) pro Jahr.
- Die wöchentliche gründliche Kontrolle dauert für zwei Mechaniker je eine Stunde pro Werkzeugkasten. Bei insgesamt 60 Werkzeugkästen und 46 Arbeitswochen im Jahr ergibt sich ein jährlicher Aufwand von 5 520 Stunden (386 800 EUR).
- Pro Jahr vermeidet der smarte Werkzeugkasten 3 Stunden an ungeplanter Wartungszeit bei Passagierflugzeugen. Der Kunde spart hierdurch Opportunitätskosten in Höhe von 69 000 EUR.

Folgende Kosten entstehen durch die Verwendung des RFID-Systems:

- Die Abschreibungsfrist beträgt 6 Jahre.
- Die RFID-Kennzeichnung führen die Hersteller zu einem Preis von durchschnittlich 1 EUR pro Werkzeug (Kosten für den Chip und die Anbringung) durch. Die Ausstattung eines Werkzeugkastens mit einem Lesegerät und Antennen kostet 2 000 EUR. Für 60 Werkzeugkästen entstehen jährliche Kosten von 21 500 EUR.
- Die Flugzeug AG setzt vier Schreib-/Lesestationen zur Auswertung der Werkzeugdaten ein, die pro Stück 1 500 EUR kosten. Dies entspricht jährlichen Kosten von 1 000 EUR.
- Der geschätzte Wartungsaufwand der Installation beträgt 150 Arbeitsstunden jährlich. Dies verursacht Kosten in Höhe von 10 500 EUR.

Unter den getroffenen Annahmen betragen die jährlichen Kosten 33 000 EUR, denen Kosteneinsparungen durch die Lösung von 500 600 EUR gegenüberstehen. Noch nicht berücksichtigt sind hierbei schwer quantifizierbare Nutzenpotenziale wie die höhere Sicherheit sowie der bessere Kundenservice. Andererseits kann die Flugzeug AG die errechneten Kosteneinsparungen nur dann erzielen, wenn die Einsparungen der Arbeitszeiten für die Kontrolle auch tatsächlich zu einer Reduktion bezahlter Arbeitsstunden führen. Es erscheint wenig realistisch, dass die Flugzeug AG durch den Wegfall der Kontrollen insgesamt tatsächlich weniger Mechaniker benötigt. Wahrscheinlicher ist, dass die Mechaniker in dieser Zeit für die Durchführung von MRO-Aktivitäten zur Verfügung stehen.

3.2 Kosten-Nutzen-Analyse der smarten Werkzeugausleihe

Die wesentlichen Nutzenpotenziale der smarten Werkzeugausleihe bestehen in der Vermeidung von Suchaktionen nach Werkzeugen, einer effizienteren Nutzung der Werkzeuge und der Sicherstellung rechtzeitiger Instandsetzung bzw. Ersatzes. In Ergänzung zu den Annahmen aus dem vorangegangenen Abschnitt gilt:

- Die Arbeitsstunde des Werkzeugmeisters kostet 70 EUR.
- Pro Woche suchen Mechaniker und Werkzeugmeister drei Stunden nach Werkzeugen. Das entspricht einem jährlichen Arbeitsaufwand von 52 Stunden (3 640 EUR).
- Die Flugzeug AG kann ihren Bestand an Werkzeugen um 5 % senken. Bei einem durchschnittlichen Wert eines Werkzeugs von 10 EUR und einem Werkzeugbestand von 1 200 entspricht dies jährlichen Kosteneinsparungen in Höhe von 100 EUR.
- Dadurch, dass stets die richtigen Werkzeuge in gutem Zustand verfügbar sind, verringert sich die ungeplante Wartungszeit bei Passagierflugzeugen um eine Stunde im Jahr. Damit sparen die Kunden Opportunitätskosten in Höhe von 23 000 EUR ein.

Folgende Annahmen gelten für die Kosten der smarten Werkzeugausgabe:

- Die Abschreibungsfrist beträgt 6 Jahre.
- Die RFID-Kennzeichnung führen die Hersteller zu einem Preis von durchschnittlich 1 EUR pro Werkzeug durch. Das Lesegerät und die Antenne für die Werkzeugausgabe kosten 2 000 EUR. Das ergibt bei 1 200 Werkzeugen jährliche Kosten in Höhe von 535 EUR.
- Der geschätzte Wartungsaufwand der Installation beträgt 50 Arbeitsstunden jährlich, was Kosten in Höhe von 3 500 EUR verursacht.

Unter den getroffenen Annahmen betragen die jährlichen Kosten ca. 4 035 EUR. Diesen stehen Kosteneinsparungen von ca. 30 000 EUR gegenüber. Genauso wie für den smarten Werkzeugkasten sind auch hierbei die schwer quantifizierbaren Nutzenpotenziale nicht berücksichtigt und es ist nicht sicher, ob die eingesparten Arbeitsstunden in gleicher Höhe zu Einsparungen bei den Kosten führen.

4 Fazit

Das in diesem Beitrag vorgestellte Anwendungsszenario zeigt, dass der Einsatz der RFID-Technologie zur Unterstützung des MRO-Prozesses in der Flugzeugwartung sinnvoll ist. Die vorgeschlagene „smarte“ Lösung stellt sicher, dass der Wartungsbetrieb die Regeln bzgl. Sicherheit und Qualität einhält sowie Prozesse und Ressourceneinsatz effizient sind. Sie trägt auch dazu bei, die Dauer ungeplanter Wartungen zu minimieren. Hierbei agiert die Technologie im Hintergrund. Mobile Geräte und smarte Objekte sind mittels einer ubiquitären Infrastruktur

auch mit klassischen ERP-Systemen verbunden. In der vorgestellten Lösung dient ein mobiles Gerät als multifunktionale Benutzerschnittstelle zum System.

Der Beitrag hat sowohl die technische Machbarkeit als auch den wirtschaftlichen Nutzen der vorgestellten Lösungen gezeigt. Dennoch existieren einige Herausforderungen technischer sowie organisatorischer Art, die vor einem Einsatz der Lösung im operativen Betrieb zu überwinden sind:

(a) Die Leistung passiver RFID-Systeme wird in einem metallischen Umfeld stark eingeschränkt. Allerdings lässt sich durch die Verwendung spezieller RFID-Tags eine funktionierende Lösung implementieren. Diese Chips sind mit Ferrit beschichtetet und verwenden eine niedrige Kommunikationsfrequenz. Hierbei zeigt sich, dass beim Erstellen von Lösungen mit Technologien des Ubiquitous Computing zusätzlich zu IT-Kenntnissen auch Ingenieurkenntnisse notwendig sind. Im konkreten Fall betrifft das die Integration der RFID-Chips in die Werkzeuge und die Einstellung der Antennen.

(b) Für Infrastrukturen des Ubiquitous Computing haben sich noch keine Standards zur Integration von Auto-ID-Technologien oder für die Modellierung von smarten Objekten durchgesetzt. Aus diesem Grund verursacht die in diesem Beitrag vorgeschlagene Lösung einen zusätzlichen Integrationsaufwand.

(c) Das vorgestellte Szenario findet im abgeschlossenen Bereich der Flugzeug AG statt. Eine wesentliche Voraussetzung für die Wirtschaftlichkeit der Anwendung sind Standards zur Produktidentifikation [KäH02]. Hierzu müssten bei der vorgestellten Lösung bereits die Hersteller der Bauteile bzw. Werkzeuge die RFID-Chips anbringen. Diese Voraussetzung könnte eine Auto-ID-Infrastruktur schaffen, wie sie beispielsweise das Auto-ID Lab am MIT entwickelt hat. Dieses Konzept beinhaltet nicht nur ein Nummerierungsschema, den so genannten Electronic Product Code (EPC), sondern umfasst auch technische Spezifikationen, z.B. die Spezifikationen von RFID-Chips, RFID-Lesegeräten und der Datenkommunikation sowie Aspekte des Datenmanagements und der Middleware, z.B. die so genannte Physical Markup Language (PML) und die Software Savant. Durch die Verwendung einer standardisierten Infrastruktur könnte das vorgestellte Szenario auf die gesamte Wertkette in der Flugzeugindustrie ausgeweitet werden, die Zulieferer, Hersteller und Dienstleistungsunternehmen umfasst.

Die Identifikation weiterer Anwendungsfälle, die von einer Ubiquitous-Computing-Infrastruktur und entsprechender Basisfunktionen für das Asset Management profitieren könnten, erscheint vielversprechend. Beispielsweise könnte die Flugzeug AG durch die Integration mit dem Asset-Management-System SAP-PLM zusätzlichen Nutzen erzielen. Dieses System ermöglicht das Management des Werkzeuglebenszyklus und steuert notwendige Wartungen der Werkzeuge und die Ersatzbeschaffung.

Literatur

[ATA03] Air Transport Association iSpec 2200 (2003) Maintenance Standards for Aviation Maintenance, www.air-transport.org/public/publications/display1.asp?nid=956

[Bro03] Brown P (2003) Companies get creative in their Inventory Management Solution. Aviation Now, April 15, 2003

[Goy03] Goyal A (2003) The Savant – Technical Manual. Auto-ID Center Technical Report, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-TR015.pdf

[GSB00] Gellersen HW, Schmidt A, Beigl M (2000) Adding Some Smartness to Devices and Everyday Things. IEEE Workshop on Mobile Computing Systems and Applications, Monterrey, USA, IEEE Press, pp 3–10

[KäH02] Kärkkäinen M, Holström J (2002) Wireless product identification: enabler for handling efficiency, customation and information sharing. Supply Chain Management 7(4): 242–252

[Kär03] Kärkkäinen M (2003) Increasing efficiency in the supply chain for short life goods using RFID tagging. International Journal of Retail & Distribution Management 31(10): 529–536

[Kub03] Kubach U (2003) Integration von Smart Items in Enterprise-Software-Systeme. HMD - Praxis der Wirtschaftsinformatik 229: 56–67

[SFL04] Strassner M, Fleisch E, Lampe M (2004) Ubiquitous Computing Environment for Aircraft Maintenance. ACM Symposium on Applied Computing

[Mec99] Mecham M (1999) Software Solutions Making MRO ‘Smarter’. Aviation Week & Space Technology 151(9): 44–45

[RSM04] Römer K, Schoch T, Mattern F, Dübendorfer T (2004) Smart Identification Frameworks for Ubiquitous Computing Applications. Wireless Networks 10(6): 689–700

[Wei91] Weiser M (1991) The Computer of the 21st Century. Scientific American 265(3): 94–104

Zahlungsverfahren mit Ubiquitous Computing

Sandra Gross
Institut für Technologiemanagement, Universität St. Gallen

Matthias Lampe
Institut für Pervasive Computing, ETH Zürich

René Müller
UBS AG, Zürich

Kurzfassung. Ubiquitous-Computing-Technologien ermöglichen die Entwicklung neuer Zahlungsverfahren. Dieser Beitrag beleuchtet den Unterschied zwischen mobilem Bezahlen (M-Payment) und ubiquitärem Bezahlen (U-Payment). Dazu analysiert er aus der Sicht von Banken und Finanzdienstleistern Anforderungen, Technologien und Anwendungsbeispiele. Die Autoren erläutern die Ergebnisse anhand der Entwicklung einer U-Payment-Testplattform, die verschiedene Zahlungsverfahren mit Ubiquitous Computing umsetzt.

1 Einleitung

Ubiquitous-Computing-(UbiComp-)Technologien ermöglichen die Weiterentwicklung mobiler Zahlungsverfahren (M-Payment). Ein Beispiel für eine ubiquitäre Technologie ist die Radio Frequency Identification (RFID). Mobiltelefone können mit einem RFID-Transponder versehen werden, der kundenindividuelle Bezahlinformationen speichert. Kassensysteme mit integrierten RFID-Lesegeräten lesen diese drahtlos und automatisch aus und ermöglichen somit neue Anwendungen.

Banken haben in der Vergangenheit trotz guter Marktprognosen schon schlechte Erfahrungen mit der Wirtschaftlichkeit mobiler Zahlungsverfahren gemacht. Deshalb ist es Ziel dieses Beitrags, einerseits ubiquitäre Zahlungsverfahren vorzustellen und andererseits diese aus Sicht von Finanzdienstleistern zu bewerten. Dazu werden im Folgenden Anforderungen und Technologien von U-Payment vorgestellt und mit Beispielen aus der Praxis verdeutlicht.

Der Beitrag ist wie folgt aufgebaut: Da es für Zahlungsverfahren mit UbiComp noch keine einheitliche Definition gibt, grenzt der folgende Abschnitt den Begriff U-Payment gegen M-Payment ab. Danach werden die Anforderungen an eine Bezahlarchitektur aus den Sichten unterschiedlicher Marktteilnehmer untersucht. Die nachstehenden zwei Abschnitte evaluieren zum einen die im M-Lab-Projekt entwickelte Testarchitektur BluePay, die ausgewählte Ansprüche umsetzt, und

zum anderen bestehende Herausforderungen in der Praxis bei einer Einführung von ubiquitären Zahlungsverfahren.

2 Vom M-Payment zum U-Payment

Dieser Abschnitt zeigt eine mögliche Entwicklung vom M-Payment zum U-Payment auf. Dazu werden jeweils Definitionen und Anwendungsfelder der Verfahren zusammengefasst.

Das *M-Payment* ist ein mobiler Zahlungsvorgang, bei dem zumindest einer der Teilnehmer ein mobiles Endgerät benutzt. Dies ist häufig ein Mobiltelefon [Kru01, IWW02, KPT02]. Andere Geräte für das mobile Bezahlen sind beispielsweise Personal Digital Assistants (PDA) oder Gegenstände, in die Transponder integriert sind und die Daten per Funk an ein Lesegerät übertragen.

Mobile Zahlungsverfahren können in folgenden Bereichen eingesetzt werden [ITW02]:

- Automatische Kassensystemzahlungen (point-of-sale, POS) wie z.B. Verkaufsautomaten, Parkscheinautomaten oder Ticketautomaten,
- betreute POS-Zahlungen, z.B. in Geschäften oder in Taxis,
- direkte mobile Bezahltransaktionen im Internet über ein mobiles Endgerät (z.B. per wireless application protocol, WAP),
- mobil unterstützte Bezahltransaktionen im Internet wie Telefonanrufe als Alternative zur Kreditkarte,
- Geldtransfers zwischen Personen (peer to peer transactions).

Die Autoren verstehen unter *U-Payments* Zahlungen, welche den Kriterien des UbiComp entsprechen. UbiComp bedeutet, dass Computer allgegenwärtig, für den Benutzer unsichtbar und in der Umgebung integriert sind. Dementsprechend wird U-Payment als das allgegenwärtige, unsichtbare und in die Umgebung integrierte Bezahlen definiert. Die mobilen Zahlungssysteme unterscheiden sich hiervon durch menschliche Interaktion. Systeme mit wenig oder ganz ohne Interaktion des Menschen kommen der Definition des U-Payments in diesem Beitrag am nächsten.

Die Prozesse, die den Bezahlvorgang auslösen, dürfen nicht durch diesen unterbrochen werden, es sei denn, der Bezahlvorgang hängt mit einer Prozessänderung zusammen. Dies könnte beispielsweise der Fall sein, wenn bei der Wartung ein Maschinenteil ausgewechselt wird, und das neue Teil automatisch den Bezahlvorgang veranlasst. Ein anderes Beispiel stellen Zahlungen zwischen Unternehmen dar, bei denen eine automatische Zahlung durch eine Echtzeitmeldung an das ERP-System des Großhändlers angestoßen werden könnte, sobald eindeutig identifizierbare Paletten den Wareneingang des Kunden passieren. Anwendungsbeispiele im Endkundenbereich sind die automatische Autobahngebühr oder in Zukunft das automatische Bezahlen im Supermarkt. Diese Bezahlungen finden immer in vordefiniertem Rahmen statt oder zusätzlich durch Abfrage einer aktiven Bestätigung durch den Kunden.

Die Beratungsfirma Accenture erstellte beispielsweise ein U-Payment-Szenario, bei dem Objekte den Zahlungsvorgang einleiten. Dieses basiert auf der Annahme, dass in Zukunft neben dem Verkauf von Produkten der Verkauf von Dienstleistungen an Bedeutung gewinnen wird, die mit dem Produkt zusammenhängen [DSt01]. Dazu werden Alltagsgegenstände oder industrielle Güter mit RFID-Transpondern und Sensoren versehen, die miteinander kommunizieren können. Verknüpft man diese RFID-Infrastruktur mit einer Micro-Payment-Infrastruktur, dann können die Objekte zusammen agieren und Bezahlvorgänge auslösen. Die Objekte sind kontextsensitiv und führen entsprechend festgelegter Regeln Kaufaktionen durch [Acc02]. Der Benutzer kann sich dann auf den Gebrauch der Gegenstände konzentrieren anstatt auf den Bezahlvorgang [DSt01].

Ein weiteres Beispiel ist Speedpass. Das System wurde von Exxon Mobil eingeführt und existiert in den USA seit 1997. Heute rechnet das Unternehmen mit mehr als 6 Millionen aktiver Kunden, die mit RFID-Transpondern ausgestattete Armbanduhren tragen oder Autoschlüsselanhänger mit dieser Technologie besitzen. In den USA akzeptieren über 7 500 Geschäfte und Tankstellen den Speedpass von Exxon Mobil als Zahlungsmittel. In Chicago und in Nordwest-Indiana kann in über 440 Schnellrestaurants damit bezahlt werden. 92 % der Speedpass-Benutzer geben an, mit dem System sehr zufrieden zu sein. Viele Tankstellen verkauften seit der Einführung von Speedpass 15 % mehr Benzin und es wurde in 18 % aller Fälle mit Hilfe dieser Technologie bezahlt. In den Geschäften hat sich der Umsatz um 4 % erhöht [Exx02].

Abb. 1. Bezahlen mit der Speedpass-RFID-Timex-Uhr[52]

Speedpass ist sehr einfach zu bedienen: Zum Bezahlen wird der Transponder einfach vor einen Leser gehalten (vgl. Abbildung 1). Er speichert nur eine eindeutige Identifikationsnummer und keine Kreditkartennummer. Die Autorisierung der Zahlung wird von Speedpass initiiert, wobei Speedpass die Verbindung zum Kreditkartenherausgeber herstellt.

[52] www.speedpass.com

3 Anforderungen an eine U-Payment-Architektur

Eine hohe Marktdurchdringung von U-Payment kann nur erreicht werden, wenn man von den kritischen Erfolgsfaktoren für mobile Zahlungssysteme lernt. Diese müssen in Abhängigkeit vom Marktteilnehmer betrachtet werden. Die Erfolgsfaktoren variieren aus Sicht der Kunden, der Händler oder der Banken.

Tabelle 1. Anforderungen an eine U-Payment-Architektur aus Bankensicht [MoF00]

Art der Anforderung	Beschreibung
Geschäftliche Prioritäten	• Die Banken authentifizieren einen Benutzer, damit er deren Bankdienstleistungen bzw. Zahlungssysteme nutzen kann. • Die Finanzdienstleistung bringt einen Mehrwert für alle beteiligten Parteien. • Geschäftsprozesse der unterschiedlichen Parteien müssen unabhängig voneinander sein. • Das Zahlungsverfahren kann um weitere Finanzdienstleistungen erweitert werden. • Bei mehreren an der Lösung beteiligten Geschäftspartnern kann jeder Partner sein Markenzeichen verwenden.
Technische Aspekte	• Die Lösung muss auf offenen Standards basieren und nichtproprietäre Technologien implementieren. • Bereits bestehende Standards sollen genutzt und wo immer möglich eingesetzt werden. • Die technische Lösung darf keine Abhängigkeiten zwischen der Bank, dem Betreiber und Endgeräten schaffen. • Es muss eine End-to-end-Sicherheit garantiert werden (Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit).
Implementierungsaspekte	• Die Implementierungskosten bei der Bank, dem Händler und dem Benutzer sollen möglichst tief gehalten werden. • Die Produkteinführungszeit ist einer der kritischsten Faktoren zur Sicherung des Erfolgs neuer Finanzdienstleistungen bzw. Zahlungssysteme.
Sicherheitsaspekte	• Grundanforderungen sind die Plattform-Sicherheit auf dem Endgerät sowie die sichere Übertragung von Daten. • In Zukunft sollen standardmäßig digitale Zertifikate zur Signierung von Transaktionen verwendet werden.

Die Anforderungen der *Kunden* betreffen mehrere Aspekte: Zunächst muss das Zahlungsverfahren für den Benutzer zweckmäßig und einfach zu bedienen sein. Es zeichnet sich idealerweise durch eine niedrige Komplexität aus, der Möglichkeit, dass der Teilnehmer das Verfahren testen kann, dass es einen hohen Verbreitungsgrad bei Händlern und Geschäften aufweist und dass es einen hohen Grad an Komfort besitzt. Der Teilnehmer hat zudem die Freiheit, die Bank, den Betreiber und das Endgerät zu wählen. Dem Kunden wie auch dem Händler muss eine möglichst hohe Sicherheit in Bezug auf Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit bei der Nutzung mobiler Finanzdienstleitung geboten werden.

Von Vorteil ist auch die Möglichkeit, das Verfahren anonym zu benutzen [HGF03, MoF00].

Der Erfolg des Systems hängt ebenfalls von der Kooperationsbereitschaft der *Händler* ab. Diese verlangen beispielsweise eine Einhaltung von Standards, einen geringen Installationsaufwand und geringe Kosten sowie eine effiziente Zahlungsabwicklung.

Banken und Finanzdienstleister andererseits erwarten ein geringes Transaktionsrisiko, Unabhängigkeit vom Betreiber und eine einfache Integration in vorhandene Systeme. Ist es beispielsweise nicht möglich, eine Lösung einfach und mit geringem Kostenaufwand in bestehende Systemlandschaften zu integrieren, kann nur schwer eine große und damit Erfolg versprechende Marktdurchdringung erreicht werden (vgl. Tabelle 1).

4 Die U-Payment-Architektur BluePay

Die U-Payment-Architektur BluePay ist eine Testplattform für Zahlungsverfahren mit Ubiquitous Computing. Sie verwendet die Technologien Bluetooth und RFID im lokalen Zahlungsverkehr. Es wurden insbesondere drei Anforderungen umgesetzt: erstens die Verwendung von offenen und bereits eingesetzten Standards wie Bluetooth und RFID, zweitens keine Abhängigkeiten zwischen Händlern und Finanzdienstleistern, da die Plattform das bestehende Finanznetzwerk zur Zahlungsabwicklung verwendet, und drittens ein geringer Implementierungsaufwand durch Anpassungen auf der Clientseite, aber nicht serverseitig.

Die Testplattform baut auf der Preferred Payment Architecture (PPA) auf, die im Rahmen des Mobey-Forums erarbeitet wurde [MoF00]. Das Mobey-Forum vertritt die Anliegen von Finanzinstituten im Bereich mobiler Dienstleistungen und diskutiert diese mit Standardisierungsgremien, Herstellern von mobilen Endgeräten, Betreibern, Beratern und Lösungsanbietern. Die vom Mobey-Forum beschriebene PPA soll keinen komplett neuen Standard definieren, sondern vielmehr eine auf den verschiedensten Standards aufbauende und auf mobile Finanzdienstleistungen angepasste, offene Architektur beschreiben. Durch die Einflussnahme in anderen Interessensvereinigungen strebt das Mobey-Forum breit abgestützte Standards an, die von Finanzdienstleistern, Geräteherstellern und Mobilfunk-Betreibern anerkannt werden. Die PPA ist technologieunabhängig konzipiert. Sie gilt somit nicht nur für das M-Payment, sondern kann auch für U-Payments angewendet werden.

Auf der U-Payment-Architektur Bluepay wurden unterschiedliche Demonstratoren implementiert, die sich für verschiedene Zahlungsanwendungen einsetzen lassen, beispielsweise im Supermarkt oder im öffentlichen Nahverkehr. Das Ziel der Demonstratoren ist es, U-Payment-Systeme zu testen, die mit Hilfe dieser Technologien realisiert sind. Hierbei interessiert insbesondere, inwieweit sich die explizite Interaktion des Kunden im Verlauf des Zahlungsvorgangs reduzieren oder sogar eliminieren lässt.

4.1 Preferred Payment Architecture

Die PPA setzt unterschiedliche Kategorien von Zahlungssystemen um (vgl. Tabelle 2). Dabei bedeutet realer POS, dass ein Kunde vor Ort bezahlt, z.B. in einem Geschäft an der Kasse. Im Gegensatz dazu bezieht sich der virtuelle POS auf Zahlungen im Internet. Da sich die Testplattform Bluepay auf den grau hinterlegten Bereich stützt, wird im Folgenden die PPA für Zahlungen am realen POS beschrieben. Informationen über die Umsetzung des virtuellen POS finden sich in [MoF00]. Anhand der Unterscheidung in Mikro- und Makrozahlungen können in der PPA unterschiedliche Sicherheitsstufen implementiert werden. Dieser Aspekt blieb bei Bluepay zunächst unberücksichtigt.

Tabelle 2. Typische gekaufte Produkte nach Art des Zahlungssystems [MoF00]

	Realer POS	Virtueller POS
Mikrozahlungen (bis ca. 10 EUR)	Physische Produkte, z.B. • Straßenbahnfahrkarte, • Parkschein, • Getränk am Automaten.	Digitaler Inhalt, z.B. • Elektronische Bilder, • Klingeltöne, • Logos für Mobiltelefone.
Makrozahlungen (ab ca. 10 EUR)	Physische Produkte, z.B. • Kinoticket, • Supermarktartikel.	Physische Produkte, z.B. • CDs, • DVDs, • Bücher. Digitaler Inhalt, z.B. • Zeitschriften-Abonnemente, • Marktdaten.

Lokale, mobile Transaktionen bieten unterschiedliche Möglichkeiten zum Einsatz von Mobiltelefonen als digitale Geldbörse. Als Hauptanforderungen an lokale Zahlungen gelten die Benutzerfreundlichkeit, die Sicherheit einer Zahlung und die Verlässlichkeit des Systems.

Als Architektur für lokale Zahlungen in der PPA wird eine von der Bank ausgegebene Chipkarte vorgeschlagen, auf der die entsprechende Zahlungsmethode eingebettet ist (vgl. Abbildung 2). Die Chipkarte basiert auf dem EMV-Standard, wobei die Abkürzung EMV für die drei kartenherausgebenden Unternehmen Europay, Mastercard und Visa steht. Zur Umsetzung lokaler Transaktionen werden drahtlose Technologien verwendet. Bluetooth wird beispielsweise eingesetzt, wenn größere Datenmengen zwischen einem Kassensystem des Händlers und einem mobilen Endgerät bidirektional ausgetauscht werden. Andere Prototypen von innovativen Zahlungssystemen verwendeten für lokale Transaktionen RFID zur Identifikation des Kunden.

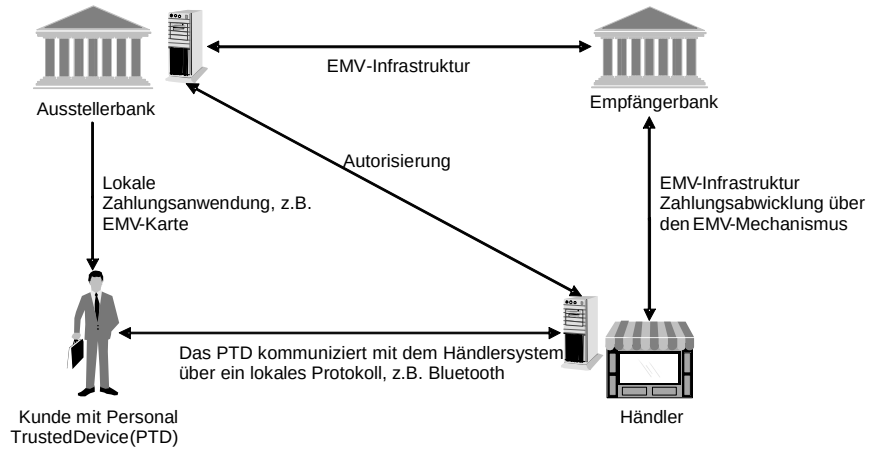


Abb. 2. PPA für Zahlungen am realen POS

4.2 Bluepay

Dieser Abschnitt geht von dem Szenario aus, dass der Kunde im Supermarkt bezahlt. Die Waren sind mit RFID-Transpondern eindeutig gekennzeichnet. Der Kunde legt die Produkte auf das Band, sodass das Kassensystem die Waren automatisch erkennt und den Warenwert für den Zahlungsvorgang berechnet.

Das Ziel der Demonstratoren war es, U-Payment-Systeme mit RFID und Bluetooth zu testen. Hierbei interessierte insbesondere, inwieweit sich die explizite Interaktion des Kunden im Verlauf des Bezahlvorgangs reduzieren oder sogar eliminieren lässt. Dazu wurden zwei Varianten betrachtet: Im ersten Fall reicht eine Identifizierung des Kunden zur Bezahlung aus, im zweiten findet ein Austausch lokaler Benutzerinformation statt.

Identifizierung zur Bezahlung

Bei denjenigen Anwendungen, bei denen das System nur Identifikationsinformationen auf dem mobilen Endgerät des Kunden speichert, befinden sich alle weiteren Bezahlinformationen wie Kreditkarteninformationen in einer Datenbank, zum Beispiel im Backend-System des Händlers (vgl. Abbildung 3).

Die Bezahlung wird durch die eindeutige Identifizierung des Kunden initiiert. Der Identifikationsmechanismus, beim Demonstrator ein RFID-Transponder mit eindeutiger Identifikationsnummer, kann dabei in einem Gegenstand untergebracht sein, den der Kunde normalerweise bei sich trägt, wie seine Armbanduhr oder sein Mobiltelefon. Das Kassensystem integriert einen RFID-Leser mit Antenne. Die Bezahlinformationen aus der Kundendatenbank im Backend-System werden dann über das Finanznetzwerk an den entsprechenden Finanzdienstleister weitergeleitet, der die Zahlung autorisiert. Der Händler muss über eine ständige

Netzwerkverbindung zum Finanzdienstleister verfügen. Bei dieser Variante ist keine Eingabe einer Geheimnummer durch den Kunden vorgesehen, da eine bequeme, einfache und schnelle Zahlung getätigt werden soll, hier Soft-Identification genannt. Über ein geeignetes Benutzer-Interface wird dem Kunden der Status der Zahlung angezeigt und er kann sie bestätigen oder ablehnen.

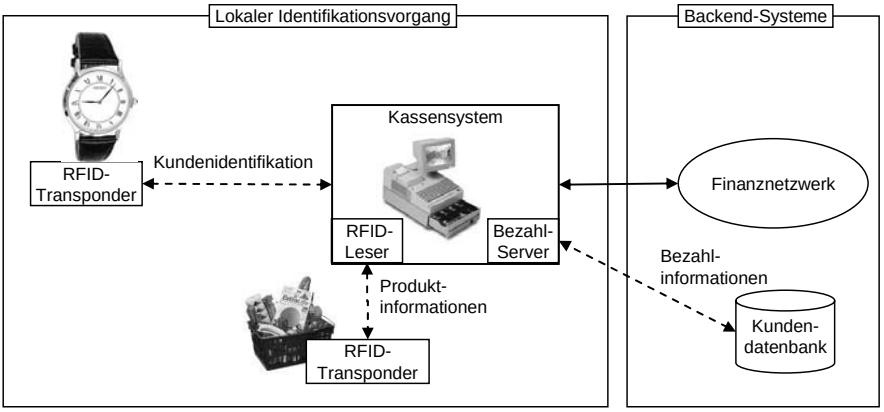


Abb. 3. Systemübersicht bei ausschließlicher Kundenidentifikation

Eine mögliche Erweiterung des Systems ist die Kombination mit einem RFID-basierten Diebstahlschutz: Produkte im Einkaufskorb, die bereits bezahlt wurden, werden auf dem RFID-Transponder markiert, sodass unbezahlte Produkte am Ausgang einen Alarm auslösen. Weiterhin kann man den Demonstrator so erweitern, dass der Kunde über das World Wide Web Zugriff auf seine Kundeninformationen erhält. So kann er Kontakt- oder Kreditkarteninformationen ändern, eine Aufstellung der getätigten Bezahlungen einsehen oder Präferenzen zu Bezahlvorgängen setzen wie Limite pro Bezahlung. Der Kunde muss sich darüber bewusst sein, dass der Händler mit der Datenbank in der Lage ist, Kundenprofile zu erstellen.

Lokaler Austausch der Bezahlinformationen

Im Unterschied zum vorher beschriebenen System benötigt der Kunde bei dieser Variante ein Gerät, auf dem sämtliche Bezahlinformationen gespeichert sind. Diese werden über eine lokale und drahtlose Verbindung ausgetauscht. Der Händler benötigt keine zusätzliche Kundendatenbank (vgl. Abbildung 4).

Die Bezahlung wird durch die Identifizierung des Bezahlgerätes initiiert, das bei diesem Demonstrator ein Mobiltelefon mit Java und Bluetooth ist. Da der Aufbau einer Bluetooth-Verbindung zwischen unbekannten Geräten im Extremfall einige Sekunden dauern kann [SiR03] und dies für den Ablauf einer automatischen Bezahlung störend ist, wird das Bezahlgerät zusätzlich über einen RFID-Transponder identifiziert, auf dem die Bluetooth-MAC-Adresse des Bezahlgerätes gespeichert ist. Dies ermöglicht ein schnelles Identifizieren des Bezahlgerätes und dadurch einen sofortigen Aufbau der Bluetooth-Verbindung zwischen dem Be-

zahlgerät und der Kasse. Über diese Bluetooth-Verbindung tauschen nun das Java-Programm „Bezahl-Client“ auf dem Bezahlgerät und das Programm „Bezahl-Server“ auf der Kasse die nötigen Zahlungsinformationen aus. Hierbei können vom Kunden festgelegte Bezahlpräferenzen geprüft werden, wie beispielsweise eine explizite Zahlungsbestätigung bei einem Betrag, der ein festgesetztes Limit überschreitet. Bei einem Demonstrator des M-Lab für UBS wurde als mobiles Endgerät ein Personal Digital Assistent (PDA) verwendet, bei dem der Kunde den Händler und den zu bezahlenden Betrag angezeigt bekommt (vgl. Abbildung 5). Er muss in diesem Fall die Zahlung über eine Geheimzahl autorisieren.

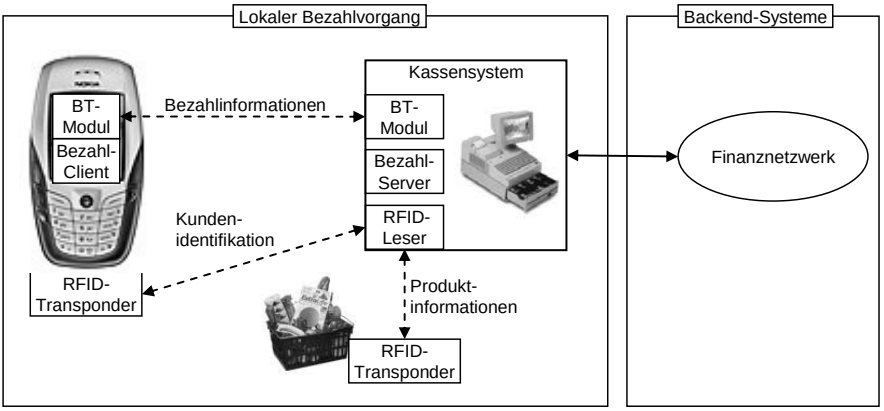


Abb. 4. Systemübersicht beim Austausch von Bezahlinformationen

Der Händler braucht keine Kundendatenbank zu führen. Wie im vorhergehenden System werden die Bezahlinformationen dann über das Finanznetzwerk an die Bezahlinstitution weitergeleitet, das die Bezahlung freigibt. Über das Benutzer-Interface wird dem Kunden der Status der Bezahlung angezeigt: entweder eine Bestätigung oder eine Warnung, falls die Bezahlung nicht freigegeben werden konnte. Der Kunde kann jederzeit auf seine Kundeninformationen über das Bezahlgerät zugreifen und sie einsehen oder ändern.

Abb. 5. Beispiel-Kundenschnittstelle beim PDA

5 Die U-Payment-Herausforderungen in der Praxis

Es gibt mehrere Herausforderungen, denen sich Banken und Finanzdienstleister bei der Umsetzung von U-Payment in der Praxis stellen müssen. Dazu zählen eine Unklarheit über Anwendungen und Geschäftsmodelle, über die technische Machbarkeit, über Datenschutz und Datensicherheit sowie über Standards. Die Standards wurden bereits im Zusammenhang mit der PPA erläutert, deshalb wird an dieser Stelle darauf verzichtet.

Für Finanzdienstleister stellt sich die Frage nach neuen *Geschäftsmodellen*, bei denen Zahlungsverfahren mit UbiComp eingesetzt werden. Sie müssen sich damit auseinander setzen, wie die durch UbiComp entstehenden Geschäftsmodelle die Rolle der Bank verändern werden, und wie man mit den neuen Technologien im Bereich mobiler Zahlungsverfahren eine hohe Marktdurchdringung erreichen kann. Des Weiteren müssen sie genaue Kosten-Nutzen-Analysen bezüglich des Mehrwertes von U-Payment durchführen.

Finanzdienstleister müssen auch die *technische Machbarkeit* beachten. Selbst bei mittlerweile etablierten Technologien wie Bluetooth ergeben sich bei deren Einsatz in der Praxis oft überraschende Probleme. Im Falle der Demonstratoren der Testplattform BluePay musste beispielsweise ein besonderes Augenmerk auf die eindeutige Kunden-Kassen-Zuordnung gelegt werden: Das bedeutet, dass der Kunde aus technischer Sicht anhand seines Identifikations- bzw. Bezahlgeräts zwar eindeutig erkannt werden konnte. Falls sich jedoch mehr als ein Kunde im Lesebereich der Kasse befand, konnte die Kasse nicht entscheiden, welcher Kunde die Bezahlung der Produkte tätigen will. Ein ähnliches Problem ergibt sich, falls zwei Kassen denselben Kunden identifizieren. Diese Probleme lassen sich zwar nicht auf einfache Art prinzipiell lösen, aber sie können durch technische Anpassungen reduziert werden, beispielsweise indem der Lesebereich der Kasse gut an die räumliche Situation angepasst wird. Dies geschieht durch Herabsetzen der Antennensendeleistung an der Kasse und durch die Benutzung einer gerichteten Antenne.

Der *Datenschutz (privacy) und die Datensicherheit (security)* müssen sichergestellt sein. Die Daten auf dem Identifikations- bzw. Bezahlgerät dürfen für Dritte nicht zugänglich sein. Außerdem stellt sich die Frage nach dem Eigentum der Daten, d.h., wer die Hoheit über die Daten im Wertschöpfungsnetz besitzt.

Bei der Implementierung der Demonstratoren lassen sich diese Fragestellungen folgendermaßen angehen: Ein Challenge-Response-Verfahren erlaubt es, die Daten sowohl auf Hardware- wie auch auf Software-Ebene zu schützen. Es gestattet den Zugriff auf die Daten beim lokalen Austausch von Bezahlinformationen nur nach erfolgreicher Authentifizierung. Außerdem muss sichergestellt sein, dass die Daten nicht während der Übertragung zwischen Bezahlgerät und Kasse durch Dritte abgehört werden können. Dies lässt sich lösen, indem man die drahtlose Verbindung auf Hardware-Ebene verschlüsselt, wie dies bei Bluetooth der Fall ist. Eine andere Möglichkeit ist die softwaremäßige Verschlüsselung der Daten, d.h., die Programme Bezahl-Client bzw. Bezahl-Server verschlüsseln die Daten vor der Übertragung. Bei der Identifizierung durch RFID nimmt die Hardware der Funkschnittstelle die Verschlüsselung vor.

6 Schlussfolgerungen

Die Analyse der Anforderungen an Zahlungsverfahren mit UbiComp ergibt, dass Finanzdienstleister dem Endbenutzer sichere, transparente und einfache Zahlungsverfahren anbieten müssen, um eine ausreichende Akzeptanz zu erreichen. Die Händler sind bei der Auswahl der Technologien und Anwendungen von Beginn an einzubinden, da ihre Unterstützung eine der Grundvoraussetzungen für die Etablierung der Verfahren am Markt ist.

Im Rahmen der Projektzusammenarbeit von UBS und M-Lab wurden Demonstratoren im Bereich lokaler Zahlungssysteme mit Hilfe der RFID-Technologie zur automatischen Identifizierung des Kunden implementiert und getestet. Das Ziel war es, im Rahmen der technischen Anforderungen der PPA die grundsätzliche technische Machbarkeit und die Einsatzmöglichkeiten von U-Payment aufzuzeigen.

In der Zukunft kann das Potenzial von U-Payment auch bei Bezahlvorgängen zwischen Unternehmen liegen: Durch UbiComp könnten Waren Bezahlungen selbstständig einleiten, z.B. in der Logistikkette. Außerdem könnten UbiComp-Technologien den Zustand von Waren automatisch überwachen und den Finanzdienstleistern exakte Kennzahlen für die Risikoüberwachung bei Kreditrisiken und -limiten in Echtzeit liefern.

Literatur

[Acc02] Accenture (2002) Ubiquitous Commerce – Autonomous Purchasing Object, www.accenture.com/xd/xd.asp?it=enweb&xd=services\technology\tech_autopurchase.xml

[DSt01] DStar (2001) Accenture Lab works on object-to-object Internet Commerce, www.hpcwire.com/dsstar/01/1120/103711.html

[Exx02] Exxon Mobil (2002) Hard-to-Shop-for People on Your Holiday List? How about an Electronic Wallet for Their Wrists? Exxon Mobil Press Release, December 4, 2002, www.exxonmobil.com/Corporate/Newsroom/Newsreleases/xom_nr_041202.asp

[HGF03] Hort C, Gross S, Fleisch E (2003) Critical Success Factors of Mobile Payment. M-Lab Working Paper No. 13, Universität St. Gallen / ETH Zürich

[ITW02] ITWorld (2002) Study: M-Commerce to be $25B Market by 2006, April 4, 2002, www.itworld.com/nl/ebus_insights/04042002

[IWW02] IWW (2002) Zahlungssysteme im Internet – eine Übersicht. Institut für Wirtschaftspolitik und Wirtschaftsforschung der Universität Karlsruhe

[KPT02] Kreyer N, Pousttchi K, Turowski K (2002) Characteristics of Mobile Payment Procedures. In: Proceedings of the ISMIS 2002 Workshop on M-Services

[Kru01] Krueger M (2001) The Future of M-Payments – Business Options and Policy Issues. Institute for Prospective Technological Studies, European Commission

[MoF00] Mobey Forum (2000) Mobile Financial Services, White Paper

[SiR03] Siegemund F, Rohs M (2003) Rendezvous Layer Protocols for Bluetooth-Enabled Smart Devices. Journal for Personal and Ubiquitous Computing 7(2):91–101

Das smarte Buch

Frédéric Thiesse
Institut für Technologiemanagement, Universität St. Gallen

Frank Gillert
Infineon Technologies AG, München

Kurzfassung. Die Bibliothek von heute hat eine Reihe neuer Aufgaben übernommen, die über die traditionelle Buchausleihe hinausgehen. Da in Zeiten knapper Budgets kein zusätzliches Personal eingestellt werden kann, bleibt nur der Weg einer Rationalisierung von Routinearbeiten rund um die verwalteten Medien, insbesondere das Aus- und Einbuchen sowie Inventuren. RFID verspricht hier eine weitgehende Automatisierung mit dem Ziel, Personal verstärkt für Kundenbetreuung und -beratung einsetzen zu können. Vor diesem Hintergrund erläutert dieser Beitrag die Einsatzmöglichkeiten für RFID in der Bibliothek und gibt einen Ausblick auf Potenziale in der Buchbranche insgesamt. Nicht zuletzt ist auch das vorliegende Buch selbst mit einem Transponder ausgestattet, dessen technische Eigenschaften in der zweiten Hälfte beschrieben werden.

1 Einführung

Den vorangegangenen Beiträgen liegt die gemeinsame Vision eines Internets der Dinge zugrunde, einer Welt smarter Alltagsgegenstände, welche mit digitaler Logik und der Fähigkeit zur Vernetzung ausgestattet sind. Nur konsequent ist es daher, auch das physische Objekt „Buch“ selbst zu einem smarten Objekt zu machen. Aus diesem Grund ist das Buch, das Sie in den Händen halten, mit einem RFID-Transponder versehen, der jedes einzelne Exemplar einzigartig macht. Was zunächst wie ein simpler Marketing-Gag aussieht, ist bei näherem Hinsehen Grundlage für bereits heute etablierte und wirtschaftliche Anwendungen der RFID-Technologie rund um Bücher und die Buchbranche. Insbesondere in Bibliotheken hat sich RFID als Nachfolger traditioneller Systeme zur Medienidentifikation profilieren können, wie folgende Beispiele zeigen:

- Der Stadtstaat Singapur ist mit über neun Millionen getaggten Einheiten in mehr als 25 Bibliotheken führend bei der Ausstattung seiner Bibliotheken mit RFID-Systemen. In der Butik Batok Community Library wurde am 21. November 1998 das weltweit erste RFID-System in einer Bibliothek in Betrieb genommen [NLB02]. Allein in dieser und den anderen Einrichtungen des National Library Board wurden seither sieben Millionen Bücher mit Transpondern

versehen. RFID bildet u.a. die Grundlage für das flexible Rückgabesystem, bei dem jedes Buch bei jeder beliebigen Bibliothek zurückgegeben werden kann.

- Die Vatikanische Bibliothek setzt im Rahmen der Einführung eines neuen Verwaltungssystems auf RFID zur Identifikation ihrer zwei Millionen Bücher, Manuskripte und anderen wertvollen Sammlerstücke [Guar04]. Musste die Bibliothek früher jedes Jahr einen ganzen Monat für die Inventur schließen, so wird die Prüfung in Zukunft in einem halben Tag mit weniger Mitarbeitern möglich sein. Das Anfassen jedes einzelnen Buchs wird durch die neue Technologie überflüssig. Angedacht sind außerdem weitere Einsatzgebiete wie die Identifikation von Angestellten und Besuchern sowie die Sicherung kostbarer Gemälde und anderer Kunstwerke.
- Auch im deutschsprachigen Raum haben sich mittlerweile zahlreiche Bibliotheken für den Umstieg auf RFID entschlossen. Die Stadtbücherei Stuttgart, die Stadtbibliothek Winterthur und die Hauptbücherei Wien sind nur einige prominente Beispiele unter vielen [Kan04]. Dabei befindet sich die Einführung der Technologie gerade erst am Anfang: Allein in Deutschland stehen der Anzahl an Installationen im zweistelligen Bereich insgesamt rund 16 000 wissenschaftliche und öffentliche Bibliotheken gegenüber.

Vor diesem Hintergrund sollen im Folgenden die Möglichkeiten und Potenziale des RFID-Einsatzes rund um das Buch genauer betrachtet werden. Nicht zuletzt wird dabei auch auf den Transponder im vorliegenden Buch eingegangen, der im letzten Abschnitt beschrieben ist.

2 Anwendungsgebiete in Bibliothek und Buchhandel

Die moderne Bibliothek des 21. Jahrhunderts hat gegenüber der traditionellen Buchausleihe eine Reihe neuer Aufgaben übernommen. Einerseits wurden neben Büchern auch Spiele, CDs, DVDs und Videos in das Programm aufgenommen, andererseits werden dem Benutzer Einrichtungen wie Internetzugänge, Cafés oder Spieleecken für Kinder geboten – teilweise rund um die Uhr. Da in Zeiten knapper Budgets kein zusätzliches Personal eingestellt werden kann, bleibt nur der Weg einer Rationalisierung von Routinearbeiten rund um die verwalteten Medien, insbesondere das Aus- und Einbuchen sowie Inventuren. RFID verspricht hier eine weitgehende Automatisierung mit dem Ziel, Personal verstärkt für Kundenbetreuung und -beratung einsetzen zu können.

In Bibliotheken ist es notwendig, jede der physischen Bestandseinheiten eindeutig identifizieren zu können, um sie formal und inhaltlich zu erschließen, aufzustellen, an ihrem Standort zu finden, auszuleihen oder zurückzugeben und aus dem Bestand zu entfernen. Zu diesem Zweck werden heute in Bibliotheken im Rahmen der automatisierten Ausleihverbuchung Mediennummern auf einem Klebeetikett in Form von OCR-Schrift oder als Strichcode eingesetzt. Die optische Zeichenerkennung („Optical Character Recognition“ (OCR)) basiert auf einer Nummer in Klarschrift, die auch für Menschen lesbar ist. Dabei wird ein normierter Zeichensatz verwendet, der durch ein Lesegerät erfasst und entschlüsselt werden kann. Robuster und deutlich weiter verbreitet ist jedoch der auch aus dem

Handel bekannte Strichcode, der in Bibliotheken heute in drei unterschiedlichen Varianten verwendet wird [Nies03].

Unabhängig von der Medienidentifikation sind darüber hinaus Systeme zur Diebstahlsicherung im Einsatz, ähnlich den aus dem Handel bekannten elektronischen Artikelsicherungssystemen („EAS“, siehe [Gill01]). Dabei werden magnetisierte Metallstreifen („EM strips“) in den Einband integriert, deren Magnetfeld bei der Ausleihe verändert wird, sodass das Buch die Bibliothek verlassen kann, ohne an den Antennen am Ausgang erkannt zu werden und Alarm auszulösen. Für Präsenzbestände können auch Streifen verwendet werden, die nicht deaktiviert werden können. Streifen und Barcodelabel werden üblicherweise übereinander angebracht, sodass das Einscannen und (De-)Aktivieren in einem Arbeitsschritt möglich ist.

Trotz der deutlichen Effizienzsteigerung der Barcode-basierten Systeme gegenüber dem klassischen Handzettelkasten sind Warteschlangen bei der Ausleihe insbesondere in Großstadtbibliotheken mit mehreren Tausend Besuchern pro Tag keine Seltenheit. Selbstverbuchungssysteme sind zwar am Markt verfügbar, bieten dem Besucher jedoch nur begrenzten Komfort, da jedes einzelne Exemplar aufgeschlagen und das Label direkt über dem Lesegerät positioniert werden muss. Auch die Inventur sowie die Suche nach verlegten oder verlorenen Medien sind weiterhin aufwendig und häufig nur mit einer vorübergehenden Schließung der Einrichtung machbar. Nicht zuletzt sind auch Verschmutzung und mechanischer Abrieb für die wenig robusten Labels ein Problem wie auch für die Lesehardware.

Demgegenüber verbindet RFID-Technologie Medienidentifikation und Diebstahlsicherung in einem einzigen Label. Den heute noch leicht höheren Kosten (der Preis für die Kombination aus Barcodelabel und Magnetstreifen liegt bei ca. 10–25 US$-Cents pro Buch) stehen die RFID-typischen Vorteile der Pulkfähigkeit und des Lesens ohne Sichtverbindung gegenüber, durch die eine deutliche Vereinfachung der repetitiven Erfassungstätigkeiten möglich wird. So ergab beispielsweise eine Analyse der Mastics-Moriches Community Library im US-Bundesstaat New York mit dem Anbieter Bibliotheca RFID Library Systems eine Beschleunigung der Ausleihe- und Rückgabeprozesse um 85 Prozent [Smar04]. Darüber hinaus kann der Transponder auch Daten wie Autor, Exemplarnummer oder Systematikgruppe dezentral speichern.

Der Einsatz ist dabei keineswegs auf die genannten Gebiete beschränkt. Im Einzelnen kann RFID in Bibliotheken bei folgenden Anwendungen zum Einsatz kommen:

- Vereinfachte Mediensicherung/-identifizierung bzw. Verbuchung ohne Sichtverbindung
- Selbstverbuchungssysteme zur Ausleihe und Rückgabe
- Ausweise zur Benutzeridentifikation (optional mit Bezahlfunktion)
- Handlesegeräte für die Inventur, Bestandspflege und Aufspüren verstellter Medien
- Buchregale mit eingebautem Lesegerät zur Bestandskontrolle in Echtzeit bzw. Analyse der Nutzung von Präsenzbeständen
- Sicherheits-Gates zum Diebstahlschutz für Check-in/Check-out
- Sortier- und Buchförderanlagen für die Rückgabelogistik

- Automatische Rückgabeboxen für die Rückgabe auch außerhalb der Öffnungszeiten

Zentrales Werkzeug zur Entlastung des Personals sind dabei die Self-Check-out-Terminals, an denen die Besucher selbst Medien aus dem System ausbuchen können (siehe Abbildung 1). Beispielsweise verfügt die Wiener Hauptbibliothek über vier dieser so genannten „EasyCheck"-Terminals, an denen bereits 40 Prozent der Besucher ihre Medien entleihen. Dabei kann ein ganzer Medienstapel in einem einzigen Durchgang gelesen und verbucht werden. Möchte ein Benutzer seine Medien nicht selbst verbuchen, kann er weiterhin die Personalverbuchung in Anspruch nehmen, bei der auch Zusatzfunktionen wie Verlängerung, Kontoeinsicht oder Bezahlen von Gebühren möglich sind, die das Selbstverbuchungsgerät nicht in jedem Fall bietet.

Abb. 1. Self-Check-out in der Hauptbücherei der Stadt Wien (Quelle: Bibliotheca)

Ein weiteres wichtiges Element vieler RFID-Installationen sind Rückgabeboxen, die dem Benutzer rund um die Uhr zur Verfügung stehen und im Zusammenhang mit einer automatischen Sortieranlage eine Einbuchung und -sortierung ohne Personalaufwand ermöglichen (siehe Abbildung 2). Inventarisierungsaktivitäten werden wiederum mit tragbaren Handlesegeräten unterstützt, bei denen im Gegensatz zum Barcode kein separates Scannen jedes einzelnen Buchs notwendig ist. Eine Komplettautomatisierung durch Antennen im Buchregal ist aufgrund der hohen Kosten hingegen bisher eher unüblich.

Abb. 2. Buchrückgabe in der Stadtbibliothek Winterthur (Quelle: Bibliotheca)

Besondere Anforderungen an RFID-Transponder stellt die Kennzeichnung von audiovisuellen Medien wie CDs und DVDs. Einerseits muss das Label trotz metallischer Bestandteile des Objekts sicher gelesen werden können, andererseits darf das Label trotz der hohen Rotationsgeschwindigkeit nicht den Abspielvorgang beeinflussen oder den CD/DVD-Player beschädigen. Zu diesem Zweck bieten mittlerweile verschiedene Hersteller spezialisierte Labels an, deren Bauform an das Jewel Case bzw. den Datenträger angepasst ist. Ein Hersteller wie Nedap bietet darüber hinaus ein in die CD/DVD-Packung integrierbares „BoosterLabel“ an, durch das die Leserate weiter verbessert werden soll (siehe Abbildung 3).

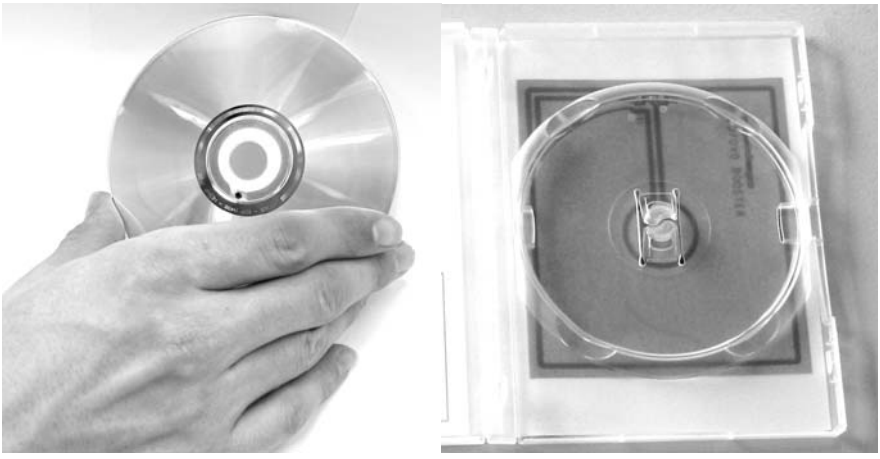


Abb. 3. CD/DVD-Transponder und „BoosterLabel“ (Quelle: Nedap)

Zusammengefasst erhoffen sich Bibliotheken von der RFID-Einführung folgende Vorteile [Kan04]:

- Zeitersparnis für Benutzer und Personal bei Verbuchungsvorgängen
- Verbesserung von Beratungsqualität und Service durch Verringerung von Routinearbeiten
- Effektivere Bestandskontrolle durch häufigere und zuverlässigere Revision
- Erhöhung der Mediensicherheit durch Diebstahlschutz und Einsparung von Verlustkosten
- Schnellere Einarbeitung von Neuanschaffungen

Mit der Automatisierung nimmt auch die Dezentralisierung von Aktivitäten in der Bibliothek zu, mit der nicht nur technische, sondern auch organisatorische Veränderungen einhergehen. Während in der traditionellen Bibliothek alle Aufgaben bei einer zentralen Theke gebündelt waren, verteilen sich in der RFID-gestützten Variante die Aktivitäten auf Personal, Besucher und technische Anlagen an verschiedenen Stellen im Gebäude [WeKe04]. Wie auch bei anderen Anwendungsszenarien wirkt sich somit der RFID-Einsatz nicht allein auf die Informationssysteme einer Bibliothek aus, sondern auch auf deren Prozesse und physische Architektur.

Gründe für den Erfolg von RFID in Bibliotheken sind vielfältig: Zunächst ist das Objekt selbst aufgrund seiner physischen Beschaffenheit (kein Metall, kein Wasser) hervorragend für eine Ausstattung mit Transpondern geeignet. Darüber hinaus handelt es sich bei Bibliotheken trotz des Entleihvorgangs um geschlossene Systeme, d.h., der Transponder kehrt stets mit dem Buch zurück und muss nicht erneuert werden, sodass die Wirtschaftlichkeit der Anwendung nicht so sehr vom Transponderpreis abhängt. Die Einführung wird durch den Umstand erleichtert, dass ein Mischbetrieb mit getaggten und ungetaggten Teilbeständen meist problemlos machbar ist. Eine aufgrund des finanziellen und personellen Aufwands oft notwendige stufenweise Installation stellt so kein größeres Problem dar [Kan04].

Die verstärkte Nachfrage nach RFID-Lösungen hat zunehmend auch Auswirkungen auf den Buchgroßhandel. Mit NBD|Biblion bietet erstmals ein Großhändler seinen Kunden auf Wunsch eine Ausstattung aller gelieferten Bücher mit Transpondern [Coll04]. NBD|Biblion verkauft pro Jahr 2,7 Millionen Bücher an niederländische Bibliotheken und verfügt über einen Marktanteil von 80 Prozent. Durch das neue RFID-Angebot erhofft sich das Unternehmen einen zusätzlichen Wettbewerbsvorteil gegenüber der Konkurrenz und langfristig auch Verbesserungen in der eigenen Logistik.

Insgesamt unterscheiden sich die Strukturen der Buchbranche – abgesehen von einigen Spezifika wie der Buchpreisbindung – nicht wesentlich von anderen Bereichen des Handels (siehe Abbildung 4). Dementsprechend sind auch die Potenziale für RFID ähnlich gelagert: Neben Warenein- und -ausgang, Lagerhaltung, der Verarbeitung von Rücksendungen und Diebstahlschutz interessieren sich Buchhändler auch für zeitnahe Bestands- und Abverkaufsinformationen aus den Läden. Ein weiteres mögliches Anwendungsgebiet ist auch die Unterbindung von Graumärkten, bei denen neue Bücher unterhalb des Ladenpreises verkauft werden, durch die Verfolgung entlang der Lieferkette. Gleichzeitig sieht sich die

Branche derzeit aber auch noch mit einigen typischen Problemstellungen konfrontiert, wie z.B. fehlenden Standards und hohen Tagpreisen.

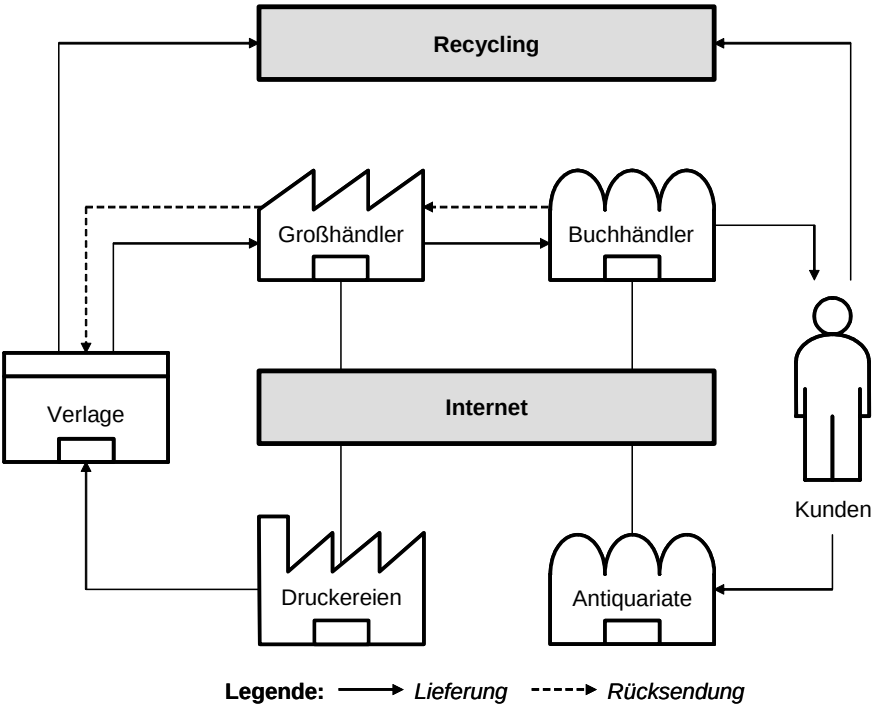


Abb. 4. Die Buch-Supply-Chain im Überblick [Ish04]

3 Über den Transponder in diesem Buch

Der in das vorliegende Buch eingeklebte Transponder verfügt über einen Infineon my-d RFID-Chip. Mit dieser Ausstattung ist das Buch bereits heute für viele der zuvor beschriebenen Anwendungen rund um Bibliotheken und Buchhandel vorbereitet. Der Chip arbeitet auf der 13,56-MHz-Frequenz gemäß dem ISO-Standard 15693 und kann je nach Lesegerät bzw. Antenne über eine Entfernung von etwa einem Meter ausgelesen werden. Die eindeutige Identifikationsnummer des Transponders umfasst 64 bit; darüber hinaus ist auf dem Chip ein 10 kbit großer EEPROM-Speicher für sonstige Daten verfügbar.

Der Speicher des Infineon-Chips ist in 125 Seiten à 8 Byte unterteilt, die einzeln adressiert, „gelockt“ (d.h. nur zum Lesen freigegeben) und mit Zugriffsrechten versehen werden können. Dieser so genannte „Chip Sharing Approach“ ermöglicht Anwendungen in der Supply Chain, bei denen jeder Akteur in der Lieferkette eine eigene Sicht auf die im Speicher abgelegten Daten haben kann.

Neben der Anwendung im Buch ist der Transponder auch für eine Reihe anderer Szenarien geeignet, u.a. Behältermanagement, Ticketing, elektronische Artikelsicherung, Tieridentifikation, Gepäckidentifikation usw.

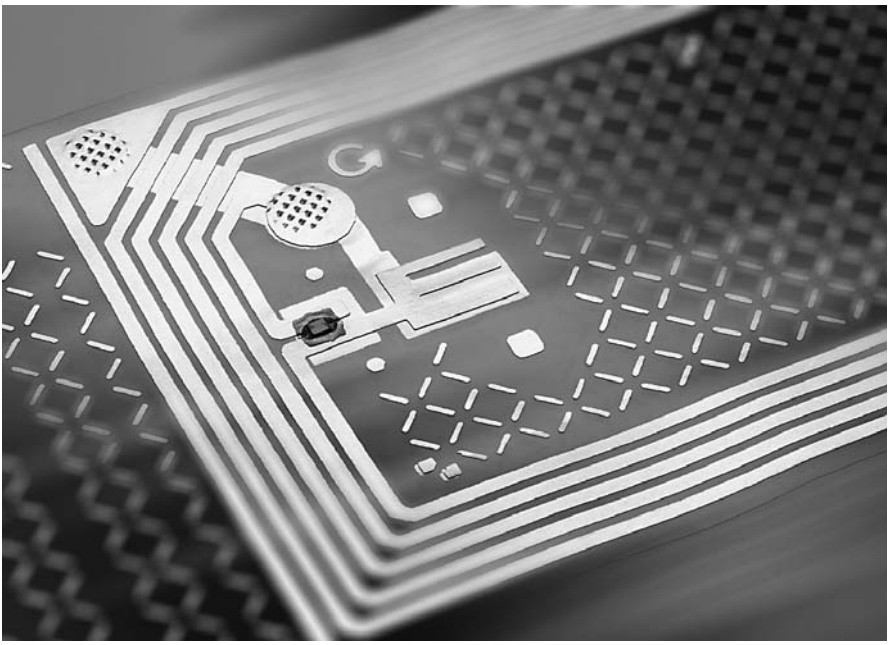


Abb. 5. Der Transponder in diesem Buch (Quelle: Infineon)

4 Fazit

Abseits der vorwiegend auf Automobilindustrie und Handel fokussierten Diskussion rund um RFID hat sich mit der Medienidentifikation und -sicherung in Bibliotheken in den letzten Jahren ein sowohl technisch robustes als auch wirtschaftliches Einsatzgebiet herausgebildet, das zunehmend mehr Anwender für sich gewinnt. Aufgrund der Eigenschaften einer Bibliothek als geschlossenes System und der für RFID günstigen physikalischen Voraussetzungen von Büchern fällt der Umstieg vom gewohnten Barcode vergleichsweise leicht.

Für den weiteren Einsatz der RFID-Technologie in Bibliotheken sind zwei Faktoren entscheidend: die Preisentwicklung und die Durchsetzung von Standards [WeKe04]. Insbesondere die Preise für RFID-Etiketten sind in der Vergangenheit durch die Anwendungen in anderen Bereichen drastisch gesunken. Die niedrigeren Investitionskosten und deren schnelle Amortisation werden vielen Bibliotheken den Einsatz von RFID erlauben. Daneben bewirkt die Durchsetzung von Standards heute eine Unabhängigkeit von einer proprietären Chiptechnologie. Um eine Austauschbarkeit von Medien zwischen Bibliotheken zu ermöglichen, wird

derzeit auch an einer Standardisierung des Datenformats auf dem Chip gearbeitet. Vor diesem Hintergrund sind die Voraussetzungen für den Einsatz von RFID auch in anderen Bereichen der Buchbranche vielversprechend.

Literatur

[Coll04] Collins J (2004) Publisher Tags All Library Books. RFID Journal, 22. September 2004, www.rfidjournal.com/article/articleview/1128/1/1

[Gill01] Gillert F (2001) Entwicklung einer Methodik zur labortechnischen Abnahme quellengesicherter Produkte und Produktverpackungen. Schriftenreihe Transport- und Verpackungslogistik, Band 52, Deutscher Fachverlag

[Guar04] The Guardian (2004) Shelf life. November 11, 2004, www.guardian.co.uk/online/insideit/story/0,13270,1347745,00.html

[Ish04] Ishikawa T, Yumoto Y, Kurata M, Makoto E, Kinoshita S, Hoshino F, Yagi S, Nomachi M, (2004) Applying Auto-ID to the Japanese Publication Business. White Paper KEI-AUTOID-WH-004, Auto-ID Lab, Keio University

[Kan04] Kandel D (2004) Funkende Bücher – Über 50 Bibliotheken im Vergleich. RFID-Forum. Ausgabe 02/2004, S 12–25

[Nies03] Niesner S (2003) RFID-Systeme zur Medienidentifikation in Bibliotheken. Diplomarbeit, Fakultät für Informations- und Kommunikationswissenschaft, Fachhochschule Köln, 2003

[NLB02] (2002) About us – Milestones. National Library Board, Singapore, www.nlb.gov.sg/fr_abtUs_milestones.html

[Smar04] Smart L (2004) Making Sense of RFID. Library Journal, October 15, 2004, www.libraryjournal.com/article/CA456770

[WeKe04] Weiss R, Kern C (2004) Zentrale und dezentrale Positionierung der Funktionseinheiten in der Bibliothek – Raumplanung für die Integration von RFID. ABI-Technik, 24(2): 135–139

Teil D: Handlungsanleitungen

RFID-Systemeinführung – Ein Leitfaden für Projektleiter

Sandra Gross
Institut für Technologiemanagement, Universität St. Gallen

Frédéric Thiesse
Institut für Technologiemanagement, Universität St. Gallen

Kurzfassung. Die Komplexität eines RFID-Projekts steigt mit zunehmender Reichweite der horizontalen bzw. vertikalen Integration. Insbesondere die notwendige Koordination mit anderen Partnern entlang der Lieferkette ist ein wichtiger Faktor für das erfolgreiche Projektmanagement. Vor diesem Hintergrund skizziert dieser Beitrag einige wesentliche Aspekte, in denen sich die RFID-Systemeinführung gegenüber anderen IT-Projekten unterscheidet, und liefert Handlungsanleitungen für die Praxis. Hierzu gehören Fragen der geeigneten Zusammensetzung des Projektteams, RFID-spezifische Aktivitäten im Vorgehensmodell sowie Hinweise zum begleitenden Change Management.

1 Einleitung

Mit zunehmender Reichweite der vertikalen und horizontalen Integration steigen auch die Komplexität eines RFID-Einführungsprojekts und damit die an das Projektmanagement gestellten Anforderungen. Während bei klassischen Insellösungen die technische Problemstellung im Vordergrund steht, sind es bei großen, unternehmensübergreifenden Projekten vor allem Aspekte der Koordination zwischen internen und externen Organisationseinheiten, mögliche Prozessveränderungen entlang der Lieferkette sowie die Einbindung unterschiedlichster bestehender Informationssysteme, die den Komplexitätsgrad eines Projekts bestimmen.

Auch wenn sich grundlegende Projektmanagementtechniken zur Planung und Kontrolle sich auch im Fall von RFID nicht wesentlich von anderen IT-Projekten unterscheiden, gibt es dennoch eine Reihe von Besonderheiten, die in diesem Beitrag betrachtet werden sollen. Ein Beispiel ist die Notwendigkeit eines „Site Survey“, d.h. einer Inaugenscheinnahme des für die Hardwareinstallation vorgesehenen Areals. Im Vordergrund des vorliegenden Beitrags stehen dabei weniger Fragen der inhaltlichen Ausgestaltung eines RFID-Systems als vielmehr Projektorganisation und Vorgehen bei der Projektdurchführung.

2 Organisation

2.1 Projektteam

Wie auch bei anderen Projekten so steht und fällt auch im Fall einer RFID-Einführung der Verlauf des Projekts mit der Zusammensetzung des Projektteams. Erfahrungen mit Großprojekten sowie einschlägige Kenntnisse im Bereich RFID-Technologie sind in jedem Fall wünschenswert und notwendig. Sind diese Anforderungen schwer durch Mitarbeiter aus dem eigenen Unternehmen zu erfüllen, sollte auch erwogen werden, für die Dauer des Projekts externe Experten mit einzubeziehen. Beim Aufbau des Projektteams wird typischerweise zwischen einem Kernteam (siehe Beispiel in Abbildung 1) und einem erweiterten Team unterschieden.

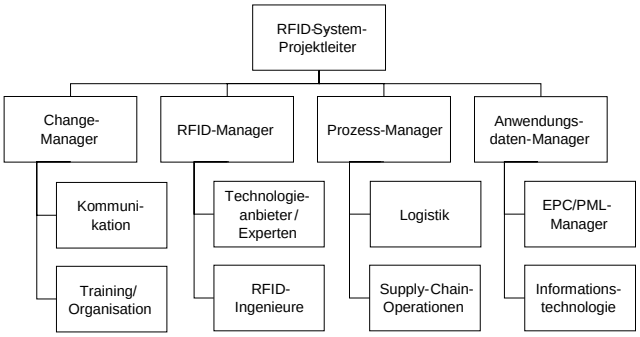


Abb. 1. Beispiel eines Kernteams für ein Supply-Chain-Management-Projekt

Das *Kernteam* ist ein Vollzeit-Projektteam, das die alleinige Verantwortung für die Umsetzung gemäß den Anforderungen des Auftraggebers trägt. Der Auftraggeber kommt in der Regel aus der obersten Führungsebene. Bei den Pilotprojekten sind in der Regel mindestens zwei bis drei Mitarbeiter vollzeitig mit dem RFID-Projekt betraut. Die Rollen im Kernteam sind:

- **Projektleiter.** Als Projektleiter für eine RFID-Einführung eignen sich insbesondere Personen, die technische Expertise mit einem fundierten Prozess-Know-how und Erfahrung aus Großprojekten in sich vereinen und so sowohl gegenüber Technikern als auch Mitarbeitern aus den betroffenen Fachabteilungen als kompetenter Gesprächspartner auftreten können.
- **Change-Manager.** Der Change-Manager sollte schon Prozessoptimierungs- und Reorganisationsprojekte durchgeführt haben und über gute Kommunikationsfähigkeiten verfügen.
- **RFID-Manager und -Ingenieure.** Diese Teammitglieder benötigen Kenntnisse und Erfahrungen mit der Auswahl und Implementierung von RFID-Systemen. Dies bedeutet beispielsweise, dass sie die technischen Eigenschaften von Lesern, Transpondern und Antennen kennen und wissen, nach welchen Kriterien der Projektleiter Technologieanbieter auswählen sollte.

- **Prozess-Manager.** Die Anforderungen an den Prozess-Manager hängen von der Anwendung ab, die umgesetzt werden soll. Für eine Track&Trace-Anwendung im Supply Chain Management sollte er beispielsweise den SCM-Prozess gut kennen und möglichst bereits Verantwortung in diesem Bereich innerhalb der Organisation getragen haben.
- **Anwendungsdaten-Manager.** Der Anwendungsdaten-Manager sollte fundierte IT-Kenntnisse, insbesondere in Bezug auf die von der RFID-Einführung betroffenen Systeme und deren zugrunde liegenden Datenbestände, besitzen.

Das *erweiterte Team* besteht aus Personen, die entweder funktionale oder operationale Verantwortung für Bereiche im Unternehmen tragen, die durch das RFID-System tangiert werden. Es können hier ebenfalls Experten, Handelspartner oder Technologieanbieter eingebunden werden. Ihre Expertise wird nur fallweise genutzt, wenn sich aus dem Projekt heraus die Notwendigkeit ergibt. Typischerweise stammen Mitglieder des erweiterten Teams aus den Bereichen Qualitätsmanagement, IT und Organisation, Vertrieb, Marketing, Personal, Recht oder Forschung und Entwicklung. Des Weiteren kann der Projektleiter bei Bedarf Antennenexperten, Verpackungsexperten, Transportexperten, Technologieanbieter, Bau- oder Werksleiter, Handelspartner sowie Kundenvertreter einbinden.

2.2 Organisationsübergreifende Koordination

Mit der Anzahl der Kooperationspartner und mit einer zunehmend globalen Ausrichtung des Projekts steigt auch die Schwierigkeit, Interessen und Anforderungen aller beteiligten Parteien miteinander in Einklang zu bringen und gemeinsame Aktivitäten zu koordinieren. Je mehr unternehmensinterne und externe Organisationseinheiten am geplanten RFID-System partizipieren, desto höher wird der organisatorische Aufwand bei der Einführung und desto mehr Prozesse müssen die Partner einander anpassen. Die Komplexität steigt zudem durch die Berücksichtigung unterschiedlicher Standards und rechtlicher Rahmenbedingungen in den Regionen und Ländern, in denen das RFID-System implementiert wird.

- **Verantwortung und Berechtigungen für Datenbestände.** Alle an der Anwendung beteiligten Unternehmen müssen sich über die Datenhoheit einigen sowie ihre Rolle zu Beginn des Projektes definieren und Geheimhaltungspflichten frühzeitig klären. Wenn Unternehmen teilweise auf dieselbe technische Infrastruktur zurückgreifen, um standardisierte Informationen über die physischen Güter in der Lieferkette zu erhalten, ergeben sich zusätzliche sicherheitsspezifische Herausforderungen, beispielsweise bei der Definition und Vergabe von Zugriffsrechten auf gemeinsame Daten.
- **Unterschiedliche Grade technischer Voraussetzungen.** Nicht alle Zulieferer, Handelspartner und Kunden könnten die RFID-Technologie zur automatischen Identifikation von Waren oder Paletten gleichermaßen nutzen, da der Stand der jeweiligen IT-Infrastruktur stark variieren kann. Daher sollte der Projektleiter in Zusammenarbeit mit diesen Partnern Altsysteme und neuere Informationssysteme gleichermaßen berücksichtigen, um die Folgen bzw. notwendige Integrationsarbeiten im Rahmen der RFID-Einführung abschätzen zu können.

- **Migration von anderen Identifikationstechnologien.** Eine weitere Herausforderung stellt die Tatsache dar, dass andere Identifikationssysteme wie beispielsweise Barcode mit den neu geschaffenen RFID-Systemen unter Umständen für begrenzte Zeit oder auch dauerhaft parallel existieren werden, bzw. RFID alte Technologien stufenweise ersetzt. Daher ist es notwendig, dass das Projektteam Redundanzen in den betroffenen Systemen untersucht, notwendige Schnittstellen definiert und bei Bedarf einen Migrationsplan erstellt.
- **Divergierende Erwartungen an die Technologie.** Die Unternehmen können unterschiedliche Vorstellungen über die Anzahl und Auswahl der umzusetzenden RFID-Anwendungen besitzen. Die automatische Identifizierung von Produkten ist beispielsweise für alle Logistikpartner interessant, die den Wareneingang besser kontrollieren wollen. Die darauf aufbauende Anwendung der automatischen Inventur jedoch könnte nur einzelne Unternehmen betreffen. Vor diesem Hintergrund ist mit allen Projektpartnern eine Klärung des zugrunde liegenden Business Case notwendig, in dem Erwartungen, Aufwände und Nutzeneffekte bewertet werden.

3 Ablauf

3.1 Vorgehensmodell

Das im Folgenden vorgestellte Vorgehensmodell unterteilt sich in die klassischen drei Phasen Analyse, Konzeption und Implementierung. Nach deren Abschluss beginnt die Nutzungszeit, d.h., das RFID-System wird kontinuierlich betrieben und gewartet bzw. gegebenenfalls um zusätzliche Komponenten oder Funktionen erweitert. Das Vorgehensmodell und die in jeder Phase erarbeiteten Ergebnisse sind in Abbildung 2 dargestellt. Folgende Aktivitäten werden jeweils in den einzelnen Phasen durchgeführt:

- **Analyse.** Ziel der Analysephase ist eine Strukturierung des Problembereichs aus Personen, Objekten, Prozessen, Informationssystemen, physikalischen Randbedingungen, strategischen Zielen des Unternehmens usw. mit dem Ziel, die durch das Projekt zu bearbeitende Aufgabenstellung herauszuarbeiten und Anforderungen an eine Lösung zu formulieren. Das Ergebnis dieser Analysephase wird in Form eines Lastenhefts (bzw. Projektauftrags) dokumentiert. Dieses umfasst neben einer inhaltlichen Vorgabe für das Projekt auch Aussagen zur Wirtschaftlichkeit, Ressourcenplanung, zeitlichen Planung und zum Auftraggeber. Im Fall von RFID sind insbesondere Aktivitäten zur Begutachtung physikalischer Randbedingungen von Orten und Objekten sowie eine Aufnahme der physischen Istprozesse von Bedeutung.
- **Konzeption.** In der Konzeptionsphase wird auf Basis des Lastenhefts ein Lösungskonzept erarbeitet und in einzelne Bausteine gegliedert. Das Konzept wird in einem Pflichtenheft dokumentiert und umfasst neben einer Darstellung des adressierten Anwendungsbereichs (z.B. in Form von Use Cases) auch eine Beschreibung von Benutzerschnittstelle und -funktionen sowie ein Datenmodell (z.B. als ER-Diagramm). Das Pflichtenheft dient wiederum als Grundlage

für eine detailliertere Systemspezifikation, in deren Kern eine IS-Architektur und Beschreibungen der einzelnen Systemkomponenten stehen. Für RFID-Systeme sind darüber hinaus auch eine Modellierung der physischen Abläufe im betrachteten Realweltausschnitt sowie die Layoutplanung, notwendige Hardwareinstallationen und Fragen der Anbringung bzw. Integration von Transpondern in oder an Gegenständen zu berücksichtigen.

- **Implementierung.** Die Implementierung hat die Entwicklung einer betriebsbereiten Lösung zum Ziel. Zu den dazu notwendigen Aktivitäten gehören Softwareentwicklung, Hardwareinstallation, Systemintegration sowie Test und Dokumentation. Die Ergebnisse der Implementierungsphase umfassen – abgesehen von der Lösung selbst – einen Projektabschlussbericht, in dem Verlauf und Resultat des Projekts dokumentiert sind, sowie eine technische Systemdokumentation und Unterlagen zur Schulung von Mitarbeitern. Darüber hinaus werden dem Auftraggeber auch Testprotokolle übergeben, die die Leistungsfähigkeit von Komponenten und Gesamtsystem belegen. Insbesondere Letzteres bedeutet im Fall von RFID unter Umständen aufwendige Tests, die nicht am Bildschirm simuliert, sondern in der realen Welt durchgeführt werden müssen. Ein Beispiel ist die Optimierung von Leseraten durch mehrfaches Durchfahren eines RFID-Lesebereichs mit einem Gabelstapler und wechselnden Produkten und Positionen auf der Palette.

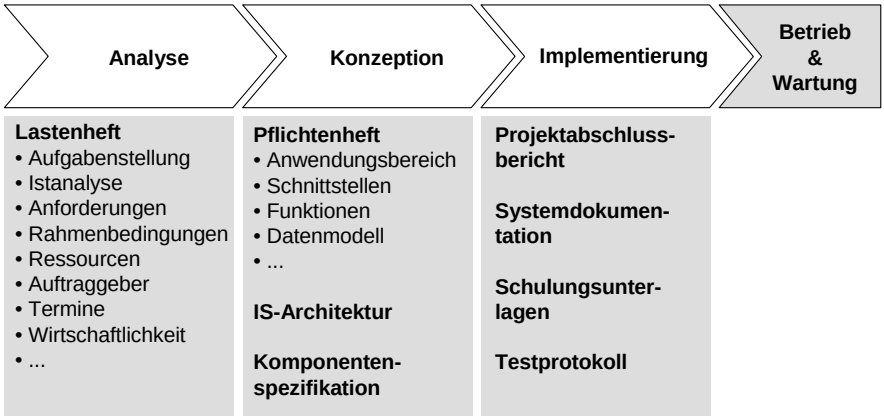


Abb. 2. Vorgehensmodell bei der RFID-Einführung

Betrieb und Wartung sind kontinuierlich ablaufende Prozesse mit sich regelmäßig wiederholenden Aufgaben. Hierzu können Administrationstätigkeiten wie das Sichern von Daten gehören, aber auch mehr oder weniger umfassende Modifikationen am System selbst – von der einfachen Fehlerbehebung bis zu einem Rücksprung in die Analysephase zwecks Erweiterung des Funktionsumfangs.

3.2 RFID-spezifische Aufgaben

Physische Objekte

Das Projektteam sollte zunächst alle Objekte identifizieren und klassifizieren, die für die zu implementierende Anwendung mit einem RFID-Transponder versehen werden. Dies können Paletten, Verpackungen oder einzelne Waren sein. Tabelle 1 fasst die zu evaluierenden Objekteigenschaften zusammen und zeigt auf, welche Anforderungen an das Tagging daraus abgeleitet werden können.

Tabelle 1. Objekteigenschaften

Objekteigenschaft	*Anforderung*
Wert des Objekts	Vom Wert des Objekts und dem von der Anwendung erwarteten Nutzen hängt ab, wie viel der Transponder kosten darf.
Spezielle Eigenschaften wie Größe, Oberflächenbeschaffenheit, Material, Inhalt	Sie bestimmen, wie der Transponder am Objekt befestigt bzw. im Objekt integriert werden kann. Metall oder Wasser am oder im Objekt würde aufgrund der Störung, die diese Materialien beim Auslesen verursachen, spezielle Transpondertypen verlangen oder kann sogar eine Lösung mit RFID verhindern.
Transponderplatzierung auf dem Objekt und Objektplatzierung in Bezug auf die Antenne des Lesegerätes	Die Transponderplatzierung und die Objektplatzierung in Bezug auf die Antenne des Lesegerätes bestimmen die erzielbare Lesereichweite.
Objekthierarchien	Die Objekte können zu Hierarchien zusammengefasst sein, die beispielsweise zwischen mit Transpondern versehener Ware und etikettierten Paletten bestehen können. Die Anwendung muss von der Lesersoftware die von ihr erwarteten Daten der entsprechenden Hierarchiestufe erhalten.
Mengengerüst	Über das Mengengerüst wird definiert, welches Datenvolumen höchstwahrscheinlich auf das Unternehmen zukommt, welche Skalierbarkeit von der Anwendung erwartet wird und wie groß die Anzahl der benötigten Transponder ausfällt.

Technologieauswahl

Bei der Technologieauswahl muss einerseits die grundsätzliche Machbarkeit einer Lösung nachgewiesen werden, andererseits muss die Entscheidung für einen bestimmten Anbieter gefällt werden. Machbarkeitsanalysen können häufig nur zusammen mit den Technologieherstellern durchgeführt werden. Die Wahl des Anbieters bestimmt maßgeblich sowohl den Implementierungserfolg als auch im Anschluss an das Projekt die Kosten für den Betrieb und die Wartung der Anwendung. Wichtige Auswahlkriterien für die Auswahl von Komponenten sind z.B. die Einhaltung von Standards und die Skalierbarkeit des Systems.

In einem zweiten Schritt sollte im Anschluss an eine Ortsbegehung („site survey“) definiert werden, welche internen und externen Organisationseinheiten an welchem Ort Lesegeräte einrichten müssen, damit das RFID-System seine Aufgabe gemäß der zu implementierenden Lösung erfüllen kann. In diesem Zusammenhang müssen sich die Projektpartner auch über die mit der Infrastruktur verbundenen Kosten einig werden. Der Erfassungsort, an dem Lesegerät und Antennen installiert werden, kann z.B. das Eingangstor einer Lagerhalle oder ein Regal im Supermarkt sein. Der Antennentyp kann beispielsweise eine Portalantenne sein, durch die ein Gabelstaplerfahrer mit Paletten beladen hindurchfährt. Für den RFID-Verantwortlichen sind die folgenden Faktoren von Bedeutung, welche die Eigenschaften der Lesegeräte und deren Erfassungsorte bestimmen:

- **Umgebungseinflüsse.** Die Eigenschaften des Ortes können technische Anforderungen determinieren. Beispielsweise gelten andere Frequenzen und erzielbare Lesereichweiten, abhängig davon, ob sich die Lesestation innerhalb oder außerhalb eines Gebäudes befindet.
- **Störfrequenzen.** In der Umgebung der Erfassungsorte kann es andere Anwendungen geben, die ähnliche oder gleiche Frequenzen wie das RFID-System benutzen. Dies hat möglicherweise zur Folge, dass eine hundertprozentige Leserate nicht garantiert werden kann. Konkurrierende Systeme sind beispielsweise WLAN oder Mobiltelefonsysteme.
- **Arbeitsablauf.** Das RFID-System sollte mit dem Arbeitsablauf im Einklang stehen, der sich durch die Anwendung ergibt. Die Konstruktion einer Portalantenne beispielsweise sollte auf die Bewegungen von Gabelstaplern im Areal ausgerichtet sein, nicht umgekehrt.
- **Antenneneigenschaften.** Die ausgewählte Antenne muss den Frequenz- und Lesereichweitenanforderungen der RFID-Anwendung genügen. Sie muss ferner vor physikalischer Zerstörung z.B. durch Maschinen geschützt sein sowie in den Erfassungsort integrierbar sein. Der Aufwand für Installation und spätere Nachjustierungen sollte gering sein.
- **Datenübertragung zwischen Antenne und Lesegerät.** Für die Datenübertragung stehen Verkabelung oder drahtlose Übertragung zur Auswahl. Für die Verkabelung muss ausreichend Platz bzw. müssen Kabelschächte vorhanden sein. Im Gegensatz dazu ist eine drahtlose Verbindung anfälliger gegenüber Störungen, dafür aber sehr flexibel für den Fall, dass sich Standorte von Lesestationen aufgrund von Prozessänderungen oder baulichen Maßnahmen verändern.
- **Stromversorgung.** Für Lesestationen und andere Systemkomponenten, die für die Anwendung im Sinne der Echtzeitanforderung kritisch sind, sollte der RFID-Verantwortliche überlegen, ob er eine zusätzliche, unterbrechungsfreie Stromversorgung einrichten sollte.
- **Netzwerke.** Das Datenaufkommen einer RFID-Installation kann unter Umständen hoch genug sein, um die Einrichtung eines zusätzlichen, vom übrigen Firmennetzwerk-LAN getrennten Netzwerks zu rechtfertigen. Vom Lesegerät muss in jedem Fall eine Netzwerkverbindung zu den Anwendungsservern mit genügend hoher Bandbreite bestehen.

Anwendungsdaten

Für eine erfolgreiche Integration der RFID-Anwendung in die bestehende Systemlandschaft des Unternehmens ist eine Definition von Anforderungen an die gelieferten RFID-Daten notwendig. Diese betreffen Aspekte wie Zeitnähe, Datenqualität sowie notwendige Schnittstellen und legen fest, unter welchen Voraussetzungen RFID-Daten von übergeordneten Systemen sinnvoll weiterverarbeitet werden können. Welche Arten von Anforderungen an das System gestellt werden, wird in Tabelle 2 anhand einiger Beispiele illustriert.

Tabelle 2. Anforderungen an RFID-Daten (Beispiele)

Kategorie	*Anforderungen*
Events und Tasks	• Zuordnung von Lesestationen, Objekten und Sequenzen von RFID-Daten zu Business Events • Geschäftsregeln und die daraus resultierenden Workflow-Regeln
Schnittstellen	• Schnittstellenspezifikationen zu betriebswirtschaftlichen Informationssystemen • Notwendige Änderungen in betriebswirtschaftlichen Informationssystemen und anderen Anwendungen • Abbildung von RFID-, Positions- und Sensordaten
Datenaggregation und Datenpfade	• Interpretation, Filterung und Management der gelesenen Daten • Verteilung der Daten
Echtzeitanforderungen	• Lesegeschwindigkeit in Echtzeit/näherungsweise in Echtzeit/nicht in Echtzeit • Zuordnung der Datenaggregationsstufe zur Echtzeitanforderung
Datengenauigkeit	• Erforderliche Leserate • Maßnahmen bei falsch oder nicht gelesenen Objekten
Datenbank	• Performance • Skalierbarkeit • Archivierungskonzept

Unterstützende Rollen und Prozesse

Neben der Ausgestaltung technischer Komponenten einer RFID-Lösung ist auch eine Reihe zusätzlicher unterstützender Prozesse bzw. Rollen notwendig, die in der Organisation implementiert werden müssen. Wichtige Aufgaben sind hier insbesondere:

- Das *Transpondermanagement* umfasst das Aufbringen neuer oder Ersetzen schadhafter Transponder am Objekt, das Verwalten von Transponder-IDs, das Einschleusen der Objekte in das System, Tests usw.
- Das *Lesegerätemanagement* ist für die Installation, Konfiguration, Ausmessung und Verkabelung der Lesegeräte und Antennen verantwortlich sowie für die Behebung von Störungen und Reparaturen.

- Zu den Aufgaben der *Systemadministration* zählt die Überwachung der Funktionsfähigkeit aller Hard- und Softwarekomponenten. Dazu gehört die Identifikation von versehentlich ausgeschalteten oder beschädigten Geräten, aber auch die Erkennung gradueller Verschlechterungen z.B. der Leserate und die Konfiguration der eingesetzten Software.

4 Kritische Erfolgsfaktoren

Entscheidend für den Erfolg eines RFID-Projekts ist nicht allein die Qualität des erarbeiteten Lösungskonzepts. Vielmehr spielt auch eine Reihe von „weichen" Faktoren eine entscheidende Rolle für den Fortgang des Projekts, für die Projektleiter und Change-Manager gleichermaßen verantwortlich sind:

- **Projektförderung.** Die Unterstützung für das Projekt durch das Management muss unternehmensintern und -extern kontinuierlich gesichert werden. Intern wird vorausgesetzt, dass sowohl die Geschäftsleitung als auch die gesamte Führungsebene das Projekt unterstützen. Für Projekte, die über das eigene Unternehmen hinausgehen, muss zusätzlich die Unterstützung der externen Kooperationspartner vorhanden sein. In einem RFID-Projekt entlang der Lieferkette könnten dies beispielsweise Zulieferer, Transportunternehmen oder Großhändler sein. Der Projektleiter sollte daher zu Beginn des Projekts mit den ausgewählten Partnern über den Zeitrahmen des Projekts, Anforderungen, Verantwortlichkeiten, Kosten und Ressourcen ein Einvernehmen erzielen.
- **Stakeholder-Management.** Der Erfolg einer RFID-Anwendung wird nicht nur von einer erfolgreichen technischen Realisierung abhängen, sondern vor allem auch davon, ob die Mitarbeiter des Unternehmens die technische Lösung akzeptieren. Intern und extern sollte der Projektleiter daher diejenigen Interessengruppen identifizieren, die einen positiven oder negativen Effekt auf den Erfolg der RFID-Anwendung besitzen können. Um den langfristigen Erfolg zu sichern, muss der Projektleiter die Unterstützung all dieser Stakeholder besitzen. Dazu sollte er regelmäßig analysieren, wie groß ihr Einfluss auf das Projekt ist und wie ihre Bereitschaft aussieht, das Projekt zu unterstützen. Bei einem Defizit müssen Maßnahmen ergriffen werden, wie beispielsweise eine gezielte Kommunikationsstrategie (s.u.). Mögliche Stakeholder-Gruppen bei einem RFID-Projekt im Supply Chain Management können insbesondere Geschäftsleitung, Lenkungsausschuss, Projektteam, operatives Management, betroffene Mitarbeiter, Kunden und Zulieferer sein.
- **Training.** Ein optimales Training ist auf diejenigen Stakeholder ausgerichtet, deren Arbeitsabläufe sich durch die Einführung eines RFID-Systems ändern. Die Lerneinheiten befähigen die jeweils zuständige Gruppe, das neue System einzurichten, zu betreiben und zu warten. Das Training dient auch dem Change Management, um Akzeptanz bei den Nutzern des zukünftigen Systems zu schaffen. Zu diesem Zweck muss ein geeigneter Trainer ausgewählt werden, der aus der Gruppe der internen oder externen Mitarbeiter rekrutiert werden kann. Die Trainer sind für die Vorbereitung des Lernmaterials und den Aufbau der Kurse verantwortlich. Sie sollten Erfahrung in Change-Management-Pro-

jekten besitzen und die Besonderheiten von RFID-Anwendungen kennen. Die Unternehmensleitung sollte das Training schon zu Beginn des RFID-Projekts unterstützen, in das Budget aufnehmen und durch das Projektteam implementieren.

- **Kommunikation.** Da die RFID-Anwendungen zahlreiche Bereiche im Unternehmen verändern können, sollte der Projektleiter Projektziele und Zeitpläne klar und verständlich an alle Mitarbeiter, Handelspartner und Kunden kommunizieren. Eine gute Kommunikationsstrategie enthält auf die Stakeholder abgestimmte Mitteilungen. Die Geschäftsleitung interessiert beispielsweise, welche Kosten sie durch eine erhöhte Transparenz im Lager einsparen kann. Die Lagerarbeiter hingegen interessieren sich für die Arbeitserleichterungen, die sich für sie in ihrer Routinearbeit ergeben. Um die Mitteilungen intern und extern während der gesamten Projektdauer adressatengerecht und regelmäßig zu verteilen, bietet sich die Entwicklung eines Kommunikationsplans an, wie er beispielhaft in Tabelle 3 skizziert ist.

Tabelle 3. Beispiel eines Kommunikationsplans

Stakeholder-Gruppe	*Medium*	*Ziel*	*Inhalt*	*Häufigkeit*
Geschäftsleitung	Präsentation	Sicherung der fortwährenden Unterstützung für das Projekt	Statusbericht	Alle 6 Monate
Mittleres Management	Informationsworkshop	Sicherung der fortwährenden Unterstützung für das Projekt	Nutzen der RFID-Anwendung	Alle 2 Monate
Lenkungsausschuss	Besprechung	Entscheidungsfindung	Benötigte Ressourcen	Einmal im Monat
Lagerarbeiter	Flyer z.B. bei der Gehaltsabrechnung	Sicherung der Akzeptanz des neuen Systems und Eingehen auf mögliche Ängste	Nutzen in der Routinetätigkeit	Einmal im Monat
Schlüsselkunden und -lieferanten	Bericht	Gewährleistung, dass das neue System reibungslos funktioniert	Schnittstellenbeschreibungen und Prozessänderungen	Bei Bedarf

Dem zuletzt genannten Punkt kommt eine besondere Bedeutung zu, sobald das RFID-Projekt auch Bereiche umfasst, in denen der Kunde in Berührung mit der Technologie kommen kann, beispielsweise auf der Verkaufsfläche eines Supermarkts. Aufgrund der Sensibilisierung der Öffentlichkeit für die möglichen Risiken von RFID – insbesondere in Bezug auf die Privatsphäre des Konsumenten – ist eine Unternehmenskommunikation auch nach außen erforderlich, die in einen Dialog mit externen Stakeholdern eintritt und über Vorgehen und Ziele des Pro-

jekts aufklärt, ohne belehrend zu wirken oder mögliche Probleme von vornherein wegreden zu wollen.

5 Zusammenfassung

Die Einführung integrierter RFID-Systeme erfordert im Vergleich zu den klassischen Insellösungen ein deutlich besser organisiertes und geplantes Projektmanagement aufseiten aller beteiligten Partner. Die Komplexität eines RFID-Projekts steigt insbesondere mit zunehmender Reichweite der horizontalen bzw. vertikalen Integration. Vor diesem Hintergrund wurden in diesem Beitrag einige wesentliche Aspekte des RFID-Projektmanagements beleuchtet, in denen sich die RFID-Systemeinführung von anderen IT-Projekten abhebt, und durch strukturierte Handlungsanleitungen für die Praxis ergänzt. Dabei sind es nicht einzelne Methoden oder Werkzeuge des Projektmanagements, die einen Unterschied ausmachen, als vielmehr Aktivitäten, wie sie beispielsweise die Abhängigkeit der RFID-Technologie von physikalischen Umgebungsbedingungen mit sich bringt.

Für viele Problemstellungen, mit denen sich das Projektteam bei der RFID-Einführung konfrontiert sieht, gibt es bislang wenig Erfahrungswerte, von wieder verwendbaren Lösungsbausteinen ganz zu schweigen. So sind u.a. die optimale Gestaltung von RFID-Antennen oder die Administration der eingesetzten Komponenten Themen, die konzeptionell bis heute noch wenig durchdrungen sind und meist eher improvisiert als geplant werden. Umso wichtiger ist daher ein professionelles Projektmanagement, welches die zu lösenden Aufgaben strukturiert angeht und deren Komplexität beherrschbar macht.

Finanzielle Bewertung von Ubiquitous-Computing-Anwendungen

Christian Tellkamp
Institut für Technologiemanagement, Universität St. Gallen

Kurzfassung. In vielen Unternehmen ist eine Wirtschaftlichkeitsrechnung Voraussetzung für größere Investitionsentscheidungen. Dieser Beitrag beschäftigt sich mit der finanziellen Bewertung von Ubiquitous-Computing-Anwendungen. Eine Kategorisierung solcher Anwendungen hinsichtlich ihrer Werttreiber soll Unternehmen helfen, mögliche Nutzenpotenziale zu identifizieren. Für die anschließende Wirtschaftlichkeitsbetrachtung wird ein auf Kosten-Nutzen-Analyse basierendes Vorgehen unter Berücksichtigung unterschiedlicher Szenarien vorgeschlagen. Beispiele aus verschiedenen Projekten illustrieren die Anwendbarkeit des vorgeschlagenen Vorgehens.

1 Herausforderungen bei der Bewertung

Die Beurteilung des wirtschaftlichen Nutzens eines Projektes spielt eine wesentliche Rolle bei größeren Investitionsentscheidungen (vgl. [Wil96]). Häufig ist eine Wirtschaftlichkeitsrechnung ein notwendiger – wenn auch nicht hinreichender – Schritt, um z.B. ein Pilotprojekt durchführen zu können [HoT94]. Im Folgenden wird ein generischer Ansatz vorgestellt, der in verschiedenen Projekten zur Beurteilung des monetären Nutzens von Ubiquitious-Computing-(UbiComp-)Anwendungen herangezogen wurde. Dazu werden UbiComp-Anwendungen in fünf Kategorien eingeteilt, die sich hinsichtlich der Werttreiber unterscheiden. Bislang gibt es nur isolierte Untersuchungen zu solchen Lösungen, z.B. zur Nutzung von Radio-Frequency-Identification-(RFID-)Technologie in der Lieferkette (z.B. [Acc02, IBM02]), welches ein konkretes Beispiel für eine Anwendung aus der Kategorie Objektverfolgung darstellt.

Unternehmen, die eine finanzielle Bewertung einer UbiComp-Anwendung durchführen möchten, stehen häufig vor drei wesentlichen Herausforderungen:

- Viele UbiComp-Anwendungen basieren auf neuartigen Technologien und waren bis vor kurzem so nicht realisierbar. In vielen Fällen gibt es nur wenige konkrete Erfahrungen und Fallbeispiele, die den tatsächlichen Nutzen demonstrieren.
- Bei bestimmten UbiComp-Anwendungen ist es schwierig, einzelne Nutzenanteile monetär zu bewerten. Hierfür kann es verschiedene Gründe geben, z.B. dass mehrere logische Zwischenschritte notwendig sind, um vom direkten Nutzen zu einer monetären Größe zu kommen, oder dass es eine längere Zeit dau-

ert, bis ein finanzieller Mehrwert sichtbar wird [WDK96]. Dieser Nutzenanteil wird im vorliegenden Beitrag als immaterieller Nutzen bezeichnet. Der immaterielle Nutzenanteil ist häufig hoch bei Anwendungen, bei denen es weniger auf Effizienzerhöhung als auf die Erhöhung der Effektivität oder eine Umgestaltung des Unternehmens geht [Nor96]. Als Beispiel sei das Pilotprojekt eines interaktiven Museums angeführt, bei dem der Nutzer mit einem Handgerät auf Ausstellungsstücke zeigen kann, um zusätzliche Informationen über diese abzurufen [FFK02]. Dieser Service kann die Qualität des Museumsbesuchs erhöhen. Wird der Service separat vom Eintrittspreis entgolten, ist die Kalkulation des finanziellen Nutzens ohne größere Probleme möglich. Anders ist es allerdings, wenn der Service bereits im Eintrittspreis enthalten ist. Dann wird es schwierig zu beurteilen, inwieweit aufgrund des Services mehr Besucher kommen oder die Eintrittspreise erhöht werden können. Auch Investitionen in eine neue IT-Infrastruktur und in Systeme mit strategischer Bedeutung sind häufig monetär schwer zu rechtfertigen [WDK96]. Die Einführung von RFID z.B. im Einzelhandel kann als ein Beispiel für eine Investition in eine neue Infrastruktur, die die bisherige Barcode-Infrastruktur ersetzt, gesehen werden. Eine halbwegs exakte Wirtschaftlichkeitsrechnung ist hier unter Umständen nur schwer möglich.

- Bestimmte UbiComp-Anwendungen betreffen nicht nur ein, sondern mehrere Unternehmen. Hier ist neben der finanziellen Beurteilung des Gesamtsystems auch eine detaillierte Betrachtung der einzelnen Unternehmen notwendig.

Häufig wird in der Praxis der Begriff „Business Case“ im Zusammenhang mit der finanziellen Bewertung eines Projektes verwendet. Hogbin und Thomas [HoT94] folgend, geht es bei einem Business Case aber um mehr als eine Abschätzung der wirtschaftlichen Vorteilhaftigkeit. Ein Business Case berücksichtigt nach Ansicht der Autoren die folgenden Aspekte: Zielsetzung und Abgrenzung des Projektes, Anforderungen, Lösungsvorschlag mit Alternativen, Beschränkungen und Risiken, greifbare und immaterielle Nutzenpotenziale sowie eine Wirtschaftlichkeitsabschätzung. Einige dieser Punkte wie Zielsetzung des Projektes, Lösungsvorschlag, Nutzenpotenziale stellen Voraussetzungen dar – zumindest bis zu einem gewissen Grad, um überhaupt eine erste Wirtschaftlichkeitsanalyse sinnvoll durchführen zu können. Im Folgenden soll aufgezeigt werden, wie eine solche Wirtschaftlichkeitsanalyse durchgeführt werden kann.

2 Ein Ansatz zur Bewertung von UbiComp-Anwendungen

UbiComp-Anwendungen lassen sich im Allgemeinen mit herkömmlichen Verfahren der dynamischen Investitionsrechnung bewerten. Mittels einer Kosten-Nutzen-Analyse, in der die einzelnen Kosten- und Nutzentreiber ermittelt werden, schätzt man die Zahlungsströme des Investitionsprojektes ab, aus denen durch Diskontierung ein Barwert ermittelt wird.

Ermittlung der Nutzentreiber

Die Ermittlung eines Nutzentreibers ist exemplarisch in Abbildung 1 dargestellt. Bei diesem Nutzentreiber wird die Ergebnisauswirkung ermittelt, die eine Erhöhung der Produktverfügbarkeit im Verkaufsregal hat, z.B. aufgrund der Nutzung von RFID-Technologie.

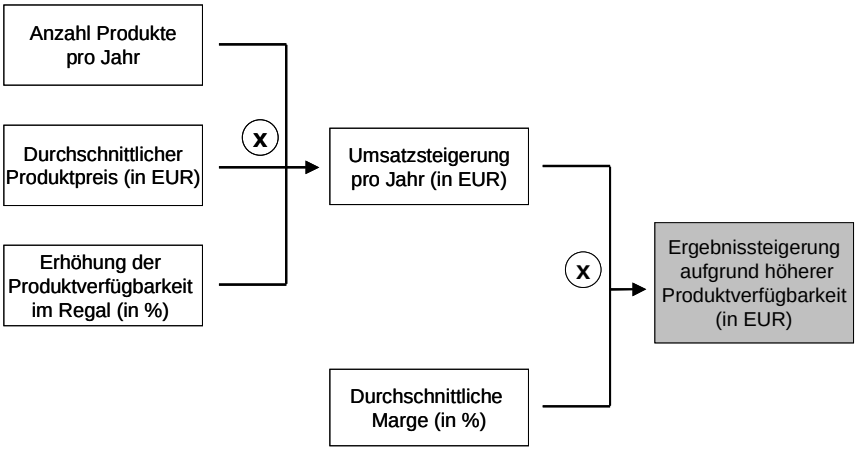


Abb. 1. Ermittlung eines Nutzentreibers am Beispiel Produktverfügbarkeit

Definition von Szenarien

Der hier vorgestellte Ansatz sieht vor, dass die Entscheidung über die Realisierung der Anwendung in zwei Schritten erfolgt: Am Anfang steht eine Pilotphase, in der die Machbarkeit überprüft wird. Nach Beendigung der Pilotphase entscheiden die Projektbeteiligten, ob das Projekt tatsächlich umgesetzt wird. Bei einer positiven Entscheidung folgen die Implementierung und anschließend der Betrieb.

Es wird vorgeschlagen, für jede UbiComp-Anwendung drei Szenarien zu betrachten, ein „realistisches“, ein „optimistisches“ und ein „pessimistisches“. Das realistische Szenario basiert auf den aus heutiger Sicht „im Mittel“ erwarteten Kosten- und Nutzengrößen. Ein optimistisches Szenario kann zusätzlich berücksichtigen, dass die Nutzenpotenziale beim Eintreten bestimmter Ereignisse auch höher ausfallen, dass weitere Nutzenpotenziale realisiert werden oder dass die Anwendung selbst oder die gewonnenen Erfahrungen in anderen Bereichen verwendet werden können. Ein pessimistisches Szenario könnte z.B. vorsehen, dass nach Abschluss der Pilotphase die Entscheidung fällt, das Projekt nicht weiter fortzusetzen. Bei einer solchen Entscheidung fällt dann kein weiterer Aufwand für Implementierung und Betrieb an. Mit Hilfe dieser Überlegungen lassen sich einige grundlegende Ideen aus dem Bereich von Realoptionen berücksichtigen. Die Investition in ein Pilotprojekt beinhaltet die Option, die Entscheidung über die Realisierung des kompletten Projektes auf Basis detaillierterer Informationen zu einem späteren Zeitpunkt treffen zu können.

Abbildung 2 zeigt eine schematische Darstellung der Zahlungsflüsse anhand eines konkreten Beispiels aus der Automobilindustrie, das im Folgenden zur Illustration verwendet werden soll. Bei dieser Anwendung werden Transportbehälter für bestimmte Teile, die in der Automobilproduktion zum Einsatz kommen, mit aktiven RFID-Transpondern ausgestattet. Im Werk werden bestimmte Zonen definiert, an deren Eingängen RIFD-Leser installiert sind. Hierdurch ist jederzeit möglich, die Positionen der einzelnen Behälter und die Bestände in den einzelnen Zonen zu bestimmen. Die Bestandsinformationen können mit den Sollbeständen abgeglichen werden. Darüber hinaus sind verschiedene Auswertungen möglich, z.B. zur durchschnittlichen Umlaufzeit eines Behälters.

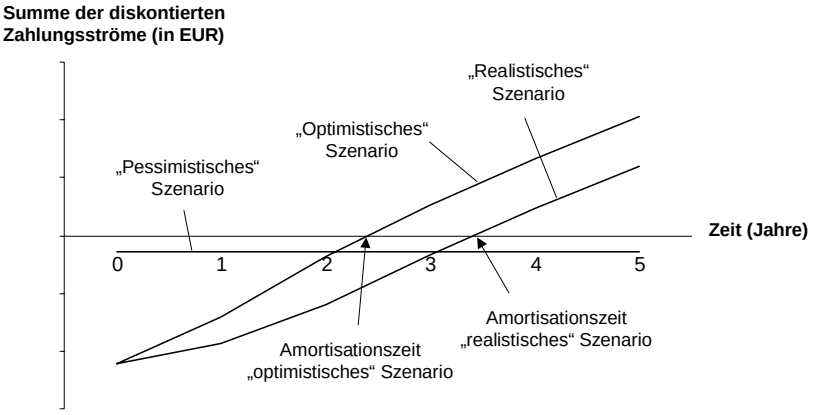


Abb. 2. Zahlungsflüsse der drei Szenarien für das Transportbehälterbeispiel

Das Projekt erscheint wirtschaftlich lohnenswert, wenn sich Kosten und Nutzen wie erwartet entwickeln (vgl. das „realistische“ Szenario in der Abb. 2). Der Kapitalwert für den „optimistischen“ Fall ist – wie zu erwarten – höher als der des realistischen Szenarios. Bei diesem Szenario wurde berücksichtigt, dass die Lösung in mehr als einem Werk eingesetzt werden kann und dass die gewonnenen Erfahrungen den Aufwand für die Implementierung in weiteren Werken reduzieren.

Sensitivitätsanalyse

Zusätzlich zu den Szenarien können Sensitivitätsanalysen durchgeführt werden. Hiermit lassen sich die kritischen Werte für einzelne Parameter ermitteln, bei deren Über- bzw. Unterschreitung der Barwert eine bestimmte Grenze erreicht und etwa vom positiven in den negativen Bereich wechselt. So zeigte sich im Transportbehälterbeispiel, dass die Anwendung vermutlich nur wirtschaftlich sinnvoll ist, wenn es mit der Lösung gelingt, die Anzahl der Transportbehälter zu reduzieren, die z.B. bei einem Produktwechsel neu zu beschaffen sind. Eine Reduzierung der derzeit anfallenden Kosten, die aufgrund von Verlust oder Suche

nach Behältern entstehen, rechtfertigt für sich allein gesehen eine Investition nicht.

Berücksichtigung immaterieller Nutzenpotenziale

In den obigen Berechnungen wurden nur die monetär bewertbaren Größen berücksichtigt. Die Nichtberücksichtigung des immateriellen Nutzens wird häufig als ein Grund für eine kurzfristige Orientierung bei der Auswahl von Investitionsprojekten und die Ablehnung viel versprechender, aber schwer monetär bewertbarer Projekte genannt [ToJ93]. Daraus wird dann gefolgert, dass eine Kosten-Nutzen-Analyse unpassend sei, um Investitionsprojekte zu beurteilen [Kap86]. Stattdessen werden Verfahren wie z.B. Nutzwertanalysen propagiert. Toraskar und Joglekar [ToJ93] diskutieren gängige Vorwürfe gegen die Verwendung von Kosten-Nutzen-Analysen und zeigen überzeugend, warum diese aus ihrer Sicht dennoch ein sinnvolles Instrument der Entscheidungsunterstützung sind.

Der immaterielle Nutzen kann auch bei einer Kosten-Nutzen-Analyse in die Entscheidung einbezogen werden, wie z.B. von Kaplan [Kap86] vorgeschlagen. Angenommen, eine initiale Bewertung, bei der nur der direkt monetär bewertbare Nutzen berücksichtigt wird, ergibt einen negativen Barwert von x. Über den monetär bewertbaren Nutzen hinaus wird ein zusätzlicher immaterieller Nutzen z.B. in Form von Verbesserungen in der Qualität und der Kundenzufriedenheit erwartet, der nicht monetär quantifiziert werden konnte. In einem zweiten Schritt lässt sich dieser jetzt in die Analyse einbeziehen. Die nun zu klärende Frage unterscheidet sich von der ursprünglichen Frage. Statt einer Abschätzung, wie hoch der immaterielle Nutzen vermutlich sein könnte, gilt es nun zu entscheiden, ob der finanzielle Gegenwert einer Steigerung von Qualität und Kundenzufriedenheit mindestens x beträgt. Die zweite Frage ist häufig leichter zu beantworten als die erste.

3 Generische Ubiquitous-Computing-Anwendungen

Eine wesentliche Herausforderung für die Bewertung neuartiger Anwendungen ist die Identifikation der relevanten Kosten- und Nutzentreiber. Dazu wird eine Einteilung von UbiComp-Anwendungen in fünf Kategorien vorgeschlagen, welche auf Grundlage einer Datenbank ermittelt wurden, in der mehr als 50 Anwendungsfälle gesammelt wurden. Für jede generische Anwendung wurden die potenziell wesentlichen Kosten- und Nutzentreiber sowie immaterielle Nutzenpotenziale identifiziert. Die vorgeschlagene Kategorisierung hat sich in diversen Projekten als hilfreich für die Bewertung erwiesen.

Tabelle 1. Generische Ubiquitous-Computing-Anwendungen

	Monitoring	Positionierung	Objektinformation	Objektverfolgung	Automatische Transaktion
Fokus	Datengenerierung mit Sensoren und Datenübertragung	Weitergabe der Position	Zugriff auf Informationen durch Nut-zer	Verfolgung eines Objekts im Zeitablauf	Automatische Auslösung von Transaktionen
Unterstützte Prozessschritte	Objekt sammelt kontinuierlich Informationen über Umwelt und eigenen Status Zentrales System kann Daten an Objekt übermitteln Nutzer kann lokal auf Daten zugreifen und diese manipulieren	Objekt übergibt Daten zur eigenen Identität und Position	Nutzer kann Informationen zum Objekt abrufen Nutzer kann Daten zum Objekt manipulieren	Objekt übergibt Daten zur eigenen Identität und Position Zentrales System oder Objekt speichert Objektposition im Zeitablauf Nutzer kann auf Positionsinformationen (und andere Daten) zugreifen	Objekt startet Transaktionen bei Erfüllung bestimmter Kriterien
Beispiele	Überwachung von Verkaufsautomaten	Flottenmanagement Nutzungsbasierte Autoversicherungsprämien	Zugriff auf Wartungsinformationen Produktauthentifizierung	Produktverfolgung Frachtverfolgung	Selbst-Checkout im Supermarkt Zugangskontrolle

Tabelle 1 gibt eine Übersicht über die fünf Kategorien (Monitoring, Positionierung, Objektinformation, Objektverfolgung, automatische Transaktionsinitiierung) und nennt Beispiele zu jeder der generischen Anwendungen. Obwohl die Prozessschritte, die von den jeweiligen Anwendungen unterstützt werden, zum Teil identisch sind, ist der Fokus der Anwendung jeweils spezifisch. Tabelle 2 zeigt beispielhaft die Kosten- und Nutzentreiber sowie die immateriellen Nutzenpotenziale für die generische Anwendung „Objektverfolgung“.

Tabelle 2. Kosten- und Nutzentreiber sowie immaterielle Nutzenpotenziale für die generische Anwendung „Objektverfolgung“

Nutzentreiber	Kostentreiber	Immaterielle Nutzenpotenziale
Erhöhte Objektverfügbarkeit Erhöhte Objektsicherheit Automatische Überprüfung der Übereinstimmung von Objektidentität und Position Bestandesreduktion bei Objekten Zugriff auf Objektposition und weitere Informationen	Aufwand für Ausrüstung der Objekte mit Transpondern, Sensoren etc. Aufwand für Betrieb Aufwand aufgrund von Fehlern bei Produktverfolgung Aufwand für Pilotanwendung Anpassen von Arbeitsprozessen und bestehenden Systemen Beschaffung von zentraler Soft- und Hardware Aufwand für Infrastruktur für Positionsbestimmung, inklusive Installation	Erhöhte Transparenz aufgrund durchgängiger Objektverfolgbarkeit Erhöhung der Flexibilität und schnellere Reaktionszeiten

4 Vorgehensvorschlag für die Bewertung

Für die Durchführung der finanziellen Bewertung einer UbiComp-Anwendung wird ein fünfstufiger Prozess vorgeschlagen, der in Abbildung 3 dargestellt ist. In einem ersten Schritt wird geprüft, inwieweit die Zielsetzung der vorgeschlagenen Lösung dem Fokus einer der generischen Anwendungen entspricht. Ist eine solche Zuordnung erfolgt, lässt sich auf Basis der generischen Kosten- und Nutzentreiber bereits eine erste Abschätzung der finanziellen Vorteilhaftigkeit durchführen. Hierzu sind die notwendigen Parameter zu schätzen (Schritt 2), aus denen ein Ergebnis, z.B. in Form eines Kapitalwerts, berechnet wird (Schritt 3). In Schritt 4 sollte dieses Ergebnis auf Plausibilität geprüft und Sensitivitätsanalysen durchgeführt werden. Zu diesem Zeitpunkt können auch immaterielle Nutzenpotenziale in die Beurteilung einbezogen werden. Dieses Ergebnis wird allerdings in den meisten Fällen noch nicht das endgültige Resultat sein. In einem fünften Schritt wird es häufig sinnvoll sein, die Berechnungen unter Berücksichtigung der spezifischen Umstände und Beschränkungen anzupassen. Auch im Anschluss hieran sollten die Ergebnisse auf Plausibilität geprüft und Sensitivitätsanalysen durchgeführt werden.

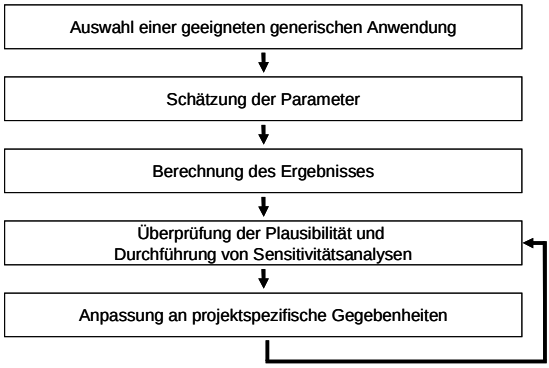


Abb. 3. Vorgehensvorschlag bei der Bewertung von UbiComp-Anwendungen

In einem ersten Schritt wird geprüft, inwieweit die Zielsetzung der vorgeschlagenen Lösung dem Fokus einer der generischen Anwendungen entspricht. Ist eine solche Zuordnung erfolgt, lässt sich auf Basis der generischen Kosten- und Nutzentreiber bereits eine erste Abschätzung der finanziellen Vorteilhaftigkeit durchführen. Hierzu sind die notwendigen Parameter zu schätzen (Schritt 2), aus denen ein Ergebnis, z.B. in Form eines Kapitalwerts, berechnet wird (Schritt 3). In Schritt 4 sollte dieses Ergebnis auf Plausibilität geprüft und Sensitivitätsanalysen durchgeführt werden. Zu diesem Zeitpunkt können auch immaterielle Nutzenpotenziale in die Beurteilung einbezogen werden. Dieses Ergebnis wird allerdings in den meisten Fällen noch nicht das endgültige Resultat sein. In einem fünften Schritt wird es häufig sinnvoll sein, die Berechnungen unter Berücksichtigung der spezifischen Umstände und Beschränkungen anzupassen. Auch im Anschluss hieran sollten die Ergebnisse auf Plausibilität geprüft und Sensitivitätsanalysen durchgeführt werden.

Abbildung 4 zeigt eine mögliche Aufbereitung für die Ergebnisse der finanziellen Abschätzung. Dargestellt sind die Ergebnisse für das „realistische“ Szenario. Die Abbildung vermittelt einen schnellen Überblick über die relative Bedeutung der einzelnen Kosten- und Nutzentreiber.

5 Bisherige Erfahrungen

Im Folgenden sollen einige Erfahrungen aus Wirtschaftlichkeitsanalysen für diverse UbiComp-Projekte dargestellt werden, die im Rahmen des M-Lab-Kompetenzzentrums durchgeführt wurden. Unter anderem wurden Analysen für folgende Projekte erstellt:

- Für eine Pharmafirma wurde untersucht, inwieweit eine Lösung, mit der die Compliance bei der Einnahme von Tabletten überwacht werden kann, wirtschaftlich lohnenswert ist.
- Bei einem Automobilhersteller wurde analysiert, unter welchen Bedingungen die Verfolgung von Ersatzteilen im Lager sinnvoll ist.

- Unter Einbeziehung von mehreren Mitgliedern des Auto-ID Centers wurde ein Internet-basiertes Tool entwickelt, mit dem der Nutzen und die Kosten von RFID-Transpondern in der Lieferkette abgeschätzt werden kann.

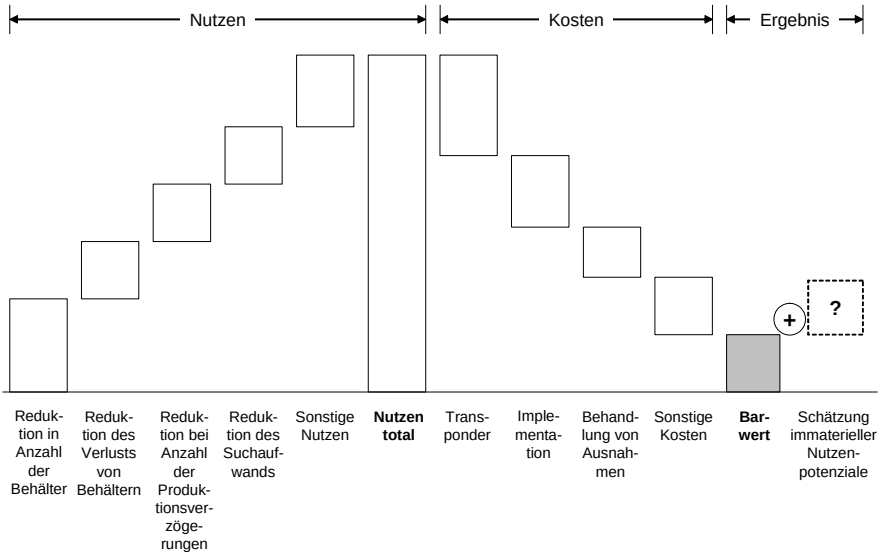


Abb. 4. Kosten- und Nutzentreiber im „realistischen" Szenario für das Transportbehälterbeispiel

Anwendbarkeit des Ansatzes

In allen bisher untersuchten Anwendungen war eine Zuordnung zu einer der generischen Anwendungen möglich. Beim ersten genannten Beispiel handelte es sich um eine Monitoring-Anwendung, bei den beiden anderen Beispielen um Anwendungen im Bereich Objektverfolgung.

Die Aufstellung der potenziell relevanten Kosten- und Nutzentreiber sowie des immateriellen Nutzens erleichterte die initiale Abschätzung der Wirtschaftlichkeit. Dennoch waren in allen Fällen individuelle Anpassungen der Berechnungen notwendig, um spezifische Umstände der Anwendung berücksichtigen zu können. Es war nicht möglich, ein allgemein gültiges Berechnungsschema für die einzelnen generischen Kategorien von UbiComp-Anwendungen zu definieren, mit dem sich die wirtschaftliche Vorteilhaftigkeit beliebiger Anwendung in dieser Kategorie berechnen ließe. Ebenso wenig ist eine A-priori-Aussage möglich, welche Arten von Anwendungen sich rechnen und welche nicht.

Während auf die Definition und Berechnung von optimistischen und pessimistischen Szenarien häufig verzichtet wurde, waren Plausibilitätsüberlegungen und Sensitivitätsanalysen unerlässlich, da in den meisten Fällen praktisch keine Wissensgrundlage vorhanden war, aus der sich konkrete Abschätzungen hinsichtlich Kosten und Nutzen ableiten ließen. Dennoch wurde häufig bereits ohne konkret

verifizierbare Zahlen deutlich, was die wesentlichen Kosten- und Nutzentreiber sind, die genauer analysiert und beobachtet werden müssen. Diese Fokussierung auf wenige kritische Treiber war häufig ein wesentliches Ergebnis der Wirtschaftlichkeitsabschätzungen.

Weitere Erkenntnisse aus Projekten

Wie bereits deutlich geworden ist, basieren viele der Anwendungen zumindest teilweise auf dem Einsatz von Transpondern. Hier hat sich bewährt, technische Restriktionen hinsichtlich der erreichbaren Leserate in die Beurteilung einzubeziehen, z.B. in Form der Berechnung der Sensitivität des Ergebnisses in Abhängigkeit von der Leserate. So lässt sich abschätzen, welche finanziellen Folgen eine Leserate von weniger als 100 % hat (z.B. Folgekosten aufgrund falscher Informationen bzw. Aufwand für die Korrektur der Lesefehler).

Auch wenn es nicht möglich erscheint, allgemeine Beurteilungskriterien aufzustellen, welche Anwendungen finanziell lohnenswert sind, so sind doch einige Aussagen hinsichtlich einzelner Kostentreiber möglich. Bei UbiComp-Anwendungen geht es häufig darum, dass eine Vielzahl von Objekten mit Transpondern, Sensoren etc. ausgestattet wird. Eine Abschätzung der damit verbundenen Kosten erlaubt häufig bereits eine erste Aussage darüber, ob eine solche Anwendung überhaupt realistisch ist. Ähnliches gilt auch für Überlegungen hinsichtlich der Anzahl der Lokationen, an denen Daten ausgelesen werden sollen. Es gilt abzuschätzen, welche Infrastruktur hierfür notwendig ist. Weitere Kosten z.B. für Integration der Daten, Prozessänderungen etc. hängen unter anderem davon ab, wie die Technologien eingesetzt werden. Geht es nur darum, Informationen, die bereits erhoben werden, jetzt zeitnäher und akkurater zu erfassen, sind die Kosten voraussichtlich geringer als in Fällen, in denen neue oder detailliertere Daten generiert, verarbeitet und ausgewertet werden müssen.

Eine gewisse Hilfestellung bei der Abschätzung des voraussichtlichen Nutzens und der Kosten können Demonstratoren oder Pilotanwendungen liefern. Allerdings ist der Mehrwert begrenzt, wenn diese im Wesentlichen nur dazu dienen, die technische Machbarkeit zu demonstrieren. Prozessverbesserungen wie z.B. Erhöhung der Produktverfügbarkeit aufgrund der Ausstattung von Produkten, Kartons oder Paletten mit RFID-Transpondern werden erst in halbwegs realistischen Anwendungsszenarien sichtbar. Diese Voraussetzungen sind bei Demonstratoren oder Pilotanwendungen häufig nicht gegeben. Soll die Wirtschaftlichkeit eines Lösungsansatzes überprüft werden, gelingt dies in der Regel nur, wenn diese Anforderung bei der Definition des Demonstrators oder Piloten direkt mit berücksichtigt wird.

Nicht in allen Fällen, in denen eine Kosten-Nutzen-Analyse durchgeführt wurde, lagen bereits konkrete Zielsetzungen oder Lösungsvorschläge vor. Im Gegenteil, häufig wurde ein umgekehrter Ansatz verfolgt: Mit Hilfe einer – notwendigerweise sehr groben – Wirtschaftlichkeitsrechnung sollten Potenziale identifiziert werden, um im Anschluss daran mit konkreten Aktivitäten (z.B. dem Ausarbeiten eines konkreten Lösungsvorschlags oder der Überprüfung der technischen Machbarkeit) zu beginnen. Dieses Vorgehen erscheint aber nur bedingt sinnvoll.

In einigen Fällen, bei denen mehrere Parteien von einer Anwendung betroffen waren, stellte sich die Frage nach der Ebene der Analyse. Gilt es, die Wirtschaftlichkeit aus der Sicht eines Unternehmens oder aus der Sicht aller Beteiligten zu beurteilen? Ganz konkret stellt sich die Frage z.B. beim Einsatz von RFID-Transpondern in der Lieferkette. Häufig gehen die Einzelhändler davon aus, dass die Produkte bereits bei der Herstellung bzw. Auslieferung mit Transpondern ausgestattet werden und dass der Hersteller zumindest einen großen Teil der Kosten trägt. Betrachtet man den Einzelhändler isoliert, kann der Einsatz von Transpondern für ihn durchaus wirtschaftlich sinnvoll erscheinen, da er die Kosten nicht zu tragen hat. Für die Einführung ist dies jedoch nicht entscheidend. Wesentliches Kriterium ist, dass (a) der Nutzen in der gesamten Lieferkette größer ist als die Kosten und (b) die Kosten so verteilt sind, dass alle involvierten Parteien profitieren. (Es sei denn, der Einzelhändler nutzt seine Einkaufsmacht und kann die Einführungen von Transpondern auch unabhängig von der Vorteilhaftigkeit für den Hersteller durchdrücken.)

Bei der Anwendung von Transpondern in der Lieferkette – aber auch bei anderen Beispielen wie dem Compliance-Management im Pharmabereich – zeigt sich, dass neben der wirtschaftlichen Betrachtung weitere Faktoren wie Akzeptanz oder organisatorische Durchsetzbarkeit einen wesentlichen Einfluss darauf haben, ob Projekte weiterverfolgt werden. Es ist schwer zu beurteilen, inwieweit die Ergebnisse von Wirtschaftlichkeitsbetrachtungen überhaupt den weiteren Projektverlauf maßgeblich beeinflussen. Die Erfahrungen aus den bisherigen Projekten haben gezeigt, dass – zumindest in den frühen Projektphasen, in denen die Abschätzungen durchgeführt wurden – die Ergebnisse nicht von entscheidender Bedeutung für das weitere Vorgehen waren.

6 Zusammenfassung und Schlussfolgerungen

In diesem Beitrag wurde ein Ansatz zur Bewertung von UbiComp-Anwendungen skizziert. Der Ansatz besteht aus (a) einem Entwurf für ein Berechnungsmodell, (b) einer Aufstellung generischer UbiComp-Anwendungen und (c) einem fünfstufigen Vorgehensvorschlag. Er soll Personen unterstützen, die Wirtschaftlichkeitsanalysen für Projekte durchführen möchten, bei denen UbiComp-Technologien eingesetzt werden.

Das Berechnungsmodell berücksichtigt gängige Methoden wie Kosten-Nutzen-Analyse, dynamische Investitionsrechnung und Szenarioanalyse und ist nicht spezifisch für die Bewertung von UbiComp-Technologien. Dies gilt ebenso für den Vorgehensvorschlag. Diese beiden Bestandteile des Ansatzes sind daher eher als allgemeine Hilfestellung für die Erstellung von Wirtschaftlichkeitsberechnungen zu verstehen.

Die fünf generischen Anwendungen, die in diesem Beitrag vorgeschlagen wurden, sollen demgegenüber konkrete Hilfestellung bei der Bewertung von UbiComp-Anwendungen geben. Bei den Kategorien handelt es sich um Monitoring, Positionierung, Objektinformation, Objektverfolgung sowie automatische Transaktionsinitiierung. Lässt sich eine angedachte konkrete Anwendung einer generischen Anwendung zuordnen, kann eine initiale Bewertung schneller durchgeführt

werden, da zu jeder generischen Anwendung bereits wesentliche Kosten- und Nutzentreiber sowie immaterielle Nutzenpotenziale aufgeführt sind. Dabei wird unterstellt, dass UbiComp-Anwendungen bez. ihrer Kosten- und Nutzentreiber sowie ihrer immateriellen Nutzenpotenziale hinreichend ähnlich sind, sodass generische Applikationen identifizierbar sind. Die bisher durchgeführten Analysen unterstützen diese Vermutung.

Aus bisher durchgeführten Projekten lassen sich einige Erkenntnisse hinsichtlich der Bewertung von UbiComp-Anwendungen gewinnen, die teilweise auch auf andere Anwendungen übertragbar sind:

- Auch wenn das für eine Analyse notwendige Zahlenmaterial häufig nicht vollständig ist, kann eine Wirtschaftlichkeitsanalyse hilfreich sein. In vielen Fällen kann sie dabei helfen, die wesentlichen Kosten- und Nutzentreiber zu identifizieren, auf die man sich nachfolgend fokussieren kann.
- Technische Restriktionen sollten in die Wirtschaftlichkeitsanalyse mit einbezogen werden. Beispielsweise sind bei bestimmten Anwendungsszenarien von RFID Leseraten von weniger als 100% zu erwarten. Die dadurch entstehenden Folgekosten sind ein Kostentreiber, den es zu berücksichtigen gilt.
- UbiComp-Anwendungen basieren häufig darauf, dass eine Vielzahl von Objekten mit Transpondern, Sensoren etc. ausgestattet wird. Eine Abschätzung der Kosten hierfür sowie für die notwendige Infrastruktur zum Auslesen der Daten kann unter Umständen schon eine erste Aussage darüber ermöglichen, ob eine Anwendung überhaupt wirtschaftlich sinnvoll sein kann.
- Demonstratoren oder Pilotanwendungen sind häufig nur von begrenztem Nutzen bei Wirtschaftlichkeitsbetrachtungen. Wenn Erkenntnisse für diesen Zweck generiert werden sollen, sollte dies bereits zu Beginn des Projektes berücksichtigt werden.
- Vor der Durchführung einer Wirtschaftlichkeitsanalyse ist es hilfreich, wenn bereits grobe Vorstellungen z.B. zur Zielsetzung sowie der technischen Machbarkeit und Umsetzung vorliegen. Anwendungsfelder ausgehend von finanziellen Betrachtungen zu finden, scheint nicht unbedingt zielführend.
- Wird eine UbiComp-Anwendung nicht nur innerhalb eines Unternehmens eingesetzt, sondern betrifft sie auch weitere Partner, so sollten Wirtschaftlichkeitsüberlegungen die Partner mit einbeziehen. In vielen Fällen wird eine Anwendung nur dann dauerhaft erfolgreich sein, wenn alle Beteiligten einen Mehrwert für sich sehen.
- Der Mehrwert von Wirtschaftlichkeitsbetrachtungen für Anwendungen, die bisher noch nicht weit verbreitet sind und bei denen der materielle Nutzen schwer abzuschätzen ist, ist naturgemäß schwer zu beurteilen. Die Erfahrungen zeigen, dass eine solche Analyse durchaus sinnvoll, aber häufig nicht entscheidend für den weiteren Projektfortschritt ist. Dies gilt unter anderem auch für Fälle, bei denen es um Infrastrukturentscheidungen geht.

Die derzeitigen Erkenntnisse zur Wirtschaftlichkeit von UbiComp-Anwendungen basieren derzeit größtenteils noch auf Überlegungen zu konkreten Anwendungsszenarien und Pilotanwendungen. Der Einsatz von UbiComp-Technologien in inner- und zwischenbetrieblichen Anwendungen steht aber erst am Anfang. Weiter gehende Erkenntnisse sind zu erwarten, wenn verstärkt reale

Anwendungen untersucht werden können. Hier kann dann insbesondere der Vergleich der zu Beginn erwarteten Nutzenpotenziale mit den tatsächlich realisierten Nutzenpotenzialen aufschlussreich sein.

Literatur

[Acc02] Accenture (2002) Auto-ID Across the Value Chain – From Dramatic Potential to Greater Efficiency & Profit. Auto-ID Center Report, archive.epcglobalinc.org/publishedresearch/ACN-AUTOID-BC-001.pdf

[FFK02] Fleck M, Frid M, Kindberg T, O'Brien-Strain E, Rajani R, Spasojevic M (2002) From Informing to Remembering – Deploying a Ubiquitous System in an Interactive Science Museum. IEEE Pervasive Computing 1(2): 13–21

[HoT94] Hogbin G, Thomas D (1994) Investing in Information Technology – Managing the Decision-making Process. McGraw-Hill

[IBM02] IBM Business Consulting Services (2002) Focus on Retail – Applying Auto-ID to Improve Product Availability at the Retail Shelf. Auto-ID Center, archive.epcglobalinc.org/publishedresearch/IBM-AUTOID-BC-001.pdf

[Kap86] Kaplan R (1986) Must CIM be justified by faith alone? Harvard Business Review 64(2): 87–95

[Nor96] Norris G (1996) Post-investment appraisal. In: Willcocks L (ed) Investing in Information Systems – Evaluation and Management. Chapman & Hall, pp 193–223

[ToJ93] Toraskar K, Joglekar P (1993) Applying Cost-benefit Analysis (CBA) Methodology for Information Technology Investment Decisions. In: Banker R, Kauffman R, Mahmood M (eds) Strategic Information Management – Perspectives on Organizational Growth and Competitive Advantage. Idea Group, Harrisburg, pp 119–142

[WDK96] Whiting R, Davies J, Knul M (1996) Investment appraisal for IT systems. In Willcocks L (ed) Investing in Information Systems – Evaluation and Management. Chapman & Hall, pp 37–57

[Wil96] Willcocks L (1996) Introduction – beyond the IT productivity paradox. In: Willcocks L (ed) Investing in Information Systems – Evaluation and Management. Chapman & Hall, pp 1–12

Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie

Marc Langheinrich
Institut für Pervasive Computing, ETH Zürich

The risk RFID technology poses to humanity is on a par with nuclear weapons
Katherine Albrecht (2003)[53]

Kurzfassung. Mit der durch Ubiquitous Computing möglichen feinmaschigen Überwachung vielfältiger Phänomene können nicht nur betriebliche Abläufe, sondern potenziell auch die daran beteiligten Lieferanten, Mitarbeiter und natürlich auch Kunden in einer noch nie da gewesenen Qualität beobachtet werden. Zwar existieren bereits seit Längerem technische Mittel und Verfahren, elektronische Informationen datenschutzkonform zu speichern und zu verarbeiten, doch ist ein direkter Einsatz dieser klassischen Technologien im Rahmen des Ubiquitous Computing aufgrund der deutlich veränderten Rahmenbedingungen oft nur begrenzt möglich. Selbst dedizierte Lösungen können im Spannungsfeld zwischen Effizienz und Bequemlichkeit auf der einen und Sicherheit und Datenschutz auf der anderen Seite in vielen Fällen den komplexen Herausforderungen smarter Umgebungen nicht gerecht werden. Der vorliegende Beitrag versucht, die komplexen Zusammenhänge im Bereich des Datenschutzes aufzuzeigen, die sich beim flächendeckenden Einsatz von Identifikationstechnologie ergeben. Insbesondere werden dabei neuere Datenschutzverfahren im Bereich der RFID-Technologie diskutiert und auf ihre Vor- und Nachteile hin untersucht.

1 Unter Beobachtung

RFID-Tags oder *Smart Labels* haben wohl wie keine andere Technologie des Ubiquitous Computing Ängste in der Bevölkerung mobilisiert, in naher Zukunft in einem Überwachungsstaat zu leben. Als Anfang 2003 der Modehersteller Benetton ankündigte, zwecks Lieferkettenoptimierung den Einsatz von RFID-Chips in Textilien seiner „Sisley"-Marke zu erwägen, brach ein unerwartet heftiger Sturm der medialen Entrüstung aus [Com03]. Nur wenige Wochen später sah sich Benetton genötigt, in einer Pressemitteilung seine Pläne zurückzuziehen [Ben03, EET03]. Ähnliche Beschwichtigungen waren Ende Oktober desselben Jahres sowohl vom Einzelhandelsgiganten Wal-Mart [CST03] als auch vom größten Rasierklingenhersteller der Welt, Gillette, zu hören [CNN03]. In allen drei Fällen hatte eine bis dato eher unbekannte Konsumentenschutzgruppe namens CASPIAN (*Consumers Against Supermarket Privacy Invasions And Numbering –*

[53] Zitiert in [Dow03]

frei übersetzt etwa: Konsumenten gegen Datenschutzvergehen und Nummerierung in Supermärkten) im Internet zum weltweiten Boykott der global agierenden Konzerne aufgerufen.[54]

Dass die mit einfachsten Mitteln agierende Protestbewegung eine solch nachhaltige Wirkung hervorruft, lässt auf den Stellenwert schließen, den das Thema Datenschutz und Privatheit in der Öffentlichkeit erlangt hat. Inzwischen gibt es kaum noch Presseartikel oder Fernsehsendungen, welche über Ubiquitous Computing berichten, ohne nachdrücklich auf die möglicherweise weit reichenden Konsequenzen bis hin zum Überwachungsstaat hinzuweisen, in dem „Schnüffelchips [...] in Joghurtbechern, Kreditkarten oder Schuhen [...] Ihr Leben durchsichtig wie Glas“ machen [Zei04]. Gleichzeitig setzt sich aber auch der Siegeszug der Kundenkarte ungebrochen fort, durch deren Nutzung Supermarktketten einen noch nie da gewesenen Einblick in das individuelle Kaufverhalten ihrer Kunden erhalten. Nach einer Emnid-Studie[55] hatten bereits im März 2002 mehr als die Hälfte aller Deutschen mindestens eine Kundenkarte, in Großbritannien waren es 2003 sogar mehr als 86 % [Sha03]. Für einen Rabatt von oft weniger als ein Prozent des Warenwertes ist ein Großteil der Verbraucher also offenbar bereit, das Kaufverhalten offen zu legen und zum Zwecke der Marktforschung und zur individuellen Angebotsunterbreitung analysieren zu lassen.

Dieser Widerspruch zwischen Besorgnis um den Verlust der Privatsphäre durch RFID-Tags einerseits und der freiwilligen Preisgabe detaillierter Informationen im Austausch für kleinste Rabatte andererseits ist allerdings weder neu noch überraschend. Sicherheit und Datenschutz waren schon immer Ausdruck des Abwägens, bei denen Bequemlichkeit und finanzielle Vorteile mit den möglichen ideellen und physischen Schäden nicht immer rational aufgerechnet wurden. Doch ist es müßig, den Konsumenten belehren zu wollen und ihn auf diesen offensichtlichen Widerspruch hinzuweisen. Vielmehr gilt es, irrationale Ängste von begründeten Vorbehalten zu unterscheiden und tatsächlich mögliche Bedrohungen für unser soziales Gefüge zu identifizieren, um bereits im Vorfeld der technischen Entwicklung potenzielle Fehlentwicklungen zu erkennen.

Der vorliegende Beitrag möchte dazu das oft nur diffus wahrgenommene Gebiet des Daten- und Persönlichkeitsschutzes zunächst in seiner Begrifflichkeit untersuchen, dessen gesellschaftliche Realitäten in Form historischer Entwicklung und aktueller Gesetzgebung beschreiben und schließlich die besonderen Herausforderungen des Ubiquitous Computing an unser Verständnis von Privatheit herausstellen. Anschließend sollen am Beispiel aktuell diskutierter technischer Datenschutzlösungen für RFID-Tags die Möglichkeiten, aber auch die Grenzen solcher Ansätze aufgezeigt und in einer abschließenden Diskussion bewertet werden.

[54] Siehe www.boycottbenetton.org
[55] Siehe www.tns-emnid.com

2 Zur Begründung des Datenschutzes

Trotz des engen Bezuges zum Internet ist der Aspekt des Schutzes der Privatsphäre und der persönlichen Daten kein neues Phänomen der Informationsgesellschaft. Debatten über die Privatsphäre haben eine lange Geschichte, über deren Zeitraum hinweg sich das Grundbedürfnis nach Privatheit in seiner Ausprägung wiederholt änderte. Bereits 1361 fand sich im englischen Recht der *Justices of the Peace Act*, der das Belauschen und heimliche Beobachten anderer unter Strafe stellte [Lau03]. 1763 folgte der berühmte Ausspruch William Pitts, seinerzeit Mitglied im englischen Parlament: *„The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail — its roof may shake — the wind may blow through it — the storm may enter — the rain may enter — but the King of England cannot enter! — all his forces dare not cross the threshold of the ruined tenement!"* [Bro39].

Eine der frühesten Definitionen von Privatheit stammt vom späteren Richter am Obersten Gerichtshof der USA, Louis Brandeis, und seinem Anwaltskollegen Samuel Warren. Bereits 1890 veröffentlichten die beiden den wegweisenden Aufsatz *The Right to Privacy* [WaB90], welcher im amerikanischen Recht die zivilrechtlichen Grundlagen für Klagen gegen die Verletzungen der Privatsphäre schaffte. Dass der Aufsatz auch heute noch eine hohe Relevanz besitzt, liegt dabei vor allem auch an den Umständen, unter denen sich Warren und Brandeis zu ihrer Publikation genötigt sahen: *„Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‚to be let alone.' [...] Numerous mechanical devices threaten to make good the prediction that ‚what is whispered in the closet shall be proclaimed from the house-tops.'"* Waren es damals die aufkommende Sensationspresse und die durch die Fortschritte in der Fotografie möglichen „Paparazzi-Fotos",[56] die nach Meinung von Warren und Brandeis eine Anpassung des Rechts erforderten, sind es heute *Smart Labels*, *Memory Amplifier* und *Smart Dust*, welche es erforderlich machen, den Schutz der Privatsphäre sowohl technisch als auch rechtlich und sozial neu zu evaluieren.

Bei aller technikgeschichtlichen Relevanz scheint allerdings Warrens und Brandeis' Definition der Privatheit als *„the right to be left alone"* aufgrund der Vielzahl von Interaktionen im heutigen Informationszeitalter kaum praktikabel. Eine zeitgemäße Definition der *informationellen Privatheit* kommt von Alan Westin, der 1967 angesichts der zunehmenden Verbreitung von maschineller Informationsverarbeitung diese wie folgt definiert: *„Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others"* [Wes67].

Neben diesem auf Datenverarbeitungsanlagen abzielenden Aspekt unterscheidet man heute weiterhin die *Privatheit der Kommunikation* (z.B. Brief- und Fernmeldegeheimnis), die *territoriale Privatheit* (der Schutz der eigenen vier Wände,

[56] Am 18. Oktober 1884 erhielt Georg Eastmann, der Gründer der Eastman Kodak Company, Patent 306 594 für die Erfindung des fotografischen Films. Statt mittels schwerer Glasplatten im Studio konnte dank Kodaks günstiger „Snap Camera" nun praktisch jedermann auch ohne Einwilligung des Subjektes einen „Schnappschuss" machen.

der sich in einem gewissen Rahmen auch auf das Auto oder den Arbeitsplatz erstreckt) sowie die *körperliche Privatheit*, also der Schutz vor ungerechtfertigten Leibesvisitationen bzw. körperlichen Untersuchungen (letztere beiden werden auch oft als *physische* oder *lokale Privatheit* zusammengefasst). Darüber hinaus geht es bei der so genannten *dezisionalen Privatheit* um die *„Sicherung der Interpretationshoheit über das eigene Leben"*, wie Beate Rössler, Professorin für Philosophie an der Universität Amsterdam, beschreibt [Rös01], d.h. um die Freiheit, unbefangen selbst entscheiden zu können: *„mit wem will ich zusammenleben; welchen Beruf will ich ergreifen; aber auch: welche Kleidung trage ich"* [Rös02]. Privatheit also als Autonomie des Individuums; als die Fähigkeit, die Frage nach der Person, die man sein will, zu stellen und zu beantworten und dann – im Privaten – auch tatsächlich nach den eigenen Wünschen zu leben.

2.1 Moderne Datenschutzgesetze

Mehr als hundert Jahre nachdem Brandeis und Warren den Grundstein für das moderne Datenschutzrecht legten, haben sich zwei grundlegende Herangehensweisen zum Schutz der Privatsphäre etabliert: der vor allem in Europa populäre Ansatz umfassender, sektorenübergreifender Datenschutzgesetze und der in den USA favorisierte Mix aus spezifischen Gesetzen und freiwilliger Selbstbeschränkung von Industrie und Handel. Die Anfang der 1990er-Jahre mit der steigenden Popularität des grenzüberschreitenden Internets oft vorausgesagte Entwertung nationaler Gesetzgebung fand allerdings nicht statt – vielmehr erfuhr dieser Bereich im ausklingenden zwanzigsten Jahrhundert eine stark zunehmende Dynamik, indem viele Staaten ihre existierenden Gesetze sowohl an aktuelle technische Entwicklungen anpassten als auch im internationalen Vergleich aktualisierten und harmonisierten.

Während bis heute in den USA keine umfassende Gesetzgebung zum Datenschutz existiert, die Staat und Privatpersonen gleichermaßen betrifft, und man es stattdessen der Industrie überlässt, durch freiwillige Selbstbeschränkung die Privatsphäre zu wahren, begann man auf der anderen Seite des Atlantiks schon früh damit, nationale Gesetzgebungen nicht nur auf alle Formen der Datensammlungen – sowohl staatlicher als auch privater Natur – anzuwenden, sondern darüber hinaus auch europaweit zu harmonisieren. Bereits 1973 und 1974 erließ der Europarat[57] mit den Resolutionen (73)22 und (74)29 zwei Richtlinien für die nationale Gesetzgebung betreffend private bzw. öffentliche Datenbanken. Im Jahr 1985 folgte mit der Konvention 108/81, dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", ein normatives Vertragswerk zur Harmonisierung nationaler Datenschutzgesetze [COE04]. Mit der 1995 verabschiedeten Europäischen Datenschutz-Direktive 95/46/EC (im Folgenden „Direktive" genannt) schaffte man schließlich ein auch über die Gren-

[57] Der Europarat ist eine seit 1949 bestehende zwischenstaatliche Organisation zur europaweiten Harmonisierung der rechtlichen und sozialen Praktiken. Ihm gehören neben den 25 Ländern der Europäischen Union 20 weitere Länder an (siehe www.coe.int).

zen Europas hinaus wirkendes internationales Werkzeug zum Schutz der Privatsphäre.

Die Direktive hat dabei zwei Kernpunkte. Zum einen verpflichtet sie die Mitgliedsstaaten der Union, innerhalb einer dreijährigen Frist eine zur Direktive kompatible, nationale Gesetzgebung zu erlassen.[58] Diese europaweite Angleichung erlaubt einen ungehinderten Informationsfluss zwischen den Mitgliedsstaaten, da die personenbezogenen Daten europäischer Bürger überall den gleichen, von der Direktive vorgeschriebenen Mindestschutz genießen. Auf der anderen Seite verbietet die Direktive explizit den Transfer personenbezogener Informationen in „nicht sichere Drittländer", d.h. Länder, deren Datenschutzgesetze nicht den gleichen Schutz bieten, wie von der Direktive vorgeschrieben. Nachdem Politiker zu verstehen gaben, dass sie durchaus willens waren, die europäischen Vertretungen nichteuropäischer Konzerne auf die Einhaltung dieser Richtlinie zu verklagen, sollten diese die persönlichen Daten von EU-Bürgern (z.B. Kundendaten, aber auch die Lohn- und Gehaltslisten der Angestellten) an die jeweiligen Konzernzentralen in Drittländer ohne ausreichende Datenschutzgesetze exportieren, begannen zahlreiche Staaten umgehend mit der Anpassung ihrer Gesetzgebung, um von der EU-Kommission als „sicheres Drittland" bewertet zu werden und dadurch Teil des europäischen Informationsbinnenmarkts zu bleiben.[59]

2.2 Fair Information Practices und informationelle Selbstbestimmung

Die von der Direktive geforderten Mindeststandards bei Datenerhebung und Datenverarbeitung sind eine konsequente Weiterentwicklung der bereits 1973 in einem Bericht des *United States Department for Health Education and Welfare (HEW)* aufgestellten *Fair Information Practices*, die Anfang der 1980er-Jahre von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) in ihrer „Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" [OEC80] aufgegriffen und als acht Grundprinzipien formuliert wurden:[60]

1. Beschränkung der Datenbeschaffung (*collection limitation*): Daten sollten in rechtmäßiger Weise und wenn immer möglich mit der Einwilligung des Datensubjekts erhoben werden.
2. Qualität der Daten (*data quality*): Die erhobenen Daten sollten dem Zwecke ihrer Erhebung angemessen, korrekt, vollständig und aktuell sein.

---

[58] Inzwischen haben alle ursprünglichen 15 Mitgliedsländer die Direktive umgesetzt.

[59] Im März 2004 waren Argentinien, die Britischen Kanalinseln, Kanada, die Schweiz und Ungarn als sichere Drittländer im Sinne der Direktive von der EU-Kommission zertifiziert (siehe europa.eu.int/comm/internal_market/privacy/adequacy_en.htm). Ein separates Abkommen, das *Safe Harbor Agreement*, regelt den Datenaustausch mit den USA [SoR03] (siehe www.export.gov/safeharbor/sh_overview.html).

[60] Ein guter Überblick zur Geschichte der *Fair Information Practices* und deren Einfluss auf heutige Gesetze findet sich in [PRC04].

3. Zweckbestimmung (*purpose specification*): Der Zweck der Datenerhebung sollte vorher festgelegt werden.
4. Limitierte Nutzung (*use limitation*): Zu einem bestimmten Zweck gesammelte Daten sollten nicht für andere Zwecke genutzt werden.
5. Sicherheit der Daten (*security*): Die gesammelten Daten sollten adäquat vor Verlust, Diebstahl oder unerlaubten Änderungen geschützt werden.
6. Transparenz (*openness*): Die Methoden der Datenverarbeitung sollten offen gelegt werden.
7. Beteiligung (*individual participation*): Dem Einzelnen sollte ein gebührenfreies Auskunftsrecht sowie die Richtigstellung und Löschung seiner Daten zustehen.
8. Verantwortbarkeit (*accountability*): Die für die Datenverarbeitung Verantwortlichen sollten für Verstöße zur Rechenschaft gezogen werden können.

Insgesamt lassen sich die *Fair Information Practices* in fünf Grundsätzen zusammenfassen: Offenheit, Datenzugriff und -kontrolle, Datensicherheit, Datensparsamkeit und individuelle Einwilligung [Cus03]. Gerade letzterer Punkt gewann dabei im Laufe der Zeit immer mehr an Bedeutung: Zwar forderten bereits die eher technisch orientierten Datenschutzgesetze der 1970er-Jahre die Möglichkeit des Einzelnen zur Korrektur personenbezogener Daten, doch geschah dies eher aus der Motivation heraus, die Richtigkeit der gespeicherten Daten zu gewährleisten, als die Datenerhebung selbst infrage zu stellen. Erst in der als Volkszählungsurteil in die Geschichte eingegangenen Entscheidung des Bundesverfassungsgerichts wurde 1983 das bis dahin geltende Persönlichkeitsrecht um die „informationelle Selbstbestimmung" ergänzt [May98].[61] In der Urteilsbegründung hieß es dazu: *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, [...] kann in seiner Freiheit, aus eigener Selbstbestimmung zu planen und zu entscheiden, wesentlich gehemmt werden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der der Bürger nicht mehr wissen könnte, wer was, wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."*

Das Konzept der informationellen Selbstbestimmung[62] stellt einen bedeutenden Schritt moderner Datenschutzgesetzgebung hin zum autonomen Individuum dar. Zum einen erweitert es die *Fair Information Practices* um einen partizipativen

[61] Auslöser war die Kontroverse um die am 27. April 1983 geplante Volkszählung, von der Bundesregierung als „Totalzählung" angekündigt, die in über hundert Verfassungsbeschwerden resultierte [Rei01].

[62] Im Englischen als *self-determination over personal data*, oder kurz, aber etwas unglücklich als *data self-determination*, übersetzt.

Ansatz, der über ein „Take it or leave it“ hinaus dem Einzelnen erlauben soll, ohne Angst vor gesellschaftlichen Nachteilen über die Verwendung seiner persönlichen Daten entscheiden zu können. Zum anderen stellt es den Schutz der Privatheit nicht mehr nur als Individualrecht dar, sondern betont die positive gesellschaftliche Komponente des Datenschutzes. Privatheit also nicht als Laune des Einzelnen, sondern als Pflicht einer demokratischen Gesellschaft, wie Julie Cohen bemerkt: *„Prevailing market-based approaches to data privacy policy […] treat preferences for informational privacy as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white. But the values of informational privacy are far more fundamental. A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collective ends“* [Coh00].

3 Datenschutzprobleme allgegenwärtiger Computer

Datenschutz war schon immer bezogen und ausgerichtet auf das technisch Machbare. War es das Aufkommen der individuellen Fotografie gegen Ende des 19. Jahrhunderts, die Warren und Brandeis beunruhigten, die Verbreitung von Telegraf und Telefon zu Beginn des 20. Jahrhunderts, die die Ausdehnung territorialer Privatrechte auf den Schutz unserer Kommunikation mit sich brachte, oder die staatliche Nutzung elektronischer Datenverarbeitungssysteme in den 1960er-Jahren, die die modernen Datenschutzgesetze mit ihrem Fokus auf die informationelle Privatheit prägten: Technik veränderte manches, was im Alltag möglich war, und stieß so schließlich auch eine Neuausrichtung unserer Vorstellung von Privatheit an. Nachdem die Kommerzialisierung des Internets Mitte der 1990er-Jahre die vorläufig letzte Welle von Gesetzesänderungen ausgelöst hatte, steht nun bereits die nächste technische Revolution bevor: die der smarten Alltagsgegenstände und allgegenwärtigen Computer.

Zwar klingt beim unbedarften Beobachter auch immer ein Aspekt von Science-Fiction mit an, wenn von „intelligenten Autos“ und „smarten Eigenheimen“ die Rede ist, vom alten Traum dienstbarer Maschinen, die mit Intelligenz versehen uns klaglos unsere Arbeit abnehmen. Doch geht es beim Ubiquitous Computing vordergründig eigentlich um etwas Banaleres, wenn auch nicht notwendigerweise weniger Nützliches: der Überwindung von Medienbrüchen [FMB03]. Mit Miniatursensoren, billigen Mikrochips und drahtloser Kommunikation lässt sich die Welt des Computers in bisher ungeahnter Weise in unseren Alltag hinein verlängern. Dies funktioniert in gewisser Weise auch in die andere Richtung, unser Alltag lässt sich ebenso in weitaus verlässlicherer (und effizienterer) Weise im Computer abbilden. Die Grenze zwischen dem Realen und dem Virtuellen scheint zu verschwinden – ein Abbild der realen Welt lässt sich immer genauer und einfacher im Computer nachspielen und damit auch vom Computer aus manipulieren.

Das Problem des Datenschutzes liegt also genau in dieser Abbildung – in der Übersetzung von Fakten der realen Welt in Informationsstückchen, in der Digitalisierung unseres Lebens zum Zwecke der automatisierten Verarbeitung. Es überrascht daher nicht, wenn Ubiquitous Computing zumindest prinzipiell die heutige

Realität des Datenschutzes in hohem Maße zu verändern vermag. Im Folgenden sollen diese Veränderungen der Datenschutzproblematik kurz erläutert und deren Implikationen anhand von Beispielen illustriert werden. Weiterhin sollen die existierenden Prinzipien für Datenschutz – die *Fair Information Practices* – im Lichte dieser technischen Entwicklung untersucht und kommentiert werden.

3.1 Eine neue Qualität der Datenerhebung

Das bewusste Beobachten der Handlungen und Gewohnheiten von Mitmenschen ist wohl so alt wie die Menschheit selbst. Während diese Art der Beobachtung in der „guten alten Zeit" noch von unseren engsten Nachbarn durchgeführt wurde, begannen mit dem Einsetzen der automatisierten Datenverarbeitung nun Maschinen diese Rolle zu übernehmen, allerdings mit einem wichtigen Unterschied: Nicht mehr nur die Abweichungen vom Alltäglichen wurden erfasst, sondern vielmehr das Alltägliche selbst wurde Gegenstand der Beobachtung.

Ubiquitous Computing erlaubt es, diese Art der Alltagsüberwachung weit über die heute mögliche automatisierte Informationsgewinnung aus Kreditkartentransaktionen, Telefonverbindungen und Internet-Nutzung hinaus auszudehnen. Dieser Qualitätssprung lässt sich anhand von fünf Aspekten beschreiben:

- **Ausdehnung.** Nicht nur die räumliche Abdeckung von Beobachtungsaktivitäten wird durch Ubiquitous Computing erweitert, sondern auch ihre zeitliche Abdeckung nimmt viel größere Ausmaße an. Angefangen von vorgeburtlichen Diagnosen, die auf der Krankenkassen-Chipkarte des Babys gespeichert werden, über Aktivitätsmuster aus Kindergärten und Schulen bis hin zur Arbeitsplatzüberwachung und Gesundheitskontrollen in Altersheimen. Und während heute der PC zuhause durch Betätigung des Ausschalters wirkungsvoll an der Datenerhebung gehindert wird, so wird es in der Vision der nahtlosen und unbemerkten Interaktion mit unsichtbaren Computern diesen Ausschalter kaum mehr geben – eine bewusste Begrenzung der Erhebung ist also kaum mehr möglich.
- **Art der Datenerhebung.** Auch wenn wir heute oftmals die Momente, in denen wir Daten über uns preisgeben, gar nicht mehr bewusst wahrnehmen, so lassen sie sich zumindest im Nachhinein meist noch rekonstruieren: Der Kreditkartenantrag enthielt Informationen über mein Einkommen, im Teilnahmeformular für das Gewinnspiel habe ich meine vier Lieblingsfilme angegeben und beim Kurzurlaub letztes Wochenende konnte meine Bank sehen, wo ich am liebsten einkaufe. Doch diese ausgezeichneten Momente der Datenerhebung verschwinden in gleichem Maße, wie die Computer selbst verschwinden und allgegenwärtig werden: Scannt eine „smarte Tasse" unbemerkt meinen Fingerabdruck, während ich aus ihr trinke? Hat diese Fußmatte einen RFID-Leser, der meine Schuhe registrieren kann? Selbst wenn man sich solcherlei Datensammlungen entziehen möchte, wird dies in Zukunft aufgrund des mangelnden Bewusstseins über die Momente dieser Erhebungen kaum noch möglich sein.
- **Datentypen.** Seit es automatisierte Datenverarbeitung gibt, haben sich die erhobenen Datensätze kaum verändert: Name, Adresse, Alter, Kaufverhalten etc. Mit Ubiquitous Computing eröffnet sich hingegen eine völlig neue Art der

„Echtzeit"-Daten – unser momentaner Aufenthaltsort, unser Gesundheitszustand, oder unsere tatsächlichen (im Gegensatz zu den von uns vorgegebenen) Vorlieben – die niemals zuvor in solch detaillierter Form ermittelbar waren. Diese umfassende Katalogisierung unserer Person könnte letztendlich unseren Beobachtern vielleicht sogar einen tieferen Einblick in unseren Charakter geben, als es uns selbst möglich ist.

- **Erhebungsgrund.** Auch der von vielen Datenschutzgesetzen vorgeschriebene klare Erhebungsgrund, also z.B. das Übermitteln meiner Adresse zwecks Zusendung eines Paketes, wird beim Ubiquitous Computing oft nur noch schwer einzugrenzen sein. Statt künstlicher Intelligenz setzt man auf eine möglichst exakte Erfassung des aktuellen Kontexts, um auch ohne echtes Verständnis der Situation eine „smarte" Reaktion zu erhalten. Oder man versucht durch hohe Redundanz, auch in der Datenerhebung, technische Unzuverlässigkeiten, z.B. beim Lesen von RFID-Tags, auszugleichen. Dieser Selbstzweck bei der Datenerhebung – das Sammeln von möglichst vielen Informationen, da später potenziell alles relevant sein kann – erschwert nicht nur die gesetzlich geforderte Zweckbindung, sondern erhöht gleichzeitig auch den Sammeleifer: Selbst scheinbar banale Informationen können durch Computeranalyse mit relevanten Fakten korreliert werden.
- **Datenzugriff.** Schließlich dürfte die Interkonnektivität zwischen vielen smarten Gegenständen ein kaum mehr zu überblickendes Datennetz schaffen, dessen Datenströme mit traditionellen Zugriffskontrollen nicht mehr zu verwalten sind: *„Everything will be connected to everything else"* [Luc99].

3.2 Herausforderungen an den Datenschutz

Wie kann nun diesem durch den Einsatz von Ubiquitous Computing begründeten Trend hin zu einer umfassenden Alltagsüberwachung entgegengewirkt werden? Einen Bauplan für die datenschutzkonforme Behandlung persönlicher Informationen liefern die oben erwähnten *Fair Information Practices*, deren praktische Umsetzung jedoch im Rahmen dieser neuen Technologie entsprechend angepasst werden muss. Zu beachten sind in jedem Fall die Grenzen eines solchen Ansatzes: Selbst eine hundertprozentige Einhaltung der Prinzipien kann keineswegs *garantieren*, dass einmal gesammelte Daten auch wirklich gemäß diesen Praktiken zum Einsatz kommen. Vielmehr etablieren sie eine Messlatte, einen Mindeststandard, dessen Einhaltung natürlich überprüft werden sollte – sei es durch staatliche oder unabhängige Organe, oder auch durch den Nutzer selbst. Wichtig ist allerdings, dass adäquate technische Mittel für solch eine Überprüfung zur Verfügung stehen. Ohne diese bleibt ein effektiver Datenschutz illusorisch, mit diesen wäre aber langfristig vielleicht sogar eine nachhaltige Verbesserung heutiger Bedingungen denkbar.

So wird beispielsweise das Prinzip der Offenheit in heutigen Datensammlungen entweder implizit durch die aktive Teilnahme des Datensubjektes (z.B. durch das Ausfüllen von Formularen) oder explizit durch eine Beschilderung (z.B. bei der Kameraüberwachung im Supermarkt) erreicht. In einer Welt voller ubiquitärer Dienste, in der die Interaktion mit dem Computer so weit in den Hintergrund tre-

ten soll, dass man sie gar nicht mehr bemerkt, tritt aber auch eine etwaige Datensammlung in den Hintergrund – die aktive Teilnahme des Einzelnen wird durch die unbemerkte Nutzung computerisierter Services also nicht nur vereinfacht, sondern vielleicht sogar unmöglich gemacht. Diesem Verschwinden von Bewusstmachung lässt sich grundsätzlich auf zwei verschiedene Arten begegnen. Eine Möglichkeit ist, den Selbstschutz des Einzelnen zu verbessern, d.h. sowohl die Erkennung als auch die Verhinderung solcher andernfalls unmerklichen Datensammlungen zu erleichtern. Auf der anderen Seite sind aber auch Mechanismen zur expliziten Ankündigung solcher Datensammlungen nützlich, die es dem Dienstanbieter erleichtern, die Tatsache der Erhebung sowie deren Parameter (d.h. welche Daten zu welchem Zweck erhoben werden) dem Einzelnen im Voraus zu melden. Letzterer Ansatz hat nicht nur den Vorteil, dass Vertrauen zwischen Kunden und Anbietern geschaffen werden kann, sondern erleichtert darüber hinaus auch die Überprüfung der so öffentlich gemachten Versprechungen hinsichtlich der Nutzung der gesammelten Daten. Ein ubiquitäres Ankündigungssystem muss dabei notwendigerweise über die bisher üblichen visuellen Methoden hinaus angeboten werden, da potenziell jeder beliebige Gegenstand infolge seiner Benutzung Daten sammeln kann. Im Gegenzug kann eine technisch aufwendigere Ankündigung aber auch weitaus mehr Möglichkeiten bieten als etwa traditionelle Mechanismen in Bild und Schrift. So könnte eine drahtlos empfangbare, maschinenlesbare Ankündigung nicht nur detailliertere Informationen enthalten, sondern auch automatisch bzw. halbautomatisch aufgrund vorher spezifizierter Präferenzen des Nutzers verarbeitet werden, um so die Datensammlung selbst im Rahmen des Möglichen anzupassen oder zumindest zu protokollieren.

Die Maschinenlesbarkeit ist vor allem deshalb wichtig, um die Überbeanspruchung der Nutzer so weit als möglich zu vermeiden: Statt im Sekundentakt vom Benutzer eine Entscheidung bezüglich einer möglichen Datensammlung zu verlangen, trifft ein automatisches System einen Großteil der Entscheidungen selber und fragt nur vereinzelt nach. Noch ist allerdings offen, ob sich persönliche Datenschutz-Präferenzen überhaupt so leicht im Voraus spezifizieren lassen. Zum einen scheint die Bandbreite an möglichen Interaktionen so groß, dass weder eine kompakte noch eine erschöpfende Beschreibung aller möglichen Dienste machbar scheint. Eine effektive Vorauswahl akzeptabler Erhebungssituationen durch den Nutzer scheint deshalb kaum praktikabel: Zu oft würde eine unberücksichtigte Ausnahme ein direktes Nachfragen nötig machen. Darüber hinaus ist fraglich, ob Theorie und Praxis persönlicher Datenschutzpräferenzen überhaupt deckungsgleich sind. Man mag beispielsweise generell etwas gegen die Verwendung seiner persönlichen Daten zu Marketingzwecken haben, doch angesichts eines finanziellen Anreizes in der Praxis dann sehr wohl bereit sein, einmal eine Ausnahme zu machen. Sollten theoretische Prinzipien und tatsächliches Handeln weit auseinander liegen, so würde ein automatisches System in vielen Fällen die falsche Wahl treffen und damit kaum vom Nutzer verwendet werden.

Solcherlei Wahlmöglichkeiten bilden die Grundlage für das zweite Prinzip der *Fair Information Practices*: das der individuellen Einwilligung. Auch hier schafft die implizite Interaktion in ubiquitären Umgebungen neue Probleme. Zwar gibt es genügend rechtlich bzw. ethisch vertretbare Situationen, in denen eine Datensammlung auch ohne die Einwilligung des Datensubjektes erfolgen kann (z.B. bei der Videoüberwachung in Supermärkten), doch sollte im Allgemeinen die Preis-

gabe persönlicher Daten eine bewusste Entscheidung des Einzelnen sein. Traditionell gilt deshalb erst die persönliche Unterschrift als Einwilligung, z.B. beim Beantragen einer Supermarkt-Kundenkarte durch das Ausfüllen und Unterschreiben des Antragsformulars. Zwar gibt es das Pendant in Form digitaler Signaturen, die für elektronische Interaktionen eine rechtsverbindliche Einwilligung bezeugen können, doch geht es bei einer ubiquitären Umgebung vielmehr um die Frage, wie solch eine Signatur als Willenserklärung vom Nutzer initiiert werden kann: Angesichts der potenziell riesigen Zahl von impliziten (Mini-)Interaktionen und der ebenso großen Bandbreite an Nutzerschnittstellen scheint es impraktikabel, bekannte Verfahren wie beispielsweise einen Bestätigungs-Knopf allgemein einsetzen zu wollen.

Am wünschenswertesten sind sicherlich solche Art Dienste, die keinerlei persönliche Daten von Nutzern benötigen bzw. diese in einer nicht identifizierbaren Form verwenden. Solange nämlich nur anonyme Daten zum Einsatz kommen, sind praktisch keine der oben beschriebenen Datenschutzpraktiken relevant – weder muss um die individuelle Einwilligung gebeten werden noch müssen etwa Sicherheitsaspekte oder Zugriffsrechte bedacht werden. Mit Hilfe von Pseudonymen können darüber hinaus personalisierte Dienstleistungen angeboten werden, ohne die wahre Identität des Nutzers kennen zu müssen. Zwar sind Anonymisierungsverfahren und Pseudonyme bereits seit längerer Zeit im Internet weit verbreitet, doch lassen sich die dabei verwendeten Techniken nur schwer ins Ubiquitous Computing übertragen. Dies liegt vor allem daran, dass ubiquitäre Datenerhebungen oftmals unmittelbarer Natur sind: Eine Kamera, ein Mikrofon oder auch ein Indoor-Lokalisationssystem nehmen anders als ein Webformular den Benutzer direkt wahr und können nicht etwa durch Verwendung eines Anonymisierungsdienstes wie anonymizer.com ohne Offenlegung der Identität des Benutzers verwendet werden. Indirekte Sensoren wie beispielsweise druckempfindliche Bodenplatten können auch ohne die direkte Wahrnehmung primärer biometrischer Attribute durch Data-Mining-Techniken Menschen an ihrem Gang identifizieren. Und die beim Ubiquitous Computing typische enge Verknüpfung der Sensorinformationen mit Ereignissen der realen Welt erlaubt selbst bei der konsequenten Verwendung von Pseudonymen eine einfache Personenidentifikation: So konnten z.B. Forscher durch Zurückverfolgung der pseudonymisierten Bewegungsdaten eines Indoor-Lokalisiationssystemes alle Benutzer des Systems anhand ihres bevorzugten Aufenthaltsortes (typischerweise das Büro des Mitarbeiters) einwandfrei identifizieren [BeS03].

Auch die Sicherheitsanforderungen an ubiquitäre Systeme gestalten sich weitaus schwieriger als bei heutigen Client-Server-Systemen, bei denen alle Nutzer im voraus bekannt sind und eine feste Benutzerschnittstelle existiert (typischerweise Tastatur und Bildschirm oder ein fest installierter Kartenleser), über die die Anmeldung explizit erfolgt. Die für das Ubiquitous Computing typische große Bandbreite an technischen Geräten bedingt eine individualisierte Sicherheitslösung in Abhängigkeit von den jeweiligen Geräteresourcen (z.B. Rechenleistung, Speicher, Batterieleistung), der Art der zu übertragenden bzw. zu speichernden Daten sowie der jeweiligen Nutzungssituation. Gerade letzterem Punkt kommt aufgrund der engen Verknüpfung des Ubiquitous Computing mit unserem täglichen Leben eine große Bedeutung zu. Peter Cochran, ehemaliger Leiter der Forschungsabteilung von British Telecom, fasst dies pointiert so zusammen: „*Do I mind anyone acces-*

sing my medical or employment records, CV, and other personal details? Frankly, I don't give a fig! [...] Should I be knocked unconscious in a road traffic accident in New York – please let the ambulance have my medical record. Please let them know that I am going deaf and that I am diabetic. I really don't want it to be a secret – I want to live!" [Coc01].

Der in den *Fair Information Practices* geforderte Datenzugriff durch den Benutzer wird in Datensammlungen ubiquitären Charakters weitaus komplexer werden, da statt einem einfachen Datensatz (z.B. einer Postadresse) dem Benutzer ein komplexes Sensorendestillat präsentiert werden müsste, das darüber hinaus in den meisten Fällen eher eine Vermutung als eine Tatsache darstellt. Wann genau sich solch vage Informationsgefüge in verwertbare bzw. disputierbare Fakten verwandeln, die damit wieder den gesetzlichen Bestimmungen zur Datenkontrolle durch den Benutzer unterliegen, wird sich wohl erst nach einigen Jahren der Erfahrung mit dieser Art von Datensammlungen feststellen lassen. Bereits jetzt abzusehen ist allerdings, dass die umfangreichen Sensorerhebungen den in Europa so wichtigen Grundsatz der Datensparsamkeit erheblich strapazieren werden: Um möglichst kontextbezogen reagieren zu können, werden zukünftige Dienstleistungen auf immer weniger Daten verzichten wollen, auch wenn deren Relevanz auf den ersten Blick nicht gegeben ist. Eine Erhebungsgrundlage „auf Verdacht" ist in unserem heutigen Verständnis von Datenschutz aber nicht vorgesehen – inwiefern man in Zukunft, nach einigen praktischen Erfahrungen mit solchen Diensten, diesen Grundsatz revidieren werden muss, bleibt abzuwarten.

Festzustellen ist in jedem Fall schon heute, dass die Techniken des Ubiquitous Computing und entsprechende Einsatzszenarios uns zwingen werden, die technische Entwicklung derart voranzutreiben, dass die in den *Fair Information Practices* enthaltenen Grundsätze datenschutzgerechter Informationsverarbeitung so weit wie möglich umsetzbar bleiben. Gleichzeitig wird auch ein Umdenken über die Umsetzbarkeit dieser Prinzipien nötig werden, damit diese nicht von der technischen Realität zur Bedeutungslosigkeit degradiert werden. Einen ersten Einblick von diesem Wechselspiel zwischen technisch Machbarem und gesellschaftlich Wünschenswertem bietet die in den letzten Jahren stark vorangetriebene Integration von RFID-Technologie in den Warenfluss des Einzelhandels. Zwar existieren solche Systeme bereits seit mehreren Jahren in der industriellen Produktion,[63] doch durch das Einbeziehen des Kunden in diesen Kreislauf werden aus den RFID-Leservorgängen potenziell personenbezogene Daten. Der von Welthandelskonzernen wie Metro oder Wal-Mart im internationalen Maßstab geplante Einsatz solcher Systeme kann so einen ersten Vorgeschmack auf die neue Realität des Ubiquitous Computing liefern.

4 RFID und Datenschutz

RFID-Tags stellen aufgrund ihrer Identifikationsmerkmale zumindest prinzipiell ein signifikantes Datenschutzproblem dar. Von Befürwortern in dieser Hinsicht

[63] In Nischenmärkten kommen bereits heute Endverbraucher mit RFID-Tags in Kontakt, z.B. bei Skipässen, Straßenmautsystemen oder auch bei Wegfahrsperren im Auto.

gerne mit dem eher harmlosen Barcode verglichen,[64] erlauben sie nämlich im Unterschied zu diesem nicht nur eine weitaus detailliertere Identifikation[65] (d.h. Seriennummern statt generische Produktbezeichnung), sondern auch das unbemerkte Auslesen dieser Information, da die Leseeinheiten keine Sichtverbindung zum Tag benötigen. Eine technische Datenschutzlösung im RFID-Bereich muss also notwendigerweise das unbemerkte (bzw. nicht autorisierte) Auslesen der Tags verhindern bzw. die individuellen Seriennummern durch generischere Informationen (z.B. Hersteller-ID statt Seriennummer) ersetzen. Aufgrund der zu erwartenden hohen Verbreitung der Tags stellt allerdings Letzteres nur bedingt eine Lösung dar: Selbst wenn RFID-Tags lediglich genauso viel Informationen bereitstellen würden wie heutige Barcodes, so wären dennoch durch die individuelle Kombination der Tags, so genannten *„Constellations"* [Wei03], Personen oft eindeutig identifizierbar.

Existierende bzw. momentan diskutierte technische Lösungen im Bereich von „RFID-Datenschutz" lassen sich in zwei Ansätze unterteilen: Anonymisierung und Pseudonymisierung. Dies lässt sich entweder durch explizites Ändern der auf dem Tag gespeicherten ID erreichen (bzw. deren Löschung), durch eine explizite Zugriffskontrolle am Tag (d.h. dem Unterbinden nicht autorisierter Lesezugriffe) oder – im begrenzten Maße – auch durch das Sichern der Kommunikation auf dem so genannten *„forward channel"*, d.h. der Kommunikation vom Leser zum Tag.[66]

4.1 „Anonymisierung" mittels Kill-Befehl

Bereits vor der durch den Benetton-Vorfall ausgelösten öffentlichen Kontroverse um RFID-Tags enthielt die 2002 publizierte Auto-ID-Spezifikation[67] [Aut02] einen so genannten „Kill"-Befehl. Die zugrunde liegende Idee ist simpel: Die von Herstellern und Händlern zur Lagerkettenoptimierung eingesetzten RFID-Tags werden beim Verkauf an den Endkunden entweder physisch entfernt oder aber, wenn ein Entfernen nicht möglich ist, dauerhaft deaktiviert. Dadurch wird ein Auslesen des Tags außerhalb des Ladens unmöglich gemacht und damit die Gefahren der unbemerkten Identifikation, der Lokalisation und Verfolgung sowie der unerlaubten Profilbildung verhindert.

Der aktuelle EPCglobal/Auto-ID-Standard schreibt zwecks Deaktivierung für alle konformen Tags einen Kill-Befehl vor, der jedoch zur Ausführung ein wäh-

---

[64] Bei der Einführung des Barcodes in den 1970er-Jahren war dieser allerdings alles andere als harmlos angesehen, sondern wurde aufgrund seines Aufbaus wiederholt als biblisches Zeichen aus der Offenbarung und damit als Teufelszeug verdammt [Rel81].

[65] Zwar können auch Barcodes beliebig detaillierte Informationen speichern, doch benötigen sie dazu mehr Platz und sind beispielsweise durch Schmutz auf dem Code anfälliger für Lesefehler.

[66] Da das Signal des Lesegerätes nicht nur Informationen zum Tag sendet, sondern auch für die Energieversorgung der RFID-Chips nötig ist, hat es typischerweise eine bis zu zehn Mal größere Reichweite als das Antwortsignal vom Tag zum Leser.

[67] Ende 2003 wurde die Arbeit des Auto-ID Centers vom EPCglobal-Konsortium übernommen.

rend oder kurz nach der Produktion auf dem Tag gespeichertes 24-Bit-Passwort erfordert, um unautorisiertes „Einschläfern“ eines Tags (z.B. im Regal) zu erschweren.[68] Erhält ein Tag das korrekte Passwort zusammen mit dem Kill-Befehl, darf es danach laut Spezifikation in keiner Weise mehr auf Signale eines Lesers reagieren [Aut03]. Wie diese Funktionalität konkret auf dem Tag implementiert wird, bleibt dem Hersteller überlassen; aus Gründen der Kosteneffizienz wird es sich allerdings in den meisten Fällen um eine softwaretechnische Lösung handeln, die dadurch – zumindest theoretisch – ein späteres Reaktivieren eines Tags durch direkten Kontakt (also durch Umgehen der dann deaktivierten Funkschnittstelle) erlauben würde.

Neben dieser unvollständigen Zerstörung des Tags gibt es zwei weitere Aspekte, die die Effektivität dieses Verfahrens aus Sicht des Datenschutzes signifikant einschränken. Zum einen ist bei einer Deaktivierung an der Ladenkasse noch immer die Überwachung (*tracking*) innerhalb des Geschäftes möglich, ebenso wie eine direkte Assoziation von Kundendaten und Einkäufen spätestens an der Kasse (z.B. beim Vorlegen einer Kredit- oder Kundenkarte während des Bezahlvorgangs). Zum anderen ist der Vorgang der Deaktivierung selbst problematisch, da der Kunde nur schwerlich überprüfen kann, ob das Tag auch wirklich deaktiviert wurde. Auch der Umstand, dass alle bekannten Verfahren bisher eine softwaretechnische Deaktivierung vorsehen, obwohl eine elektromagnetische Deaktivierung analog zu heutigen Transponder-basierten Diebstahlsicherungen durchaus denkbar wäre,[69] lässt Zweifler vermuten, dass eine spätere (und für den Kunden unbemerkte) Reaktivierung der Tags möglich ist – eine Befürchtung, die bereits bei einer genaueren Untersuchung existierender Prototypen bestätigt wurde: So stellte sich beim Besuch des Metro-Future-Stores durch die „RFID-Aktivistin“ Catherine Albrecht im Februar 2004 heraus, dass Metros „Deaktivatoren“ lediglich die Metro-eigene Produktnummer vom RFID-Tag löschen, das Tag mitsamt seiner Hardware-Seriennummer „aus technischen Gründen“ allerdings unberührt lassen [Foe04].

Praktiker führen darüber hinaus an, dass eine flächendeckende Ausstattung mit so genannten „Kill Stations“ unrealistisch sei [Sta03], da Geschäfte mit kleinem Umsatz (z.B. ein Kiosk) kaum in die dazu nötige Infrastruktur investieren könnten, obwohl dort nichtsdestotrotz Produkte mit integriertem RFID-Tag verkauft würden. Ebenso sind heutige Prototypen der Kill-Stationen noch nicht in der Lage, mehrere Tags auf einmal zu deaktivieren: Kunden müssen aufgrund des Passwort-Schutzes mühsam einen Artikel nach dem anderen nach dem Einkauf manuell stumm schalten – ein Aufwand, den ein Großteil der Kunden vermutlich kaum bereit sein dürfte, zu betreiben.[70]

Nicht zuletzt geht durch ein permanentes Deaktivieren der RFID-Tags natürlich auch eine Vielzahl von sekundären Nutzungsmöglichkeiten verloren, wie z.B.

---

[68] Während in der ursprünglichen Spezifikation lediglich 8 Bit vorgesehen waren, wird für die nächste Generation bereits die Verwendung von 32 Bit in Betracht gezogen.

[69] Ein Zerschneiden oder Abreißen ist nur bei der Anbringung auf Etiketten praktikabel.

[70] Die derzeit einzige verfügbare Lösung, der NCR EasyPoint-Kiosk [NCR03], kann bisher nur jeweils ein einziges Tag pro Deaktivierungsvorgang ausschalten [RFI03]. Theoretisch sollte es allerdings möglich sein, auch mehrere Dutzend Gegenstände, z.B. eine gesamte Einkaufstasche, auf einmal zu deaktivieren.

der oft beschworene intelligente Kühlschrank und ähnliche smarte Haushaltsgeräte; jeglicher Folgeservice (z.B. bei Kleidung die automatische Auswahl passender Accessoires) und schlussendlich die Automatisierung bei Umtausch, Reparatur und Recycling. Dabei könnten bei einer großräumigen Verbreitung der RFID-Technologie und nicht „gekillten" Tags nicht nur Hersteller und Einzelhandel von einem gesteigerten Konsumverhalten durch autonome Besteller in Form intelligenter Kühltruhen profitieren – auch der Kunde mag es schätzen, wenn sein Kühlschrank ihn auf bald ablaufende Milch hinweist bzw. er nicht umständlich den Kassenzettel zur Reklamation aufbewahren muss, da der Artikel selbst alle relevanten Reklamationsinformationen direkt im RFID-Tag speichert.

Schlussendlich läuft die Kritik am Kill-Tag-Ansatz also darauf hinaus, dass weder die Zerstörung für den Kunden überprüfbar ist noch dadurch das gesamte Problem der Überwachung beseitigt wird, selbst wenn die Zerstörung verlässlich einsetzbar wäre, da vor dem Gang zur Kasse bereits Daten gesammelt werden können. Ebenso scheint ein flächendeckender Einsatz weder praktikabel noch wünschenswert: Zum einen verlangen Kill-Tags hohe Investitionen für Händler mit geringem Umsatz (da teure Kill-Stationen beschafft werden müssten) und einen hohen persönlichen Einsatz vom Kunden selbst (der nach dem Einkauf erst umständlich durch Eingabe Dutzender Deaktivierungs-Codes seine Waren stumm schalten müsste) bzw. dem jeweiligen Händler (der zwecks automatischer Deaktivierung an der Kasse ein aufwendiges Schlüsselmanagement implementieren muss). Andererseits würde durch das Abschalten der Tags ein signifikanter Anteil an nützlicher Zusatzfunktionalität – sowohl für die Industrie als auch den Verbraucher – verloren gehen.

4.2 Pseudonymisierung mittels MetaIDs (Hash-Locks)

Als Alternative zur „Alles oder Nichts"-Mentalität des Kill-Befehls kamen schon früh Ansätze ins Spiel, die zum Ziel hatten, die Nutzdaten des RFID-Tags (in den meisten Fällen also dessen ID bzw. den darauf befindlichen Produktcode) vor unerlaubtem Auslesen zu schützen. Sobald ein Produkt in den Besitz des Kunden übergeht, erhält dieser die Kontrolle über die Ausgabe des integrierten RFID-Tags und kann so selektiv entscheiden, wer welche Informationen vom Tag auslesen kann.

Das grundlegende Verfahren wurde bereits 2002 von Sarma et al. vorgestellt [SWE02]. Es basiert auf mathematischen Einwegfunktionen, so genannten „One-Way Hashes", welche die Eigenschaft besitzen, sich relativ einfach berechnen zu lassen, jedoch ein Zurückrechnen auf die Eingabewerte der Funktion praktisch unmöglich machen. Um nun ein RFID-Tag zu „verschließen", wählt ein RFID-Leser einen beliebigen Schlüssel k, bildet mit Hilfe der Einwegfunktion den Hash dieses Schlüssels $h(k)$ (genannt „MetaID") und schreibt diesen auf das zu verschließende Tag. Um ein späteres „Aufschließen" des Tags zu ermöglichen, speichert darüber hinaus der Besitzer (bzw. dessen Lesegerät) den Schlüssel k unter der daraus erzeugten MetaID $h(k)$ in einer Datenbank ab. Tags, die mit einer solchen MetaID beschrieben wurden, antworten auf alle Leseanfragen lediglich mit dieser MetaID, nicht aber mit den „wahren" Informationen (z.B. der auf dem Tag

gespeicherten EPC-Nummer). Will der Besitzer des Tags die im Tag enthaltenen Informationen später wieder verfügbar machen, so liest er zunächst die MetaID des Tags aus, schlägt in seiner Datenbank den für diese MetaID passenden Schlüssel *k* nach und sendet diesen an das Tag. Nachdem das Tag seinerseits wieder den Hashwert *h*(*k*) dieses Schlüssels *k* gebildet hat, kann es diesen mit seiner MetaID vergleichen. Bei Übereinstimmung löscht es die MetaID und gibt dadurch den vollen Zugriff auf seine Informationen wieder frei.

Eine RFID-Zugriffskontrolle mit Hash-Schlüsseln bietet mehrere Vorteile: Auch wenn im mathematischen Sinne keine absolute Sicherheit gegeben ist, so ist das Zurückrechnen auf den ursprünglichen Schlüssel mit einem solch erheblichen Aufwand verbunden, dass für alle praktischen Einsatzgebiete im Konsumentenbereich das Wissen um solch eine MetaID einem unautorisierten Leser keine Kontrolle über die wahren Tag-Informationen bietet. Gleichzeitig ist aber eine Hash-Funktionalität vergleichsweise einfach auf dem Tag zu implementieren [Wei03], liegt also auch für billigste Tags preislich im Bereich des Möglichen – ein gewichtiger Vorteil gegenüber komplexeren Ansätzen, die sich der symmetrischen oder asymmetrischen Kryptografie bedienen [NTR03] und deshalb wohl vorerst nur für hochpreisliche Tags abseits des Massenmarktes infrage kommen.

4.3 Pseudonymisierung durch variable MetaIDs

Während MetaIDs zwar einen effektiven Schutz vor unerlaubtem Auslesen der durch sie geschützten Tag-Informationen (z.B. der EPC des Gegenstandes) bewirken, so ermöglichen sie allerdings immer noch die unauffällige Verfolgung (Tracking) von Personen. Denn auch wenn die MetaID nicht die „wahre“ ID eines Gegenstandes darstellt, so eignet sie sich aufgrund ihrer relativen Dauerhaftigkeit als Identifikationsmerkmal für den Gegenstand und damit in vielen Fällen auch für den Besitzer.

Eine konsequente Weiterentwicklung in dieser Richtung stellen „Randomized Hash-Locks“ dar [WSR03]. Mit ihnen soll verhindert werden, dass durch wiederholtes Auslesen einer MetaID ein Bewegungsprofil erstellt werden kann. Dazu antworten Tags nicht mehr wie zuvor direkt mit ihrer MetaID, sondern generieren diese bei jedem Auslesevorgang dynamisch neu. Ein auf dem Chip integrierter Zufallszahlengenerator liefert dazu die Zufallszahl *r*, welche verkettet mit der „wahren“ ID des Tags als *hash*(ID||*r*) gehasht wird. Als Antwort erhält ein Leser nun jedes Mal eine neue Zufallszahl *r* (im Klartext) sowie einen neuen Hashwert *h*. Um daraus die ID des Tags zu berechnen, muss der Leser über eine Liste aller ihm bekannten IDs verfügen – eine Bedingung, die für Privatpersonen mit einigen Hundert mit Tags versehenen Gegenständen durchaus realistisch scheint. Zusammen mit der Liste generiert der Leser einfach der Reihe nach jeweils den Hash *hash*(ID_i||*r*), bis er einen übereinstimmenden Hashwert gefunden hat. Dadurch ist ihm nun implizit die ID des Tags bekannt – ein Freischalten des Tags ist nicht mehr nötig. Erst bei Weitergabe des getaggten Gegenstandes (z.B. zwecks Umtausch oder Rückgabe) würde durch Senden der wahren ID zum Tag dieser wieder freigeschaltet, analog zu dem oben beschriebenen einfachen Hash-Lock-Verfahren.

Auch wenn diese Lösung nicht kryptografisch robust ist,[71] da – zumindest theoretisch – aufgrund der Konstruktion des Hashes ein Angreifer durch wiederholtes Auslesen immer neu generierter MetaIDs Rückschlüsse auf die den Hashwerten zugrunde liegende ID ziehen könnte, so erfüllt sie dennoch zwei wichtige Voraussetzungen für RFID Privacy: Sie verhindert sowohl das unautorisierte Auslesen von auf dem Tag gespeicherten Informationen als auch das unbemerkte Verfolgen von getaggten Gegenständen (und damit den sie tragenden Personen). Darüber hinaus erscheint sie wirtschaftlich machbar, da Zufallszahlengeneratoren bereits heute schon für Auto-ID-konforme Tags der nächsten Generation vorgesehen sind. Sobald allerdings einmal die ID eines Gegenstandes bekannt ist (z.B. bei dessen Rückgabe), kann aufgrund der Struktur dieses Verfahrens beim gezielten Durchsehen von Log-Dateien schnell der Gegenstand (und damit auch sein Benutzer) rückwirkend identifiziert werden.

Als Alternative schlagen Ohkubo et al. deshalb so genannte *„Chained Hashes"* vor, bei denen ein Tag nach jeder Ausgabe seiner MetaID diese neu berechnet und den alten Wert überschreibt [OSK03]. Zwecks kryptografischer Robustheit kommen dabei zwei unterschiedliche Hashverfahren zum Einsatz: Das eine hasht jeweils die aktuelle MetaID, um zur nächsten MetaID zu gelangen (d.h. die neue MetaID wird als $\text{MetaID}_{i+1}=hash_{Chain}(\text{MetaID}_i)$ berechnet). Das andere Hashverfahren wird vor der eigentlichen Ausgabe noch einmal auf die momentane MetaID angewandt (d.h. an den Leser wird $hash_{Ausgabe}$(MetaID) ausgegeben), um keinerlei Rückschlüsse auf die folgende neu berechnete MetaID zu geben. Der RFID-Leser muss, wie auch schon bei dem Random-Hash-Lock-Verfahren von Weis et al., über eine Liste aller ihm bekannten RFID-Tags (bzw. deren IDs) verfügen. Zur Identifikation eines Tags vergleicht der Leser dessen Ausgabewert mit der gehashten MetaID jedes ihm bekannten Tags, wobei die MetaID sich durch mehrfaches Anwenden von $hash_{Chain}$ auf die ID des Tags ergibt, also zu $hash_{Ausgabe}(hash^{i}_{Chain}(\text{ID}))$. Um nicht endlos oft $hash_{Chain}$ anwenden zu müssen, muss der Leser bzw. die Hintergrundinfrastruktur „mitzählen", wie oft die MetaID eines jeden Tags bereits neu gehasht wurde – ein Mitsenden dieses Wertes *i* vom Tag zum Leser würde das Verfahren analog zu den Random-Hash-Locks einer rückwirkend möglichen Identifikation aussetzen. Im Gegensatz zum Verfahren von Weis et al. bietet es aber (ohne das Mitsenden von *i*) den Vorteil, dass ein Bekanntwerden der MetaID zum Zeitpunkt *t* die Anonymität aller vorherigen Logeinträge dieses Tags nicht beeinträchtigt: Während bei Weis et al. jede Antwort direkt auf der „wahren" ID des Tags basiert (und damit bei der Kompromittierung der ID sich alle existierenden Logeinträge eindeutig zuordnen lassen), so müsste ein Angreifer beim Verfahren von Ohkubo jeweils eine Hash-Funktion invertieren, um auf den unmittelbar vorausgehenden Wert des Tags zu schließen – eine

[71] Weis et al. schlagen dazu eine Erweiterung vor, welche zusätzlich zum fixen Pseudozufallszahlengenerator ein über einen geheimen Schlüssel *k* parametrisierbares Ensemble von Pseudozufallsfunktionen (PRF) auf dem RFID-Tag verwendet. Statt direkt einen Hashwert aus ID und Zufallszahl *r* zu berechnen, verknüpft das Tag seinen ID-Wert per XOR mit $f_k(r)$. Das Lesegerät muss den geheimen Schlüssel *k* kennen und kann so die passende PRF f_k ermitteln, $f_k(r)$ berechnen und dadurch den ID-Wert bestimmen. Obwohl kryptografisch robuster, sind Weis et al. skeptisch, ob sich PRF-Ensembles kostengünstig auf Massen-Tags unterbringen lassen.

solche Invertierung ist praktisch jedoch unmöglich. Einen Mittelweg favorisieren Henrici und Müller [HeM04], die jeweils die beiden letzten MetaIDs eines Tags in einer Datenbank speichern und nach jedem Auslesen eine zufällige neue MetaID auf dem Tag setzen. Mittels einer beiden Seiten bekannten *TransactionID* (TID), die nach jedem Lesevorgang um eins erhöht wird, können Replay-Attacken verhindert bzw. die neue MetaID auf dem Rückkanal verschlüsselt werden.[72] Der Vorteil dieses Verfahrens ist die einfachere Tag-Hardware, der Nachteil liegt in der aufwendigen Datenhaltung und -synchronisation.

Einen anderen Weg gehen Inoue und Yasuura [InY03], die statt eines fixen Verfahrens zur Berechnung der MetaID einfach eine vom Benutzer völlig frei wählbare private ID vorschlagen. Wie schon beim Hash-Lock-Verfahren ist die „wahre" Information auf dem Tag gesperrt, solange eine private ID gesetzt ist. Zum Setzen bzw. Löschen einer privaten ID schlagen die Autoren einen physisch gesicherten Kanal vor, z.B. direkten Kontakt bzw. eine unmittelbare Nähe von nur wenigen Zentimetern zum Lesegerät. Obwohl sie dadurch die Komplexität des Tags niedrig halten und ohne jegliche Hardware-Modifikationen auskommen, erhöht sich durch den nun notwendigen physikalischen Zugriffsschutz der Aufwand für den Benutzer. Solange die selbst gewählte private ID bestehen bleibt, ist, anders als beim Random-Hash-Lock-Verfahren, eine Nachverfolgung des Tags möglich – ein besorgter Besitzer müsste also regelmäßig die private ID neu setzen.[73] Dafür können bei frei gewählten privaten IDs Logdateien nicht mehr nachträglich durchsucht werden, solange der Besitzer nicht selbst eine Liste der verwendeten privaten IDs anlegt und diese (ungewollt) einem Angreifer zur Verfügung stellt. Um die Komplexität auf dem Tag weiter zu vermindern, geben die Autoren noch eine Variante ihres Verfahrens an, welche sich mit Nur-Lese-Tags implementieren lässt. Dazu muss allerdings der weltweit eindeutige EPC auf zwei Tags pro Produkt verteilt werden (indem z.B. die ID von Hersteller und Produkt auf der Umverpackung, die Seriennummer aber am Produkt selbst angeheftet wird), um dann beim Verkauf an den Kunden durch Entfernen des Hersteller-Tags eine nicht mehr eindeutige Rest-Seriennummer im Produkt zu belassen. Während so die direkte Zuordnung des verbleibenden Tags zum Produkt verhindert wird (also z.B. das berühmt-berüchtigte Beispiel von der ausgelesenen Unterwäsche), gelten die Benutzeridentifikationsprobleme einer fixen MetaID aber weiterhin.[74]

---

[72] Das Tag speichert dazu zusätzlich zur aktuellen TID die TID der letzten erfolgreichen Transaktion und sendet die Differenz zwischen den beiden zusätzlich zur (gehashten) TID als Teil seiner Antwort an das Lesegerät. Diese Differenz erlaubt es der Datenbank, bei verloren gegangenen Nachrichten die gespeicherte TID mit der auf dem Tag gespeicherten TID zu vergleichen.

[73] Dies allerdings jeweils nur außerhalb der Reichweite eines Lesegerätes und komplett für alle mitgeführten Tags, da sonst die Umbenennung einfach nachverfolgbar wird.

[74] Neugierige Zeitgenossen könnten sich allerdings immer noch einen Spaß daraus machen, die Liste der an mir auslesbaren Tags mit meinen sichtbaren Kleidungsstücken zu vergleichen, um so festzustellen, wie *lange* ich meine nichtsichtbaren Kleidungsstücke schon am Stück trage.

4.4 Distanz-basierte Zugriffskontrolle

Einen anderen Weg zur Authentisierung von Lesegeräten gehen Fishkin und Roy [FiR03]: Basierend auf dem Prinzip *Distance implies Distrust* schlagen sie vor, in Abhängigkeit von der Signalstärke eines Lesegerätes dynamisch mehr oder weniger detaillierte Informationen vom Tag zurückzuliefern. Als Beispiel geben sie fünf verschiedene Informationsniveaus an: Bei Level 0 antwortet das Tag lediglich mit „Ich bin ein Objekt", bei Level 1 liefert es generische Klassenattribute (z.B. bei einem Hemd Farbe und Art des Stoffes) zurück, während bei Level 4 beispielsweise detaillierte Kaufinformationen (Preis, Zeit und Ort des Erwerbs) preisgegeben würden. Zur Distanzmessung selbst schlagen die Autoren verschiedene Methoden vor, die jeweils über unterschiedliche Vor- und Nachteile verfügen. Die verlässlichste Möglichkeit ist die der Triangulation, d.h., mindestens drei (zeitsynchronisierte) Tags müssen ihr empfangenes Signal an eine Basisstation melden, welche dann durch Ermittlung der Laufzeitunterschiede den relativen Ort des Lesegerätes ermitteln kann und entsprechend die Tags informiert.

Der immense Infrastrukturbedarf einer solchen Lösung (eine vertrauensvolle Basisstation, ein kryptografischer Schutz vor illegalen Lesegeräten, zeitsynchronisierte Tags und schließlich eine komplette Signalanalyse auf dem Tag) scheint kaum für einen realistischen Einsatz zu sprechen, auch wenn man statt einer kompletten Signalanalyse alternativ lediglich die Variationen in der Signalstärke betrachten kann (was weniger aufwendig, allerdings auch weniger genau ist). Ohne jede Infrastruktur kommt schließlich die dritte Alternative aus, die Analyse des Signal-Rauschabstandes: Je höher dessen Standardabweichung, desto weiter ist ein Tag vom Lesegerät entfernt. Diesen Wert könnten Tags jeweils individuell berechnen, wobei allerdings die Variationen erheblich wären, da das Niveau des Hintergrundrauschens von einer Vielzahl von Faktoren abhängig ist und sich dementsprechend bei gleicher Distanz zwischen Lesegerät und Tag stark ändern kann.

Auch wenn das Grundprinzip dieses Ansatzes einfach ist, ist dessen praktische Umsetzung heikel. Zum einen ist die Signalstärke an einem Tag stark abhängig von dessen Orientierung – ändert sich die Lage des Tags relativ zum Lesegerät, so erscheint dieses plötzlich weiter entfernt, als es in Wahrheit ist, was zwar unter Datenschutzgesichtspunkten tolerierbar wäre, eine verlässliche Anwendung aber nahezu unmöglich macht.[75] Auch verzerren metallische Gegenstände und Wasser[76] das Energiefeld einer Antenne erheblich, was verlässliche Signalstärkemessungen außerhalb einer Laborumgebung signifikant erschwert. Zwar sind die Autoren hoffnungsvoll, dass eine Kombination der obigen Verfahren, zusammen mit

[75] Ein gutes Beispiel sind die heutzutage bereits weit verbreiteten RFID-basierten Zugangskontrollen in Skigebieten: Um zu vermeiden, dass versehentlich das Tag des Nebenmannes ausgelesen wird, müssen die Leseradien der Gatter relativ klein gehalten werden – ein Umstand, der die Skifahrer oft zu einer Reihe kreativer Bewegungen zwingt, bis der in der Jacke oder Hose mitgeführte RFID-Skipass erkannt wird.

[76] Da der Mensch zu 45–60 % aus Wasser besteht, „stören" natürlich auch schon Personen den Empfang von RFID-Antennen.

aufwendiger konstruierten Antennen auf den Tags,[77] solch einen Ansatz praktikabel machen, doch dürften sowohl die mangelnde Verlässlichkeit einer solchen Lösung als auch deren erhöhte Kosten weder Kunden noch Hersteller zufrieden stellen. Denn selbst wenn eine einigermaßen stabile Positionierung der Lesestation durch die Tags möglich wäre, würde sich aller Voraussicht nach die „Bedienung“ eines solchen entfernungsbasierten Authentisierungssystems durch den Besitzer der getaggten Gegenstände schwierig gestalten, da ohne jegliches Feedback ein Nachvollziehen des Datenflusses zwischen Tag und Lesestation praktisch unmöglich ist und so ein versehentliches Ausgeben von Daten bereits aufgrund einer unachtsamen Bewegung droht. Nicht zuletzt bleibt es natürlich auch fraglich, ob die von den Autoren vorgeschlagene streng hierarchische Aufteilung von Tag-Informationen in vielen Fällen überhaupt sinnvoll ist.

4.5 Abhörsichere Antikollisionsprotokolle

Auch wenn mit einem der oben beschriebenen Verfahren lediglich autorisierte Lesestationen Zugriff auf die auf dem RFID-Tag gespeicherten Informationen haben sollten, so besteht aufgrund der Sendeleistungs-Asymmetrie zwischen Lesegerät und Tag die Möglichkeit, dass Daten, die vom Leser zum Tag gesendet werden, von nicht autorisierten Lesestationen mitgehört werden. Denn aufgrund der Energiekopplung zwischen Lesestation und RFID-Tag hat das vom Lesegerät erzeugte Feld immer die vielfache Reichweite des vom Tag reflektierten Rückkanals. Dies ermöglicht es unbeteiligten Dritten, die vom Leser an das Tag gesendeten Informationen noch in relativ weiter Entfernung mitzuhören

Dies ist vor allem dann kritisch, wenn die Tag-ID selbst darunter ist, wie es bei gängigen, auf Binärbäumen basierenden Antikollisionsprotokollen der Fall ist [LLS00]. Bei einer weit verbreiteten Variante dieser Protokolle bestimmt z.B. ein vom Leser ausgesendetes ID-Präfix, welche Tags antworten sollen. Solange es zu einer Kollision kommt (d.h. solange zwei oder mehr Tags mit diesem Präfix im Empfangsbereich des Lesegerätes sind), erhöht der Leser die Länge des Präfixes (indem er z.B. eine „1“ anhängt), bis sich ein einzelnes Tag „singularisieren“ lässt. Anschließend ersetzt er das zuletzt angehängte Bit durch das Inverse und fährt – falls bei diesem Präfix ebenfalls Kollisionen auftreten – mit dem Erhöhen des Präfixes fort.

Sollten sich beispielsweise die Tags „1001“ und „1011“ in Reichweite befinden, würde infolge der ersten Kollision vom Leser zunächst das Selektions-Präfix „1“ gesendet. Da beide Tags dieses Präfix teilen, kommt es erneut zu einer Kollision. Das Präfix „11“ würde im Anschluss auf keinen der Tags passen und das Lesegerät würde alternativ das Präfix „10“ prüfen. Hier kommt es wieder zu einer Kollision. Erst beim Präfix „100“ und dem anschließenden Präfix „101“ würde sich jeweils nur ein einziges Tag melden. Durch diese explizite Partitionierung des Suchraumes lässt sich eine beliebige Anzahl von Tags einzeln selektieren.

[77] So genannte 2-D-Antennen besitzen eine „L“- bzw. „X“-förmige Antenne und können weitgehend unabhängig von ihrer zweidimensionalen Ausrichtung relativ zum Lesegerät ausgelesen werden, auch wenn immer noch Signalstärke-Variationen in Abhängigkeit ihrer räumlichen Ausdehnung auftreten.

Aufgrund der für die Energieversorgung der Tags nötigen starken Sendeleistung der Lesestationen kann ein Angreifer so allerdings, je nach Kombination der Tags, jeweils die Präfixe der selektierten Tags mitprotokollieren – bei Tags mit fortlaufenden Seriennummern wären dies im Allgemeinen die kompletten IDs.

Weis et al. [WSR03] schlagen zur Abhilfe vor, den Leser statt eines kompletten Präfixes lediglich das Kommando „Sende nächstes Bit" an die Tags senden zu lassen. Solange sich die jeweiligen Präfixe der Tags nicht unterscheiden (d.h. alle senden den gleichen Bitwert), tritt keine Kollision auf und der Leser kann sich die den Tags gemeinsame Bitfolge merken. Tritt an Stelle *i* eine Kollision auf, wählt der Leser mittels eines „Select"-Befehls wie gewohnt einen Teilbaum aus, allerdings ohne wie oben das gesamte Präfix (also Bits 1–*i*) zu senden, sondern indem er Bit_{i-1} und Bit_i mit XOR verknüpft und den resultierenden Wert an die Tags sendet. Die Tags bilden nun ihrerseits das XOR ihres Bit_{i-1} (welches ja mit dem Bit_{i-1} des Lesers identisch ist) und dem gesendeten Wert und vergleichen diesen mit ihrem Bit_i. Bei Übereinkunft betrachten sie sich als selektiert und antworten mit ihrem nächsten Bit_{i+1}. Der Angreifer, dem lediglich der Vorwärtskanal (d.h. die Befehle des Lesegeräts, nicht aber die Antworten der RFID-Tags) zur Verfügung steht, kann Bitstellen ohne Kollision nicht abhören (da die Lesestation lediglich ein „Sende nächstes Bit" verschickt und die Antworten der Tags auf große Distanz nicht empfangen werden) und auch keine Rückschlüsse über den selektierten Teilbaum machen, da durch das XOR mit einem ihm unbekannten Wert (Bit_{i-1}) der selektierte Bitwert an Position *i* ebenso unbekannt bleibt.[78] Damit sich die Tags die jeweils aktuelle Bitstelle merken können, müssen sie allerdings auch mit (teurem) dynamischem Speicher ausgerüstet werden.

Eine alternative Antikollisionsmethode kann potenziell ohne Informationsverbreitung auf dem Vorwärtskanal auskommen: Bei den auf dem Aloha-Modell basierenden Verfahren antwortet jedes Tag mit einer individuellen, zufälligen Zeitverzögerung auf das Signal des Lesegerätes [Vog02]. Je nach Größe des zur Verfügung stehenden Zeitraumes (die das Lesegerät den Tags mitteilt), verteilen sich so die Antworten zufällig und können im besten Fall völlig kollisionsfrei zurückgeliefert werden. Um die Performanz dieses Verfahrens zu verbessern, besteht allerdings in einigen Protokollen die Möglichkeit, alle fehlerfrei erkannten Tags explizit „stumm zu schalten", damit bei einigen wenigen Kollisionen nicht die gesamte Tag-Population wiederholt ausgelesen werden muss. Falls nicht alternative Selektionsmechanismen (z.B. ein Hashwert oder eine dem Tag bekannte Zufallszahl) verwendet werden, wäre ein entfernter Angreifer natürlich in der Lage, die kompletten IDs der erkannten und stumm geschalteten Tags mitzuprotokollieren.

Die aktuelle Auto-ID/EPCglobal-Tag-Spezifikation [Aut03] beinhaltet deshalb einen Zufallszahlengenerator auf dem Tag, welcher sowohl aus Effizienzgründen wie auch aus Sicherheitsgründen eingesetzt wird. Statt mit der wahren ID (typischerweise dem EPC) antworten Tags gemäß dieser Spezifikation innerhalb eines Lesezyklus jeweils mit einer neu generierten Zufallszahl und werden auch über

[78] Die drei Tags *00101*, *00001* und *00110* würden beispielsweise mittels folgender Befehle (die abgehört werden könnten) vom Leser identifiziert: *GetNext*, *GetNext*, *GetNext* (Kollision Tag_1 und Tag_2), *Select(1)* (Kollision Tag_1 und Tag_3), *Select(0)* (Tag_1 identifiziert), *Select(1)* (Tag_3 identifiziert), *Select(0)*, *GetNext* (Tag_2 identifiziert).

diese (wie oben besprochen) stumm geschaltet. Um die wahre ID schlussendlich auszulesen, kann nach vollständiger Erfassung aller Tags über diese temporäre Zufalls-ID die volle ID vom Tag angefordert werden. Dadurch wird nicht nur einem entfernten Angreifer die Möglichkeit genommen, auf dem Vorwärtskanal die wahren IDs der singularisierten Tags mitzuhören, sondern auch die Geschwindigkeit des Antikollisionsprotokolls erheblich erhöht, da die Zufallszahl mit deutlich weniger Bits (12) auskommen kann als die global eindeutige EPC-ID (96) und so kürzere Übertragungszeiten möglich sind.[79]

4.6 Das Blocker-Tag

Die wohl einfachste vorgeschlagene Zugriffskontrolle für RFID-Tags baut auf dem oben beschriebenen Binärbaum-basierten Singularisations-Protokoll auf und verfolgt einen Denial-of-Service-Ansatz [JRS03]. Juels et al. schlagen vor, ein so genanntes *Blocker-Tag* mitzuführen, welches auf jede mögliche ID reagiert und durch sein ständiges Antworten nicht nur ein schnelles Scannen unmöglich macht (da nun praktisch mehrere Billiarden Tags präsent zu sein scheinen und von einem binärbaumbasierten Antikollisionsprotokoll eins nach dem anderen ausgelesen werden müssen), sondern auch tatsächlich vorhandene Tags effektiv in dieser Masse von virtuellen Tags versteckt. Der Vorschlag der Autoren sieht vor, das Blocker-Tag mit zwei separaten Antennen auszustatten, die auf jede Präfix-Singularisation sowohl mit „0“ als auch mit „1“ antworten, also eine Kollision verursachen, bzw. bei der schlussendlichen Singularisation einer einzelnen ID diese ID zu simulieren. Ein Leser, der auf ein solches Blocker-Tag stößt, würde effektiv blockiert[80] bzw. müsste nach dem Auslesen einiger tausend solcher virtuellen Tags abbrechen.

Um diesen Effekt in der Praxis nutzbar zu machen, schlagen Juels et al. vor, mit Blocker-Tags nur bestimmte Teilbäume – also z.B. alle Tag-IDs, die mit „1“ beginnen – so zu blockieren. Statt an der Kasse mit einem Kill-Befehl permanent deaktiviert zu werden, könnten erworbene Gegenstände durch Umschreiben ihrer ID von „0...“ auf „1...“ in diese vom Blocker-Tag ihres Besitzers geschützten Zone „einsortiert“ werden.[81] Analog zu den von Fishkin und Roy [FiR03] vorgeschlagenen unterschiedlichen Informationszonen könnten durch solch ein Verfahren verschiedene Privatheitszonen implementiert werden, indem Präfixe mit zwei oder mehr Bits verwendet werden und diese entweder mit mehreren physischen Blocker-Tags einzeln blockiert bzw. mit einem einzelnen, aber konfigurierbaren Blocker-Tag dynamisch freigegeben werden.

Damit Lesegeräte nicht „aus Versehen“ solch einen geschützten Teilbaum abfragen und dadurch ungewollt blockiert werden, könnte ein einfaches Signalisationsverfahren die Präsenz eines Blocker-Tags und dessen geschützten Teilbaum

[79] Dies gilt natürlich nur, falls sich viele Tags im Feld des Lesegerätes befinden, da ansonsten der Aufwand für das separate Auslesen der EPC-ID zu groß wird.

[80] Ein komplettes Auslesen von z.B. 2^{64} Tags würde selbst bei einer Leserate von über 100 000 Tags pro Sekunde mehr als 4 Millionen Jahre benötigen.

[81] Um den Aufwand für Kunden zu minimieren, könnten Händler Blocker-Tags bereits in die für Kunden bereitgestellten Tragetaschen integrieren.

ankündigen, z.B. über eine reservierte Tag-ID, die vor Beginn eines eigentlichen Lesevorgangs von Lesestationen abgefragt würde. Weiterhin besteht das Problem, dass Blocker-Tags nicht nur die persönlichen Tags einer einzelnen Person schützen, sondern bei physischer Nähe auch ungewollt Tags anderer unlesbar machen. Juels et al. schlagen hierfür vor, Hunderte von Privatheitszonen einzurichten, um so die Wahrscheinlichkeit zu minimieren, dass zwei Personen ihre persönlichen Tags in die gleiche Zone eingeteilt haben. Je mehr unterschiedliche Zonen (und damit individuelle Blocker-Tags) es jedoch gibt, desto besser lassen sich Blocker-Tags selbst zur Identifikation einer einzelnen Person verwenden.

Der größte Vorteil des Blocker-Tag-Ansatzes ist sicherlich der geringe Infrastrukturaufwand, da Tags nahezu unverändert und Lesegeräte mit nur minimalen Softwareänderungen verwendet werden könnten. Dem gegenüber steht allerdings die geringe Verlässlichkeit des Verfahrens: Implementiert man Blocker-Tags kostengünstig als passive Systeme, kann eine ungünstige Lage zur Leseantenne schnell die vermeintlich geschützten Tags sichtbar machen. Will man Privatheitszonen verwenden, müssen Tags darüber hinaus mit wiederbeschreibbarem Speicher ausgerüstet werden, was die Preise in die Höhe treibt. Auch Störungen durch das eigene Blocker-Tag bzw. Blocker-Tags Dritter scheinen vorprogrammiert: Mein automatisches Waschprogramm schlägt fehl, weil ich mein Blocker-Tag in der Hosentasche vergessen habe, und mein Kühlschrank übersieht die Hälfte meiner Einkäufe, weil mein Nachbar (mit störendem Blocker-Tag) mir beim Einräumen meiner Lebensmittel hilft. Darüber hinaus ist es natürlich auch denkbar, dass eine genaue Analyse des Energiefeldes es einem speziellen Lesegerät erlauben würde, eine künstlich hervorgerufene Kollision (bzw. eine lediglich virtuell präsente ID) von einer echten (d.h. aufgrund der tatsächlichen Anwesenheit eines Tags erzeugten Kollision bzw. ID) zu unterscheiden, da in diesem Falle zwei oder mehr verschiedene Tags antworten.

4.7 RFID in Banknoten

Als aus Datenschutzsicht besonders heikel gilt die Idee, RFID-Tags in Banknoten zu integrieren. Bereits vor dem Start des Euro-Bargelds im Januar 2002 kündigte die Europäische Zentralbank (EZB) an, solch eine Maßnahme zur Verbesserung der Fälschungssicherheit bzw. Geldwäschekontrolle bis spätestens 2005 zu erwägen [Yos01]. Auch bei Lösegeldforderungen stünde so eine unauffällige Möglichkeit zur Verfügung, Banknoten zu kennzeichnen und deren Auftauchen im Geldmarkt frühzeitig zu registrieren.

Anders als bei der Kennzeichnung von Konsumgegenständen sind die oben skizzierten Lösungen wie Kill-Tags oder Hash-Lock-basierte Verfahren nicht einsetzbar: Eine vollständige Kontrolle des Besitzers über den RFID-Tag eines Geldscheins würde der ursprünglichen Idee hinter der Banknotenkennzeichnung zuwiderlaufen. Dennoch sind die Kassandra-Rufe der Konsumentenschutzgruppen womöglich verfrüht: Auch wenn Banknoten in Zukunft für einzelne Nennwerte (z.B. für 200- und 500-Euro-Scheine) oder sogar komplett mit RFID-Tags ausgerüstet würden, so wäre es für Diebe keineswegs ein Leichtes, die Geldbörsen ahnungsloser Passanten zu durchleuchten, um unauffällig ein möglichst lohnendes

Opfer ausfindig zu machen. Zum einen sind RFID-Tags mit einer großen Reichweite für die Anforderungen von Zentralbank und Sicherheitsorganen nicht nötig, wenn nicht sogar kontraproduktiv, da die bei größeren Leseabständen nötigen Antikollisionsprotokolle die Lesegeschwindigkeit vermindern und den Preis der Tags in die Höhe treiben würden. So haben beispielsweise die von der EZB u.a. in Betracht gezogenen µ-Chips von Hitachi [Mar03] in ihrer Grundkonfiguration lediglich eine Reichweite von wenigen Millimetern – kaum ausreichend, um unbemerkt in der Brieftasche ausgelesen zu werden. Zum anderen ist es ein Leichtes, Geldbörsen mit einem Einsatz aus Aluminiumfolie herzustellen, welche skeptischen Zeitgenossen die Nichtauslesbarkeit ihrer mitgeführten Bargeldbestände quasi garantieren würden.

Auch das oft angeführte Ausspionieren des Bargelds durch clevere Marketingfachleute, die einzelne Banknoten ihren jeweiligen Kunden zuzuordnen versuchen, scheint bei näherer Betrachtung kaum praktikabel. Soll das Kaufverhalten einzelner Kunden studiert werden, bietet heute bereits die an der Kasse vorgezeigte Kundenkarte alle Möglichkeiten. Um ein globales Kaufverhalten von Kunden – analog zu den heutigen Kreditkartentransaktionen – mit RFID-Bargeld zu analysieren, wäre nicht weniger nötig als ein zentrales Bargeldregister aller weltweiten (oder zumindest nationaler) Bargeldbewegungen – bei der Vielzahl der dabei involvierten Parteien ist dies weder wirtschaftlich noch gesellschaftlich realistisch. Auch ein in [JuP03] als Beispiel angeführter lokaler Zusammenschluss einzelner Händler zwecks (heimlichen) Ausspionierens gemeinsamer Kunden wäre nicht nur fast überall ein schweres Vergehen gegen geltendes Datenschutzrecht, sondern würde sich im Rahmen eines händlerübergreifenden Kundenkartensystems wie z.B. Payback [Loy04] weitaus einfacher und verlässlicher implementieren lassen.

Sieht man von Schreckensvisionen der Verschwörungstheoretiker ab, welche Strafverfolgungsbehörden die Bewegungen individueller Banknoten durch den flächendeckenden Einsatz von Lesegeräten in Echtzeit verfolgen lassen,[82] gibt es nur wenige Gründe, die einen Einsatz von RFID-Tags in Banknoten rechtfertigen könnten. Sicherheitstechnische Zusatzinformationen, wie beispielsweise digitale Signaturen von Seriennummern, um Fälschern das Erfinden von Seriennummern zu verunmöglichen, lassen sich ebenso gut als 2-D-Barcodes direkt auf die Banknote drucken (hier würden RFID-Tags höchstens ästhetische Zwecke erfüllen). Allenfalls wäre ein Auslesen dieser Informationen mittels RFID geringfügig einfacher (wenn auch nicht notwendigerweise verlässlicher), doch würde die Gefahr des unerlaubten (und unbemerkten) Auslesens diese Erleichterung in der gesellschaftlichen Diskussion mehr als aufwiegen. Ebenso wären aufgrund der hohen Packungsdichte von Banknoten automatische Inventarisierungen etwa bei Banken, analog zur Lagerinventur beim Einzelhandel, mit heutiger RFID-Technologie wohl kaum durchführbar [Eco02]. Und ein Aufspüren von „heißen“ Banknoten, beispielsweise aus einem Bankraub oder einer Entführung, wäre mit den oben

[82] Ein solches System würde sich, wie erwähnt, durch den Einsatz einer wenigen Cent teuren Aluminiumfolie leicht sabotieren lassen. Auch die von Albrecht [Alb02] befürchteten Banknoten mit „Gedächtnis“, welche auf ihren RFID-Chips ihre Aufenthaltsorte speichern, um sie später den Sicherheitsorganen zugänglich zu machen, sind praktisch unmöglich verlässlich (und wirtschaftlich) zu implementieren.

erwähnten optischen IDs fast ebenso praktikabel (oder unpraktikabel) wie mit funkbasierten, vorausgesetzt Einzelhändler würden Lesegeräte einsetzen, die einen automatischen Abgleich mit gesuchten Seriennummern ermöglichen. Die Tatsache, dass ein Funkchip sich dem Nachdrucken bzw. Kopieren entziehen würde und auf dem grauen Markt kaum zu beschaffen wäre, könnte allerdings existierende Sicherheitsmerkmale in dieser Richtung (z.B. eingewobene Silberstreifen) verstärken helfen, da so Verkaufsautomaten (nicht aber Menschen) Fälschungen leichter erkennen könnten.

Auch wenn also funkbasierte Seriennummern auf Banknoten noch kaum den erheblichen Aufwand rechtfertigen würden, den eine Einführung von RFID-Chips mit sich bringen würde: Falls deren Einsatz erfolgt, muss Sorge getragen werden, dass eine zu Strafverfolgungszwecken installierte Infrastruktur nicht ungewollte Datenspuren erzeugt, unabhängig von der verwendeten Technologie. RFID-Chips ohne externe Antenne, ähnlich dem seit einiger Zeit verfügbaren 0,6x0,6 mm großen µ-Chip von Hitachi, mit mehreren hundert Bits WORM-Speicher[83] und einem Leseradius von nur wenigen Millimetern, würden zwar die Fälschungssicherheit erhöhen, ohne die viel zitierten (Allmachts-)Visionen einer Echtzeitverfolgung von Erpressern und Geldwäschern Wirklichkeit werden zu lassen, wären aber bezüglich Daten- und Konsumentenschutz wohl eher bedenkenlos einsetzbar. Eine darauf aufbauende Verfolgung der Bargeldströme durch den Einzelhandel wäre zwar prinzipiell machbar, doch erscheint ein derartiges Anliegen (zumindest heutzutage) weder politisch noch wirtschaftlich durchsetzbar, unabhängig davon, ob WORM-RFID-Chips oder optisch erkennbare Seriennummern auf Geldscheinen angebracht sind.

4.8 RFID in Reisepässen

Im Gegensatz zu den nur vage bekannten Plänen, RFID-Tags in Banknoten zu integrieren, ist die Ausstattung von Reisepässen mit Funkchips bereits beschlossene Sache. Die im Mai 2004 von der *International Civil Aviation Organization* (ICAO) verabschiedete Spezifikation für maschinenlesbare Reisedokumente (MRTD – *Machine Readable Travel Documents*) verlangt die digitale Speicherung des Passbildes in jedem Reisepass. Optional dürfen passausgebende Behörden auch Fingerabdrücke und Irisbilder in die zur Speicherung vorgeschriebenen RFID-Chips einbringen[84] [Küg05]. Während die Authentizität der Informationen durch eine digitale Unterschrift gewährleistet sein muss, ist die Verschlüsselung des Auslesevorgangs zur Gewährleistung der Vertraulichkeit optional. Um das unerlaubte Auslesen des Chips zu verhindern, ermöglicht ein optionaler Mechanismus die Verwendung eines optisch auszulesenden Zugriffsschlüssels, ähnlich des von Juels und Pappu [JuP03] im Zusammenhang mit Banknoten vorgeschlagenen Verfahrens. Um sich gegenüber dem RFID-Tag zu authentisieren, benötigt

[83] Write-Once-Read-Many, d.h. einmal von der Zentralbank beschrieben, würde sich die Information nicht mehr ändern lassen.

[84] Die Mitgliedsstaaten der EU haben sich im Dezember 2004 darauf geeinigt, ebenfalls Fingerabdrücke in EU-Reisepässe aufzunehmen [Pou04].

ein Lesegerät einen in der maschinenlesbaren Zone[85] abgelegten Schlüssel, der zunächst optisch ausgelesen werden muss [Küg05]. Aus dem so abfragbaren Geburtsdatum, der Passnummer und dem Ablaufdatum des Passes wird der Zugriffsschlüssel *K* berechnet, welcher vom Lesegerät an das RFID-Tag gesendet werden muss, um einen mehrstufigen dynamischen Schlüsselfindungsprozess zu starten. Die auf dem Tag gespeicherten Daten können danach mit dem soeben vereinbarten dynamischen Schlüssel ausgelesen werden. Dies verhindert das selbst von Sicherheitsexperten oft befürchtete Auslesen von Passdaten aus einer Menschenmenge: *„[P]ickpockets, kidnappers, and terrorists can easily – and surreptitiously – pick Americans or nationals of other participating countries out of a crowd“* [Sch04]. Ein Angreifer, der es auf eine ganz bestimmte Person abgesehen hat, könnte allerdings die zur Berechnung des Schlüssels nötigen persönlichen Informationen in Erfahrung bringen, um dann gezielt nach einem auf diesen Schlüssel antwortenden Reisepass zu suchen. Dies setzt natürlich voraus, dass die gesuchte Person den Reisepass ungeschützt, d.h. ohne beispielsweise einen Umschlag aus Aluminiumfolie, bei sich trägt. Auch in diesem Fall scheint es sowohl billigere als auch verlässlichere Methoden zu geben (z.B. die Gesichtserkennung per Kamera).

Eine weitere Komplikation stellen die weiterführenden Pläne der EU für den Einsatz von RFID bei Visa dar. Genauso wie der enge Kontakt von Banknoten ein Auslesen der dicht zusammengerückten RFID-Tags verunmöglicht, würde ein mit mehreren RFID-Visa ausgestatteter RFID-Reisepass kaum verlässlich lesbar sein [Let04].

4.9 Allgemeine Sicherheitsaspekte

Unabhängig vom Potenzial zur Überwachung und Verfolgung von Privatpersonen sind RFID-Lösungen im industriellen Bereich natürlich auch unter sicherheitstechnischen Gesichtspunkten zu evaluieren. Einzelhändler laufen durch die umfassende Kennzeichnung aller ihrer Produkte Gefahr, nicht nur ihre eigene Inventur zu vereinfachen, sondern auch der Konkurrenz die genaue Überwachung ihres Warenbestands zu ermöglichen: Ein morgendlicher Besucher mit verstecktem Lesegerät könnte mit einem einfachen Rundgang durch die Regalreihen leicht die Warenbewegungen von Tag zu Tag aufnehmen. Ebenso sind automatisierte Zahlungssysteme und Diebstahlsicherungen, welche auf RFID-Tags basieren, durch gefälschte RFID-Tags, einfache Störsender und Abschirmfolien leicht zu umgehen. [BSI04] beschreiben eine Reihe verschiedener Angriffsarten, die die Integrität eines RFID-Systems gefährden können: das Fälschen von Inhalten, das Fälschen von Tag-Identitäten, das Fälschen von Reader-Identitäten, das Deaktivieren von Tags, das physische Ablösen von Tags, das Abhören der Kommunikation und das Blocken bzw. Stören des Auslesens. Weis et al. [WSR03] schlagen zum Schutz einer kommerziellen RFID-Infrastruktur eine Kombination aus Lesege-

[85] Die maschinenlesbare Zone (MRZ – *Machine Readable Zone*) bezeichnet die beiden optisch auslesbaren Textzeilen heutiger Reisepässe, in denen der Name, das Geschlecht, die Passnummer sowie das Ausstellungs- und Ablaufdatum des Passes vermerkt sind.

rätsdetektoren (zum Aufspüren unautorisierter Lesegeräte), „vokalen“ Kill-Standards (gerade deaktivierte Tags machen auf einer speziellen Frequenz auf ihre Abschaltung aufmerksam, um ein unbemerktes Deaktivieren zu verhindern) und aufgedruckten Zugriffsschlüsseln, welche z.B. manuelle Umschaltung zwischen Hash-Lock- und Randomized-Hash-Lock-Modus bzw. bei Schlüsselverlust eine Freischaltung des Tags ermöglichen, vor. Umgekehrt sollten Lesegeräte Antworten von Tags mit anomalen Charakteristiken (z.B. Signalstärke, Antwortzeit) ignorieren, um ein Tag-Spoofing zu verhindern. Auch die Verwendung von Frequency-Hopping wird empfohlen (indem z.B. der Leser dem Tag jeweils die zu verwendende Frequenz vorgibt), um eine Verbindungsübernahme durch unautorisierte Lesegeräte zu verhindern.[86] Weiterhin helfen Maßnahmen wie die oben beschriebenen abhörsicheren Antikollisionsprotokolle, auf dem Vorwärtskanal nicht unbeabsichtigt Informationen über die gerade ausgelesenen Tags weiterzugeben.

5 Zusammenfassung und Beurteilung

Mit dem Kill-Befehl steht das wohl am weitesten fortgeschrittene technische Schutzverfahren für RFID-Tags zur Verfügung, welches wirkungsvoll, wenn auch nicht unbedingt immer überprüfbar, einen Großteil der Gefahren für den Datenschutz beim Einsatz von RFID beseitigt. Der momentan vorgesehene Passwortschutz scheint jedoch kaum praktikabel – der für das Passwortmanagement nötige Aufwand steht in keinem Verhältnis zu den Vorteilen eines solchen Verfahrens, nämlich ein unerlaubtes Deaktivieren der Tags zu verhindern. Ein effektiver Diebstahlschutz lässt sich weitaus einfacher auf operationeller Ebene realisieren, indem beispielsweise selbst mit Tags versehene Waren auch weiterhin offen in einen Einkaufswagen gelegt werden müssen, statt es dem Kunden zu erlauben, diese bereits im Laden z.B. in die Jackentasche zu stecken. Ein Entfernen bzw. Zerstören der Tags geschieht dabei allerdings nicht nur auf Kosten der Hersteller und Händler, die dadurch auf Folgenutzungen ihrer Identifikationssysteme verzichten müssen, sondern auch zu Ungunsten des Verbrauchers, der in Zukunft vielleicht selbst ein Interesse an einer automatischen Identifikation etwa von Lebensmitteln oder Kleidern durch seine smarten Haushaltsgeräte haben könnte. Nichtsdestotrotz wird aber wohl anfangs die Option, ein Produkt mit einem leicht entfernbaren bzw. automatisch deaktivierten RFID-Tag erwerben zu können, allein schon aus ethischen Gründen dem Konsumenten angeboten werden müssen. Dies entspricht dem in vielen Ländern üblichen datenschutzrechtlichen Grundsatz, dass, wenn immer möglich, eine Service-Variante angeboten werden muss, die ohne bzw. nur mit minimaler Datenerhebung auskommt.[87] Eine gemeinsame Entschließung der Teilnehmer an der Internationalen Konferenz der Datenschutzbe-

[86] Frequency-Hopping für RFID-Tags ist im US-amerikanischen 915-MHz-Band bereits vorgeschrieben [Aut03].

[87] So wurde beispielsweise beim Bau des ersten vollautomatischen Highway-Mautsystem Kanadas, dem Expressway 407, in Zusammenarbeit mit dem Privacy Commissioner von Ontario eine vollständig anonym nutzbare Abrechnungsalternative entwickelt [Cav98].

auftragten im November 2003 zum Thema RFID wies nachdrücklich darauf hin, dass die Grundsätze des Datenschutzrechtes auch für RFID-Systeme gelten und dass die Prinzipien der Datensparsamkeit, Transparenz, Zweckbindung und Wahlmöglichkeit gegeben bleiben müssen [DPC03].

MetaID-Verfahren erlauben es stattdessen, trotz aktiviert gebliebenem RFID-Tag die „wahre" Identifikation des Gegenstandes, also z.B. seine EPC, gegenüber nicht autorisierten Lesegeräten zu verbergen – einem unbemerkten Auslesen der Unterwäschenmarke auf offener Straße wäre dadurch ein Riegel vorgeschoben. Schutz vor einer unerlaubten bzw. unbemerkten Personenverfolgung (Tracking) ist damit allerdings nicht möglich, ebenso wenig wie mit graduellen Zugriffsverfahren, welche je nach Zugriffslevel mehr oder weniger detaillierte Informationen zurückliefern (also etwa Produkt-Typ vs. Seriennummer). Denn selbst ohne eindeutige IDs bleiben aufgrund der bestimmten Kombination („Constellation") von Tags Personen immer noch eindeutig identifizierbar.[88] Variable-MetaID-Verfahren bieten zwar durch die ständig wechselnden IDs einen effektiveren Schutz vor Tracking, gehen aber mit einem erhöhten strukturellen Aufwand in den Bereichen Lesegeräte und Datenbanken einher. Auch kann der ID-Wechsel selbst in vielen Fällen trivial nachvollzogen werden, wenn z.B. keine oder nur wenige andere Personen in der Nähe sind. Nicht zuletzt muss man natürlich beachten, dass sich durch ein Verfahren wie den Randomized-Hash-Locks der Sicherheitsbereich vom Tag hin zum smarten Haus des Besitzers verschiebt. Denn sobald die in den eigenen Lesegeräten gespeicherten IDs bzw. Schlüssel bekannt sind, kann sowohl in Echtzeit als auch nachträglich in Log-Dateien die gesuchte Person durch ihre Gegenstände identifiziert werden.

Energiebasierte Verfahren sind aufgrund ihrer einfachen Heuristik – Distanz bedingt Misstrauen – zwar attraktiv, doch scheinen sie nicht nur wegen der damit verbundenen technischen Probleme unpraktikabel, sondern auch infolge ihres für den Benutzer nur schwer intuitiv fassbaren Verhaltens (bei welcher Distanz werden welche Daten ausgegeben?). In ihrer einfachsten Ausprägung könnte der Ansatz allerdings eine gute Richtschnur bieten für die Konzeption RFID-basierter Lösungen: Wähle die Reichweite der eingesetzten Tags so niedrig wie möglich. So sollten RFID-Tags für Banknoten, die die Fälschungssicherheit erhöhen sollen, über eine Lesedistanz von nur wenigen Millimetern verfügen – jede höhere Reichweite verstärkt die Gefahren für die Privatsphäre, ohne dem Zweck des Systems besser zu dienen. Analog dazu kämen für die Identifikation von Paletten und Kartons Tags mit großer Reichweite infrage, für die eigentlichen Produkte solche mit überaus geringer (also einige wenige Zentimeter – ausreichend, um im Reklamationsfall die Kaufdaten auszulesen bzw. in Regalen den Bestand zu überwachen, aber nicht, um von der Straße aus in Häusern Diebesgut aufzustöbern).

Blocker-Tags sind auf den ersten Blick durch ihren einfachen, aber effektiven Aufbau eine interessante Alternative für den Kill-Befehl, vor allem in ihrer

[88] Unter „Tracking" ist dabei weniger eine Echtzeit-Verfolgung als eine A-posteriori-Suche in verteilten Log-Dateien zu verstehen, um z.B. einen bestimmten Tathergang zu rekonstruieren. Auch wenn Überwachungen in Echtzeit denkbar sind, so wäre die Zusammenführung der Informationen in einem zentralisierten System, beispielsweise von den Strafverfolgungsbehörden betrieben, nicht nur äußerst kostspielig, sondern im Vergleich zu traditionellen Überwachungsmethoden auch weitaus unzuverlässiger.

Grundvariante ohne komplizierte Privatheitszonen. Sie könnten Verwendung finden eingebettet in Papiertüten von Supermärkten und anderen Geschäften, um Kunden ein „sorgenfreies“ Nachhausetragen ihrer Einkäufe zu ermöglichen, wenn auch eine mit Aluminiumfolie ausgelegte Tasche dieses verlässlicher (und womöglich billiger) erreichen könnte. In der Form von Uhren oder Gürteln könnten sie, als aktive Variante mit größerer Reichweite, allerdings durchaus Käufer finden. Doch der erhöhte Aufwand für den Konsumenten, je nach Situation die richtige Einstellung für seinen Blocker-Tag zu finden, um nicht Probleme bei der Nutzung von ihm gewünschter Dienste zu bekommen, dürfte wohl den Großteil der Bevölkerung davon abhalten und lässt deshalb die standardisierte Einführung dieses Verfahrens kaum realistisch erscheinen.

Allen technischen Verfahren gemein ist der Aufwand für den Einzelnen, der sich so vor unerlaubten Leseversuchen bzw. Personenverfolgungen zu schützen versucht. Ein Hauptkritikpunkt aller dieser Möglichkeiten ist deshalb auch, dass sie die Verantwortung vom Hersteller und Händler auf den Kunden abwälzen, der nun selber sehen muss, dass die von ihm erworbenen Gegenstände ihm nicht zum Nachteil gereichen. Weitaus kundenfreundlicher sind hingegen legislative Ansätze, die bereits im Voraus die Sammlung solcher Daten verbieten würden, sodass es gar nicht erst zu einer unautorisierten Nutzung kommen darf. Bestehende Datenschutzgesetze in vielen Ländern, allen voran die der Europäischen Union, aber auch in Kanada oder Australien, verbieten schon heute viele der möglichen Szenarien, vor denen Konsumentengruppen beim Einsatz von RFID warnen. Ein heimliches Überwachen zu Marketingzwecken wäre darüber hinaus kaum zu verbergen – weitaus wahrscheinlicher ist eine Entwicklung analog zu den heute bestehenden Kundenkarten, bei denen der Kunde vorher in einer expliziten Einverständniserklärung den Händlern die Überwachung etwa im Austausch für Rabatte erlaubt. Doch auch dann bleibt angesichts der Dimensionen einer solchen Datensammlung die Möglichkeit bestehen, dass der Gesetzgeber früher oder später explizite Grenzen für die Erhebung zieht.

Wie werden wir also in einer Zukunft voller smarter Alltagsgegenstände, intelligenter Umgebungen und mit Tags versehenen Lebensmitteln leben? Viele der oben beschriebenen technischen Verfahren zum Schutz vor unerlaubtem Auslesen von RFID-Tags werden sich wohl kaum am Markt durchsetzen können. Statt komplizierter Kill-Tags dürfte sich so beispielsweise anfangs eher die physische Entfernung bzw. Zerstörung der Tags etablieren (d.h., sie werden auf Umverpackungen bzw. Anhängern angebracht werden), später könnte die drahtlose Entwertung integrierter Tags an der Kasse hinzukommen – allerdings ohne dass deren Abschaltung durch ein Passwort geschützt würde.[89] Allenfalls Verfahren, die sich ohne größeren Mehraufwand (sowohl preislich wie auch in der Bedienung) in existierende Protokolle integrieren lassen, haben eine reale Chance (und praktische Berechtigung), sich in technischen Spezifikationen wie denen von EPCglo-

[89] Bereits heute können viele auf einfachen RFID-Tags basierende Diebstahlsicherungen mit einem ausreichend starken Magnetfeld heimlich deaktiviert werden. Mittels Kameraüberwachung und stichprobenartigen Kontrollen durch Angestellte werden wohl auch in Zukunft solche Art Diebe ermittelt werden müssen. Dies bedingt natürlich auch, dass in absehbarer Zukunft Lebensmittel immer noch offen in einen Einkaufskorb gelegt werden müssen, statt bereits am Regal in unseren Jackentaschen zu verschwinden.

bal wieder zu finden – wie beispielsweise einige der oben vorgestellten abhörsicheren Antikollisionsprotokolle: statt totaler Sicherheit durch komplexes Schlüsselmanagement also eher die Nutzung verbesserter Protokolle zur Begrenzung der Sendereichweite von Tag-IDs. Ein gezieltes Ausspionieren einzelner Personen wird also immer noch möglich bleiben, in Anbetracht des erheblichen Aufwandes allerdings analog zur heutigen individuellen Beschattung eher die Ausnahme sein als die Regel. Darüber hinaus wäre allerdings eine solche gezielte Überwachung sogar leichter zu bemerken als beispielsweise heutige Teleobjektive und Richtmikrofone, da sich das elektromagnetische Feld eines RFID-Lesers vor geeigneten Messinstrumenten nicht verbergen lässt. Natürlich bleibt die Gefahr des Zusammenführens verschiedener Logdateien, doch hier ist weit mehr der Gesetzgeber als der Entwickler gefordert, der rechtzeitig Rahmenbedingungen für die Speicherdauer und die etwaige Offenlegung solcher Datensammlungen festlegen muss.

Nicht zuletzt bietet sich sogar die Gelegenheit, durch die konsequente Integration der *Fair Information Practices* in technische Protokolle auf lange Sicht hinaus den heutigen Schutz der Privatsphäre vielleicht sogar noch zu verbessern. So könnten zukünftige Lesegeräte etwa als Teil des Ausleseprotokolls ihre eigene Identität melden und dadurch Verbrauchern die Gelegenheit geben, nachzuvollziehen, wer wann welche Informationen ausgelesen hat. Als Teil eines vom Gesetzgeber geforderten Standards wäre so die Kontrolle unerlaubter Lesevorgänge durch unabhängige Datenschützer deutlich vereinfacht und damit der Verbraucherschutz gestärkt [FSL04].

RFID-Tags sind dabei allerdings nur ein Aspekt einer umfassend informatisierten Zukunft [BCL03], wenn auch wohl momentan in der medialen Diskussion einer der prominentesten [Bor04]. Sie machen jedoch deutlich, dass rein technische Lösungen allein wohl kaum in der Lage sein werden, eine Welt voll von unsichtbaren Computern und deren oft unbemerkter Kommunikation untereinander wirkungsvoll zu gestalten – erst im Zusammenspiel mit rechtlichen und sozialen Komponenten können unterstützende technische Maßnahmen eine Umgebung schaffen, die unseren Vorstellungen von Privatsphäre entspricht [Lan01]. Gleichzeitig wird aber auch klar, welchen Einfluss der Entwurf technischer Protokolle und Systeme auf die gesellschaftlichen Möglichkeiten hat, und zwar nicht nur im Bereich des Datenschutzes [Les99]. Wenn wir es schaffen, dieses Zusammenwirken zwischen sozialem Diskurs, gesellschaftlichen Normen und technischer Entwicklung innerhalb des Ubiquitous Computings zu erkennen und uns nutzbar zu machen, dann sollte eine „Diktatur der Technik“,[90] wie sie beispielsweise Steven

[90] Der damalige Bundesverfassungsgerichtspräsident Ernst Benda fasste in einem Interview nach dem Volkszählungsurteil seine privaten Gedanken so zusammen: „Das Problem ist die Möglichkeit der Verselbstständigung der Technik, dass die Gegebenheiten und Zwangsläufigkeiten der Technik so eine Art eigene Diktatur errichten. Also nicht die Diktatur von Menschen über Menschen mit Hilfe der Technik, sondern die Diktatur der Technik über die Menschen“ [Rei01].

Spielberg in seiner düsteren Hollywood-Vision *Minority Report*[91] aufzeigt, auch weiterhin Fiktion bleiben.

Literatur

[Alb02] Albrecht K (2002) Supermarket Cards – The Tip of the Retail Surveillance Iceberg. Denver University Law Review 79(4): 534–539, 558–565, www.nocards.org/AutoID/overview.shtml

[Aut02] Auto-ID Center (2002) 860 MHz-960 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Recommended Standard, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

[Aut03] Auto-ID Center (2003) 860 MHz-935 MHz Class 0 Radio Frequency Identification Tag Protocol Specification Candidate Recommendation, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[Ben03] Benetton (2003) No microchips present in garments on sale. Benetton Press Release, April 4, 2003, www.benetton.com/press/sito/_media/press_releases/rfiding.pdf

[BeS03] Beresford AR, Stajano F (2003) Location Privacy in Pervasive Computing. IEEE Pervasive Computing 2(1): 46–55

[BCL03] Bohn J, Coroama V, Langheinrich M, Mattern F, Rohs M (2003) Allgegenwart und Verschwinden des Computers: Leben in einer Welt smarter Alltagsdinge. In: Grötker R (Hrsg) Privat! Kontrollierte Freiheit in einer vernetzten Welt. Heise-Verlag, S 195–245

[Bro39] Brougham HP (1839) Historical Sketches of Statesmen Who Flourished in the Time of George III (1): 52. Zitiert in: Platt S (Hrsg, 1989) Respectfully quoted: a dictionary of quotations requested from the Congressional Research Service. Library of Congress, Washington D.C., www.bartleby.com/73

[Bor04] Borchers D (2004) Medien und Informatik: Frischkäse bitte bei Kasse 3 melden: Funketiketten wecken diffuse Ängste. Neue Zürcher Zeitung, 5. März 2004

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (2004) Risiken und Chancen des Einsatzes von RFID-Systemen: Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. SecuMedia

[Cav98] Cavoukian A (1998) 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner / Ontario, www.ipc.on.ca/userfiles/page_attachments/407-e.pdf

[CST03] Chicago Sun-Times (2003) Lifestyle: Chipping away at your privacy. November 9, 2003, www.suntimes.com/output/lifestyles/cst-nws-spy09.html

[CNN03] C|Net News.com (2003) Networking: Gillette shrugs off RFID-tracking fears. August 14, 2003, news.com.com/2100-1039_3-5063990.html?tag=cd_mh

[Coc01] Cochrane, P (2000) Head to Head. Sovereign Magazine Spring 2000: 56–57, www.cochrane.org.uk/opinion/archive/articles/prof.htm

[91] Aufbauend auf einem Roman von Philip K. Dick [Dic57] und nach intensiven Diskussionen mit namhaften Zukunftsforschern entwirft Spielberg eine Antivision unserer Zukunft, die halb Polizeistaat, halb Werbehölle ist.

[Coh00] Cohen JE (2000) Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52(1373). Zitiert in [SoR03]

[Com03] ComputerWeekly.com (2003) Privacy concerns as Benetton adds "smart tags" to clothing line. March 13, 2004, www.computerweekly.com/Article120113.htm

[COE04] Council of Europe (2004) Legal Affairs: Data Protection, www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection

[Cus03] Cushman R (2003) Privacy / Data Protection Project: Fair Information Principles and Practices, privacy.med.miami.edu/glossary/xd_fair_info_principles.htm

[Dic57] Dick PK (1957) Minority Report. Fantastic Universe

[Dow03] Downes L (2003) Don't fear new bar codes. USA Today: 23A, September 25, 2003, www.usatoday.com/usatonline/20030925/5532478s.htm

[DPC03] Resolution on Radio Frequency Identification. 25th International Conference of Data Protection and Privacy Commissioners, November 2003, www.privacyconference2003.org/commissioners.asp

[Eco02] The Economist (2002) Science and Technology: Where's the Smart Money? February 9–15, 2002, www.economist.com/printedition/index.cfm?d=20020209

[EET03] EETimes (2003) Semiconductors: Benetton backs off RFID deployment. April 5, 2003, www.eetimes.com/semi/news/OEG20030405S0001

[FMB03] Fleisch E, Mattern F, Billinger S (2003) Betriebswirtschaftliche Applikationen des Ubiquitous Computing: Beispiele, Bausteine und Nutzenpotentiale. HMD – Praxis der Wirtschaftsinformatik 229: 5–15

[FSL04] Flörkemeier Ch, Schneider R, Langheinrich M (2004) Scanning with a purpose – supporting the Fair Information Principles in RFID protocols. Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004

[FiR03] Fishkin KP, Roy S (2003) Enhancing RFID Privacy via Antenna Energy Analysis. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[Foe04] FoeBud – Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (2004) FoeBuD deckt auf: Versteckte RFID in Metro-Payback-Kundenkarte, www.foebud.org/texte/aktion/rfid

[HeM04] Henrici D, Müller P (2004) Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A, Mattern F (Hrsg) Proceedings of the 2nd International Conference on Pervasive Computing (Pervasive 2004). Springer-Verlag, LNCS 3001, pp 219–224

[InY03] Inoue S, Yasuura H (2003) RFID Privacy Using User-controllable Uniqueness. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[JuP03] Juels A, Pappu R (2003) Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: Wright R (Hrsg) 7th International Conference on Financial Cryptography (FC 2003), Guadeloupe, French West Indies, Springer-Verlag, LNCS 2742

[JRS03] Juels A, Rivest RL, Szydlo M (2003). The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker

[Küg05] Kügler D (2005) Risiko Reisepass. c't, (3): 84–89

[Lan01] Langheinrich M (2001) Privacy by Design: Principles of Privacy-Aware Ubiquitous Systems. In: Abowd GD, Brumitt B, Shafer S (Hrsg) Proceedings of Ubicomp 2001. Springer-Verlag, LNCS 2201, pp 273–291

[Lau03] Laurant C (2003) Privacy and Human Rights 2003. Privacy International, London, UK, www.privacyinternational.org/survey/phr2003

[LLS00] Law C, Lee K, Siu KY (2000) Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pp 75–84, portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal

[Les99] Lessig L (1999) Code and Other Laws of Cyberspace. Basic Books, New York

[Let04] Lettice J (2004) EU biometric RFID scheme unworkable, says EU tech report. The Register, December 23, www.theregister.co.uk/2004/12/23/eu_rfid_visa_trashes_self/

[Loy04] Loyalty Partner GmbH (2004) PAYBACK Bonusprogramm und Loyalty Partner, www.payback.de

[Luc99] Lucky RW (1999) IEEE Reflections Column: Connections. IEEE Spectrum 36(3), www.boblucky.com/spectrum.htm

[Mar03] Mara J (2003) Euro Scheme Makes Money Talk. Wired News, July 9, 2003, www.wired.com/news/privacy/0,1848,59565,00.html

[May98] Mayer-Schönberger V (1998) Generational Development of Data Protection in Europe. In: Agre PE, Rotenberg M (Hrsg) Technology and Privacy: The New Landscape. MIT Press, pp 219-242

[NCR03] NCR (2003) Will RFID Automate the Point of Sale? NCR Provides Systems to Test Wireless Tags at Checkout, www.ncr.com/media_information/2003/sep/pr091203.htm

[NTR03] NTRU Cryptosystems Inc. (2003) GenuID. www.ntru.com/products/genuid.htm

[OSK03] Ohkubo M, Suzuki K, Kinoshita S (2003) Cryptographic Approach to „Privacy-Friendly“ Tags. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[OEC80] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2004) Organization for Economic Co-operation and Development (OECD).
Deutsche Übersetzung unter www.datenschutz-berlin.de/gesetze/internat/bde.htm

[Pou04] Poulsen K (2004) EU goes on biometric LSD trip. The Register, February 3, 2004, www.theregister.co.uk/2005/02/03/biometric_lsd_trip/

[PRC04] Privacy Rights Clearinghouse (2004) A Review of the Fair Information Principles: The Foundation of Privacy Public Policy, www.privacyrights.org/ar/fairinfo.htm

[Rei01] Reissenberger M (2001) 50 Jahre Bundesverfassungsgericht: Volkszählung. DeutschlandRadio, Sendung vom 4. Januar 2004, www.dradio.de/homepage/schwerpunkt-verfassungsgericht-010904.html

[Rel81] Relfe MS (1981) When Money Fails. League of Prayer, Montgomery, USA

[RFI03] RFID Journal (2003) NCR Prototype Kiosk Kills RFID-Tags, 25. September 2003, ww.rfidjournal.com/article/view/585

[Rös01] Rössler B (2001) Der Wert des Privaten. Suhrkamp Verlag

[Rös02] Rössler B (2002) Den Wert des Privaten ergründen. digma: Zeitschrift für Datenrecht und Informationssicherheit 2(3): 106–113

[SWE02] Sarma SE, Weis SA, Engels DW (2002) RFID Systems and Security and Privacy Implications. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Springer-Verlag, LNCS 2523

[Sch04] Schneier B (2004) RFID Passports. Schneier on Security Weblog, 4. Oktober 2004, www.schneier.com/blog/archives/2004/10/rfid_passports.html

[Sha03] Shabi R (2003) The Card Up Their Sleeve. The Guardian, July 19, 2003, www.guardian.co.uk/weekend/story/0,3605,999866,00.html

[SoR03] Solove DJ, Rotenberg M (2003) Information Privacy Law. Aspen Publishers

[Sta03] Stapleton-Gray R (2003) Scanning the Horizon: A Skeptical View of RFIDs on the Shelves. RFID Privacy Workshop, Massachusetts Institute of Technology, www.rfidprivacy.org/papers/stapleton-gray3.pdf

[Vog02] Vogt H (2002) Efficient Object Identification With Passive RFID Tags. In: Mattern F, Nagshineh M (eds) Proceedings of the 1st International Conference on Pervasive Computing (Pervasive 2002). Springer-Verlag, LNCS 2414: 98–113

[WaB90] Warren S, Brandeis L (1890) The Right to Privacy. Harvard Law Review 4(193)

[Wei03] Weis SA (2003) Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, Massachusetts Institute of Technology, May, 2003, theory.lcs.mit.edu/~sweis

[WSR03] Weis SA, Sarma SE, Rivest RL, Engels DW (2003) Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. 1st International Conference on Security in Pervasive Computing, Boppard, March 2003. Springer-Verlag, LNCS 2802: 201–212

[Wes67] Westin, A (1967) Privacy and Freedom. Atheneum, New York

[Yos01] Yoshida J (2001) Euro Bank Notes to Embed RFID Chips by 2005. EETimes, 19. Dezember 2001, www.eetimes.com/story/OEG20011219S0016

[Zei04] Zeidler M (2004) RFID: Der Schnüffel-Chip im Joghurtbecher. Westdeutscher Rundfunk, Köln, 8. Januar 2004, www.wdr.de/tv/monitor/beitrag.phtml? bid=554&sid=108

Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung

Frédéric Thiesse
Institut für Technologiemanagement, Universität St. Gallen

Kurzfassung. Der Erfolg bei der Einführung neuer Technologien hängt zu einem großen Teil auch von der öffentlichen Akzeptanz und der Kommunikation über die mit ihnen verbundenen Risiken ab. Im Fall von RFID dreht sich die Diskussion vor allem um die möglichen Folgen für die Privatsphäre durch Missbrauch bzw. Manipulation der mittels RFID erhobenen Daten. Vor diesem Hintergrund untersucht der vorliegende Beitrag die Wahrnehmung von RFID-Technologie in der Öffentlichkeit als Risiko für die informationelle Selbstbestimmung, identifiziert Handlungsbedarfe für das Risikomanagement von Technologieanbietern/-anwendern und diskutiert mögliche Handlungsoptionen. Dabei liegt der Fokus nicht auf einzelnen technischen Eigenschaften von RFID, sondern auf der Entwicklung einer umfassenderen Strategie, die Ängste und Erwartungen der Konsumenten in den Vordergrund stellt.

1 Einführung

Technologien und Anwendungen der Radiofrequenz-Identifikation (RFID) erfahren derzeit ein großes Interesse seitens der Forschung und betrieblichen Praxis, darüber hinaus aber auch in Medien und Gesellschaft. Während sich Unternehmen von RFID vor allem operative Effizienzgewinne in ihren internen Prozessen erhoffen und Kosten-Nutzen-Gesichtspunkte in den Vordergrund stellen, wurden in letzter Zeit auch Stimmen laut, die auf die möglichen Risiken des RFID-Einsatzes verweisen und eine umfassende Technikfolgenabschätzung fordern. So zählt beispielsweise die Rückversicherung SwissRe RFID bzw. Technologien des Pervasive Computing im Allgemeinen neben Nanotechnologie und der Creutzfeldt-Jakob-Krankheit zu den derzeit drängendsten „emerging risks“ [Sch04].

Die mit RFID assoziierten Risiken umfassen sowohl direkte Auswirkungen der elektromagnetischen Strahlung auf die Gesundheit als auch indirekte ökonomische Konsequenzen wie den auf die zunehmende Automatisierung eventuell folgenden Personalabbau [Duc03]. Die mit Abstand am häufigsten geäußerte Befürchtung betrifft jedoch die Möglichkeiten des Missbrauchs der mittels RFID generierten Daten und unerwünschte Eingriffe in die Privatsphäre des Einzelnen. Hier reichen die Ängste der Bevölkerung von der Analyse und Auswertung des individuellen Verbraucherverhaltens bis zur allgegenwärtigen Überwachung durch die als „Schnüffel-Chips im Joghurtbecher“ [Zei04] titulierten RFID-Transponder.

Zusätzlich angeheizt wird die Diskussion durch Aktionen und Kampagnen von „Pressure Groups“ [Wha98] wie der US-amerikanischen Vereinigung „Consu-

mers Against Supermarket Privacy Invasion and Numbering (CASPIAN)“ oder des deutschen „Vereins zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)“. Beispielsweise führten die medienwirksame Verleihung des so genannten „Big Brother Award“ an die Metro AG und eine Demonstration vor dem Metro Future Store in Rheinberg am 28. Februar 2004 letztlich zu einem Rückzug der dort eingesetzten RFID-basierten Kundenkarten. Dass diese Aktionen keine Einzelfälle darstellen, zeigen weitere Beispiele in Europa und den USA, z.B. CASPIANs Aufruf zum Boykott von Gillette-Produkten aufgrund von Tests mit RFID-Transpondern in Rasierklingenpackungen (siehe Abbildung 1).

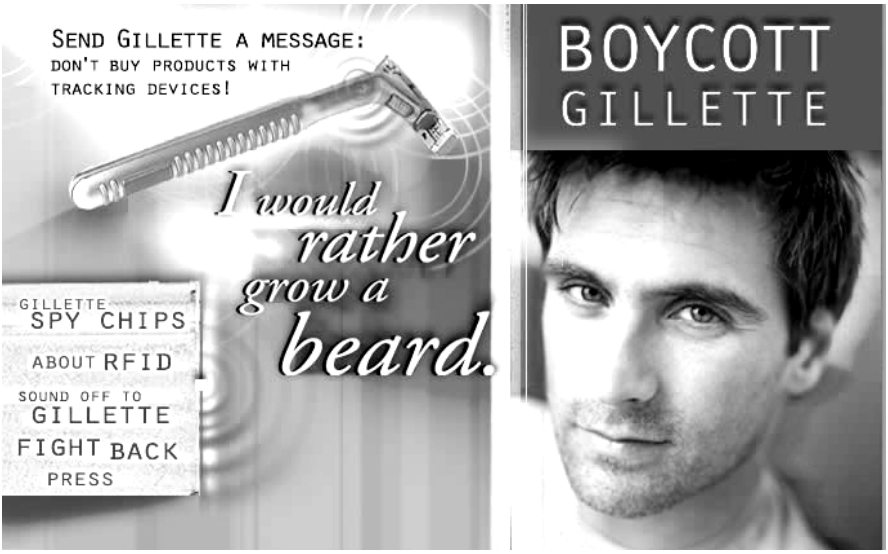


Abb. 1. Webseite www.boycottgillette.com

In der Auseinandersetzung mit RFID-Gegnern nahmen Handel, Produzenten und Technologieanbieter gegenüber der zuweilen stark emotionalisierten Debatte bisher eine eher defensive, reagierende Position ein, die von einer sehr zurückhaltenden Informationspolitik und einem Rückzug auf eine Argumentation rund um technische Eigenschaften von RFID gekennzeichnet war. Wie die Entwicklung von Risikothemen in der Vergangenheit vielfach gezeigt hat, ist einer solchen Strategie jedoch in den meisten Fällen kein Erfolg beschieden, sondern birgt vielmehr die Gefahr einer massiven Ablehnung seitens der Kunden und damit eines Scheiterns der Technologieeinführung in sich.

Vor diesem Hintergrund unternimmt der vorliegende Beitrag den Versuch einer Analyse der Wahrnehmung von RFID in der Öffentlichkeit sowie der gegen ihre Anwendung vorgebrachten Argumente und diskutiert mögliche Instrumente zur Entwicklung einer umfassenden Strategie zum Umgang mit dem Risikothema RFID. Dabei bildet die Technologiebetrachtung nur einen Aspekt unter anderen. Zu diesem Zweck wird im Folgenden nach der Einführung der grundlegenden

Konzepte auf Basis von Nachrichtenmeldungen und Internet-Diskussionsforen die Problemstellung herausgearbeitet. Darauf aufbauend werden im Anschluss Handlungsebenen identifiziert und mögliche Handlungsoptionen vorgestellt.

2 Grundlagen

2.1 Risiken

Die Einführung neuer Technologien ist fast immer auch mit einer Diskussion über die mit ihr verbundenen Risiken verknüpft. Der Begriff des Risikos bezeichnet dabei im Gegensatz zur realen Gefahr ein soziales Konstrukt [Slo99, Tac01], dessen individuelle Wahrnehmung von zahlreichen Faktoren bestimmt wird, wie z.B. Bildung, Beruf, Zugehörigkeit zu einer bestimmten Subkultur usw. [Fin02, WiH89]. Was für den einen eine ernst zu nehmende, nicht akzeptable Gefahr darstellt, kann so in anderer Perspektive als eher unbedrohlich erscheinen.

Dabei unterscheiden sich insbesondere Expertenurteile drastisch von der Risikobewertung durch Laien [SFL81]. Während der Experte Risiken vor allem quantitativ definiert und andere Formen der Riskowahrnehmung typischerweise als irrational ablehnt, hat der Laie einen eher intuitiven, qualitativen Risikobegriff, der nicht auf das Produkt von Schadenswahrscheinlichkeit und -ausmaß reduziert ist [ReL91]. Inwiefern ein Risiko von Laien als hoch oder niedrig eingeschätzt wird, ist wesentlich von der Bekanntheit des Risikos, der Freiwilligkeit der Risikoübernahme, der Schrecklichkeit der Folgen bzw. dem katastrophischen Potenzial sowie dem Nutzen der Technologie abhängig [Hen90, Slo92]. So wird z.B. regelmäßig das Risiko durch radioaktive Strahlung oder BSE geschädigt zu werden weit höher eingeschätzt als die Möglichkeit eines Verkehrs- oder Arbeitsunfalls, obwohl die Statistik eine deutlich andere Sprache spricht [TrM03].

Eine wesentliche Schlussfolgerung für den Umgang mit Risiken ist daher, dass Kommunikation über diese sich nicht allein um die Konsequenzen bei Eintreffen des zunächst nur potenziellen Risikos drehen darf, sondern auch den Risikoentstehungsprozess selbst beeinflussen muss [Jon01]. Ist das Risikothema hingegen erst einmal etabliert, können Unternehmen und Staat nur noch reagieren [Wie94]. Dies wird darüber hinaus durch den Umstand erschwert, dass der Einzelne die zur Risikobeurteilung herangezogenen Informationen als glaubwürdiger einschätzt, wenn sie z.B. von Ärzten, Freunden oder Umweltschutzgruppen stammen als von staatlichen Behörden, Verbänden oder einzelnen Firmen [TrM03].

Eine besondere Rolle bei der Risikowahrnehmung kommt in diesem Zusammenhang den Medien zu. Einerseits dienen sie der Öffentlichkeit als wichtigste Informationsquelle zu IT-bezogenen Risiken. So rangieren Fernsehen und Tageszeitungen deutlich vor allen anderen Quellen, während Informationsmaterial der Technologieanbieter selbst nur von einer kleinen Minderheit wahrgenommen wird [SjF01]. Andererseits verstärken Medien die ohnehin bereits vorhandenen Informationsasymmetrien durch eine Präferenz für negative Ereignisse in ihrer Berichterstattung [KoK91, WiH89].

Eine weitere Schwierigkeit, die speziell den Umgang mit technischen Risiken betrifft, ist die in den letzten Jahrzehnten grundsätzlich gewandelte Einstellung

der Gesellschaft gegenüber dem technischen Fortschritt insgesamt. Während in den 60er-Jahren des letzten Jahrhunderts die überwiegende Mehrheit der bundesdeutschen Bevölkerung Technik als Segen betrachtete, haben seit den 80er-Jahren die Technologieskeptiker deutlich die Oberhand gewonnen [WiH89]. Dies legt die Vermutung nahe, dass in Zeiten von Wirtschaftswunder und Mondlandung viele der aktuellen Technologiediskussionen grundsätzlich anders verlaufen wären als heute.

Entwickelt sich ein Risikothema zu einer Krise, so kann dies für betroffene Unternehmen schwerwiegende Konsequenzen haben [WOL02], wie Beispiele der letzten Jahre zeigen (siehe [Can02] für eine Sammlung von Fallstudien). Dies können unmittelbare Umsatzeinbußen durch den Rückzug aus einzelnen Märkten sein, aber auch langfristigere Schäden des Unternehmens- oder Markenimage, negative Auswirkungen auf Börsenkurse und Investoren oder politische Auflagen und Beschränkungen durch den Gesetzgeber [Wie94]. Um dies zu verhindern, ist ein frühzeitiges und professionelles Risikomanagement vonnöten, welches Konflikteskalationen vermeidet, bevor das Problem mit fortschreitender Entwicklung vom Unternehmen nicht mehr beeinflusst werden kann.

Das Ziel aller Anstrengungen ist dabei die Vermittlung von Wissen, vor allem aber der Aufbau von Vertrauen gegenüber den involvierten Institutionen [Sie01]. Dies gilt im Besonderen auch für die Informations- und Kommunikationstechnik, in deren Zusammenhang zumeist mentale, soziale und politische Risiken diskutiert werden [Jun91].

2.2 Privacy

Eine der allerersten Formulierungen eines Rechts auf Privatheit geht zurück auf Warren und Brandeis, die 1890 ihr Konzept als „the right to be let alone" [WaB90] definierten. Ausschlaggebend für die Beschäftigung mit dem Thema war damals noch die Berichterstattung der Bostoner Regenbogenpresse sowie die zunehmende Verbreitung von Fotoapparaten: „[…] and numerous mechanical devices threaten to make good the predicition that 'what is whispered in the closet shall be proclaimed from the house-tops'."

In der Neuzeit sind es vor allem Informations- und Kommunikationstechnologien, die als Bedrohung der individuellen Privatsphäre gesehen werden. Im Gegensatz zur „physical privacy", die sich auf den physischen Zugriff auf eine Person bezieht, steht im Zusammenhang mit IuK-Technologien insbesondere die „information privacy" (auf Deutsch etwa: „informationelle Selbstbestimmung") im Vordergrund [Smi01]. Den Begriff beschreibt z.B. Westin als „the right to control information about oneself" [Wes67]. Die Herausgabe von persönlichen Informationen ist dabei auf der einen Seite ein alltäglicher notwendiger Vorgang, ohne den ein soziales oder ökonomisches Miteinander nicht möglich wäre [Wes03]. Auf der anderen Seite hat der Einzelne in der heutigen Zeit aufgrund des Einsatzes von IT nahezu keine Chance mehr, die Folgen dieser Offenheit für seine Person abzuschätzen.

Die neue Bedrohung von Privatheit hat ihre Grundlage in der Möglichkeit zur dauerhaften Speicherung und Verknüpfung von Informationen über das Indivi-

duum: Hatte vor der Einführung von Computertechnik in wirtschaftliche Abläufe persönliche Information noch keinen greifbaren Wert über die einzelne Transaktion hinaus und entzog sich einer weiteren Verwendung, wurde es so auf einmal möglich, aus zahlreichen atomaren Einzeldaten detaillierte Profile von Kunden und ihrem Kaufverhalten zu erstellen [CuB03, Spi98].

Mit RFID und anderen ubiquitären Technologien entsteht nun eine neue Qualität der Datenerhebung (siehe hierzu auch den Beitrag von Marc Langheinrich in diesem Buch). Diese geht über die bisher gängige Praxis der Informationsgewinnung aus Kreditkartentransaktionen oder Telefonverbindungen hinaus durch

- die räumliche und zeitliche Ausdehnung von Beobachtungsaktivitäten,
- die fehlende Erkenn- und Rekonstruierbarkeit der Datenerhebung,
- die Erhebung neuer Datentypen durch Echtzeitüberwachung,
- den immer weniger nachvollziehbaren Erhebungsgrund sowie
- den unkontrollierbaren Datenzugriff durch extreme Interkonnektivität.

Im Fall von RFID entsteht die Privacy-Problematik insbesondere durch die weltweit eindeutige Identifizierbarkeit jedes Gutes durch ein Nummerierungsschema wie den „Electronic Product Code (EPC)“ [SBE01] und die mögliche Verknüpfung mit dem Besitzer, welches prinzipiell ein automatisches Tracking von Personen möglich macht [SWE02]. Darüber hinaus verfügt RFID gegenüber dem gängigen Barcode über eine Reihe weiterer Privacy-relevanter Eigenschaften, wie dem Lesevorgang ohne Sichtverbindung und der Möglichkeit zur Speicherung von Daten auf dem Objekt selbst.

Entscheidend ist dabei, dass die eigentliche Datenauswertung keineswegs RFID-spezifisch ist, sondern z.B. auf herkömmlichen Data-Mining-Verfahren beruht. RFID wirkt jedoch als Enabler-Technologie, die die dazu notwendigen Basisdaten je nach Einsatzgebiet in einer zuvor nicht gekannten Quantität und Genauigkeit liefern kann.

3 Analyse der öffentlichen Diskussion

Im Folgenden sollen die Darstellung und Wahrnehmung von Risiken der RFID-Technologie in Bezug auf Privacy genauer untersucht werden. Da sowohl Anti-RFID-Kampagnen in Form diverser Homepages als auch die Berichterstattung und deren öffentliche Diskussion zu einem großen Teil im Internet stattfinden, liegt es nahe, dieses Medium als Ausgangspunkt für die weitere Analyse heranzuziehen. Den nachfolgenden Aussagen liegt eine Untersuchung auf Basis der „7-Tage-News” des Heise-Verlags (www.heise.de) zugrunde, einem auf IT spezialisierten Newsticker eines Herausgebers mehrerer Computermagazine im deutschsprachigen Raum. Diese Auswahl erscheint geeignet, da a) der Fokus auf IT eine große Zahl RFID-bezogener Nachrichten erwarten lässt, b) der Inhalt sich jedoch nicht nur an ein Fachpublikum richtet und c) die an jeden Newseintrag angeschlossenen Diskussionsforen eine unmittelbare Betrachtung der Reaktion auf einzelne Nachrichten erlaubt (vgl. [Ric01] für eine Analyse der Diskussion von Risikothemen in Internet-Newsgroups am Beispiel BSE).

In einem ersten Schritt wurden über eine Volltextsuche nach den Stichworten „RFID" und „Transponder" alle relevanten RFID-Nachrichten der letzten Jahre ermittelt, wobei Texte, die sich auf andere Themen (z.B. TV-Satelliten) bezogen, manuell wieder aus der Liste entfernt wurden. Anschließend wurden all jene Nachrichten identifiziert, die die Auswirkung von RFID auf information privacy zum Thema hatten. Als Resultat dieses Untersuchungsschritts ergibt sich Abbildung 2, in der die Zahl der gesammelten Nachrichten pro Quartal bis Ende 2004 dargestellt ist.

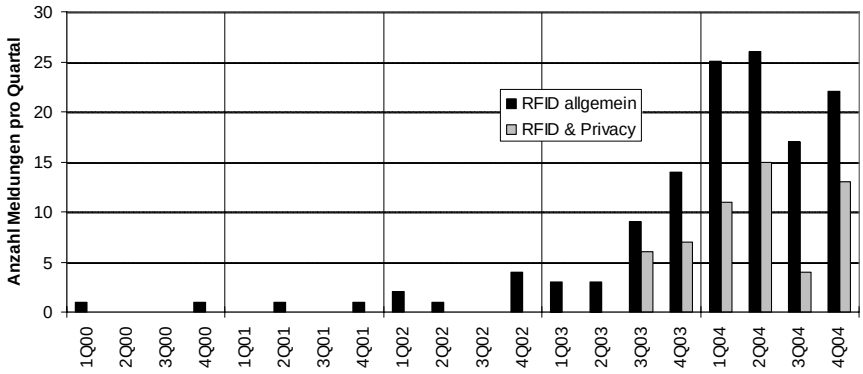


Abb. 2. RFID-bezogene Nachrichten im Heise-Newsticker

Wie sich hier zeigt, wurde Privacy Mitte 2003 schlagartig zum Thema und ist seither unmittelbar mit RFID verknüpft bzw. als Risikothema etabliert. Beginn dieser Entwicklung war eine Meldung vom 8.7.2003 über die Veröffentlichung 68 scheinbar vertraulicher Dokumente über die Pläne des Auto-ID Centers und seiner Sponsoren für die RFID-Einführung durch die Organisation CASPIAN. Der Beitrag nannte als Motivation für den Einsatz der Technik u.a. die Möglichkeit, das Kaufverhalten und die finanziellen Verhältnisse von Verbrauchern ohne deren Wissen zu analysieren. Darüber hinaus wurde passiven RFID-Transpondern die Fähigkeit zugeschrieben, über bis zu 30 Meter hinweg identifizierbar zu sein.

Beobachtet man den Umgang von Technologieanbietern und Anwendern mit derartigen Meldungen im weiteren Zeitverlauf, so fällt ein sich wiederholendes Muster aus Aktion und Reaktion auf, wobei Unternehmen gegenüber den agierenden Pressure Groups stets in die Defensive gedrängt sind und mit einem raschen Rückzug aus einzelnen Anwendungsbereichen bzw. Projekten reagieren. Einige prominente Beispiele sind in Tabelle 1 zusammengefasst. Obwohl die dargestellten Ereignisse nicht notwendigerweise kausal zusammenhängen, entsteht so der Eindruck, die Industrie sei bei der heimlichen Einführung einer für den Konsumenten wenig vorteilhaften Technologie auf frischer Tat ertappt worden.

Tabelle 1. Aktion & Reaktion in der Auseinandersetzung um RFID

Firma	Datum	Ereignisse
Benetton / Philips	11.3.2003	*Aktion:* Benetton kündigt an, zukünftig RFID-Tags in Sisley-Textilien einnähen zu wollen. CASPIAN ruft daraufhin zwei Tage später im Internet zu einem Boykott von Benetton-Produkten auf.
	9.4.2003	*Reaktion:* Benetton verkündet in einer Pressemeldung, auf RFID in Textilien verzichten zu wollen.
Wal-Mart / Gillette	8.7.2003	*Aktion:* CASPIAN veröffentlicht 68 als „confidential" gekennzeichnete Dokumente des Auto-ID Centers, zu dessen größten Sponsoren Wal-Mart und Gillete zählen. Wal-Mart hatte zuvor am 30.4. ein RFID-Pilotprojekt zur automatisierten Inventur im Verkaufsraum gestartet.
	9.7.2003	*Reaktion:* Wal-Mart stoppt das Pilotprojekt und kündigt an, RFID nur noch in der internen Logistik einsetzen zu wollen.
Tesco / Gillette	22.7.2003	*Aktion:* Der britischen Handelskette Tesco wird vorgeworfen, Kunden bei der Entnahme von Rasierklingen aus dem Regal mittels RFID zu erfassen und automatisch zu fotografieren.
	15.8.2003	*Reaktion:* Gillette bestreitet alle Vorwürfe; Tesco gibt zu, „sicherheitsrelevante Vorteile" der RFID-Technik getestet zu haben. Der Pilotversuch wurde Ende Juli 2003 beendet.
Metro	1.2.2004	*Aktion:* FoeBuD demonstriert vor dem Metro Future Store gegen den Einsatz RFID-basierter Kundenkarten.
	27.2.2004	*Reaktion:* Metro tauscht 10 000 Kundenkarten gegen solche ohne RFID-Tag um.

In einem zweiten Schritt der Untersuchung wurde analysiert, wie die Reaktionen der Leser der Heise-Seiten auf RFID-Nachrichtenmeldungen ausfielen. Die thematische Ausrichtung des Newstickers lässt wegen fehlender Repräsentativität der Teilnehmer an den Diskussionen zwar keine statistische Auswertung zu, die Forenbeiträge selbst erlauben jedoch eine qualitative Betrachtung von Sprache, Diskussionsstil und Argumentation.

Die Kritikpunkte der Diskussionsteilnehmer an RFID lassen sich thematisch in den folgenden vier Aussagen zusammenfassen:

- **Unsichere Technik.** Die Fähigkeiten der Technologie sind in weiten Teilen unklar. Offensichtlich scheint jedoch, dass RFID nur unzureichend Funktionen zur Sicherstellung der Datensicherheit implementiert.
- **Unklarer Nutzen.** Sinn und Zweck der RFID-Einführung ist nicht ersichtlich. Dies betrifft den nicht nachvollziehbaren Nutzen auf Unternehmensseite, vor allem aber hat der Konsument selbst keinen Vorteil von der Technologie. Der Missbrauch von Kundendaten erscheint als naheliegendstes Einsatzgebiet für RFID.
- **Fehlende Glaubwürdigkeit.** Den Aussagen von Handelskonzernen und Produzenten kann kein Glauben geschenkt werden. Die zurückhaltende Informationspolitik zeigt, dass RFID-Anwender etwas zu verbergen haben.

- **Unzureichende Gesetzeslage.** Bestehende Gesetze reichen zum Schutz des Individuums vor RFID nicht aus. Der Gesetzgeber ist aufgerufen, den Einsatz von RFID zu verbieten oder zumindest stark einzuschränken.

Die Diskussion selbst verläuft in den meisten Fällen stark emotionalisiert und einzelnen Beiträgen haftet allzu häufig der Charakter von Verschwörungstheorien an, d.h., Staat und Wirtschaft wird per se die Absicht unterstellt, RFID zur Überwachung von Privatpersonen einsetzen zu wollen. Der Vergleich zur orwellschen Dystopie „1984" oder Huxleys „Brave new world" findet sich in zahlreichen Texten wieder. Dies korrespondiert auffällig mit einer Häufung sachlich falscher Vorstellungen von den Möglichkeiten von RFID als Überwachungstechnologie. Beispielsweise äußern viele Forenteilnehmer die Befürchtung, RFID-Transponder und ihre Träger seien per Satellit weltweit lokalisierbar.

Zusammengefasst lässt sich auf Grundlage der betrachteten Forendiskussionen feststellen, dass die Wahrnehmung von RFID als Risiko für die Privatsphäre des Einzelnen von massiven Ängsten und einem tief sitzenden Misstrauen gegenüber den Anwenderfirmen gekennzeichnet ist. Dabei wird auch deutlich, dass ein Mangel an Information seitens der Verbraucher eine, aber keineswegs die einzige Ursache für die Ablehnung der Technologie ist. Handlungsdefizite seitens der Unternehmen bestehen vielmehr auf mehreren Ebenen, wohingegen es den Pressure Groups erfolgreich gelungen ist, das Thema zu besetzen, die öffentliche Wahrnehmung auf die zweifellos vorhandenen Risiken von RFID zu konzentrieren und Nutzenpotenziale weitgehend auszublenden.

4 Elemente einer Privacy-Strategie

Vor dem Hintergrund der beschriebenen Haltung der Konsumenten gegenüber RFID stellt sich für Unternehmen die Frage, welche Mittel ihnen noch zur Verfügung stehen, um die Risikowahrnehmung in ihrem Sinn zu beeinflussen. Ziel ist dabei stets, Wissen über die Technologie zu vermitteln bzw. dort, wo dies nicht möglich ist und Unsicherheit vorherrscht, den Aufbau eines Vertrauensverhältnisses zu fördern, welches diese Unsicherheit überwinden hilft.

Aufbauend auf den zuvor beschriebenen vier Kernaussagen der RFID-Skeptiker lassen sich unmittelbar entsprechende Handlungsebenen mit jeweils eigenen Gestaltungsobjekten und Zielen ableiten (siehe Abbildung 3):

- **Technologie.** Auf der technischen Ebene gilt es, RFID-Systeme um Funktionen zu ergänzen, die einen Datenmissbrauch unmöglich machen oder zumindest erschweren.
- **Prozesse.** Ziel auf der Prozessebene ist die Erhöhung des Nutzens für den Kunden bei gleichzeitiger Reduktion der Risiken auf ein Minimum durch begleitende organisatorische Maßnahmen.
- **Dialog.** Der Risikodialog in und mit der Öffentlichkeit sowie dem einzelnen Konsumenten zielt auf die Wiedergewinnung verlorener Glaubwürdigkeit ab.

- **Regeln.** Regeln dienen der für alle Seiten verbindlichen Festlegung, welche Anwendungen bzw. Handlungsweisen im Zusammenhang mit der Technologie als zulässig gelten oder nicht.

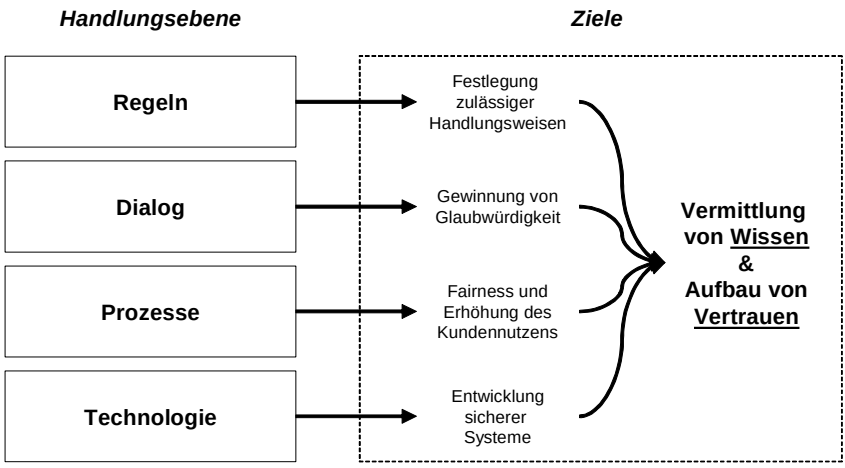


Abb. 3. Handlungsebenen für das Risikomanagement

4.1 Technologie

Die Möglichkeiten zur Sicherung des Datenschutzes auf technischer Ebene sind vielfältig und umfassen neben allgemeinen Maßnahmen zur IT-Sicherheit auch RFID-spezifische Konzepte, um das unkontrollierte Lesen von Transpondern sowie die Manipulation der darauf gespeicherten Informationen zu verhindern. Wie auch im Beitrag von Langheinrich ausgeführt, findet sich in der Literatur hierzu eine Reihe unterschiedlicher Ansätze [Cav04, JRS03, Kum03, SWE02, WSR03]:

- **Abschirmung.** Der einfachste Schutz vor Zugriff auf den Transponder durch Dritte ist die physikalische Abschirmung analog einem faradayschen Käfig mittels eines metallischen Netzes oder einer Folie.
- **Störsender.** Die Kommunikation zwischen Transponder und Lesegerät kann durch den Einsatz eines Störsenders verhindert werden.
- **Blocker-Tag.** Bei der iterativen Suche des Lesers nach einer Transponder-ID antwortet der Blocker-Tag stets mit einer passenden ID, sodass der Leser keine Chance hat, die in seiner Umgebung befindlichen Transponder zu erkennen.
- **Kill-Kommando.** Das im Transponder implementierte Kill-Kommando dient zur dauerhaften Deaktivierung, z.B. bei der Übergabe eines Produkts an den Käufer an der Supermarktkasse.

- **Hash-Lock-Verfahren.** Der Tag wird über einen Hash-Wert, der aus einem Zufallsschlüssel generiert wird, gesperrt und reagiert nur noch auf Anfragen, die über diesen Hash-Wert autorisiert sind. Zu einem späteren Zeitpunkt kann der Transponder dann mit Hilfe des Schlüssels wieder entsperrt werden.
- **Distanz-basierte Zugriffskontrolle.** Art und Umfang der vom Transponder gesendeten Informationen werden vom Abstand zum Lesegerät (ermittelt z.B. durch Feldstärke oder Triangulation) abhängig gemacht.
- **Abhörsichere Antikollisionsprotokolle.** Abhörsichere Antikollisionsprotokolle vermeiden die Übertragung kompletter Tag-IDs auf dem Vorwärtskanal (d.h. vom Leser zu den Tags), sodass ein Abhören aus weiter Entfernung verhindert wird.

Einige der genannten Verfahren scheitern bereits an mangelnder Praktikabilität aufgrund zu hoher technischer Anforderungen, Komplexität für den Benutzer oder der Tatsache, dass verschiedene RFID-Anwendungen auf diese Weise durch technische Funktionalität von vornherein unmöglich gemacht werden, z.B. im Rahmen von Mehrwegsystemen. Das aus Kundensicht gravierendste Problem ist jedoch, dass die gewonnene zusätzliche Sicherheit nicht spürbar bzw. sichtbar wird und vor allem keine Möglichkeit zur zuverlässigen Verifikation besteht. Trotz aller Notwendigkeit technischer Weiterentwicklung kann das Ziel der verbesserten Technologieakzeptanz somit auf diese Weise allein nicht erreicht werden.

4.2 Prozesse

Mit der Änderung von Abläufen auf der Prozessebene können in zweierlei Hinsicht Anreize geschaffen werden, die die Einstellung von Konsumenten gegenüber der RFID-Technologie positiv beeinflussen. Einerseits sollten Prozesse so gestaltet sein, dass dem Kunden der Eindruck von „procedural fairness", d.h. dem fairen Umgang mit ihm im Rahmen geschäftlicher Aktivitäten, vermittelt wird [CuA99]. Wesentlicher Faktor ist in diesem Zusammenhang neben dem Wissen über Abläufe die Kontrolle über dieselbigen [CuB03], z.B. durch Opt-in-Wahlmöglichkeiten. „Opt-in" bezeichnet hierbei die Notwendigkeit, im Rahmen einer Geschäftsbeziehung eine Entscheidung für einen Service (z.B. die Zusendung personalisierter Werbemails) bewusst treffen zu müssen, während „Opt-out" die positive Entscheidung durch Voreinstellungen vorwegnimmt und der Kunde gezwungen ist, explizit zu widersprechen [MaL01, Win01]. Opt-in setzt dabei voraus, dass dem Kunden die Folgen einer positiven Entscheidung klar offen gelegt werden.

Andererseits kann durch verbesserte Prozesse die Bereitschaft des Kunden zur Technologieakzeptanz durch zusätzliche Leistungen und Nutzeffekte erhöht werden. So konnte in zahlreichen Untersuchungen auf Grundlage des weit verbreiteten „Technology Acceptance Model (TAM)" [Dav89] zu E-Mail, Telemedizin und anderen IT-Themen gezeigt werden, dass die Akzeptanz auf Nutzerseite im Wesentlichen von der wahrgenommenen Einfachheit der Nutzung sowie der wahrgenommenen Nützlichkeit einer Technologie abhängig ist [ChL03, McC03]. Es kann daher mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass ansprechend gestaltete Dienste auf RFID-Basis auch einen positiven Einfluss auf

die Akzeptanz der Technologie selbst hätten. Beispiele für derartige Dienste sind [FlD03, SpB04]:

- Beschleunigter Bezahlvorgang an der Supermarktkasse durch automatische Erfassung aller eingekauften Waren im Einkaufskorb.
- Produktinformationen, die der Kunde im Geschäft oder daheim abrufen kann, z.B. Verbraucherinformationen, Bedienungsanleitungen oder Softwareupdates.
- Wartungs- und Reparaturdienste, die als Service über das Internet angeboten werden, sowie effizientere Durchführung von Rückholaktionen und Bearbeitung von Garantiefällen.
- Vermeidung von Fälschungen von Luxusgütern, Autoersatzteilen oder Medikamenten, die durch einen RFID-Transponder eindeutig als Original identifiziert und deren Weg in der Lieferkette zurückverfolgt werden kann.

4.3 Dialog

Im Gegensatz zu vielen anderen Branchen wird im Handel der Begriff der „customer relation" weitgehend auf „customer loyalty" reduziert. Ziel entsprechender Loyalty- oder Frequency-Programme ist weniger der Aufbau einer Beziehung zum Kunden als die Erhöhung der Transaktionshäufigkeit durch Schaffung von Anreizen [Win01], z.B. durch Rabattkarten (vgl. hierzu beispielsweise die Beschreibung des Loyalty-Programms der Handelskette Tesco bei [HHP04]). Während somit auf der einen Seite der Aufbau einer Beziehung des Kunden zum Unternehmen unterbleibt, führt die Art und Weise der Datensammlung in den gängigen Kundenkartensystemen zu einem Vertrauensverlust seitens der Kunden [Fle03].

Vor diesem Hintergrund kommt dem offenen Dialog mit Kunden unabhängig von der einzelnen Transaktion eine wichtige Rolle in der (Wieder-)Gewinnung von Vertrauen und Glaubwürdigkeit zu. In der konkreten Auseinandersetzung um RFID herrschen hingegen Strategien vor, die auf das Herunterspielen von Risiken bzw. die Belehrung der Öffentlichkeit ausgerichtet sind, oder schlichte Kommunikationsenthaltung – Kommunikationsstrategien also, die wenig geeignet erscheinen, um den Konsumenten für das Unternehmen zu gewinnen. Wiedemann nennt folgende typische Fehler in der Kommunikation, die sich nahezu 1:1 in der aktuellen Diskussion wiederfinden [Wie94]:

- Verleugnung und defensive Informationspolitik
- Beschwichtigung (Versuch des „Weg-Redens")
- Aggressive und konfrontative Auseinandersetzungen sowie Polemik
- Nur Worte, keine Taten
- Zu späte Information
- Reaktive Informationspolitik
- Mangelnde Klarheit und Verständlichkeit der Informationen
- Unzureichender Bezug auf die vorhandenen Informationsbedürfnisse und Vorstellungen der Öffentlichkeit

Die Entwicklung eines konstruktiven Dialogs ist aufgrund häufig verhärteter Fronten und Verständigungsprobleme schwierig. Nichtsdestotrotz sind z.B. die Bereitschaft zu Interviews, praktische Demonstrationen, Kooperation mit Interessenverbänden, Vermittlung von Experten usw. langfristig erfolgreiche Maßnahmen einer offenen und offensiven Kommunikationskultur [WiH89].

4.4 Regeln

Die Festlegung verbindlicher Regeln kann entweder durch Gesetze und Verordnungen oder in Form einer Selbstverpflichtung erfolgen. Während die Einbindung der neutralen Institution des Staates einen gewissen Vertrauensbonus mit sich bringt, hat die Selbstverpflichtung der Industrie den Vorteil informellerer Kontrollmechanismen. In beiden Fällen ist für die Entwicklung einer Strategie zunächst wichtig, bereits bestehende Regelungen zu kennen.

In den USA und Europa haben sich im Verlauf der letzten Jahrzehnte grundsätzlich verschiedene Herangehensweisen zum Schutz der Privatsphäre etabliert (siehe Tabelle 2) [Smi01]: Dem vor allem in Europa favorisierten Ansatz umfassender, sektorenübergreifender Datenschutzgesetze steht in den USA ein Mix aus spezifischer Gesetzgebung und freiwilliger Selbstbeschränkung von Industrie und Handel gegenüber. Vor diesem Hintergrund erklärt sich u.a. die amerikanische Forderung nach einem „RFID Bill of Rights" [Gar02], wohingegen entsprechende Vorhaben in Europa bereits im Vorfeld verworfen wurden.

Tabelle 2. Unterschiede im Datenschutzrecht in USA und Europa

	USA	Europa
Legislativer Ansatz	sektoriell	universell
Regulative Struktur	Selbstinitiative und freiwillige Kontrolle	zentralisierte Behörde (Beauftragter, Registrierstelle oder Lizenzierung)
Rechte des Datensubjekts	Keine oder Opt-out (anwendungsabhängig)	Prüfung / Korrektur, Opt-out (teilw. Opt-in)
Rolle von Privacy in der Gesellschaft	Verhandlungssache	Menschenrecht

Unabhängig von der Gesetzeslage erfüllt eine öffentliche Selbstverpflichtung darüber hinaus die Aufgabe, das Bekenntnis eines Unternehmens zur Einhaltung bestimmter Standards nach außen zu dokumentieren. Beispiele hierfür sind die vorgeschlagene Kennzeichnung EPC-bestückter Produkte (siehe Abbildung 4) [EPC04] oder auch die organisatorische Verankerung in Form eines „Chief Privacy Officer" [HB01, Jon04].

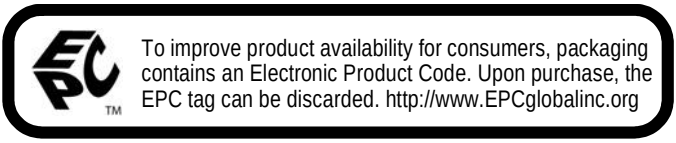


Abb. 4. Label zur Kennzeichnung von Produkten mit EPC-Transpondern

5 Zusammenfassung und Ausblick

Wie die vorangegangenen Ausführungen gezeigt haben, ist die Wahrnehmung von RFID als Risiko mittlerweile etabliert und entwickelt sich in ähnlicher Weise wie auch bereits andere technologische Risikothemen in der Vergangenheit. Inwiefern das Thema das Stadium der Krise erreicht oder vorher abflaut, ist derzeit noch völlig offen und hängt vom weiteren Verlauf der Auseinandersetzung ab (siehe Abbildung 5 in Anlehnung an [CHK00, S. 14]). Ob es den Technologieanbietern und -anwendern gelingt, die öffentliche Wahrnehmung noch zu drehen und das Thema positiv zu besetzen, wird in jedem Fall wesentlich von der gewählten Risikomanagementstrategie bestimmt.

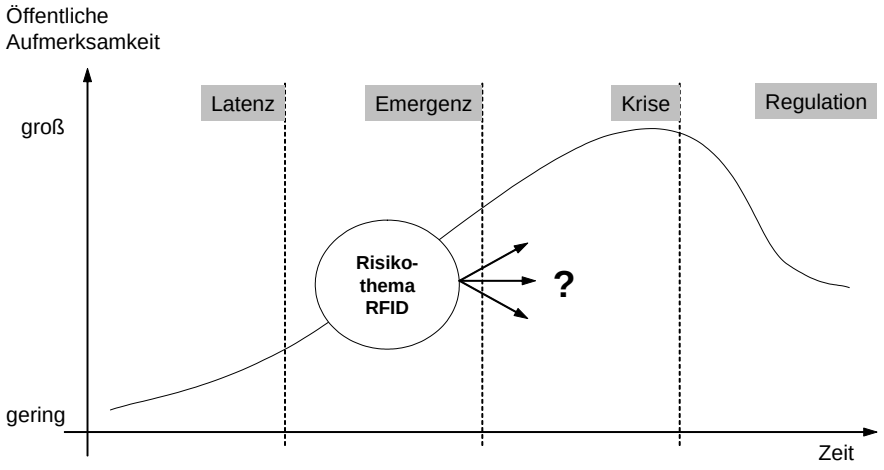


Abb. 5. Lebenslauf des Risikothemas RFID

Durch ihren Rückzug aus einzelnen kritischen Anwendungsbereichen und die Entscheidung, RFID zunächst nicht auf Einzelproduktebene, sondern nur auf Paletten und Umverpackungen einzusetzen (siehe hierzu z.B. Angaben der METRO Group zum geplanten RFID-Roll-out in [Met04]), haben Industrie und Handel etwas Zeit gewonnen. Mit der Weiterentwicklung der Technologie bei gleichzeitig sinkenden Preisen werden jedoch voraussichtlich nach und nach auch Anwendungen wirtschaftlich attraktiv werden, die aktivierte Transponder auf Einzelpro-

dukten über den Kauf- und Bezahlvorgang hinaus beim Kunden voraussetzen. Vor diesem Hintergrund können der vorliegende Beitrag und insbesondere das vorgestellte Ebenenmodell als ein Gestaltungsrahmen für das Risikomanagement jenseits der derzeit noch zumeist vorherrschenden technologiezentrischen Sichtweise dienen.

Literatur

[Can02] Cantwell B (2002) Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies. Auto-ID Center White Paper, archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-016.pdf

[Cav04] Cavoukian A (2004) Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. Information and Privacy Commissioner Ontario, Toronto

[CHK00] Carius R, Henschel C, Kastenholz HG, Nothdurft W, Ruff F, Uth HJ, Wiedemann PM (2000) Risikokommunikation für Unternehmen. Verein Deutscher Ingenieure (VDI)

[ChL03] Chau PYK, Lai, VSK (2003) An Empirical Investigation of the Determinants of User Acceptance of Internet Banking. Journal of Organizational Computing and Electronic Commerce 13(2): 123–145

[CuA99] Culnan MJ, Armstrong P (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10(1): 104–116

[CuB03] Culnan MJ, Bies RJ (2003) Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues 59(2): 323–342

[Dav89] Davis F (1989) Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly 13(3): 319–339

[Duc03] Duce H (2003) Public Policy: Understanding Public Opinion. Executive Briefing, Auto-ID Center, archive.epcglobalinc.org/publishedresearch/cam-autoid-eb002.pdf

[EPC04] EPCglobal Consumer Information (2004) EPCglobal Inc., www.epcglobalinc.org/consumer/index.html

[Fin02] Finucane ML (2002) Mad Cows, Mad Corn & Mad Money: Applying What We Know About the Perceived Risk of Technologies to the Perceived Risk of Securities. The Journal of Psychology and Financial Markets 3(4): 236–243

[FlD03] Fleisch E, Dierkes M (2003) Ubiquitous Computing aus betriebswirtschaftlicher Sicht. Wirtschaftsinformatik 41(6): 661–670

[Fle03] Fletcher K (2003) Consumer power and privacy: the changing nature of CRM. International Journal of Advertising 22(2): 249–272

[Gar02] Garfinkel SL (2002) Adopting Fair Information Practices to Low Cost RFID Systems. International Conference on Ubiquitous Computing, Göteborg

[HB01] Harvard Business Review (2001) Chief Privacy Officer. Harvard Business Review, 78(6): 20–21

[Hen90] Hennen L (1990) Risiko-Kommunikation: Informations- und Kommunikationstechnologien. In: Jungermann H, Rohrmann B, Wiedemann PM (Hrsg) Risiko-

Konzepte – Risiko-Konflikte – Risiko-Kommunikation. Forschungszentrum Jülich, S 209–258

[HHP04] Humby C, Hunt T, Phillips T (2004) Scoring Points: How Tesco Is Winning Customer Loyalty. Kogan Page, London

[Jon01] Jones KE (2001) BSE, Risk and the Communication of Uncertainty: A Review of Lord Phillips' Report from the BSE Inquiry. Canadian Journal of Sociology 26(4): 655–666

[Jon04] Jonietz E (2004) Tracking Privacy. Technology Review 107(6): 74-75

[JRS03] Juels A, Rivest R, Szydlo M (2003) The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Atluri V (ed) Proceedings of the 8th ACM Conference on Computer and Communications Security, pp 103–111

[Jun91] Jungermann H, Inhalte und Konzepte der Risikokommunikation. In: Jungermann, H, Rohrmann B, Wiedemann PM (Hrsg) Risikokontroversen – Konzepte, Konflikte, Kommunikation. Springer-Verlag, S 335–354

[KoK91] Koren G, Klein N (1991) Bias against negative studies in newspaper reports of medical research. Journal of the American Medical Association 266(13): 1824–1826

[Kum03] Kumar R (2003) Interaction of RFID Technology and Public Policy. RFID Privacy Workshop @ MIT

[Lan01] Landt J (2001) Shrouds of Time: The History of RFID. AIM Inc.

[MaL01] Mattern F, Langheinrich M (2001) Allgegenwärtigkeit des Computers - Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller G, Reichenbach M (Hrsg) Sicherheitskonzepte für das Internet. Springer-Verlag

[McC03] McCloskey D (2003) Evaluating Electronic Commerce Acceptance with the Technology Acceptance Model. Journal of Computer Information Systems 4(2): 49–57

[Met04] METRO Group (2004) Leitlinien für den RFID-Roll-out der METRO Group. METRO Group, Düsseldorf

[ReL91] Renn O, Levine D (1991) Credibility and trust in risk communication. In: Kasperson RE, Stallen PJM (eds) Communicating Risks to the Public. Kluwer, Dordrecht, pp 175–218

[Ric01] Richardson K (2001) Risk news in the world of Internet newsgroups. Journal of Sociolinguistics 5(1): 50–72

[SBE01] Sarma S, Brock D, Engels DW (2001) Radio Frequency Identification and the Electronic Product Code. IEEE Micro 21(6): 50–54

[Sch04] Schneider R (2004) Emerging Risks - Analyse or Exclude. Reinsurance Lecture at The Institute of London, London, www.iilondon.co.uk/pdf/RSchneider140104.pdf

[SFL81] Slovic P, Fischhoff B, Lichtenstein S (1981) Facts and Fears: Societal Perception of Risk. Advances in Consumer Research 8(1): 497–502

[Sie01] Siegrist M (2001) Die Bedeutung von Vertrauen bei der Wahrnehmung und Bewertung von Risiken. Arbeitsbericht Nr. 197, Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart

[SjFr01] Sjöberg L, Framm J (2001) Information Technology Risks as Seen by the Public. Risk Analysis 21(3): 427-441

[Slo92] Slovic P (1992) Perception of risk: Reflections on the psychometric paradigm. In: Krimsky S, Golding D (eds) Social theories of risk. Praeger, Westport, pp 117–152

[Slo99] Slovic P (1999) Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk Analysis 19(4): 689–701

[Smi01] Smith HJ (2001) Information Privacy and Marketing: What the U.S. should (and shouldn't) learn from Europe. California Management Review 43(2): 8–33

[SpB04] Spiekermann S, Berthold O (2004) Maintaining privacy in RFID enabled environments: Proposal for a disable-model. Workshop on Security and Privacy in Pervasive Computing, International Conference on Pervasive Computing

[Spi98] Spinello RA (1998) Privacy Rights in the Information Economy. Business Ethics Quarterly 8(4): 723–742

[SWE02] Sarma S, Weis S, Engels D (2002) RFID Systems, Security & Privacy Implications. Auto-ID Center White Paper, http://archive.epcglobalinc.org/publishedresearch/MIT-AUTOID-WH-014.pdf

[Tac01] Tacke V (2001) BSE as an organizational construction: a case study on the globalization of risk. British Journal of Sociology 52(2): 293–312

[TrM03] Trumbo CW, McComas KA (2003) The Function of Credibility in Information Processing for Risk Perception. Risk Analysis 23(2): 343–353

[WaB90] Warren SD, Brandeis LD (1890) The Right to Privacy. Harvard Law Review 4(5): 193–220

[Wes03] Westin A (2003) Social and Political Dimensions of Privacy. Journal of Social Issues 59(2): 431–453

[Wes67] Westin A (1967) Privacy and Freedom. Atheneum, New York

[Wha98] Whawell P (1998) The ethics of pressure groups. Business Ethics 7(3): 178–181

[Wie94] Wiedemann P (1994) Krisenmanagement & Krisenkommunikation. Arbeiten zur Risiko-Kommunikation Heft 41, Forschungszentrum Jülich

[WiH89] Wiedemann P, Hennen L (1989) Schwierigkeiten bei der Kommunikation über technische Risiken. Arbeiten zur Risiko-Kommunikation Heft 9, Forschungszentrum Jülich

[Win01] Winer RS (2001) A Framework for Customer Relationship Management. California Management Review 43(4): 89–105

[WOL02] Watson T, Osborne-Brown S, Longhurst M (2002) Issues Negotiation – investing in stakeholders. Corporate Communications 7(1): 54-61

[WSR03] Weis SA, Sarma S, Rivest RL, Engels DW (2003) Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. 1st International Conference on Security in Pervasive Computing, Boppard, March 2003. Springer-Verlag, LNCS 2802: 201–212

[Zei04] Zeidler M (2004) RFID: Der Schnüffel-Chip im Joghurtbecher. Monitor, Westdeutscher Rundfunk, Köln, 8. Januar 2004, www.wdr.de/tv/monitor/pdf/040108f_rfid.pdf

Über die Herausgeber

Prof. Dr. Elgar Fleisch ist seit 2002 Extraordinarius für Technologiemanagement und Direktor am Institut für Technologiemanagement an der Universität St. Gallen (HSG). Er ist außerdem seit Oktober 2004 ordentlicher Professor für Informationsmanagement am Departement für Management, Technologie und Ökonomie der ETH Zürich. Elgar Fleisch studierte Wirtschaftsinformatik an der Universität Wien und verfasste anschließend an der Wirtschaftsuniversität Wien und am Institut für höhere Studien in Wien seine Dissertation an der Schnittstelle zwischen Künstlicher Intelligenz und Produktionsplanung. 1994 wechselte Elgar Fleisch an die Universität St. Gallen und leitete am Lehrstuhl von Prof. Hubert Österle Forschungsprojekte im Bereich „Business Networking". 1996–97 gründete und führte er die IMG Americas Inc. in Philadelphia, USA. 2000 erhielt Elgar Fleisch die Privatdozentur der Universität St. Gallen und wurde zum Assistenzprofessor ernannt.

Heute forscht Elgar Fleisch in den Bereichen „betriebswirtschaftliche Aspekte des Ubiquitous Computing" und „Management industrieller Dienstleistungen". Er leitet zusammen mit Prof. Friedemann Mattern von der ETH Zürich das Gemeinschaftsprojekt M-Lab und ist Co-Chair der Auto-ID Labs, einem Netzwerk aus sechs internationalen Forschungseinrichtungen (u.a. MIT und Universität Cambridge), welches die Infrastruktur für das „Internet der Dinge" spezifiziert. Elgar Fleisch ist außerdem Mitgründer der intellion AG sowie Mitglied zahlreicher Steuerungsausschüsse in Forschung, Lehre und Praxis.

Prof. Dr. Friedemann Mattern ist an der ETH Zürich tätig und leitet dort das Fachgebiet „Verteilte Systeme". Er studierte Informatik in Bonn und promovierte 1989 an der Universität Kaiserslautern, danach hatte er Professuren an der Universität des Saarlandes in Saarbrücken sowie an der Technischen Universität Darmstadt inne. Mit seinem Wechsel an die ETH Zürich im Jahr 1999 begann er mit dem Aufbau einer Forschungsgruppe für Ubiquitous Computing, seit 2002 steht er dort auch dem neu gegründeten Institut für Pervasive Computing vor.

Friedemann Mattern ist an mehreren Industriekooperationen und Forschungsprojekten zum Thema Ubiquitous und Pervasive Computing beteiligt. Er ist Mitbegründer des M-Lab und koordiniert das Ladenburger Kolleg „Leben in einer smarten Umgebung", an dem Forschungsgruppen von sieben Universitäten beteiligt sind. Er ist im Technologiebeirat namhafter Konzerne vertreten, Mitglied verschiedener wissenschaftlicher Akademien, Mitherausgeber mehrerer Fachzeitschriften und Buchreihen (u.a. „Lecture Notes in Computer Science", LNCS) und initiierte eine Reihe internationaler Fachkonferenzen, darunter die PERVASIVE-Konferenzserie. Seine derzeitige Lehrtätigkeit umfasst die Gebiete verteilte Systeme und Algorithmen, Rechnernetze sowie Ubiquitous Computing.