UNIVERSITÄT
KOBLENZ · LANDAU

Integration mobiler RFID-Erfassung in das Supply Chain Management

Diplomarbeit

zur Erlangung des Grades eines Diplom-Informatikers im Studiengang Informatik

vorgelegt von

Sven Westenberg

Betreuer: Prof. Dr. J. Felix Hampe, Institut für Wirtschafts- und Verwaltungsinformatik, Fachbereich Informatik,
Dipl.-Inform. Götz Botterweck, Institut für Wirtschafts- und Verwaltungsinformatik, Fachbereich Informatik

Koblenz, im September 2006

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Mit der Einstellung dieser Arbeit in die Bibliothek bin ich einverstanden. Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.

Koblenz, im September 2006

_____

(Sven Westenberg)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Überblick

1.1 Einleitung

Die Informations- und Telekommunikationstechnologie durchdringt immer deutlicher das Alltags- und Berufsleben vieler Menschen und Unternehmen. Unter den Begriffen *Ubiquitous Computing* und *Pervasive Computing* wird die Allgegenwärtigkeit von sehr kleinen, intelligenten Gegenständen in verschiedenen Umgebungen und die immer stärkere Durchdringung der Informationstechnologie verschiedenster Bereiche zusammengefasst. Die *Radio Frequency Identification* (RFID) Technologie ermöglicht das berührungslose Identifizieren von Objekten und das Lesen und Schreiben von Daten auf kleinen, drahtlosen Geräten (Tag, Transponder, Chip). Die Einsatzmöglichkeiten sind vielfältig. RFID-Tags können Barcodes ersetzen, indem jeder Tag mit einer elektronischen, eindeutigen ID versehen wird. Sie können als Authentifikationsmerkmal beim *Mobile Payment* oder als Schlüsselersatz (Wegfahrsperre eines Fahrzeugs) verwendet werden. Des Weiteren erleichtert eine elektronische Erfassung von Objekten im *Supply Chain Management* (SCM) die Integration von Prozessen der Beschaffung, der Produktion, des Transports, der Logistik und des Vertriebs. Diese Erleichterung sollte sich im geschäftlichen Umfeld natürlich nicht nur in den Prozessen, sondern auch in den wirtschaftlichen Ergebnissen, niederschlagen.

Da die technischen Möglichkeiten bestehen, zu jedem Zeitpunkt für das menschliche Auge nicht sichtbare Verbindungen zu sich in Reichweite befindlichen Tags herzustellen, müssen unbedingt auch die Aspekte der Sicherheit, des Datenschutzes und der Privatsphäre beachtet werden.

1.2 Gegenstand der Arbeit

Diese Arbeit ist in drei Abschnitte gegliedert. Der erste Teil behandelt die technischen Aspekte der RFID-Technologie, der zweite Teil beschreibt die organisatorische und wirtschaftliche Bedeutung von RFID im SCM und der letzte Teil schildert die Entwicklung einer Plattform zur Anbindung von mobilen RFID-Geräten anhand eines konkreten Anwendungsfalls. Diese Dreiteilung der Arbeit wird mit der Abbildung 1.1 verdeutlicht.

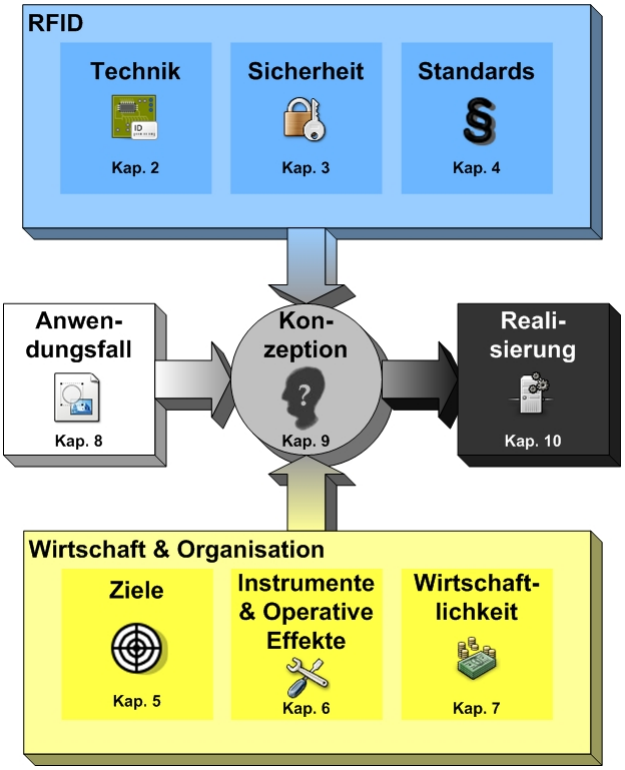


Abbildung 1.1: Übersicht über die Inhalte der Arbeit.

Zu Beginn jeden Kapitels wird diese Grafik in verkleinerter Form angezeigt. Zusätzlich wird das aktuelle Kapitel in der Grafik schwarz markiert, so dass dem Leser die Einordnung dieses Kapitels in den Gesamt-Zusammenhang verdeutlicht wird.

Im nachfolgenden Kapitel 2 wird zunächst ein Überblick über die technischen Funktionen, Möglichkeiten und Einschränkungen von RFID gegeben. Innerhalb einer Einordnung in die anderen, verfügbaren Identifikationsmöglichkeiten

wird im Speziellen auch ein Vergleich zum Barcode gezogen. Kapitel 3 zeigt aktuelle Fragestellungen zu Sicherheitsbedenken und mögliche Lösungsansätze auf. Obwohl RFID schon seit den vierziger Jahren des letzten Jahrhunderts eingesetzt wird, gibt es bis heute keinen weltweit etablierten Standard. Aus diesem Grund wird in Kapitel 4 die aktuelle Situation der Standardisierung diskutiert.

Kapitel 5 beinhaltet die Potentiale von RFID im SCM und die angestrebten Ziele beim praktischen Einsatz. Mit den Handlungsmöglichkeiten und den resultierenden organisatorischen und strategischen Effekten in Kapitel 6 schließt der theoretische Teil der Arbeit mit einer Betrachtung des wirtschaftlichen Kosten–Nutzen-Verhältnisses in Kapitel 7.

Im dritten Teil der Arbeit steht die Entwicklung einer Plattform zur Anbindung von mobilen RFID-Geräten an bestehende Betriebliche Informationssysteme[1] (BIS) im Zentrum. Eine Vielzahl von Geschäftsprozessen bieten sich als potentielle Kandidaten zur Verbesserung der Integration[2] an. Diese Arbeit behandelt einen exemplarischen Geschäftsprozess, der durch den Einsatz solch einer Plattform optimiert werden kann. Dieser Prozess ist so nicht in der Praxis zu finden, ähnelt aber durchaus der gängigen Praxis im Bereich des Behältermanagements innerhalb der *Supply Chain* (Lieferkette). Im Unterschied zu bereits existierenden Lösungen liegt der Fokus dieses Prozesses auf der mobilen Erfassung von RFID-Daten. In Kapitel 8 wird der Prozess näher beschrieben und erläutert. Anschließend wird aus den Erkenntnissen der ersten beiden Teile der Arbeit ein Konzept zur Umsetzung des RFID-Systems und Optimierung des Prozesses entwickelt. Im letzten Kapitel 10 des Hauptteils wird dann schließlich die Realisierung des Prototyps beschrieben.

Geschlossen wird diese Arbeit durch ein Fazit und einen Ausblick auf mögliche weitere Arbeiten.

Um einen ersten Überblick über den Aufbau eines RFID-Systems zu erhalten, wird an dieser Stelle kurz auf die Komponenten des Prototyps eingegangen.

[1] Mögliche Betriebliche Informationssysteme zur Anbindung eines RFID-Systems könnten z. B. sein: Warenwirtschaftssysteme (WWS, WaWi), *Enterprise Resource Planning*-Systeme (ERP) oder Produktionsplanungssysteme (PPS).

[2] Der Begriff Integration wird in verschiedenen Wissenschaftsbereichen sehr unterschiedlich definiert. Eine Auswahl von Definitionen und die gültige Definition für diese Arbeit befindet sich in dem entsprechenden Kapitel 6.1.1. In diesem Fall ist Integration mit dem Begriff „Einbindung“ gleichzusetzen.

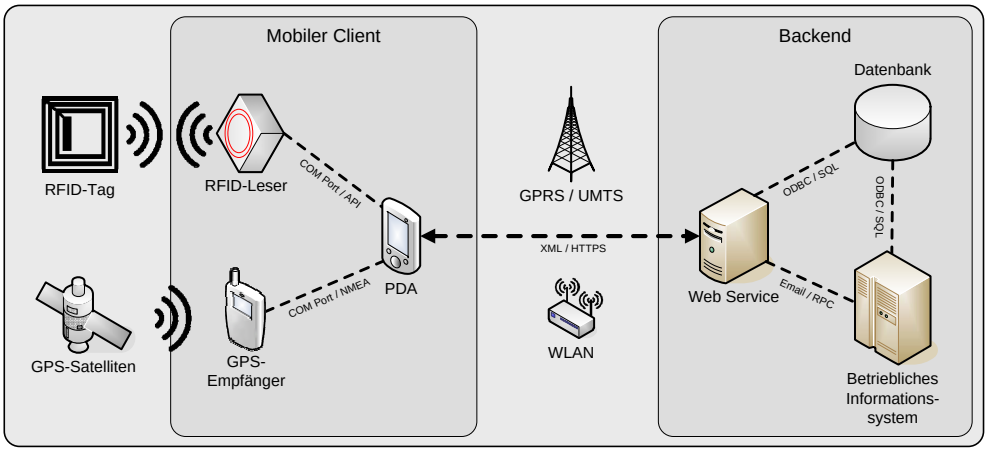


Abbildung 1.2: Komponenten der Architektur des RFID-Systems.

Damit eine nahtlose Integration des Systems in die bestehende Systemlandschaft möglich ist, verteilen sich die Komponenten auf bereits bestehende oder auf neue Einrichtungen, die als Erweiterungen zu sehen sind. Eine mögliche Unterteilung der gesamten Plattform in die verschiedenen Komponenten sieht wie folgt aus:

- am Container befestigte RFID-Tags,
- der mobile RFID-Leser (PDA) mit Netzwerk-Anbindung,
- die mobile Infrastruktur (öffentliche oder private Netzwerke) übernimmt den Daten-Transport,
- die übertragenen Daten werden vom Backend (ein oder mehrere Server) empfangen und dem angeschlossenen Betrieblichen Informationssystem zur Verfügung gestellt,
- das Betriebliche Informationssystem verarbeitet die gelieferten Daten.

Die zu dieser Aufzählung entsprechende Abbildung 1.2 verdeutlicht den Zusammenhang der Komponenten in grafischer Form.

Das mobile Gerät sollte ein *Personal Digital Assistant* (PDA) oder *Handheld* in einer Standard-Ausführung sein, so dass die erforderliche Hardware frei und

gut erhältlich ist (ggf. sogar austauschbare Komponenten). Zur Kommunikation ist die RFID- und eine Netzwerkkomponente notwendig, zur Positionsbestimmung zusätzlich ein GPS-Empfänger. Die Anwendung auf dem mobilen Gerät hat die Aufgabe, die Hardwarekomponenten einzubinden, die gelesenen Daten zu sammeln und anschließend zu versenden. Dabei sollte die Bedienung intuitiv und einfach sein.

1.3 Motivation

Mit RFID bietet sich dem gewerblichen Umfeld eine zusätzliche Option zu den bisherigen Identifikationsmerkmalen. Aus diesem Grund lohnt eine genauere Betrachtung der technischen, organisatorischen und wirtschaftlichen Möglichkeiten.

Die Nutzung der RFID-Technologie bietet großes Potential, betriebliche Geschäftsprozesse zu optimieren. Zu einen bieten sich interne Prozesse in Produktion und Transport zur Optimierung an, indem Automatisierung gefördert, Medienbrüche vermieden und Parallelisierung geschaffen werden kann. Zum anderen können überbetriebliche Prozesse durch Einbindung externer Parteien in bestehende Prozesse integriert werden oder sogar neue Prozesse geschaffen werden. Durch eine insgesamt erhöhte Integration der verschiedenen Prozesse können Fehler vermieden, Durchlaufzeiten verringert und damit Kosten eingespart werden. Zusätzlich bieten diese neuen Prozesse Möglichkeiten zur Erweiterung von Dienstleistungen und neuer Geschäftsfelder. Somit können die vorhandenen, betrieblichen Systeme in den Bereichen des *Supply Chain Managements* und *Customer Relationship Managements* um neue Funktionen und Dienste erweitert werden. Geschäftspartner können verstärkt in die Prozesse eingebunden und der Kundenkontakt kann durch die erhöhte Transparenz intensiviert werden. Neben diesen Vorteilen entstehen Synergien zwischen verschiedenen Parteien, so dass Geschäftsbeziehungen ausgebaut werden können.

1.4 Fragestellungen

In dieser Arbeit werden verschiedene, zentrale Fragen behandelt, deren Antworten wichtige Erkenntnisse für den Einsatz von RFID im SCM beinhalten können. Obwohl ein exemplarischer Geschäftsprozess als Anwendungsfall dient,

wird eine allgemeine Betrachtung und Bewertung angestrebt. Dabei werden die folgenden Forschungsfragen untersucht:

1. Wo liegt bei der mobilen Erfassung der Unterschied zur der stationären Erfassung? Welcher Mehrwert kann entstehen? Wo liegen die Gefahren?

2. Welche Architektur verspricht eine sinnvolle und flexible Anordnung der Komponenten? An welcher Stelle der Architektur sind die funktionalen Komponenten angesiedelt? Von welcher Komponente wird welche Information geliefert/empfangen und weitere Prozesse angestoßen?

3. Kann auf dem mobilen Gerät eine Anwendung entwickelt werden, die unabhängig von den verwendeten Hardware-Komponenten einsetzbar ist? Wie lässt sich diese Anwendung in einer komponentenbasierten Architektur realisieren?

4. Welche Sicherheitsaspekte sind bei der Kommunikation und den mobilen Datenträgern zu beachten?

5. Welche Einsatzszenarien im *Supply Chain Management* sind unter Berücksichtigung von wirtschaftlichen Aspekten denkbar?

1.5 Vorgehensweise

Der Markt der RFID-Technologie befindet sich in einem stetigen Wachstum. Es gibt inzwischen viele Anbieter, verschiedene technische Ansätze und Einsatzgebiete im gewerblichen Umfeld. Aus diesem Grund beschäftigen sich die beiden ersten Teile der Arbeit mit der Information über die am Markt befindlichen Lösungen in allen Bereichen von RFID und SCM. In der Arbeitsgruppe Betriebliche Kommunikationssysteme der Universität Koblenz wurden bis zu dem Zeitpunkt des Beginns dieser Diplomarbeit keine praktischen Implementierungen von RFID-Lösungen unternommen. Der Großteil der Informationen stammt aus den Internet-Angeboten der Hersteller und Händler. Zusätzlich bieten Messen, Roadshows und die vorhandene Literatur eine gute Ausgangslage zur Erfassung der aktuellen Situation aller in der Arbeit behandelten Themen. Diese Themen lassen sich grob in RFID-Technologie, Sicherheitsaspekte, Standardisierungsbemühungen, Bedeutung für das SCM, Wirtschaftlichkeit und Möglichkeiten zur Realisierung von RFID-Systemen unterteilen.

Das beispielhafte, praktische Szenario diente als Grundlage zur Entwicklung des Prototyps zur Erfassung von mobilen RFID-Daten. Die Anforderungen an diese Anwendung grenzten die möglichen zu verwendenden Komponenten ein, so dass nach einem Marktüberblick die optimale Auswahl an Komponenten getroffen werden konnte. Aufgrund der ausgewählten Komponenten wurde anschließend die Architektur der Plattform festgelegt. Diese Architektur bestimmt in weiten Teilen die Funktionalität und die Kommunikationswege zwischen den Komponenten.

In den nachfolgenden Schritten wurde die Plattform realisiert, indem notwendige Anwendungen, Datenbanken und Geräte eingerichtet wurden, so dass ein Testbetrieb möglich war. Anhand des exemplarischen Geschäftsprozesses wurde die Funktionsweise der Plattform und die Kommunikation zwischen den Komponenten aufgezeigt.

1.6 Abgrenzungen und Einschränkungen

Diese Arbeit soll eine allgemeine Sicht auf die Potentiale und Herausforderungen von RFID im SCM haben, kann jedoch nicht auf alle möglichen Szenarien angewandt werden. Da neue Anwendungen andere Anforderungen an die Lösungen stellen, kann kein Anspruch auf Vollständigkeit erhoben werden.

Die Wirtschaftlichkeitsanalyse in Kapitel 7 kann keine quantitativen Ergebnisse liefern, da keine veröffentlichten Daten vorliegen, die als Grundlage für eine derartige Analyse dienen könnten. Aus diesem Grund wird eine qualitative Bewertung vorgenommen. Des weiteren sind viele Vorteile eines RFID-Systems nicht-monetärer Art, so dass eine Bewertung ex ante nicht möglich ist.

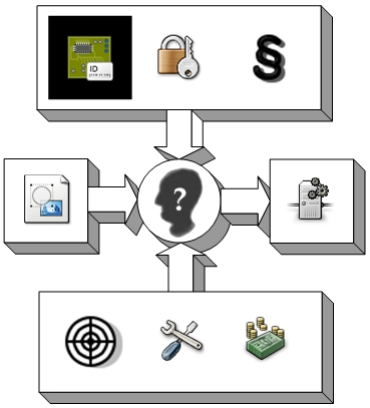
Die entwickelte Plattform stellt die empfangenen Daten mit einer offenen Schnittstelle zur Verfügung (z. B. Datenbank in Backend). Die Integration in bestehende Betriebliche Informationssysteme ist nicht Bestandteil dieser Arbeit, weil kein allgemeines Verfahren zur Integration in alle am Markt befindlichen Systeme existiert. Aus diesem Grund wird eine offene Schnittstelle zur Nutzung angeboten.

Dem Anspruch der Verwendung jeglicher am Markt verfügbarer, mobiler Produkte kann das mobile Gerät nicht gerecht werden. Es gibt eine Vielzahl von Architekturen für PDAs und Handhelds. Da jedoch teilweise auf sehr

hardwarenahe Daten zugegriffen werden muss, wird eine weit verbreitete Architektur gewählt. Ebenso verhält es sich bei der Wahl des Betriebssystems (z. B. Windows CE) und der Entwicklungsumgebung (Java/C++/.NET) [Dunlap u. a. 2003, S. 1 ff.].

Kapitel 2

RFID – eine Einführung



Dieses Kapitel behandelt die grundlegenden Eigenschaften von RFID. Zunächst wird eine Positionierung innerhalb verwandter Technologien vorgenommen. Anschließend wird die zu Grunde liegende Technik genauer erläutert, damit die technischen Möglichkeiten und Einschränkungen deutlich werden. Diese technischen Rahmenbedingungen bestimmen in weiten Teilen das spätere Auswahlverfahren zum Einsatz der adäquaten RFID-Komponenten und sind deshalb von hoher Bedeutung. Nachfolgend werden dann exemplarisch die wichtigsten und in der Praxis aktuell vorkommenden Anwendungsgebiete diverser Branchen genannt. Dieses Kapitel schließt mit einem Vergleich zwischen dem weit verbreiteten Barcode und der RFID-Technologie. Es wird deutlich gemacht, welche Vor- und Nachteile zwischen den beiden Alternativen bestehen, so dass eine Beurteilung der Potentiale von RFID gegenüber dem Barcode möglich ist.

2.1 Einordnung von RFID im Auto-ID-Umfeld

Unter dem Begriff Auto-ID werden verschiedene Technologien zur Identifizierung von Gütern, Produkten, Menschen oder Tieren zusammengefasst. Ein Zusammenschluss von verschiedenen Universitäten hat es sich zur Aufgabe gemacht, diesen Begriff zu prägen und die Forschung auf diesem Feld voran zu

Abbildung 2.1: Beispiel eines EAN 13 Barcodes [GS1 Germany 2005].

treiben. Die entstandene Organisation heißt Auto-ID Labs[3] und wird in Europa von den Universitäten ETH Zürich in der Schweiz und der Universität Cambridge in England vertreten.

Zu den Auto-ID-Technologien gehören neben RFID die Barcodes, OCR (*Optical Character Recognition*)[4] sowie *Smart Cards*[5]. Teilweise werden in der Literatur biometrische Verfahren (Fingerabdruck, Stimmerkennung, Retina, usw.) zur Identifikation von Menschen und Tieren dem Auto-ID-Umfeld zugeschrieben [vgl. Finkenzeller 2002, Kap. 1.1.3].

Barcodes sind sehr verbreitet und werden für eine Vielzahl von Anwendungen verwendet. Beim einfachen Barcode bestimmen die zu codierenden Informationen eine Kombination von Strichen und Lücken zwischen den Strichen. Der bekannteste Vertreter der einfachen Barcodes ist der EAN 13 (*European Article Number*) Code, welcher zur Identifikation von Handelsartikeln verwendet wird (siehe Abbildung 2.1). Des Weiteren werden häufig auch die Codierungen Code 39, Code 128, Codabar, Interleaved 2 of 5 und EAN 8 verwendet. Zusätzlich existieren 2D-Barcodes welche nicht nur in einer Dimension, sondern auch quer zu Hauptrichtung Informationen speichern. Das Auslesen bedarf dadurch zwar mehr Aufwand, hat aber den Vorteil einer höheren Datendichte.

OCR ist weniger weit verbreitet als der Barcode, hat sich aber stellenweise in den Bereichen der Produktion und den Dienstleistungen etabliert. Im Bankensektor wird OCR eingesetzt, um z. B. Überweisungsträger oder Schecks einzulesen. Leider wird durch die sehr aufwändige Technik der Einsatz dieser

[3] Die Homepage des Auto-ID Labs ist unter `http://www.autoidlabs.org/` zu erreichen.
[4] OCR ist die optische Erfassung von Zeichen und die anschließende Erkennung zur digitalen Weiterverarbeitung.
[5] Smart Cards bestehen in der Regel aus einer Plastikkarte im Scheckkarten Format und einem kleinen Chip auf dem die Identifikationsinformationen enthalten sind. Durch physischen Kontakt mit einem Leser kann der Inhalt ausgelesen werden.

Abbildung 2.2: Beispiel eines Odette-Labels [T. L. Ashford 2005].

Technologie recht teuer, so dass häufig andere Lösungen zum Einsatz kommen [vgl. Finkenzeller 2002, S. 3 f.].

In der Praxis werden Güter häufig mit einer Kombination aus Barcode und OCR identifiziert. In der Automobilindustrie kommen das *Odette-Label* (siehe Abbildung 2.2) und dessen Nachfolger *Global Transport Label* (GTL) zum Einsatz. Beide Labels bestehen aus mehreren Feldern mit Barcodes und Informationen in menschlich lesbarer Schrift. Somit kann in der Produktion von Zulieferern und Herstellern diejenige Technologie verwendet werden, die bereits vorhanden ist oder für als die geeignetste angesehen wird.

Bei *Smart Cards* kann man zwischen zwei verschiedenen Ausprägungen unterscheiden. Es gibt einfache Speicherkarten, die als reine Datenträger (Telefonkarte, Versichertenkarte) fungieren, und Karten mit integriertem Mikroprozessor, die auch auf den Chip geschriebene Programme ausführen können [Finkenzeller 2002, S. 4 ff.]. Sie werden häufig in sicherheitskritischen Gebie-

ten benutzt, wie EC (*Electronic Cash*)[6] oder GSM (*Global System for Mobile Communications*)[7].

RFID-Tags weisen eine gewisse Ähnlichkeit zu *Smart Cards* auf. Die Informationen werden ebenfalls auf einem kleinen Chip gespeichert. Jedoch bedarf es zur Kommunikation keines direkten Kontaktes, sondern der Zugriff auf die im Chip enthaltenen Daten und die Energieversorgung erfolgt kontaktlos über elektromagnetische Felder. Die grundlegende Technik und weitere, wichtige Eigenschaften werden im nachfolgenden Unterkapitel genauer erläutert.

2.2 Technische Grundlagen

Grundsätzlich besteht jedes RFID-System aus mindestens zwei Komponenten. Dies ist zum einen der Tag und zum anderen die Schreib- und Lesevorrichtung. Im Folgenden wird davon ausgegangen, dass ein RFID-Leser auch Tags beschreiben kann. Dies entspricht dem allgemeinen, praktischen Gebrauch des Begriffs RFID-Leser [vgl. Finkenzeller 2002, S. 7]. Zur Weiterverarbeitung der gelesenen Informationen ist der Leser in der Regel mit einer Anwendung oder einem Betrieblichen Informationssystem verbunden.

Der Tag selbst besteht aus weiteren Einzelteilen. Zur Kommunikation und der Energieaufnahme dient eine Spule oder eine Antenne[8]. Die nutzbaren Informationen werden auf einem Silizium-Chip gespeichert. Der Chip kann entweder bei der Herstellung mit einer eindeutigen, nicht veränderbaren Nummer (ID) versehen oder zusätzlich dazu mit frei verwendbarem Speicher[9] ausgestattet werden. Höherwertige Chips bieten alternativ auch einen kleinen Mikroprozessor, der bestimmte Rechenoperationen ausführen kann (z. B. Verschlüsselungsoperationen). Diese Komponenten werden auf die unterschiedlichste Art und Weise zusammengebaut. Die möglichen Bauformen sind vielfältig und reichen von Papieretiketten über Glasröhrchen bis hin zu massiv gegossenen Gehäusen. Üblicherweise fasst man die inneren Komponenten des Tags (Spule/Antenne, Chip, Mikroprozessor), also alle funktionalen Komponenten unabhängig von

[6] Mit Hilfe von EC-Karten wird das bargeldlose Bezahlen ermöglicht.

[7] GSM ist ein Standard, der das digitale Mobilfunknetz zur Telefonie und Datenübertragung beschreibt.

[8] Die Wahl zur Verwendung von Spule oder Antenne wird bestimmt durch die eingesetzte Frequenz. Dieses Thema wird in Kapitel 2.2.2 behandelt.

[9] Man unterscheidet zwischen ROM, der nur einmal vom Nutzer des Tags beschrieben werden kann, und RAM/EEPROM, der unbeschränkt oft neu beschrieben werden kann.

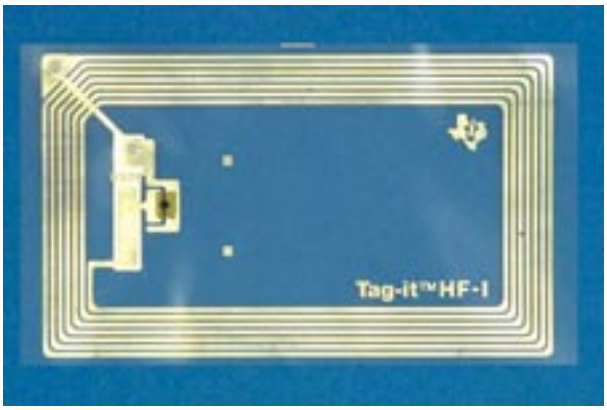


Abbildung 2.3: Inlay eines HF-Tags von Texas Instruments [TI HF 2006].

der Bauform, unter dem Begriff *Inlay* zusammen. Abbildung 2.3 zeigt ein *Inlay* eines Tags im HF-Frequenzbereich.

Den Leser kann man in drei Komponenten unterteilen. Zur Kommunikation mit dem Tag wird eine Spule oder Antenne verwendet, die das elektromagnetische Feld erzeugt und die Antwort des Tags empfängt[10]. Des Weiteren ist die Steuereinheit als aktive Komponente für alle Operationen (Lesen, Schreiben, Interpretation der Signale, usw.) verantwortlich. Als dritte Komponente dient eine Schnittstelle zur Kommunikation mit nachgelagerten Einrichtungen. Dies kann z. B. eine USB[11], RS-232[12] oder Bluetooth[13] Schnittstelle sein, die mit Rechnern oder mobilen Erfassungsgeräten verbunden ist.

2.2.1 Unterscheidungsmerkmale innerhalb von RFID

Aufgrund der Vielzahl verschiedener Anwendungen – und damit auch Anforderungen an Tags und Leser – bedarf es mehrerer verschiedener Ausprägungen von RFID-Systemen. Diese Ausprägungen spiegeln sich in verschiedenen Eigenschaften wieder, die im Folgenden kurz erläutert werden.

[10] Auf die Kommunikation zwischen Tag und Leser wird im nachfolgenden Kapitel 2.2.2 detailliert eingegangen.

[11] Der *Universal Serial Bus* ist eine kabelgebundene Verbindung zu Rechnern oder anderen Komponenten mit entsprechender Schnittstelle.

[12] RS-232 bezeichnet eine serielle, kabelgebundene Schnittstelle, die häufig ein Ein- und Ausgabegeräte genutzt wird. USB ersetzt RS-232 immer mehr, jedoch hat RS-232 in der Industrie immer noch eine hohe Verbreitung.

[13] Bluetooth ist ein Standard für die Datenübertragung per Funk. Der Standard wird von der IEEE (http://www.ieee.org) unter der Bezeichnung IEEE 802.15.1 verwaltet.

Frequenz

Die wichtigste Eigenschaft zur Kategorisierung von RFID-Systemen ist die Frequenz, in der die Kommunikation zwischen Leser und Tag stattfindet. Dabei unterteilt man die verwendeten Frequenzen in drei Kategorien: *Low Frequency* (LF, 125 kHz, 135 kHz), *High Frequency* (HF, 13,56 MHz, 27,125 MHz) und *Ultra High Frequency* (UHF, 868 MHz, 915 MHz, 2,45 GHz, 5,8 GHz).

Die Frequenz bestimmt maßgeblich weitere Eigenschaften – wie Reichweite, Energieverbrauch und Materialverträglichkeit – welche in den folgenden Abschnitten behandelt werden. Da die mögliche Bandbreite der Datenübertragung proportional mit der Frequenz steigt, bestimmt die Frequenz auch die Dauer bestimmter Operationen. Dies kann bei Anwendungen, bei denen sich die Tags bewegen (z. B. auf Fließbändern), von großer Bedeutung sein. Ein wichtiges Kriterium ist der Preis für Tags verschiedener Frequenzen. Allerdings kann man Tags der verschiedenen Frequenzbereiche nur sehr grob vergleichen. Wegen ihrer aktuell hohen Verbreitung haben Tags des HF-Bereichs tendenziell den niedrigsten Preis. Durch das vermehrte Aufkommen von UHF-Systemen ist jedoch zu erwarten, dass die Preise im UHF-Bereich fallen. Die Auflage – also die Anzahl der Tags einer Bestellung – bestimmt dabei den Preis pro Tag stärker als die gewählte Frequenz. Verlässliche Informationen über die Preisentwicklung der verschiedenen Frequenzbereiche sind derzeit nicht verfügbar. Im UHF-Bereich sind die kontinentalen Unterschiede der erlaubten Frequenzbänder zu beachten. In Europa ist die Frequenz 868 MHz, in den USA 915 MHz erlaubt und in Japan ist 950–956 MHz geplant. Diese hoheitlichen Vorschriften liegen in den unterschiedlichen Vergabepraktiken für Frequenzen der Länder und den Vorschriften zu den Emissionen begründet.

Reichweite

Die maximale Reichweite zwischen Tag und Leser wird durch viele Faktoren bestimmt und ist selbst für einen Frequenzbereich nicht fix. Sie wird durch folgende Einflüsse bestimmt:

- Frequenz: Je höher die Frequenz, desto größer ist die maximale erreichbare Reichweite.[14]
- Ausrichtung: Der Winkel zwischen Tag und den Feldlinien bestimmt die Energiemenge, mit der der Tag gespeist wird. Ist der Winkel annähernd senkrecht, dann wird mehr Energie aufgenommen als wenn der Winkel gegen 0° geht.
- Geschwindigkeit: Bewegt sich der Tag innerhalb des Feldes, dann ändert sich die zu empfangene Energiedichte, so dass kein stetiger Betrieb möglich ist.
- Anzahl der Tags: Je mehr Tags sich die vorhandene Energie des Feldes teilen, desto weniger Energie erhält jeder einzelne.
- Umgebung: Bestimmte Materialien dämpfen die Felder unterschiedlich stark (siehe Kapitel 2.2.3).
- Energieversorgung: Haben Tags eine eigene Energieversorgung, dann kann die Reichweite erheblich gesteigert werden.
- Sendeleistung des Lesers: Der Leser bestimmt, wieviel Energie er selbst zur Verfügung hat und wieviel er zur Kommunikation verwendet.
- Energiebedarf des Tags: Verschiedene Tags haben unterschiedlichen Energiebedarf, je nachdem ob sie nur ihre 1-Bit ID übermitteln oder gar komplexe Berechnungen durchführen.

Eine grobe Einteilung der Reichweiten wird von [Finkenzeller 2002, Kap. 2.3] vorgeschlagen. Systeme, die bis 1 cm Reichweite operieren, werden *Close Coupling Systems* genannt[15]. Alle Frequenzen können innerhalb dieser Reichweite

[14] Diese Aussage gilt im Speziellen für RFID-Systeme. In der Physik verringert sich die Reichweite von Strahlung mit ansteigender Frequenz (bei gleicher Leistung). Selbstverständlich gilt dieses physikalische Gesetz auch für RFID-Systeme, jedoch spielen bei der Lese-Reichweite auch andere Faktoren eine große Rolle (z. B. Effektivität von Antennen bei verschiedenen Frequenzen, Unterschied zwischen Nah-/Fernfeld, Umgebungseinflüsse, siehe auch in Kapitel 2.2.2).

[15] Trotz der geringen Lesereichweite von unter 1 cm (also im Grunde das Auflegen einer Karte auf einen Leser) werden diese RFID-Systeme als kontaktlos kategorisiert. *SmartCards* hingegen brauchen einen direkten, physischen Kontakt mit dem Leser.

eingesetzt werden. Die Verwendung bietet sich an, wenn bestimmte Sicherheitsaspekte gewahrt werden müssen, z. B. bei Zutrittskontrollen oder Bezahlungen. Die nächste Kategorie *Remote Coupling Systems* hat eine Reichweite bis ungefähr 1 m. Die Wahl dieser Einteilung wird durch die technische Umsetzung der Kommunikation bestimmt. Fast alle Systeme bis 1 m Reichweite benutzen die induktive Kopplung zwischen Leser und Tag. Zwei häufig eingesetzte Standards (ISO/IEC 14443 und ISO/IEC 15693, siehe Kapitel 4) fallen in diese Kategorie, so dass sehr viele Systeme mit dieser Technik betrieben werden, weil sie inzwischen sehr ausgereift und stabil ist. Systeme, die über eine Reichweite von mehr als 1 m verfügen, werden *Long-Range Systems* genannt. Die zu Grunde liegende Technik mit Hilfe von elektromagnetischen Wellen liegt im UHF- und Mikrowellen-Bereich. Dadurch können Reichweiten bei passiven Tags bis zu 5 m und bei aktiven von 15-100 m erreicht werden. Auf die technischen Unterschiede zwischen induktiver Kopplung und elektromagnetischen Wellen wird in Kapitel 2.2.2 detailliert eingegangen.

Speicherkapazität

Die physische Abmessung und der Preis eines Tags werden u. a. auch durch die Speicherkapazität bestimmt. Es gibt einfache Ausführungen, die nur eine unveränderliche ID beinhalten, die zwischen einem[16] und n Bit groß ist, wobei n selten größer als 256 ist. Diese Tags dienen zur reinen Identifizierung und unterscheiden sich dadurch kaum vom Barcode.

Tags mit zusätzlichem Speicherplatz bieten hingegen die Möglichkeit, benutzerdefinierte Daten auf dem Tag abzulegen. Dies ermögliche neue Anwendungsfälle, bei denen Daten dezentral am Objekt abgelegt und gelesen werden können. Dabei kann die Größe von wenigen Bytes bis 128 kB variieren. Die Struktur des Speichers ist nur in wenigen Standards fest vorgeschrieben, so dass verschiedene Hersteller oft unterschiedliche Strukturen in ihren Tags verwenden. Meist sind die Speicher in Blöcke (Zeilen) mit vier Bytes unterteilt.

[16] Ein Einsatzgebiet für Tags mit einem einzigen Bit ist die Diebstahlsicherung, bei der geprüft wird ob der Tag vorhanden ist oder nicht.

Fast alle Tags akzeptieren nur Zeichen aus dem Standard ASCII Zeichensatz mit sieben Bit pro Zeichen.[17]

Bei wiederbeschreibbarem Speicher kommen verschiedene Speicherarten in Frage [vgl. Finkenzeller 2002, Kap. 2.5.4]. Zum einen wird bei passiven, induktiv gekoppelten Systemen EEPROM- oder Flash-Speicher eingesetzt, weil diese die Informationen auch dann speichern, wenn keine Stromversorgung anliegt. Zum anderen wird bei aktiven Systemen mit eigener Stromversorgung häufig SRAM verwendet, da SRAM keine Einschränkungen in der Struktur[18] des Speichers hat. Lese- und Schreibvorgänge können ohne Beachtung der Einteilung des Tags in Blöcke vorgenommen werden. FRAM[19] ist ein Sonderfall, da diese Speicherart neben den beiden o. g. zusätzlich weitere Vorteile bietet: höhere Schreibgeschwindigkeit, längere Speicherdauer und geringerer Energieverbrauch. Die aktuelle Verbreitung von FRAM in RFID-Tags ist noch relativ gering, wird aber sicherlich in Zukunft stetig zunehmen.

Energieversorgung

Wie bereits in den vorangegangen Abschnitten erwähnt, spielt die Energieversorgung eine wichtige Rolle beim Einsatz von RFID. Da die Übertragung von Informationen über Felder geschieht, wird Energie benötigt, die diese Felder aufbaut. Da die Leser immer eine eigene Stromversorgung haben, unterscheidet man grundlegend in zwei Arten von RFID-Systemen, die durch die Energieversorgung des Tags bestimmt werden. Es gibt passive Tags, die keine eigene Stromversorgung besitzen, und aktive Tags, die die eigene Stromversorgung in Form einer kleinen Batterie im Tag selbst mitführen.

Passive Tags werden durch die Energie, die in dem vom Leser aufgebauten Feld steckt, gespeist. Diese Energie wird kurzzeitig in einem kleinen Kondensator gespeichert, so dass der Tag in der Lage ist, auf die vom Leser initiierte

[17] Diese Einschränkung ist nur bei der Verwendung von den von den Herstellern gelieferten APIs *Application Programming Interface* gegeben. Greift die Software zur Steuerung des Lesers direkt auf den Speicher des Tags zu, dann können die Informationen auch benutzerdefiniert interpretiert werden.

[18] Bei Flash-Speicher können einzelne Bytes nicht gelöscht werden. Da Flash-Speicher in Sektoren angeordnet ist, können auch nur ganze Sektoren gelöscht werden. Beim Beschreiben können zwar allerdings einzelne Bytes geschrieben werden, aber sind diese Bytes bereits mit Informationen belegt, dann müssen sie erst sektorweise gelöscht werden.

[19] *Ferroelectric Random Access Memory* ist ein Speicher auf der Grundlage von ferroelektrischen Kristallen. FRAM ist nichtflüchtig, kann häufig beschrieben werden und ist unempfindlich gegenüber Temperaturschwankungen.

Operation zu reagieren und zu antworten. Bis zur Beendigung der Transaktion muss der Tag dabei ununterbrochen mit Energie versorgt werden. Dabei unterscheidet man die zwei Arten der induktiven und der elektromagnetischen Kopplung, je nachdem in welchem Frequenzbereich das System operiert. Im Kapitel 2.2.2 werden diese physikalischen Eigenschaften näher erläutert.

Aktive Tags hingegen sind nicht auf die Energie des Feldes des Lesers angewiesen. Sie beziehen die Energie aus einer kleinen Batterie, um Operationen durchzuführen oder dem Leser zu antworten. Dadurch wird der Tag natürlich erheblich größer, schwerer, teurer, erfordert mehr Wartungsaufwand und ist anfälliger gegenüber Umwelteinflüssen[20], jedoch steigen die Reichweite und die Richtungsunabhängigkeit. Allerdings versorgt die Batterie den Tag nicht ununterbrochen mit voller Energie [vgl. Finkenzeller 2002, S.81]. Wenn der Tag nicht gerade kommuniziert oder Operationen ausführt, dann befindet er sich in einem *Stand-by* (oder *Sleep*) Zustand, in dem nur der Speicher versorgt wird, um die Daten zu erhalten. Baut ein Leser ein Feld auf und der Tag ist in Reichweite, dann wird eine bestimmte induzierte Spannung überschritten, welche den Tag dann aktiviert (*Wake Up Signal*). Nach Beendigung der Transaktion geht der Tag dann selbstständig zurück in den *Stand-by* Zustand.

Sicherheitsanforderungen

Bei bestimmten Anwendungen möchte der Benutzer oder Betreiber von RFID-Tags nicht, dass Dritte oder Unbekannte Zugriff auf die im Tag gespeicherten Daten haben. Diese Sicherheitsanforderungen können durch dezentrale Authentifizierung und Verschlüsselung erfüllt werden.

Dabei kann unter den folgenden Ausprägungen von Zugriffsbeschränkungen unterschieden werden:

- Kein Zugriff: Leser haben keinen Zugriff auf Daten des Tags (auch nicht auf die ID).
- Lesezugriff auf ID: Leser dürfen nur die ID des Tags auslesen. Zugriff auf den Speicher ist nicht gestattet.
- Lesezugriff auf ID und Speicher: Alle Daten auf dem Tag dürfen gelesen aber nicht verändert werden.

[20] Da Batterien sowohl bei sehr hohen als auch bei sehr niedrigen Temperaturen drastisch an Kapazität verlieren können, spielt die Umgebung des Tags eine wichtige Rolle.

- Partieller Zugriff: Vereinzelt erlauben Tags das blockweise Vergeben von Rechten, d. h. verschiedene Leser oder Gruppen von Lesern dürfen nur über bestimmte Bereiche des Tags verfügen.
- Vollzugriff: Leser dürfen die ID lesen und alle Daten des Speichers lesen und ändern.

Entscheidend für die Auswahl und Vergabe der Rechte ist die vorgesehene Anwendung der Tags. Abgesehen von dem allgemeinen Sicherheitsbedürfnis des Benutzers kann die Reichweite der Anwendung über die Sicherheitsmaßnahmen entscheiden [Finkenzeller 2002, Kap. 2.5.3]. Man unterscheidet grob zwei Arten von Systemen bezüglich ihrer Anwendungsreichweite: geschlossene und offene Systeme[21]. In geschlossenen Systemen besteht tendenziell weniger Gefahr vor unberechtigtem Lesen oder sogar Manipulationen. Aus diesem Grund ist der Einsatz von einfachen, ungeschützten Tags auf abgegrenzten Firmengeländen durchaus denkbar. In offenen Systemen hingegen ist der physische Zugang zu RFID weitaus einfacher und unüberwachter möglich. Bei Anwendungen bei denen persönliche oder andere kritische Daten geschützt werden sollen, bleibt keine Alternative zu dem Schutz durch Authentifizierung oder Verschlüsselung. Eine Sammlung möglicher Bedrohungen und Lösungen wird in Kapitel 3 behandelt.

Damit Tags diese erhöhte Sicherheit erfüllen können, brauchen sie neben Antenne/Spule und Speicher einen Mikroprozessor, der die notwendigen Berechnungen ausführt und anschließend den Zugriff regelt. Diese intelligenten Tags[22] sind teurer als einfache Tags. Leider gibt es dazu noch keine Standards, die eine einheitliche und herstellerübergreifende Lösung bieten, jedoch wird die Nachfrage der Betreiber nach Sicherheitsmerkmalen die Standardisierungsbemühungen beeinflussen.

Zusätzliche Funktionen

Die erwähnten aktiven Tags bieten zusätzlich weitere optionale Funktionen. Da durch die eigene Energieversorgung kein Feld eines Lesers von Nöten ist,

[21] Im späteren Verlauf dieser Arbeit wird eine dritte, aber bisher wenig beachtete Art von Anwendungen eingeführt, die kollaborativen Systeme (siehe Kapitel 6.1.1).

[22] Im allgemeinen Sprachgebrauch wird oft von „intelligenten“ Tags gesprochen, wobei der Autor auf die Gefahr von Missverständnissen hinweisen möchte. Die Mikroprozessoren führen lediglich vorher einprogrammierte Algorithmen aus und besitzen keine eigene Intelligenz.

können Tags auch bestimmte Aufgaben wahrnehmen, wenn kein Leser in Reichweite ist. Durch das Anbringen von Sensoren zur Temperatur-, Druck- oder Feuchtigkeitsmessung[23] kann der Tag auch dazu genutzt werden, bestimmte Umgebungszustände der Objekte zu überwachen. Dadurch kann eine Qualitätskontrolle von kritischen Gütern, wie z. B. Gefriergut, erreicht werden. Die Empfänger dieser Güter können die Einhaltung der günstigen Umgebungsbedingungen (z. B. Kühlkette) überwachen und gegebenenfalls die Annahme nicht ordnungsgemäß behandelter Güter ablehnen.

Aber nicht nur das Protokollieren dieser Sensordaten ist möglich, sondern ebenfalls das aktive Eingreifen des Tags bei Eintritt eines bestimmten Ereignisses. Meldet ein Sensor einen bestimmen Wert, der den eingestellten Schwellenwert über- oder unterschreitet, dann wird der Tag aktiv und sendet den entsprechenden Hinweis an einen Leser. Die an den Leser angeschlossene Anwendung kann dann die notwendigen Maßnahmen treffen, wie z. B. einen Signalton einschalten, eine Meldung absetzen oder die Steuerung von Maßnahmen zur Korrektur der Umgebungsbedingungen übernehmen. Dies könnte bei dem Überschreiten eines Temperatur-Schwellenwertes das Einschalten einer Kühlung sein.

Die in diesem Unterkapitel behandelten Funktionen von RFID-Tags können schematisch in der Abbildung 2.4 zusammengefasst werden. Die in der Abbildung genannten Begriffe Kryptographie, Dezentralisierung und Pulkfähigkeit werden in den folgenden Kapiteln näher erläutert.

In [Strassner und Fleisch 2005, S. 51] werden drei große Probleme in der Praxis mit den technischen Eigenschaften von RFID geschildert. Bei einer Umfrage über gescheiterte RFID-Projekte antworteten die befragten Unternehmen, dass entweder die Erfassungsreichweite zu gering, die gemessene Fehlerrate zu hoch gewesen sei oder Probleme bei metallischem Umfeld aufgetreten seien. Die wichtigen Faktoren bei der Bewertung der Reichweite wurden bereits in diesem Kapitel diskutiert. Den beiden anderen Problemen hingegen wird in den nächsten beiden Unterkapiteln Beachtung geschenkt.

[23] Die drei exemplarisch genannten Umgebungsmerkmale Temperatur, Druck und Feuchtigkeit sind nur eine kleine Auswahl der zu überwachenden Größen. Die technischen und operativen Möglichkeiten und Anforderungen können sehr stark variieren und entwickeln sind ständig weiter.

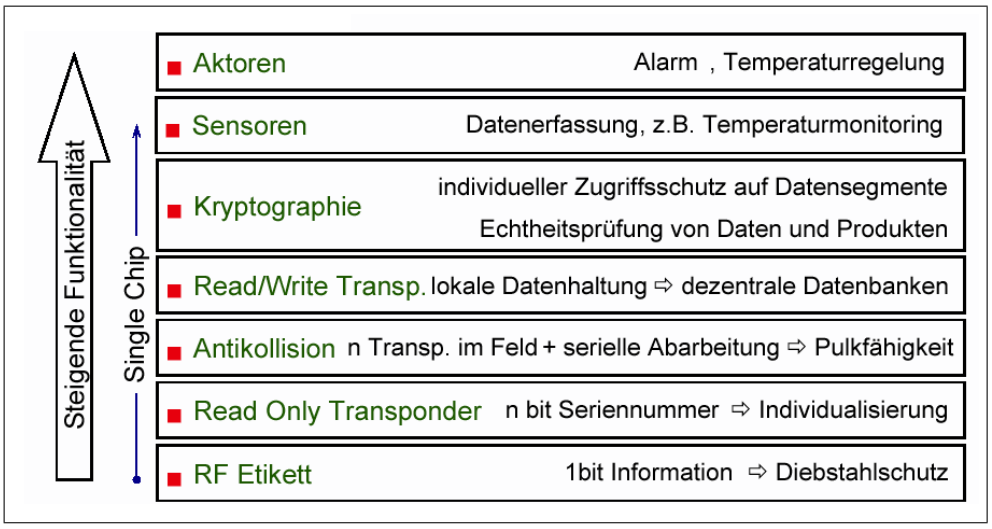


Abbildung 2.4: Funktionalitäten von RFID-Tags [Schmidt 2006].

2.2.2 Kommunikation zwischen Leser und Tag

Wie bereits mehrfach erwähnt, besteht das Medium der Kommunikation und die Übertragung der Energie bei passiven Tags aus elektromagnetischen Feldern. In diesem Unterkapitel wird auf diese Aspekte eingegangen, so dass die physikalischen Grundlagen von RFID deutlich werden. Grundlegend muss man zwischen zwei verschiedenen physikalischen Abläufen unterscheiden, denn die Abläufe im LF- und HF-Frequenzbereich unterscheiden sich von denen im UHF- und Mikrowellen-Bereich. Ursache dafür sind die physikalischen Eigenschaften von elektromagnetischen Feldern. Abhängig von der Entfernung zum Ursprung der Felder verändert sich das magnetische Feld zu einem elektromagnetischen Feld in Form von Wellen.

Nahfeld – Fernfeld

Jede bewegte elektrische Ladung wird von einem magnetischen Feld umgeben. Ein mit Strom durchflossener Leiter erzeugt ebenfalls ein Magnetfeld, welches sich kreisförmig um den Leiter ausbreitet. Formt man diesen Leiter zu einer Spule, dann entsteht ein Magnetfeld, wie in Abbildung 2.5 zu erkennen ist. Dabei wird die Stärke des Magnetfeldes H durch die physikalischen Parameter Länge der Spule d, Anzahl der Windungen n und Stromstärke I bestimmt.

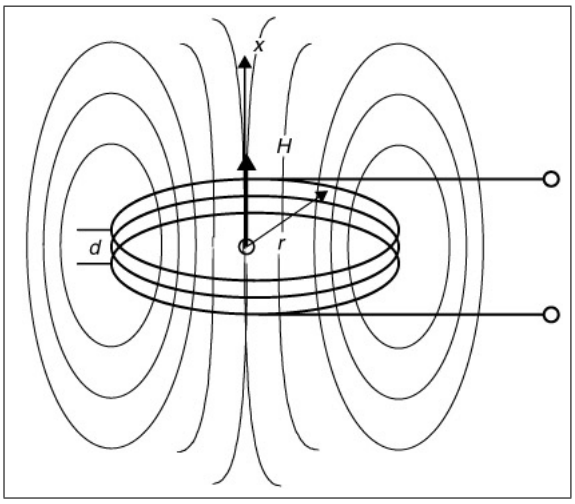


Abbildung 2.5: Magnetfeld um eine stromdurchflossene Spule [Finkenzeller 2002, Abb. 4.3].

Wird an der Spannungsquelle ein Gleichstrom angelegt, dann ist das Magnetfeld stabil und gleichförmig. Bei einer Quelle mit Wechselspannung U einer Frequenz f wird das Magnetfeld abwechselnd auf- und abgebaut. Somit entstehen an der Spule Magnetfelder, die sich mit Lichtgeschwindigkeit c von der Spule entfernen. Durch die angelegte Wechselspannung wird der magnetische Fluss Φ (und damit die Flussdichte B) ständig verändert. Jeder Wechsel des magnetischen Flusses bewirkt jedoch den Effekt der Induktion, die eine Spannung und damit auch ein elektrisches Feld erzeugt.[24] Die zeitliche Änderung von elektrischen Feldern, also das Auf- und Abbauen der Felder, bewirkt jedoch wiederum die Erzeugung von magnetischen Feldern. Durch den periodischen Wechsel von magnetischen und elektrischen Feldern entstehen elektromagnetische Felder, welche im Allgemeinen als elektromagnetische Wellen oder Strahlung bezeichnet werden.[25] Die Frequenz der angelegten Wechselspannung bestimmt dabei die Wellenlänge λ der Wellen.

$$\lambda = \frac{c}{f}$$

[24] Die Induktion wurde größtenteils von Michael Faraday entdeckt und war Grundlage für die Faradayschen Gesetze.

[25] James Clerk Maxwell gilt als bedeutendster Forscher im Bereich der Elektrizität. Seine Maxwellgleichungen dienen heute noch als Grundlage für die Wechselwirkung von elektrischen und magnetischen Feldern.

Liegt die Wellenlänge zwischen 380 und 780 nm, dann sind die Wellen für das menschliche Auge sichtbar und wir nennen diese Strahlung Licht.[26] Viele weitere Informationen zu diesem Thema sind bei [Finkenzeller 2002, Kap. 4] zu finden. Eine anschauliche Animation über die Entstehung von elektromagnetischen Wellen bietet [Komma 2006].

Das initiale, von der Spule erzeugte Magnetfeld wird als Nahfeld bezeichnet. Die elektrischen Wellen, die durch wechselseitige Induktion entstehen, werden als Fernfeld bezeichnet. Der Übergang vom Nahfeld zum Fernfeld ist praktisch fließend, jedoch kann die Größe des Nahfeldes s des von der Spule erzeugten Magnetfeldes abhängig von der Wellenlänge der erzeugten Strahlung, also auch von der angelegten Frequenz, berechnet werden. Die folgende Formel wird allgemein zur näherungsweisen Berechnung der Größe des Nahfeldes benutzt [siehe Finkenzeller 2002, S. 117 f.]:

$$s = \frac{\lambda}{2\pi}$$

Mit Hilfe der beiden genannten Formeln kann man nun für die meist verwendeten RFID-Frequenzen die maximale Größe des Nahfeldes ausrechnen. In der Tabelle 2.1 sind die relevanten Größen aufgeführt.

Frequenz f	Wellenlänge λ	Größe Nahfeld s
125 kHz	2,4 km	381,7 m
13,56 MHz	22,1 m	3,5 m
868 MHz	34,5 cm	5,5 cm
915 MHz	33,8 cm	5,2 cm
2,45 GHz	12,2 cm	1,9 cm

Tabelle 2.1: Physikalische Größen verschiedener RFID-Frequenzen [vgl. Finkenzeller 2002, Tab. 4.6].

Wie man aus den Werten der Spalte „Größe Nahfeld s“ erkennen kann, unterscheidet sich die Reichweite des Nahfeldes sehr stark zwischen den einzelnen

[26] Die Erzeugung von Licht ist mit den bei RFID verwendeten Methoden (Spule/Antenne, Wechselstrom) nicht möglich. Da die sichtbare elektromagnetische Strahlung viel kürzere Wellenlängen im Nanometer-Bereich hat und damit viel energiereicher ist, dürfte die Antenne nur zwischen 190 und 390 nm lang sein und die Frequenz des Wechselstroms müsste über 384 THz liegen. Atome haben einen Durchmesser zwischen 0,1 und 0,6 nm, so dass die Antenne nur etliche hundert Atome lang sein dürfte. Die aufzubringende Energie von über 1 eV würde diese Antenne umgehend zerstören. Licht wird z. B. durch Wärmestrahlung (Glühbirne), ionisiertes Gas (Neonröhre) oder die Sonne erzeugt.

Frequenzen. Diese berechneten Reichweiten sind jedoch nur theoretisch mit RFID nutzbar, da die Energie des Nahfeldes mit zunehmender Entfernung zu stark von der Quelle abnimmt[27]. In der Praxis sind deswegen deutlich geringere Entfernungen bei der Nutzung des Nahfeldes möglich.

Alle Tags kommunizieren über Felder mit dem Leser, jedoch benötigen nur die passiven Tags die Energie der Felder zur Kommunikation. Aktive Tags haben eine eigene Energieversorgung und erreichen dadurch höhere Reichweiten.

LF und HF

Bei der Nutzung des Nahfeldes wird die Energie des magnetischen Feldes von einer Spule (siehe Abbildung 2.3) durch Induktion aufgenommen. Stehen die Feldlinien senkrecht zu der Spule, dann wird die aufgenommene Energie maximiert. Wichtige Größen beim Einsatz der induktiven Kopplung zweier Spulen sind die Spulengröße, die Anzahl der Windungen und die verwendete Frequenz.

Die RFID-Frequenzen im LF- und HF-Bereich eignen sich sehr gut für die induktive Kopplung mit passiven Tags, da die Reichweite des Nahfeldes genügend groß ist und weil die Bauform der Spulen wenige Windungen und kleine Durchmesser zulässt. Der induzierte Strom wird in einem kleinen Kondensator gespeichert, um die notwendige Energie für die Kommunikation zu erhalten. Die Kommunikation selbst geschieht durch Lastmodulation des magnetischen Feldes [vgl. Sarma u. a. 2003, S. 458]. Der Tag moduliert die Impedanz[28] des Feldes, verbraucht also mehr oder weniger Energie. Diese Schwankungen kann der Leser erkennen und interpretieren, so dass auf diese Weise Informationen vom Tag zum Leser übertragen werden können. Eine sehr detaillierte und mathematische Beschreibung dieser Vorgänge findet sich in [Finkenzeller 2002, Kap. 4.1.10].

UHF und Mikrowelle

Im Unterschied zu den LF- und HF-Frequenzbereichen ist die Nutzung des Nahfeldes im UHF- und Mikrowellen-Bereich nicht sinnvoll. Die sehr geringe

[27] Die Feldstärke des Magnetfeldes nimmt mit der dritten Potenz im Verhältnis zum Abstand ab.

[28] Die Impedanz ist der Wechselstromwiderstand, welcher sich aus dem Quotient der Spannung und der Stromstärke berechnet. Der Ohmsche Widerstand ist das Pendant bei Gleichspannung und Gleichstrom.

Reichweite des Nahfeldes erfordert eine andere technische Umsetzung der Energieübertragung und der Kommunikation bei hohen Frequenzen. Außerhalb des Nahfeldes bietet sich die Nutzung des Fernfeldes in Form der elektromagnetischen Wellen an. Durch die veränderten, physikalischen Eigenschaften des Feldes müssen bestimmte Anpassungen an Tag, Leser, Kommunikation und Energieaufnahme vorgenommen werden.

Anders als im Nahfeld kann die Induktion nicht mehr als Grundlage genommen werden, so dass eine elektromagnetische Kopplung verwendet werden muss. Die Bauform des Tags und des Lesers verändert sich von Spulen zu Antennen (siehe Abbildung 2.6), also Hertzschen Dipolen[29]. Antennen emittieren bei einer angelegten Wechselspannung elektromagnetische Wellen, welche von anderen, entsprechenden Antennen empfangen werden können. Die Antennen der Tags nehmen somit die Energie der Wellen[30] auf und speichern sie in kleinen Kondensatoren. Zur Kommunikation mit dem Leser werden die elektromagnetischen Wellen von der Antenne des Tags reflektiert. Die zu sendenden Informationen werden dabei durch Modulation der Leistung der zurückgestrahlten Strahlung gleicher Frequenz codiert. Dies geschieht durch das Ein- oder Ausschalten eines Lastwiderstandes im Tag. Der Leser kann diese modulierten Wellen anschließend detektieren. Diese Methode ist vergleichbar mit der Radar-Technik, die ebenfalls auf der Reflektion von elektromagnetischen Wellen basiert. Allgemein wird diese Methode als *Backscatter* (auch *modulated backscatter* oder modulierter Rückstrahlquerschnitt) bezeichnet. Auch diese Technik wird von [Finkenzeller 2002, Kap. 4.2] ausführlich beschrieben.

Eine große Rolle für die effektive Nutzung des Fernfeldes spielt das Design der Antennen. Da hauptsächlich Dipolantennen verwendet werden, ist die Antennenlänge der wichtigste Parameter beim Einsatz einer bestimmten Frequenz. Eine Antenne sollte mindestens die halbe Wellenlänge λ der verwendeten Strahlung lang sein, um einen guten Wirkungsgrad zu haben [vgl. Finkenzeller 2002, S. 130]. Betrachtet man nun die Wellenlängen der Frequenzen aus Tabelle 2.1, dann wird deutlich warum höhere Frequenzen effektivere Antennen ermöglichen und damit auch größere Lese-Reichweiten erzielen. Wenn

[29] Ein Hertzscher Dipol ist ein aufgebogener Schwingkreis aus kapazitiven und induktiven Elementen, so dass man an jedem Ende der Antenne einen der zwei Pole erhält.

[30] Elektromagnetische Wellen sind nichts anderes als beschleunigte Ladungen, welche von der Empfangsantenne aufgenommen werden. Durch die Trennung von positiven und negativen Ladungen an den Enden der Antenne wird eine Spannung induziert.

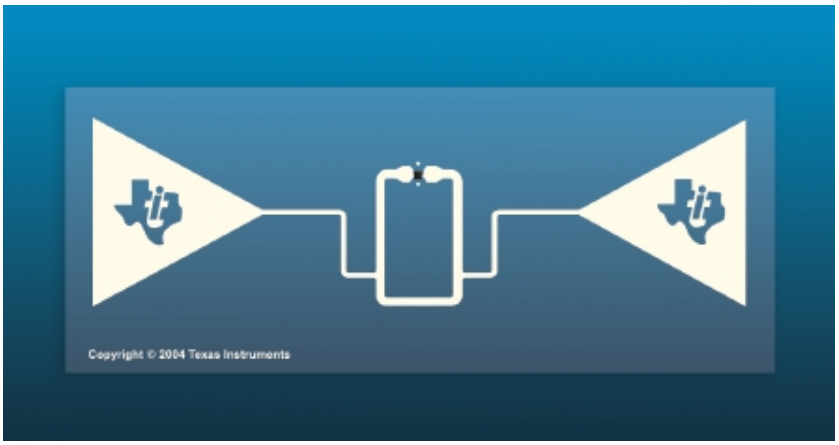


Abbildung 2.6: Inlay eines UHF-Tags von Texas Instruments [TI UHF 2006].

man HF-Systeme mit 13,56 MHz im Fernfeld einsetzen würde, dann wäre eine gute Antenne über elf Meter lang. Im Mikrowellen-Bereich bei 2,45 GHz hingegen ist eine Antenne mit guten Abmessungen lediglich ca. 6,1 cm lang. Der Einbau einer solchen Antenne in einen Tag ist realistisch – im Gegensatz zu elf Meter langen Antennen. Aus diesem Grund sind die Lese-Reichweiten bei RFID-Systemen mit höheren Frequenzen größer. Es gibt neben der Länge der Antenne noch viele weitere Möglichkeiten das Design der Antenne dem Einsatzzweck anzupassen [siehe Finkenzeller 2002, S. 130 f.].

Kollisionsbehandlung

In den bisherigen Beschreibungen wurde stets die Kommunikation zwischen einem Tag und einem Leser angenommen. Allerdings ist dieses Szenario natürlich theoretisch. Da viele Objekte mit Tags ausgestattet und mehrere Leser gleichzeitig aktiv sein können, kann es beim Lesen oder Schreiben zu Kollisionen in der Kommunikation kommen. Mehrere Tags können sich in der Reichweite eines Leser befinden oder mehrere Leser versuchen gleichzeitig, auf einen Tag zuzugreifen [vgl. Sarma u. a. 2003, S. 460]. Treten Kollisionen auf, dann können die empfangen Daten entweder gar nicht verwendet werden oder die Daten werden verfälscht und anschließend fehlerhaft verarbeitet. Weitere Probleme sind die Erkennung von Kollisionen und die gegenseitige Unkenntnis der Tags untereinander. Aus diesen Gründen ist eine Methode zur Anti-Kollision un-

bedingt notwendig. Ist ein RFID-System mit einer Anti-Kollisionsbehandlung ausgestattet, dann spricht man von der Pulkfähigkeit.

Bei der Tag-Anti-Kollision befinden sich mehrere Tags in der Reichweite eines Lesers. Man kann die Vorgehensweise der Leser in zwei Kategorien einteilen. Bei der ersten Kategorie sendet der Leser an alle Tags in der Umgebung das gleiche Signal und wartet anschließend auf die Reaktion der Tags. Dieses Verfahren nennt man probabilistisch oder *Broadcast*. Probabilistisch wird es genannt, weil der Erfolg korrekter Antworten nicht sichergestellt sein kann und nur mit einer bestimmten Wahrscheinlichkeit eintritt. Die Tags antworten nicht sofort dem Leser, sondern warten eine zufällige Zeit ab und antworten erst dann. Kollisionen werden dadurch nicht ausgeschlossen, aber die Wahrscheinlichkeit verringert. Die verwendeten Algorithmen heißen *ALOHA* und *Slotted ALOHA* und werden in [Finkenzeller 2002, Kap. 7.2.4] detailliert vorgestellt. Die Reichweite des Systems und die in der Anwendung mögliche Anzahl der Tags bestimmen, ob und welches Verfahren zum Einsatz kommt. Bei *Close Coupling Systems*, die häufig bei Bezahlvorgängen verwendet werden, ist die Kollisionsbehandlung wegen der geringen Reichweite meist nicht notwendig.

Die zweite Kategorie der Vorgehensweise ist die deterministische oder *Multi-Access* Zugriffsmethode. Die Zugriffe des Lesers auf Tags erfolgen nicht zeitgleich, sondern einzeln und nacheinander. Da die IDs der Tags dem Leser nicht bekannt sind, muss er versuchen, jede einzelne ID zu erraten. Eine Methode ist der Aufbau eines binären Suchbaumes über alle erdenklichen IDs und das Testen jedes Knotens des Baums [Sarma u. a. 2003, S. 460 f.]. Der Leser sendet eine Anfrage mit dem aktuellen Präfix der ID an die Tags und wartet auf eine Antwort. Bleibt eine Antwort aus, dann wird dieser Zweig des Baumes verworfen und der nächste Knoten bearbeitet. Am Ende dieser Prozedur hat der Leser alle Tags identifiziert und kann die einzelnen Tags mit ihrer ID ansprechen. Alle anderen Tags antworten dem Leser nicht. Auf diese Weise können eine Vielzahl von Tags verwaltet werden, so dass auch Systeme mit hoher Reichweite verwendet werden können. Des Weiteren entscheidet die Frequenz über die Dauer dieses Vorgangs.[31] UHF- und Mikrowellen-Systeme bieten sich

[31] Die zur Verfügung stehende Bandbreite steigt proportional mit der verwendeten Frequenz. Deswegen sind bei hoher Frequenz in einem gleichen Zeitabschnitt mehr IDs zu prüfen als bei niedriger Frequenz.

aus diesen Gründen für den Einsatz von deterministischen Methoden zur Anti-Kollision an. Technisch möglich sind natürlich auch andere Umsetzungen in anderen Frequenzbereichen.

Befinden sich zwei Leser in gegenseitiger Reichweite, so überlagern sich ihre Felder gleicher Frequenz und die Kommunikation ist nicht mehr möglich. Folglich können die Leser nicht gleichzeitig mit einem Tag kommunizieren. Es gibt zwei grundlegende Ansätze, die verfolgt werden können, um dieses Problem zu lösen. Die erste Lösung ist eine zentrale Steuerung der Leser bei der eine Anwendung oder elektronische Schaltung die Lesevorgänge steuert und darauf achtet, dass immer nur ein Leser zu einem Zeitpunkt Operationen ausführt. Die zweite Möglichkeit ist eine dezentrale Steuerung der Leser untereinander [vgl. Sarma u. a. 2003, S. 461 f.]. Voraussetzung dafür ist allerdings eine zusätzliche Funktionalität der Tags, die sich einen Zustand merken müssen und diesen an die Leser senden können. Greift ein Leser auf einen Tag zu, dann reagiert der Tag nur noch exklusiv auf diesen einen Leser und alle anderen Leser werden ignoriert oder erhalten bei einem Zugriffsversuch eine entsprechende negative Antwort. Dieses Vorgehen ist möglich, weil auch jeder Leser eine eindeutige ID besitzt, die der Tag identifizieren kann.

Die Kollisionsbehandlung ist ein Teil der Spezifikation der Luftschnittstelle (*Air-Interface*) zwischen Tag und Leser und Bestandteil von Standards (siehe Kapitel 4). Viele Hersteller versuchen sich mit eigenen Anti-Kollisions-Methoden – und damit einer Missachtung von Standards – von Mitbewerbern abzugrenzen. Die Benutzung von Tags und Lesern, die nicht die gleiche Methode verwenden, ist nicht möglich, so da die Hersteller versuchen, die Kunden an sich zu binden. Aus diesem Grund gibt es eine Vielzahl von verschiedenen Implementierungen der Anti-Kollision.

Lesefehler

Wenn Fehler beim Lesen von RFID-Tags auftreten, dann unterscheidet man zwischen zwei Arten. Der erste Fehler ist, dass versäumt wird überhaupt ein Tag zu lesen (*no-read*). Der Leser hat keinerlei Kenntnis von der Präsenz des Tags. Folglich wird auch keine weitere Verarbeitung des Objekts angestoßen. Dieser Fehler führt zu inkonsistenten Datenbeständen oder falscher Weiterverarbeitung des Objekts innerhalb einer denkbaren Fertigungslinie. Da dieser Fehler meist organisatorische Konsequenzen zur Folge hat, ist es nicht möglich

eine allgemeine Aussage zur Behebung des Fehlers zu treffen. Im Einzelfall ist dann zu prüfen, ob die Ursache des Fehlers in dem Ablauf oder der technischen Ausprägung des Systems liegt.

Der zweite mögliche Fehler ist ein falsches Auslesen von Daten des Tags (*false-read*). Der Leser hat dann wenigstens die Information, dass ein Tag in Reichweite ist. Es ist zunächst erst einmal noch offen, ob die Daten, die gelesen wurden auch korrekt sind. Allgemein geschieht die Verifizierung mit Hilfe von Prüfsummen. [Finkenzeller 2002, Kap. 7] schlägt drei verschiedene Verfahren zur Prüfung der Datenintegrität vor. Die einfachste Methode ist die Paritätsprüfung bei der lediglich die Summe aller Bits als Grundlage zum Vergleich dient. Der Nachteil ist, dass eine gerade Anzahl von Bitfehlern keinen Übertragungsfehler identifiziert. Etwas weniger anfällig ist der *Longitudinal Redundancy Check* (LRC), welcher alle Bytes mit der Exklusiv-Oder (XOR) Operation verknüpft. Diese Methode ist recht schnell und einfach zu implementieren, aber ziemlich anfällig, wenn sich mehrere Bytes ändern. Die aufwändigste und sicherste Methode ist der *Cyclic Redundancy Check* (CRC), welcher bei vielen anderen Anwendungen[32] eine sichere Fehlererkennung bietet. Methoden zur Fehlerkorrektur werden bis jetzt noch nicht eingesetzt. Die Lösung des Problems einer fehlerhaften Übertragung wird durch eine Neuübertragung gelöst.

Tendenziell erschweren verschiedene Faktoren das Auslesen der Tags. Diese sind z. B. Pulkerfassung (*Bulk Scanning*) oder Umgebungen mit Metall oder Flüssigkeiten (siehe folgendes Unterkapitel 2.2.3).

2.2.3 Flüssigkeiten und Metalle

Obwohl RFID-Systeme relativ gering anfällig gegen Umwelteinflüsse sind, gibt es zwei Materialien, die bei direktem Kontakt mit dem Tag Probleme beim Lesen und Schreiben verursachen können. Dies sind Flüssigkeiten – im Speziellen Wasser – und Metalle.

> „Metal and liquid have been described as the 'kryptonite to RFID' as they can play havoc with RFID signals." [Michael und McCathie 2005, S. 628]

[32] Neben der Übertragung der Daten bei RFID wird CRC häufig bei vielen Arten der Datenübertragung (z. B. bei Ethernet, Bluetooth) oder zur Prüfung von Datenintegrität (Veränderung einer Datei) eingesetzt.

Allgemein kann man die verschiedenen, störenden Effekte auf elektromagnetische Felder in Dämpfung (Absorption), Streuung, Reflexion und Verstimmung einteilen. Bei der Dämpfung werden die Funksignale von einem Material aufgenommen und in Wärme umgewandelt. Dadurch wird das Feld geschwächt oder sogar komplett vom Material aufgenommen. Teilweise wird auch der Begriff Absorption[33] verwendet, wenn Metalle, elektrisch leitende Flüssigkeiten oder sogar menschliche oder tierische Körper Felder dämpfen. Bei der Streuung wird die Strahlung in verschiedene Richtungen abgelenkt, was ein Abnehmen der Dichte der Felder zur Folge hat. Der Grad und Effekt der Störung ist abhängig von den chemischen und physikalischen Eigenschaften der verschiedenen Materialien. Metall- und Wasser-Oberflächen reflektieren Strahlung unter verschiedenen Voraussetzungen, wie z. B. Auftreffwinkel und Grenzschicht zwischen zwei Materialien. Durch Reflexion ändert sich die Reichweite und Form der Felder, so dass eine Kommunikation oft nicht mehr möglich ist. Bei der Verstimmung hingegen wird die ursprüngliche Frequenz der Felder verändert. Treffen elektromagnetische Wellen auf wellenförmige Oberfläche oder Kunststoff, dann kann durch die veränderte Frequenz die Grundlage für die Kommunikation verloren gehen. Diese allgemeinen Probleme sind nicht RFID-spezifisch, sondern gelten für die alle Formen der Kommunikation mit Hilfe von elektromagnetischen Feldern oder Wellen (Funk).

Viele Flüssigkeiten absorbieren elektromagnetische Strahlung. Dieser Effekt wirkt sich selbstverständlich negativ auf die physikalischen Eigenschaften von RFID-Systemen aus, da sowohl die Kommunikation als auch die Energieübertragung für passive Tags von denen vom Leser aufgebauten Feldern abhängt. Besonders Wasser absorbiert im höchsten Maße UHF- und Mikrowellen-Strahlung. Grund dafür ist die Größe des Wasser-Moleküls und die Eigenschaft, dass Wasser ein Dipol ist. Die Folge ist, dass das Wasser-Molekül durch die Strahlung in seiner Resonanzfrequenz angeregt wird. Somit wird fast die komplette Energie in Wärme umgesetzt. Sobald also Wasser zwischen Tag und Leser gerät, ist zumindest im hohen Frequenzbereich ein Auslesen so gut wie nicht möglich. Induktiv gekoppelte Systeme hingegen werden weniger stark

[33] Die Absorption ist der physikalische Vorgang, wenn Materie Strahlung oder Felder aufsaugt. Der Effekt dessen ist die Dämpfung, die sich in einem Energieverlust der Feldes bemerkbar macht.

von Flüssigkeiten beeinflusst. Zeit- und kostenaufwändige Tests von verschiedenen Ausprägungen von RFID-Systemen sind sowohl bei der Verwendung von Flüssigkeiten als auch von Metallen empfehlenswert.

Sind RFID-Tags direkt auf metallischen Oberflächen angebracht, dann ergeben sich ebenfalls Leseprobleme. Liegen die Spulen oder Antennen aus Metall direkt auf der Metalloberfläche auf, dann induzieren die magnetischen oder elektromagnetischen Felder ihre Energie eben nicht nur in die Elemente der Tags, sondern größtenteils in die Oberfläche des Untergrundes. Dies verursacht einen Fluss von freien Ladungsträgern je nach Richtung der Feldlinien. An der Oberfläche des Metalls entstehen Wirbelströme, die der Ursache entgegenwirken[34] [Finkenzeller 2002, S. 74 f.]. Diese der Ursache entgegengesetzte Wirkung dämpft das anliegende Feld und damit den magnetischen Fluss. Der Tag kann somit nicht mehr genügend Energie aufnehmen oder durch Lastmodulation/*Backscatter* mit dem Leser kommunizieren. Diese Einschränkung gilt für Frequenzen in allen Bereichen. UHF-Frequenzen sind zwar tendenziell weniger anfällig als induktiv gekoppelte Systeme, aber in der Praxis scheitern auch UHF-Tags bei direktem Kontakt mit Metall.

Eine Lösung dieses Problems kann durch das Vermeiden des direkten Kontakts des Tags mit der Metalloberfläche erreicht werden. Dies kann entweder durch genügend Abstand oder einen hochpermeabelen[35] Ferrit[36] zwischen Tag und Oberfläche realisiert werden. Eine Möglichkeit nicht nur den Abstand, sondern auch den Winkel von Tag zu Oberfläche zu verändern ist der *FlagTag* (siehe Abbildung 2.7), der eine Entwicklung der Firmen SATO[37] und UPM Raflatac[38] ist. Das Etikett ist in der Mitte faltbar, so dass ein Teil an dem Objekt befestigt wird und der andere das *Inlay* enthält. Dadurch steht der Tag senkrecht zur Metalloberfläche und verbessert die Lesbarkeit enorm. Der Nachteil dieser Lösung ist, dass der Tag relativ einfach vom Objekt zu entfernen ist – sowohl absichtlich als auch unabsichtlich. Eine weitere, häufig eingesetzte Lösung des Problems ist das Anbringen eines Ferritkerns zwischen den Tag und die Metalloberfläche. Dieser Ferritkern ist durchlässig für Magnetfelder, aber isoliert elektrische Ladungen. Diese Kombination erlaubt es dem

[34] Dieser physikalische Effekt ist als die Lenzsche Regel bekannt.
[35] Die Permeabilität bezeichnet die Durchlässigkeit von Materie für magnetische Felder.
[36] Ferrite sind elektrisch schlecht oder nicht leitende Materialien, wie z. B. Eisenoxide oder andere Metalloxide.
[37] http://www.sato-europe.com
[38] http://www.rafsec.com

Abbildung 2.7: Angebrachter FlagTag senkrecht zur Oberfläche [SATO FlagTag 2006].

Tag ohne die in die Oberfläche induzierten Ladungen und deren Wirbelströme mit dem Leser zu kommunizieren. Die Dicke des Ferritkerns liegt unter einem Millimeter, so dass der Tag nur unwesentlich vorsteht und das unbeabsichtigte Abstreifen vom Objekt erschwert wird (siehe Abbildung 9.1). Selbstverständlich sind die Kosten für diese *Mount-on-Metal*-Tags höher als bei Tags ohne diesen Ferritkern.

2.3 Allgemeine Einsatzgebiete

Die bisherigen genannten, technischen Eigenschaften von RFID-Systemen lassen erahnen, welche Potentiale RFID in den verschiedensten Branchen bietet. Die vielen möglichen Ausprägungen von RFID-Systemen machen die Auswahl des geeignetsten Systems aufwändig und schwierig. Allerdings ist die richtige Auswahl die Voraussetzung für den erfolgreichen Einsatz.

Elgar Fleisch nennt im Zusammenhang mit den Perspektiven von Auto-ID-Technologien allgemein die Basisaufgaben Identifikation, *Tracking & Tracing* (T&T), Qualitätssicherung, Verrechnung, Risikobewertung und Kundenverhaltensanalyse [Fleisch u. a. 2003, S. 30]. Daraus entstünden dann Potentiale

neue, Kosten sparende Geschäftsprozesse zu schaffen. Diese Prozesse seien angesiedelt in den folgenden Bereichen: Quellennachweis, Fälschungssicherheit, 1:1 Marketing, *Mass Customizing*, Wartung und Reparatur, Diebstahl und Schwund, Rückrufaktion, Sicherheit und Haftung, Überwachung, Entsorgung und Wiederverwertung und *Data Capturing* [Fleisch 2001, S. 181].

Dieses Unterkapitel listet die Einsatzgebiete auf, in denen RFID aktuell in der Praxis die größte Verwendung findet.

Industrie und Produktion

Die Identifikation von Objekten und das Anbringen von zusätzlichen Daten bieten in der Produktion große Vorteile. Bei einer großen Anzahl verschiedener Werkzeuge kann die Identifikation des richtigen Werkzeugs Fehler vermeiden und Prozesse beschleunigen. Des Weiteren kann die Wartung oder Reparatur von Werkzeugen oder anderen Objekte effektiver eingehalten werden, so dass Kosten und Fehler vermieden werden können. Durch die dezentrale Datenhaltung am Objekt erhalten Fertigungslinien neue Möglichkeiten, um die Automatisierung der Produktion zu erhöhen.

Durch eine eindeutige Identifikation kann jedes Produkt von den anderen Produkten der gleichen Charge[39] unterscheiden werden. Dies birgt Potentiale für den Gewährleistungsnachweis von Kunden gegenüber dem Lieferanten. Lieferanten hingegen können die Historie eines Produktes genauer protokollieren und ggf. außergewöhnliche Ereignisse während der Produktion nachvollziehen. Bei hochwertigen Produkten kann die Fälschungssicherheit erhöht werden, weil durch die eindeutige Identifikation der Produkte der Nachweis beim Hersteller angefordert werden kann.

Handel

Im Einzelhandel bietet sich mit der Auszeichnung jedes Artikels eine schnelle und zentrale Preisänderung an. Dies ist sowohl an den Regalen, die durch integrierte Leser die ausgelegten Waren erkennen können, als auch an der Kasse, die die Preise aus einer zentralen Anwendung ausliest und nicht vom Preisschild auf dem Artikel, möglich. So können Angebote oder Aktionen sehr schnell und effizient ausgezeichnet werden.

[39] Eine Charge ist die Menge gleichartiger Produkte eines zusammenhängenden Produktionsprozesses.

Abbildung 2.8: Gepäckwagen mit RFID-Leser [Hülsenbeck 2006, S. 16].

Durch das Anbringen von Lesern an den Einkaufswagen (vgl. ähnlich dem Gepäckwagen in Abbildung 2.8) oder an der Kasse können die im Wagen liegenden Artikel durch Pulkerfassung gelesen und die Preise der Artikel zu einer Rechnung zusammengefasst werden. Dies beschleunigt den Vorgang und macht das Auflegen der Artikel auf das Band an der Kasse unnötig. Zurzeit gibt es zwei große Händler, die sich sehr stark mit RFID auseinandersetzen: die METRO Gruppe[40] und Wal-Mart[41].

Nicht nur für Einzel- sondern auch für Großhändler ergeben sich durch RFID weitere Anwendungen im Bereich der Lieferkette (*Supply Chain Management*), der Logistik (Lager, Transport) und des Containermanagements. Da sich diese Arbeit im Besonderen mit dieser Branche beschäftigt, werden die dazugehörigen Einsatzgebiete und Potentiale in den Kapiteln 5 und 6 behandelt.

[40] http://www.future-store.org
[41] http://www.walmart.com

Medizin

Auf gekennzeichneten Blutkonserven wird ihr Verfallsdatum gespeichert. Somit können sie frühzeitig vernichtet werden, falls das Datum überschritten ist. Des Weiteren ist es möglich, die Konserven mit einem Temperatursensor zu versehen, damit die sie nach einer unsachgemäßen Lagerung nicht verwendet werden.

An mit RFID versehenen Krankenhausbetten wird die Medikation für den Patienten ausgezeichnet. Ein Alarm wird ausgelöst, falls eine falsche oder nicht erlaubte Medikation erfolgt. Dies hat zur Voraussetzung, dass Medikamente mit RFID-Tags versehen werden. Bis zum heutigen Zeitpunkt ist dies aber nur vereinzelt der Fall. Die Firma Pfizer[42] stattet beispielsweise ihr Produkt Viagra[43] mit Tags aus, um sich vor Fälschungen zu schützen.

Ticketing

Verschiedene ÖPNV-Betreiber[44] setzen RFID-Karten ein, damit sich ihre Kunden schnell und bequem eine Fahrt buchen können. Das Ziehen einer Karte am Automat oder der Kauf beim Fahrer entfällt damit. Die Rechnung aller Fahrten wird dem Kunden monatlich gestellt. Eine ähnliche Variante hat die Lufthansa[45] schon in den Neunziger Jahren eingeführt. Die „Miles & More“ Karte ermöglicht es dem Kunden, die Buchung eines Fluges kurzfristig per Telefon zu machen und dann am Flughafen nur durch das Auslesen der Karte die Bordkarte zu erhalten. Dadurch wird das *Check-In* auf wenige Minuten verringert. Die Abrechnung erfolgt ebenfalls nicht sofort, sondern monatlich.

Ebenfalls seit Jahren wird in Skigebieten der Skipass in Form von RFID-Tags verwendet. Der Tag kann in Uhren oder Plastikkarten untergebracht sein und mehrmals verwendet werden. Durch das schnellere Erfassen der Skifahrer an den Eingängen der Gondeln und Lifte wird der Vorgang einfacher und die Schlangen kürzer. Die Betreiber haben über die Skipässe mehr Kontrolle, da Fälschungen erschwert und Missbrauch[46] vorgebeugt werden kann.

[42] http://www.pfizer.com
[43] http://www.viagra.com
[44] Die Abkürzung ÖPNV steht für den Öffentlichen Personen Nahverkehr.
[45] http://www.lufthansa.de
[46] Die Benutzung eines Skipasses von zwei Fahrern kann durch Sperrung des Tags für wenige Minuten nach dem Passieren eines Eingangs verhindert werden.

Zur FIFA Fussball-Weltmeisterschaft 2006™ [47] werden die Tickets mit RFID-Tags versehen, um die Tickets mit den persönlichen Daten des Käufers zu versehen. Dadurch können die personalisierten Tickets auf dem Schwarzmarkt nicht verkauft werden. Allerdings ist zum heutigen Zeitpunkt noch offen, wie beim Betreten des Geländes die Daten der Person mit den Daten auf dem Tag verglichen werden sollen.

Zutrittskontrolle

Eindeutige Kennzeichnungen ermöglichen die detaillierte Vergabe von Berechtigungen verschiedenster Art. Physische Zugangskontrollen von geschützten Firmengeländen, Räumen oder Safes lassen sich mit RFID-Systemen erreichen. Der Tag ersetzt dann den herkömmlichen Schlüssel. Der Schließ-Mechanismus wird nicht mehr durch die Mechanik des Schlüssels und des Schlosses bestimmt, sondern durch die Anwendung, die an dem RFID-Leser angeschlossen ist. Dadurch kann ohne großen Aufwand eine Protokollierung aller Personen, die die Lokation betreten haben, durchgeführt werden. Des Weiteren lässt sich auf diese Art die Zeiterfassung[48] von Mitarbeitern in einem Schritt realisieren.

Diebstahlschutz

Mit RFID-Tags gekennzeichnete Artikel können durch große Gates[49] am Ausgang von Geschäften oder Lagern erkannt werden. Sind diese nicht bezahlt oder gebucht, dann kann durch einen Alarm der potentielle Diebstahl gemeldet werden.

Weitere Anwendungen werden schon seit etlichen Jahren in der Automobilindustrie praktiziert. Die Wegfahrsperre ist ein RFID-System, welches aus einem in der Lenksäule integriertem Leser und einem in den Schlüssel eingegossenen Tag besteht. Befindet sich nicht der richtige Tag in der Nähe des Zündschlosses, so kann das Auto nicht gestartet werden. Ebenso wurde die Zentralverriegelung von Autos mit RFID umgesetzt. Leser an den beiden vorderen Türen erkennen den Schlüssel in Reichweite und öffnen die Verriegelung.

[47] http://fifaworldcup.yahoo.com/06/

[48] Im Grunde sind dies die „Kommt“ und „Geht“ Meldungen an die Betriebsdaten-Erfassung (BDE).

[49] Gates sind RFID-Leser mit sehr großen Antennen. Sie werden an Ein- oder Ausgängen sowie an Toren von Lagern oder Fabriken benutzt, um den gesamten, passierenden Bereich zu überwachen.

Aus praktischen Gründen kann der Fahrer das Öffnen und Schließen mit einem Knopfdruck bestätigen, um ungewollten Öffnungen vorzubeugen.

Tieridentifikation

Schon seit Jahren werden Tiere mit RFID-Tags versehen, um sie identifizieren zu können. Dies hat in der modernen Tierhaltung verschiedene Vorteile und steigert im Wesentlichen die Effizienz. Beispielsweise können interne Steuerungen über die Anzahl der Tiere pro Gatter oder bei der individuellen Fütterungsmenge vorgenommen werden. Der Halter hat einen Überblick über die gesamte Population und deren wichtige Daten, wie z. B. Alter oder Herkunft. Zusätzlich kann der Lebenslauf des Tieres gespeichert werden, in dem eventuelle Impfungen, Krankheiten oder sonstige Informationen, die für den Verkauf oder die Schlachtung notwendig sein könnten, protokolliert werden. Schließlich könnten die immer wieder auftretenden Epidemien oder Seuchen bestimmter Rassen schneller eingedämmt werden, da die Herkunft und der Stammbaum der Tiere transparenter ist.

Wenn es die Möglichkeit der Kennzeichnung von Tieren gibt, dann liegt es nahe, dass auch der Mensch prinzipiell dauerhaft mit RFID-Tags versehen werden kann. Diese Idee ist einer der größten Albträume vieler Datenschützer und zu Recht besorgter Bürger. Den Gefahren und Problemen bei der Identifikation von Menschen ist ein großer Teil des Kapitels 3 gewidmet.

Sport

Bei Wettkämpfen erhalten Sportler einen kleinen Tag, der an den Schuhen oder anderen Ausrüstungsgegenständen befestigt wird. Dieser Tag identifiziert zunächst den Sportler, indem z. B. die Startnummer mit der RFID-ID verknüpft wird. An bestimmten Stellen der Strecke kann dann kontrolliert werden, ob der Sportler diese passiert oder unerlaubterweise einige dieser Kontrollpunkte ausgelassen hat. Exakte Zeitmessungen sind wegen der Ausdehnung der Felder nicht möglich, aber realisierbar ist eine in etwa sekundengenaue Erfassung, die bei Ausdauer-Sportarten, wie Marathon oder Radrennen, ausreichend ist.

Bibliothek

Große Bibliotheken stellen nach und nach ihr Nummern- oder Barcode-System auf RFID um, weil dadurch viele Arbeiten einfacher werden. Der Ausleihvorgang wird erheblich beschleunigt, nicht ausgeliehene Bücher können am Ausgang detektiert werden und falsch einsortierte Bücher in den Regalen können mit mobilen Lesern sehr schnell gefunden und korrekt einsortiert werden. Verschiedene Stadtbibliotheken verwenden inzwischen RFID-Systeme. Sogar der Vatikan hat ebenfalls ein RFID-System für seine fast zwei Millionen Bibliotheksobjekte eingeführt, von denen aber erst die öffentlich zugänglichen Bücher und Manuskripte erfasst werden [Libbenga 2004].

Sonstige Einsatzgebiete

In Österreich und manchen Staaten der USA werden aktive Tags in Fahrzeuge eingebaut, um die Mauterfassung technisch umzusetzen. Die vom Mautsystem-Betreiber verkauften Tags werden hinter die Windschutzscheibe der Fahrzeuge installiert und können so während der Fahrt von den an den Straßen installierten Lesern erfasst werden.

Viele Anwendungen im Bereich der Fälschungssicherheit werden in den nächsten Jahren in verschiedenen Brachen forciert. Teure Textilien sollen mit RFID-Tags versehen werden, die dem Käufer garantieren können, dass das Produkt keine Fälschung ist.

Ebenfalls in der allgemeinen Diskussion ist das Ausstatten von Banknoten mit winzigen Tags. Dadurch könnte das Fälschen von Banknoten zwar nicht verhindert, aber das Erkennen der „Blüten“ sehr viel einfacher werden.

Seit November 2005 gibt es in Deutschland einen neuen Reispass[50], der ebenfalls einen RFID-Tag enthält. Auf dem Tag werden die relevanten Personendaten inklusive biometrischer Informationen (Gesichtsgeometrie, ab 2007 auch der Fingerabdruck) in verschlüsselter Form abgelegt. Ab 2008 soll der neue Pass dann flächendeckend eingeführt werden.

Neben der direkten Verbindung von Tag und Objekt kann man im Bereich des Marketings neue Szenarien erwarten. Durch die Personalisierung des Marketings kann das eventuell gewünschte 1:1 Verhältnis zwischen Kunde und Anbieter geschaffen werden. Somit könnten durch das Marketing neue Dienstleis-

[50] http://www.neuer-reisepass.de

tungen geschaffen werden, die den Kunden intensiver und effizienter informieren und betreuen. An dieser Stelle sei wiederum angemerkt, dass der Wahrung der Privatsphäre und des Datenschutzes Folge geleistet werden soll. In dem nachfolgenden Kapitel 3 wird darauf explizit eingegangen.

Zusätzliche Kombinationen mit anderen Techniken

Einfache, passive Tags sind zwar Grundlage der meisten Anwendungen und Einsatzgebiete, jedoch bieten sich zusätzlich zu RFID weitere Techniken an, die in Kombination neue Anwendungen ermöglichen. Diese Techniken können sein: die bereits erwähnte Kopplung von aktiven Tags mit Sensoren, *ZigBee*[51], *Global Positioning System* (GPS), *Near Field Communication* (NFC) oder Mobiltelefone. Diese neuen Kombinationen bedeuten für RFID-Systeme einen Mehrwert an Mobilität und neue Möglichkeiten durch *Location Based Services* (LBS) oder *Real Time Location Services* (RTLS)

Durch die Kopplung von Sensoren an aktive Tags entsteht für viele Anwendungsbereiche ein Mehrwert. Daten können während dem Transport oder der Lagerung gesammelt und sogar umgehend ausgewertet werden. Die gängigsten Größen, welche überwacht werden können sind Druck, Temperatur, Lichtintensität, Zeit, Bewegung/Erschütterungen, Füllstand und Luftfeuchtigkeit. Durch die Möglichkeit die gesammelten Daten auf dem Tag zu speichern, kann die Historie des Objekts genau protokolliert werden. Zusätzlich dazu könnte der Tag beim Eintreten eines bestimmten Zustandes die Verbindung zu einem Leser aufbauen und das Ereignis melden. Häufige Einsatzgebiete sind dabei neben der Logistik und dem Transportwesen sicherheitskritische Umgebungen, wie Chemieanlagen oder Flugfelder auf Flugplätzen. Viele Sensornetze werden heutzutage allerdings mit anderen Techniken betrieben, wie z. B. *ZigBee* zur Funkübertragung. Allerdings könnte je nach Anwendungsfall eine Lösung mit RFID preisgünstiger sein als mit *ZigBee*.

Neben Sensoren können auch GPS-Empfänger mit RFID-Tags gekoppelt werden. Dies eröffnet neue Anwendungsfälle, wenn die Position eines Objekts von Bedeutung ist. Da GPS einen direkten Sichtkontakt zu den Satelliten benötigt[52], können GPS-Empfänger nur außerhalb von Gebäuden benutzt werden.

[51] ZigBee ist ein Standard der IEEE (http://www.ieee.org, IEEE 802.15.4) zur Kommunikation über Funk. Im Unterschied zu RFID war ZigBee für die Vernetzung von Kleingeräten gedacht.

[52] Der Grund für den direkten Sichtkontakt ist die relativ geringe Sendeleistung der Satelliten.

In den seltensten Fällen ist eine Nutzung in Gebäuden möglich. In der Telematik dienen dann die Ortsinformationen für eine optimale Nachverfolgung und Berechnung der idealen Route. Im Bereich des *Tracking & Tracing* können Objekte geortet und deren Wege nachverfolgt werden. Denkbare Szenarien finden sich auf Flughäfen, auf denen Gepäckwagen geortet werden, oder privaten Firmengeländen, auf denen Lastwagen oder Standorte von Wechselbrücken[53] identifiziert werden müssen. Bewegt sich ein Objekt auf nicht abgeschlossenen Arealen, dann können ortsabhängige Dienste (*Location Based Services*) angeboten werden. Diese Dienste werden von Mobilfunk-Anbietern für z. B. Privatanwendungen angeboten, indem über die Position des Mobiltelefons innerhalb des GSM-Netzwerkes die aktuelle Position des Telefon-Eigentümers bestimmt wird. Die angebotenen Informationen beschränkten sich dabei jedoch auf nahe Restaurants oder EC-Automaten. Für den gewerblichen Zweck gibt es sicherlich das größte Potential in der Logistik und im Transportwesen und damit natürlich auch im SCM. Ebenfalls ist die Ortung von Personen möglich. Dies kann beim Aufenthalt von Personen in gefährlichen Umfeldern nützlich sein, bei denen die Position eine große Rolle spielt, z. B. bei der Bedienung von Maschinen. Das bekannteste Produkt im Bereich von *Real Time Location Services* bietet derzeit Siemens[54] mit dem RFID-System „MOBY R“[Siemens 2006]. MOBY R bietet Lokalisierung von verschiedensten Objekten in Echtzeit[55]. Dabei schlägt Siemens den Einsatz zur Ortung von Fahrzeugen, Staplern, Zuliefern, Instandhaltern, Materialboxen und Containern vor. Zusätzlich sind Szenarien mit Sicherheitsfunktionen denkbar, wie z. B. Zugangskontrolle, Personen- und Fahrzeugkontrolle.

Eine der RFID verwandte Funktechnologie ist *Near Field Communication*. NFC wurde von Philips[56] und Sony[57] als Alternative zu RFID entwickelt. Anders als bei herkömmlichen RFID-Systemen kennt NFC keine Trennung

[53] Eine Wechselbrücke ist ein Container, der genau auf einen Aufbau eines LKW passt und somit transportiert werden kann. Zusätzlich hat der Container vier Stützbeine, auf denen er bei der Entladung abgestellt wird. Der LKW wird dadurch sehr schnell und einfach mit Wechselbrücken be- und entladen.

[54] http://www.siemens.com

[55] Der Begriff „Echtzeit“ kann in diesem Kontext besser mit dem Adjektiv „zeitnah“ umschrieben werden. Die in der Informatik (insbesondere bei Betriebssystemen) gebräuchliche Definition von Echtzeit, welche eine garantierte Berechnung von bestimmten Operationen in vorgegebenen Zeitintervallen bedeutet, kann hier nicht verwendet werden.

[56] http://www.philips.com

[57] http://www.sony.com

zwischen Leser und Tag. Ein NFC-Gerät ist gleichzeitig sowohl Tag als Leser. Integriert in mobile Geräte, wie Mobiltelefone oder PDAs, können damit neue Anwendungsgebiete erschlossen werden. Die Reichweite beträgt dabei nur wenige Zentimeter, da die Betriebsfrequenz im HF-Bereich bei 13,56 MHz liegt. Gemeinsam mit Nokia[58] gründeten die beiden genannten Firmen das NFC-Forum[59], welches die Forschung und Standardisierung von NFC vorantreiben soll. Auf den Webseiten des NFC-Forums werden diverse Beispiel-Applikationen vorgestellt, welche das Alltagsleben vereinfachen sollen. Über NFC soll das Konfigurieren von verschiedenen Geräten einfacher werden. Drucker, Headsets und andere Kleingeräte können ihre Konfigurationen für Bluetooth oder WLAN per NFC aushandeln und somit schneller und einfacher miteinander kommunizieren. Des Weiteren können Kontaktdaten zwischen zwei Mobiltelefonen über NFC ausgetauscht werden (*Peer-to-Peer*). Das dritte Beispiel ist ein *Smart Poster*, welches ein kleines NFC Gerät enthält. Man kann sich als Passant vor dem Poster eine Vorschau der Veranstaltung in Form eines kleinen Videos herunterladen, anschließend die Tickets kaufen und dann bei der Veranstaltung die NFC-Daten als Eintrittskarte benutzen. Einen erfolgreichen Feldversuch führte der Rhein-Main-Verkehrsverbund in Hanau mit NFC als elektronischer Fahrkarte durch, so dass nun die weltweit erste kommerzielle Nutzung von NFC folgt [Philips 2006]. Ein erstes für die Allgemeinheit erhältliches NFC-Gerät ist das Mobiltelefon Nokia 3220.

Zusammenfassender Ausblick

Zusammenfassend kann man als Grund für das Wachstum von RFID insbesondere den Preisrückgang, den Fortschritt in der Zuverlässigkeit der Technik und den vermehrt aufkommenden Einsatzgebieten sehen. Die Vorhersagen zur Preisentwicklung sind sehr unscharf und deswegen kritisch zu betrachten. In Abbildung 2.9 wird versucht die Preisentwicklung der verschiedenen Komponenten eines RFID-Systems darzustellen. Die Kosten für die reine Hardware werden – den Autoren der Abbildung nach – sinken und die Kosten für die Integration der Daten und Funktionen eher zunehmen. Sicherlich ist diese Vermutung nicht falsch, da die Preise für die Tags und Leser tatsächlich fallen,

[58] http://www.nokia.com
[59] http://www.nfc-forum.org/

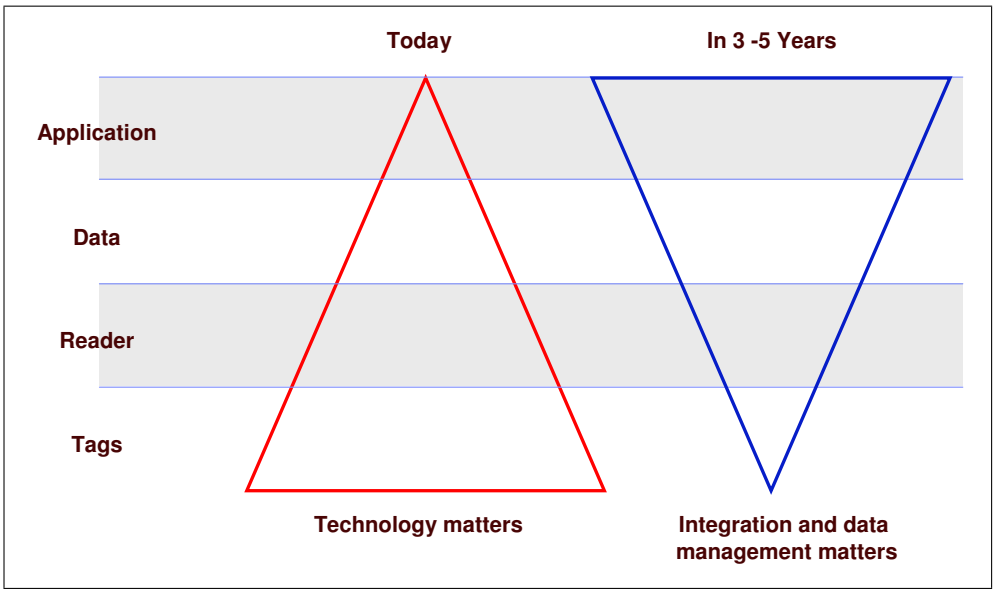


Abbildung 2.9: Trend der Kosten-Verhältnisse unter den RFID-Komponenten [Rindle 2006, S. 6].

jedoch wird in der Grafik nur das Verhältnis zwischen verschiedenen Kosten angedeutet. Absolute Voraussagen sind natürlich schwieriger zu treffen.

Vor allem profitierten die Prozesse im SCM und CRM (sowie dem *Product Data Management* (PDM)) in Folge von Qualitäts- und Effizienzsteigerungen [Fleisch u. a. 2003, S. 30] von RFID-Systemen. In den nachfolgenden Kapiteln wird auf die Bedeutung von RFID als Auto-ID-Technologie innerhalb des SCM näher eingegangen.

Zurzeit wird im Bereich der SCM eine rege Debatte[60] über die richtige Frequenz für bestimmte Anwendungen geführt. In der Pharmaindustrie führte ODIN[61] eine Studie durch, welche die richtige Frequenz für drei Standard-Verpackungen von Medikamenten finden sollte [RFID Update 2006b]. Dabei wurden Tablettenflaschen, Blisterverpackungen und Flaschen mit Flüssigkeiten mit Tags aus dem HF- und dem UHF-Bereich getestet – also auch Umgebungen mit Flüssigkeiten und Metallen. Die Frequenzen aus dem HF-Bereich konnten

[60] Im Englischen wird die „Debatte“ eher etwas martialischer mit *Battle* (Schlacht) umschrieben.
[61] http://www.odintechnologies.com

dabei Vorteile gegenüber dem UHF-Bereich erzielen. Allerdings ist die Allgemeingültigkeit des Ergebnisses nicht gegeben, da die Studie ausschließlich auf Produkte und Prozesse in der Pharmaindustrie ausgelegt war. ODIN führt in der Studie an, dass ca. 50 % der Ergebnisse in andere Branchen übertragbar seien. In den Kapiteln des zweiten Abschnitts dieser Arbeit wird die Diskussion über die richtige Frequenz im SCM und dem Behältermanagement noch einmal aufgegriffen.

2.4 RFID im Vergleich zum Barcode

In diesem Kapitel wird der weit verbreitete Barcode mit der aufkommenden RFID-Technik verglichen. Beide Techniken dienen dazu, Objekte zu identifizieren und die ID in elektronischer Form weiter zu verarbeiten. Der größte Unterschied besteht bei der Übertragung der Daten vom Tag/Etikett zum Leser. In der folgenden Aufzählung werden die Hauptunterschiede kurz erläutert:

- Sichtkontakt
  Barcodes brauchen einen direkten Sichtkontakt, um vom Leser gelesen zu werden. Dies erfordert, dass die Barcodes an relativ leicht zugänglichen Stellen des Objektes angebracht sein müssen, was die Auswahl der Position des Barcodes auf die sichtbare Oberfläche einschränkt. Bei teuren oder optisch ansprechenden Objekten könnte dies jedoch nicht gewünscht sein.[62] Sind Objekte mit einem nicht lichtdurchlässigen Material verpackt, dann können die Barcodes im Gegensatz zu RFID-Tags nicht gelesen werden.

- Orientierungsabhängigkeit
  1D-Barcodes müssen in einer quer zu den Strichen des Barcodes verlaufenden Linie gelesen werden. 2D-Barcodes sind nicht in der Richtung eingeschränkt, müssen aber mit einer Kamera senkrecht zu dem Barcode ausgelesen werden. RFID-Tags können aus allen Richtungen ausgelesen werden. Abhängig von der Spulen-/Antennenform und der Energie des Lesers ergeben sich jedoch Schwankungen in der Reichweite.

[62] Uhren oder Armaturenbretter von Autos sind Beispiele, bei denen aufgeklebte Barcodes sicherlich das Aussehen beeinflussen.

- Lesereichweite
  Die Lesereichweite von Barcode-Lesern ist meist auf ca. 0,5 m beschränkt. Industrielle Leser haben sicherlich größere Reichweiten, die aber die RFID-Reichweiten von bis zu 5 m bei UHF-Frequenzen (passiv) nicht erreichen können.

- Datenmenge
  Barcodes können nur wenige Zeichen (lt. [Finkenzeller 2002, Tab. 1.2] zwischen ein und 100 Byte) codieren, wobei RFID-Tags bis zu 128 kB speichern können.

- Veränderbarkeit
  Sind Barcodes einmal gedruckt, dann sind sie nicht mehr zu verändern (statisch). Anders hingegen RFID-Tags, welche bis auf ihre eindeutige ID über wiederbeschreibbaren Speicherplatz verfügen können (dynamisch). Somit ist eine mehrfache Verwendung durchaus denkbar.

- Verschmutzungsgefahr
  Sind die meist schwarzen Linien des Barcodes verschmutzt, dann kann der Lesevorgang nicht erfolgreich ausgeführt werden. Dies gilt natürlich auch, wenn der Sichtkontakt durch Überkleben oder teilweise Zerstörung beeinträchtigt wird.

- Eindeutigkeit
  Durch die relativ geringe Speicherkapazität von Barcodes, werden häufig nicht einzelne Objekte, sondern eher ganze Aufträge, Chargen oder sogar lediglich die Artikelnummer im Barcode codiert. Eine eindeutige Identifizierung und Rückverfolgung ist dann nicht mehr möglich. Die ID von RFID-Tags ist weltweit immer eindeutig.[63]

- Pulkfähigkeit
  Barcodes können nur mit sehr viel Aufwand im Pulk gelesen werden (sofern alle Barcodes sichtbar sind). RFID bietet die Möglichkeit, viele Objekte in kurzer Zeit ohne Sichtkontakt zu lesen.

[63] Der Aufbau der ID und die Regelung der Vergabe von Teilen der ID zur Erreichung einer weltweiten Eindeutigkeit werden in Kapitel 4.2 behandelt.

- Sensorik
  Barcodes können nicht mit Sensoren jeglicher Art gekoppelt werden, da sie keine elektronischen Möglichkeiten haben, die Daten weiter zu verarbeiten.

- Kommunikation
  Barcodes können nicht von sich aus eine Verbindung zu einem Leser herstellen. Aktive Tags hingegen können diese Funktion erfüllen und eine Verbindung aufbauen.

- Sicherheit
  Bei Barcodes ist lediglich eine Verschlüsselung der zu codierenden Zeichenkette vor dem Erstellen des Barcodes denkbar. Einen Schutz wie Authentifikation oder Verschlüsselung der Kommunikation wie bei RFID (siehe Kapitel 3) gibt es nicht.

- Sonneneinstrahlung
  Bei intensiver Sonneneinstrahlung kann der Barcode-Leser „geblendet“ werden und die reflektierten Lichtstrahlen nicht detektieren, so dass der Lesevorgang nicht erfolgreich ist.

- Duplizierbarkeit
  Barcodes können einfach kopiert oder neu ausgedruckt werden. RFID-Tags müssen industriell mit lithographischen[64] Methoden hergestellt werden und sind nur mit sehr hohem Aufwand zu kopieren. Auf die Fälschungssicherheit wird in Kapitel 3 noch näher eingegangen.

- Lesegeschwindigkeit
  Barcodes können nur einzeln und nacheinander gelesen werden. Ein Lesevorgang dauert je nach Leser und Anwendung ca. 1-3 Sekunden. RFID-Tags hingegen können sehr viel schneller ausgelesen werden, so dass die Dauer zwischen wenigen Millisekunden und ca. 0,5 Sekunden liegt.

- Kosten
  Die Kosten für den Ausdruck eines Barcodes sind deutlich geringer als

[64] Elektronische Chips werden durch das Bestrahlen von Leiterplatten mit optischem oder ultraviolettem Licht hergestellt. Ursprünglich war die Lithographie das Drucken von Bildern durch ein Negativ, welches in einen Stein graviert war.

die Kosten für einen RFID-Tag, da für den Barcode im einfachsten Fall lediglich ein wenig Farbe auf einem Objekt benötigt wird – eventuell zusätzlich ein selbstklebendes Papieretikett. RFID-Tags bestehen dagegen aus mehreren und aufwändig herzustellenden Komponenten.

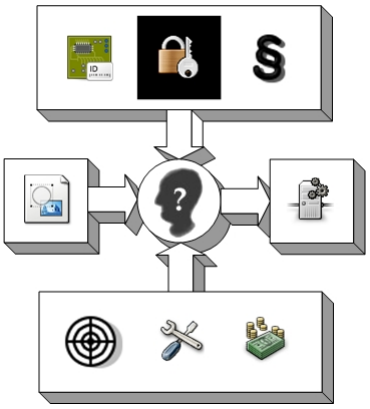
- Herstellung
  Barcodes sind einfach selbst herzustellen. Die zu codierende Zeichenkette kann problemlos in den Strichcode umgewandelt und ausgedruckt werden. RFID-Tags dagegen sind nur industriell herstellbar und somit für den Endanwender nur käuflich erhältlich.

- Materialeinflüsse
  Barcodes können – anders als RFID-Tags – auf metallischen Oberflächen oder Objekte mit Flüssigkeiten angebracht werden. Die Probleme und Möglichkeiten von RFID-Tags mit bestimmten Materialien wurden bereits in Kapitel 2.2.3 angesprochen. Allerdings sind Barcodes je nach Ausführung empfindlich gegenüber Hitze, Staub oder Feuchtigkeit, z. B. wenn der Barcode auf Papier gedruckt ist. In der Regel sind RFID-Tags gegen diese Einflüsse unempfindlich.

Aus diesen unterschiedlichen Eigenschaften beider Techniken wird deutlich, dass je nach Anforderungen der Anwendung eine Entscheidung für die richtige Technologie getroffen werden muss. Eine allgemeine Aussage, für welche Anwendung welche Technologie adäquat ist, kann nicht getroffen werden. In den folgenden Kapiteln werden weitere wichtige Eigenschaften von RFID behandelt, welche für den effektiven Einsatz von Bedeutung sind.

Kapitel 3

Sicherheitsrelevante Bedenken und umweltbelastende Einflüsse



In der Öffentlichkeit wird zurzeit eine wichtige Diskussion über die Sicherheitsbedenken beim Einsatz von RFID geführt. Der Leser sollte stets die Auswirkungen jeglicher Entscheidungen auf die Sicherheit des betreffenden RFID-Systems hinterfragen. Aus diesem Grund wird dieses Thema an dieser frühen Stelle der Arbeit platziert, denn die nachfolgenden Themen beinhalten an verschiedenen Stellen sicherheitsrelevante Aspekte. Eine wichtige Tatsache dabei ist die Trennung zwischen dem Einsatz von RFID im gewerblichen und im privaten Sektor. Die Definition von Sicherheit im gewerblichen Sektor beinhaltet häufig den Schutz vor ungewollten Auslesen oder die Abwehr von Angriffen, wobei im Privatbereich natürlich die Wahrung der Privatsphäre die wichtigste Rolle spielt.[65]

In Deutschland und vermehrt auch in anderen deutschsprachigen Ländern wird die Kritik an RFID hauptsächlich durch den „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.“ (FoeBuD)[66] voran getrieben. Der Verein hat die Kampagne „StopRFID“ ins Leben gerufen, um die Allgemeinheit über die Gefahren von RFID zu informieren. Zusätzlich werden

[65] Die Verletzung der Privatsphäre im gewerblichen Sektor ist damit nicht ausgeschlossen, jedoch spielt dieses Problem in der Arbeit eine untergeordnete Rolle.
[66] http://www.foebud.org

von dem FoeBuD Forderungen und Positionspapiere bereitgestellt, welche diesen Gefahren entgegenwirken sollen. Aktuell wird das Ticketing bei der FIFA Fussball-Weltmeisterschaft 2006™ und dem FutureStore der METRO Gruppe sehr kritisch betrachtet. In Zuge dessen verlieh der FoeBuD der METRO im Jahre 2003 und dem WM-Organisationskomitee des DFB im Jahre 2005 jeweils den „BigBrotherAward“[67] in der Kategorie Verbraucherschutz.

3.1 Kommunikation als kritische Komponente

Wie bereits in der Einleitung in Kapitel 1.1 geschildert, durchdringt das *Ubiquitous* und *Pervasive Computing* immer stärker unser Alltags- und Berufsleben. Allgemeine Merkmale des *Pervasive Computing* sind Miniaturisierung, Einbettung, Vernetzung, Allgegenwart und Kontextsensitivität [BSI 2004, S. 19]. RFID ist eine Technologie, die sich sehr gut eignet, in *Smart Things* integriert zu werden.

Im Folgenden wird davon ausgegangen, dass alle RFID-Systeme mindestens die folgenden, allgemeinen Eigenschaften erfüllen [vgl. BSI 2004, S. 13]. Dabei kann von speziellen Funktionen für bestimmte Anwendungen abstrahiert werden, weil diese grundlegenden Eigenschaften für das Verständnis der Sicherheitsbedenken vollkommen ausreichend sind.

- Eindeutige ID: Jeder Tag enthält eine weltweit eindeutige ID, welche nicht veränderbar oder duplizierbar ist.
- Kontaktloses Auslesen: Die auf dem Tag gespeicherten Daten können über eine Funkverbindung ausgelesen werden.
- Auslesen auf Abruf: Die auf dem Tag enthaltenen Daten werden entweder durch die Leseoperation eines Lesers oder durch ein auslösendes Ereignis eines Sensors am Tag versendet.

In [BSI 2004, S. 14] wird zusätzlich die Integrität von RFID-Systemen durch drei weitere Punkte beschrieben. Die Beziehung einer ID zu einem Tag muss eindeutig sein. Die ID darf nicht von einem Tag auf einen anderen Tag übertragen werden und darf somit den einen physischen Tag nicht verlassen. Des Weiteren sollte ein Objekt immer nur mit dem Tag ausgestattet bleiben, mit

[67] http://www.bigbrotherawards.de

dem es ursprünglich ausgestattet wurde – also ein Tag für die gesamte Lebenszeit des Objekts. Die dritte Beziehung besteht zwischen dem Leser und dem Tag. Bei der Verwendung von Authentifikation oder Verschlüsselung müssen nicht autorisierte Leser abgelehnt werden.

Ausgehend von diesen Eigenschaften und Beziehungen wird in den folgenden Unterkapiteln auf die Themen Datenschutz, Privatsphäre, Industriespionage und Fälschungssicherheit als wichtigste Bedrohungen eingegangen. Die angenehmen Eigenschaften der *Smart Things* sind gleichzeitig auch die Gründe warum RFID sicherheitsrelevante Bedenken schürt. Nicht sichtbare Funkverbindungen bieten das unangenehme Potential, ungebetene Lesevorgänge ohne die Kenntnis des Menschen durchzuführen. Aus diesem Grund wird in den folgenden Unterkapiteln hauptsächlich der Fokus auf die Kommunikationskomponenten gesetzt. Denkbar sind auch mechanische Angriffe auf Tags oder die Kopplung von Tag und Objekt, der Einsatz von Störsendern oder das Blocken von Tags sowie Software-Angriffe auf das Backend. Diese und weitere Szenarien werden in [BSI 2004, S. 14 f.] aufgelistet.

3.1.1 Datenschutz und Privatsphäre

Die Begriffe Datenschutz und Wahrung der Privatsphäre werden häufig synonym verwendet, sollen aber für diese Arbeit wie folgt unterschieden werden. Die Privatsphäre ist der Teil des Lebens einer Person, welcher nicht für die Öffentlichkeit zugänglich sein soll. Mit Öffentlichkeit kann im äußersten Fall sogar die eigene Familie oder die nächsten Freunde gemeint sein. Datenschutz im weitesten Sinne beinhaltet den Schutz der Privatsphäre, bedeutet jedoch auch den Schutz von Daten jeglicher Art, also auch der Schutz von Daten von Firmen oder nicht natürlichen Personen[68]. Somit muss ebenfalls zwischen sich in Umlauf befindlichen Konsum- und Industrieprodukten unterschieden werden. Konsumprodukte erreichen den Einzelhandel und somit den Verbraucher, wobei Industrieprodukte häufig nur in Produktionsstätten oder in der Lieferkette anzutreffen sind. Das Datenschutzrecht kommt erst dann zum Tragen, wenn die Möglichkeit besteht, Daten mit Personen zu verknüpfen [vgl. Eicar 2006, Kap. 5.1].

[68] Nicht natürliche Personen sind meist juristische Personen (GmbH, AG) oder teilrechtsfähige Vereinigungen (OHG).

Dem aufmerksamen Leser stellt sich beim Zusammenhang von Technik und Datenschutz oder Privatsphäre die Frage, inwiefern denn die Technik für eventuellen Missbrauch verantwortlich gemacht werden kann? In dieser Arbeit wird RFID als ein Werkzeug für die Verwirklichung von bestimmten Anwendungen gesehen. RFID ermöglicht sowohl sinnvolle als auch moralisch nicht einwandfreie Verwendungen und wird somit als *Enabler* angesehen. RFID – als technische Möglichkeit – ist weder gut noch böse, sondern neutral.[69]

[Nedden 2005, S. 1 f.] schlägt eine Unterscheidung von drei Ausgangskonstellationen im Datenschutz vor. In der ersten Konstellation sammelt der Tag keine personenbezogenen Daten. Eine Person kann jedoch durch die Nähe eines Produktes identifiziert werden und somit auch der Weg einer Person vorbei an mehreren Lesern. Nedden vergleicht diese Situation mit einer Videoüberwachung in Gebäuden. Bei der zweiten Konstellation erhebt der Tag personenbezogene Daten und identifiziert damit ein Individuum eindeutig. In diesem Fall besteht natürlich die Gefahr der Erfassung von kritischen Daten und auch der Verletzung der Privatsphäre. In der letzten Konstellation werden die Daten nicht auf dem Tag gespeichert, wohl aber in irgendeiner Form zentral abgelegt und zu einem späteren Zeitpunkt zusammengeführt. Auf diese Art lassen sich Profile von Personen (*Tracking*) erstellen. Auch [Ohkubo u. a. 2005, S. 68] führt im privaten Bereich ebenfalls die mögliche Verbindung zwischen Mensch und Produkt (z. B. eine Geldbörse mit einem Tag wird vom Besitzer meist mitgeführt) als Gefahr des *Trackings* an.

Eine wichtige Rolle bei den privaten Verbrauchern spielt das Bewusstsein, dass man beim Kauf ein Produkt erwirbt, welches mit einem RFID-Tag versehen ist. Alleine das Wissen um den Tag an einem Produkt lässt dem Käufer die Entscheidung, das Produkt erst gar nicht zu kaufen, den Tag zu entfernen oder den Tag zu deaktivieren[70]. In der Zukunft wird es auch im privaten Haushalt Anwendungen geben, die die Informationen auf den Tags nutzen. Das bekannteste Beispiel dafür ist der Kühlschrank, der abgelaufene oder fehlende

[69] In der Geschichte der Menschheit gibt es viele Beispiele, in denen wissenschaftliche oder technische Erkenntnisse für schreckliche Taten eingesetzt wurden. Alfred Nobel erfand das Dynamit zur Arbeitserleichterung im Bergbau und nicht für den Krieg. Albert Einsteins Spezielle Relativitätstheorie ($E = mc^2$) war Grundlage für den Bau der Atombombe.

[70] Welche weiteren, technischen Möglichkeiten zum Entfernen von Tags denkbar sind, wird in Kapitel 3.2 behandelt.

Produkte meldet [Garfinkel u. a. 2005, S. 39]. Wenn ein Verbraucher diese Anwendungen nutzen möchte, dann braucht er sicherlich auch eine Möglichkeit diese Tags zu deaktivieren.

Ist sich der Verbraucher jedoch bewusst, dass er Produkte mit Tags mit sich führt, aber keine Kenntnis davon hat, dass ein Leser ihn scannt und damit seine Produkte identifiziert, dann wiederum wird es für den Verbraucher sehr schwer zu entscheiden, ob er seine Tags lieber deaktiviert oder ob er den Mehrwert der Tags nutzt. An dieser Stelle müssen dann zusätzliche Schutzmechanismen wirksam werden (siehe Kapitel 3.2).

[Sarma u. a. 2003, S. 465 f.] fasst die allgemeinen Sicherheitsziele wie folgt zusammen: Tags dürfen nicht die Privatsphäre kompromittieren, Informationen dürfen nicht an Unbefugte gelangen und Langzeit-Verbindungen zwischen Mensch und Produkt (*Tracking*) dürfen nicht gespeichert werden. Als möglichen Ansatz führt er einen vom Tag zufällig generierten *Output*, Verschlüsselung und Authentifikation an (siehe Kapitel 3.2).

In [Eicar 2006] beschreibt die *Eicar*[71] *Task Force on RFID* datenschutzrechtliche Aspekte im Zusammenhang mit RFID anhand drei verschiedener Szenarien. Diese Szenarien sind sehr praxisnah und symbolisieren verschiedene Ausprägungen von Verbindungen von Mensch zu RFID-Tag. Jedes Szenario wird zusätzlich anhand der aktuellen Gesetze bewertet, so dass dem Leser schnell deutlich wird, welche Situation welche Rechte und Pflichten beinhaltet.

Im gewerblichen Bereich sind ebenfalls Szenarien denkbar, welche aus Datenschutz-Gründen einer Diskussion würdig sind. Die Firma CityWatcher[72] markiert ihre Mitarbeiter mit dem VeriChip[73], welcher den Zugang zu sicherheitskritischen Räumen und Gebäuden ermöglicht [Schüler 2006]. Diese Markierung geschieht durch eine Injektion des Chips unter die Haut, so dass eine dauerhafte Verbindung zwischen Tag und Mensch vorgenommen wird. Selbstverständlich können diese Mitarbeiter auch außerhalb des Firmengeländes identifiziert werden.

Ein weiteres Beispiel ist das IBM-Produkt[74] RFID Asset Tracking:

[71] Eicar (http://www.eicar.org) ist eine private Organisation, die es sich zur Aufgabe gemacht hat, die Verbreitung von Computer-Viren und anderen schadhaften Code einzudämmen. Der Eicar Test-Virus ist der bekannteste Virus zum Testen eines Virenscanners.
[72] http://www.citywatcher.com
[73] http://verichipcorp.com
[74] http://www.ibm.com

> „Zum Einsatz kommt eine solche Lösung zum Beispiel in der petrochemischen Industrie. Die Einhaltung strenger gesetzlicher Sicherheitsbestimmungen verlangt hier eine permanente Überwachung des Aufenthaltsorts der Mitarbeiter oder wichtiger Betriebsmittel wie Werkzeuge. Das Sicherheitspersonal kann mit Hilfe der IBM Lösung im Notfall die mit einem RFID-Tag ausgestatteten Personen identifizieren und lokalisieren, um sie schnell aus der Gefahrenzone zu evakuieren.“ [IBM 2006]

Diese beiden Beispiele betreffen jeweils sicherheitskritische Lösungen, jedoch gibt es inzwischen auch Einsatzgebiete zur Lokalisierung von Ärzten in Krankenhäusern. Das Ziel ist durch eine zentrale Steuerung der Ärzte eine optimale Versorgung der Patienten zu erreichen. Der Arzt, der gerade keine Behandlung macht und sich örtlich am nächsten zu einem neuen Fall befindet, wird alarmiert und zu dem neuen Fall gebeten. Diese Lösung erhöht die Effizienz z. B. in einer Notfallstation. Die Ärzte hingegen stehen unter ständiger Überwachung der Position und ihrer Verrichtung.

3.1.2 Industriespionage

Eine Gefahr im rein gewerblichen Umfeld ist das Ausspionieren von RFID-Daten der Produkte eines Unternehmens durch die Konkurrenz. Bisher sind Artikel mit ungeschützten Tags ausgestattet und deshalb auch mit handelsüblichen Lesern zu scannen. Aber nicht das einmalige Lesen ist die Absicht der Mitbewerber, sondern das Überwachen und Verfolgen vieler Tags eines Produktes über eine längere Zeit [Weis u. a. 2004, S. 202].

Die SCM-Daten sind für die Mitbewerber von hoher Bedeutung, weil sie einen direkten finanziellen Wert darstellen [Gao u. a. 2005, S. 164]. Ein Beispiel aus der Lieferkette wird in [Garfinkel u. a. 2005, S. 37] vorgestellt. Ein Vertreter könnte die Produkte des Mitbewerbers gleichzeitig in mehreren Geschäften beschaffen und dann die Dynamik beim Auffüllen der Artikel überwachen. Weiterhin könnten ganze Auslagen von Produkten entweder in den Regalen oder schon bei der Anlieferung in den Umverpackungen gelesen werden. Durch die eindeutige Nummerung wird dem Mitbewerber eine ganze Flut von Informationen zugänglich gemacht.

Die Tags müssten durch geeignete Maßnahmen gegen unberechtigtes Lesen geschützt werden. Diese Maßnahmen werden in Kapitel 3.2 angesprochen.

3.1.3 Echtheitsnachweis

Die Industrie hat eine große Nachfrage, ihre Produkte vor Fälschungen zu schützen. Man kann den Begriff „Echtheitsnachweis“ (für Produkte mit RFID-Tag) synonym mit dem Begriff der „Fälschungssicherheit“ verwenden. Den Begriff „Fälschungssicherheit“ trifft man häufig in der Literatur an, jedoch wird bei genauerer Betrachtung nicht die eigentliche Fälschung verhindert, sondern ein Original wird lediglich mit Hilfe von RFID besser von der Fälschung unterscheidbar gemacht.[75]

Tendenziell bieten sich hochwertige und sicherheitskritische Produkte zum Kennzeichnen mit RFID an. Bei hochwertigen Produkten wird der Mehraufwand durch den hohen Preis gerechtfertigt. Die sicherheitskritischen Produkte hingegen werden geschützt, da Fälschungen einen potentiellen Schaden anrichten können und dann Kosten entstehen oder gar Menschen gefährdet werden.

Die amerikanische Lebensmittel und Medikamente Verwaltung des Gesundheitsministeriums (*Food and Drug Administration*, FDA)[76] empfiehlt den Herstellern von Arzneimitteln das Auszeichnen von Verpackungen mit RFID-Herkunftsnachweisen [FDA 2004], um den Echtheitsnachweis zu erbringen. Wie bereits erwähnt, setzt Pfizer für sein Produkt Viagra bereits RFID-Kennzeichnungen auf den Verpackungen ein.

Bei allen Formen des Echtheitsnachweises muss beachtet werden, dass erst nach einem Lesevorgang entschieden werden kann, ob das Produkt echt oder gefälscht ist. Bis zum heutigen Zeitpunkt haben praktisch keine Privatpersonen einen RFID-Leser, so dass die Kontrolle der Medikamente nicht selbst durchgeführt werden kann. Im Fall der Medikamenten-Kennzeichnung muss sich der Verbraucher auf die Apotheker verlassen, der ihnen die Medikamente beschafft. Eine mögliche Lösung wäre ein für den Kunden zugänglicher RFID-Leser in der Apotheke.

Ein weiteres Einsatzgebiet ist die Flugzeugindustrie. Flugzeugteile werden mit Tags versehen, um die Herkunft und Echtheit festzustellen. Zusätzlich werden die Tags dann dazu verwendet die Wartung zu vereinfachen und Reparaturen schneller zu erledigen. Ebenfalls wurde bereits erwähnt, dass Reisepässe

[75] Die Möglichkeit RFID-Tags zu fälschen wird im weiteren Verlauf des Unterkapitels beschrieben.

[76] http://www.fda.gov

und eventuell sogar Geldnoten mit Tags ausgestattet werden sollen, damit die Echtheit der Dokumente nachgewiesen werden kann.

In [BSI 2004, S. 51] wird die Möglichkeit angesprochen, die Tags zu emulieren. Geräte mit höherer Funktionalität[77] können dazu verwendet werden, das Vorhandensein von echten Tags vorzutäuschen. Dabei kann der Dateninhalt frei gewählt werden. Der Emulator ist zwar deutlich größer als ein Tag, kann aber dafür sehr flexibel eingesetzt werden. Auf diese Weise können Tags kopiert, ausgetauscht oder neu erschaffen werden. Der Leser erkennt den Unterschied nicht. Dieses Verfahren wird bei der Überwindung der Wegfahrsperre von Autos eingesetzt, indem dem Zündschloss ein Schlüssel mit korrekter RFID-ID vorgetäuscht wird.

Das Ändern des originalen Tags, also das Ändern der in den Chip geätzten ID, dagegen ist sehr viel schwerer [TRS 2006]. Das Herstellen von Kopien von Tags oder das Kippen eines einzelnen Bits einer ID kann nur mit Hilfe von sehr teuren, technischen Anlagen zur Chipherstellung realisiert werden. Für nichtindustrielle Personen ist das Kopieren somit so gut wie unmöglich. Also sind *read-only* Tags nicht zu fälschen oder ändern, außer dem bereits erwähnten Einsatz von Emulatoren.

3.2 Möglichkeiten zur Lösung der Kommunikationsbedenken

In vorherigen Kapitel wurden einige der möglichen Bedrohungen beim Einsatz von RFID erwähnt. Diesen Bedrohungen kann jedoch durch verschiedene technische und organisatorische Methoden entgegengewirkt werden. Diese Methoden sind unterschiedlicher Art und werden in diesem Unterkapitel angesprochen. Oft bietet sich der Einsatz verschiedener Lösungen an oder sogar die Kombination von verschiedenen Lösungen. Die Anforderungen eines RFID-Systems bestimmen die zu verwendende Methode und dem damit verbundenen Mehraufwand für die Softwareentwicklung und der technischen Ausstattung. Somit steigert ein erhöhter Sicherheitsgrad meist auch die Kosten des Gesamtsystems.

[77] Die erweiterte Funktionalität besteht darin, dass die ID nicht fest in einen Chip gegossen ist, sondern durch eine variable Schaltung oder Software generiert und an die Spule/Antenne gesendet wird.

3.2.1 Kill-Switch

Der *Kill-Switch* ist eine Möglichkeit einen Tag dauerhaft zu deaktivieren. Dieser gedachte Schalter wird von einem Leser betätigt und muss vom Tag entsprechend quittiert werden. Der Tag wird dadurch nicht physisch zerstört, sondern in einen bestimmten Zustand (z. B. *„killed“*) versetzt. Dieser Zustand wird erreicht, indem bestimmte beschreibbare Bereiche des Tags mit Nullen überschrieben werden. Dadurch ist dann keine Kommunikation mit Lesern mehr möglich. Der ursprüngliche Zustand vor dem Deaktivieren lässt sich nicht mehr wiederherstellen, so dass ein einmal deaktivierter Tag nie wieder zu verwenden ist. Der „EPC Class-1 Gen-2“-Tag[78] ist ein Beispiel eines sehr weit verbreiteten Tags, welcher mit einem *Kill-Switch* ausgestattet ist (siehe Dokumentation des *Kill*-Befehls in [EPC 2005, S. 58]). Bei diesen Tags wird der Schalter jedoch durch ein Passwort geschützt, so dass nicht jeder Leser und Anwender dazu in der Lage ist, die Tags unbrauchbar zu machen.

Mit Hilfe der Deaktivierung von Tags kann man den Sicherheitsansprüchen der Endanwender gerecht werden. Der Tag kann beim Verlassen eines Geschäftes oder Lagers deaktiviert werden, so dass eine spätere Identifizierung nicht mehr möglich ist. Damit ist dann aber klar, dass eventuelle Vorteile der eindeutigen Identifizierung (z. B. Garantieansprüche) nicht mehr genutzt werden können.

Eine weitere Möglichkeit einen Tag zu deaktivieren ist selbstverständlich die physische Zerstörung der Komponenten, also der Spule/Antenne oder des Chips, durch äußere Einflüsse wie z. B. einer Schere oder Zange. Eine verwandte, aber weitaus elegantere Möglichkeit den Tag zu zerstören ist das „Durchbrennen“ von metallischen Komponenten durch die Einwirkung des Feldes eines RFID-Lesers. Bei der Produktion des Tags wird eine Sollbruchstelle vorgesehen, die bei Einwirkung eines sehr starken Feldes schmilzt [vgl. BSI 2004, Kap. 7.7.6.2]. Starke Felder bewirken die Induktion einer hohen Spannung, so dass sich die metallischen Komponenten erwärmen.[79] Besitzt der Tag keine Sollbruchstelle, dann können durch das starke Feld auch andere Komponenten, wie Dioden oder Transistoren, überlastet und damit zerstört werden.

[78] Der UHF „EPC Class-1 Gen-2“-Tag wird von der EPCglobal Inc™ (http://www.epcglobalinc.org) spezifiziert und von vielen verschiedenen Herstellen produziert. Mehr zu dem EPCglobal Inc™ (EPC) Standard im Kapitel 4.

[79] Die Funktionsweise ist mit einer elektrischen Sicherung zu vergleichen. Die Sicherung schmilzt, wenn die Stromstärke im Stromkreis zu groß wird.

3.2.2 Blocker-Tag

Ein Blocker-Tag ist ein spezieller Transponder, der sehr viele Tags zum gleichen Zeitpunkt simuliert. Der Leser bekommt dann bei einem Lesevorgang Antworten von hunderten oder tausenden Tags. Andere Tags, die in der Nähe sind und eigentlich gelesen werden sollen, werden dann zwar auch gelesen, aber der Leser kann diese nicht von den vielen simulierten unterscheiden.[80] Oft sind Blocker-Tags mit aktiver Energieversorgung ausgestattet, damit die Reichweite größer und die Gefahr der Abschirmung geringer wird. Manche Blocker-Tags lassen sich sogar mit den gewünschten Adressbereichen konfigurieren. Da manche Anti-Kollisions-Methoden binäre Suchbäume (siehe 2.2.2) aufbauen, antworten manche Blocker-Tags sogar gleichzeitig mit den beiden möglichen Antworten „0“ und „1“ [BSI 2004, S. 47]. Dies setzt das Vorhandensein von zwei Antennen im Blocker-Tag voraus.

Der Nutzen dieser Blocker-Tags ist jedoch nur räumlich beschränkt und bietet keinen verlässlichen Schutz, da der zu blockende Tag immer noch vorhanden ist und gelesen werden kann. Bewegt sich der Tag außerhalb der Reichweite des Blocker-Tags, dann ist er wieder eindeutig lesbar und der Schutz ist nicht mehr gegeben.

3.2.3 Passwort

Der Zugriff auf Tags kann durch den Schutz mit einem Passwort beschränkt werden. Das Passwort ist dann auf dem Tag abgelegt und muss von dem Leser übermittelt werden, bevor er die ID lesen kann. [Garfinkel u. a. 2005, S. 39] bemerkt dazu, dass dadurch ein paradoxes Problem entsteht, weil der Leser für das richtige Passwort die ID des Tags benötigt, die er ja erst erhält, wenn das Passwort korrekt ist. Entweder muss der Leser dann alle Passwörter ausprobieren oder die Passwörter aller Tags sind identisch. Beide Möglichkeiten sind nicht ideal. Das Testen aller Passwörter kann im Einzelfall zu lange dauern, da sich bewegende Tags schnell außerhalb der Reichweite geraten können. Sind alle Passwörter eines RFID-Systems identisch, dann ist der Schutz der Tags insgesamt natürlich sehr viel geringer, denn das Abhören eines Lesevorgangs kann einem Angreifer das Passwort für alle Tags des Systems beschaffen. Um

[80] Man kann die Situation des blockierten Lesers mit einem *Denial of Service* Angriff vergleichen.

dem entgegenzuwirken müsste die Kommunikation verschlüsselt sein und ein zufälliges Element enthalten, damit die bei statischer Verschlüsselung denkbaren Replay-Attacken nicht mehr möglich sind.

Denkbar ist der Einsatz von Tags mit einfachem Passwortschutz in kleinen, überschaubaren Umgebungen, damit das aufwändige Passwort-Management nicht zu komplex wird. Somit bieten sich kleine Geschäfte außerhalb der Lieferkette oder private Haushalte für diese Lösung des Schutzes der RFID-Tags an.

3.2.4 Kryptographie

Den effektivsten, aber auch aufwändigsten, Schutz vor ungewolltem Auslesen der Tags bieten kryptographische Methoden. Mit Hilfe von Authentifikation und Verschlüsselung kann die Kommunikation zwischen Leser und Tag für potentielle Angreifer fast unüberwindbar gestaltet werden. Im vorherigen Unterkapitel wurde die einfachste Form der Authentifikation – der Passwortschutz – bereits vorgestellt. [Sarma u. a. 2003, Kap. 4.4] stellt einen solchen Ansatz vor, weist aber gleichzeitig auf die bereits genannten Nachteile, wie z. B. die fehlende Dynamik, hin.

Durch die Authentifikation des Lesers soll der Tag feststellen können, dass der Leser berechtigt ist, die Daten des Tags zu erhalten oder zu verändern. Die Verschlüsselung dagegen sorgt dafür, dass Dritte die übertragenen oder gespeicherten Daten nicht interpretieren können. Im Allgemeinen werden zu beiden Zwecken Schlüssel (*keys*) verwendet. Diese sind spezielle Zeichenfolgen, die nach Prüfung durch mathematische Berechnungen den Zugriff gewähren oder verweigern. Diese Berechnungen heißen Verschlüsselungsalgorithmen.

Nach [Garfinkel u. a. 2005, S. 39] stellen sich damit den Entwicklern dieser Systeme zwei grundlegende Probleme. Erstens müssen diese Schlüssel verwaltet werden (*Key Management*) und zweitens sollte die Verschlüsselung dynamisch und nicht statisch sein, damit – wie bereits im vorherigen Kapitel angesprochen – die Gefahr von Replay-Attacken vermieden wird. Dynamisch wird die Verschlüsselung dann, wenn sich die übertragenen Daten durch ein veränderliches Element von einem Lesevorgang zum nächsten verändern, obwohl dann

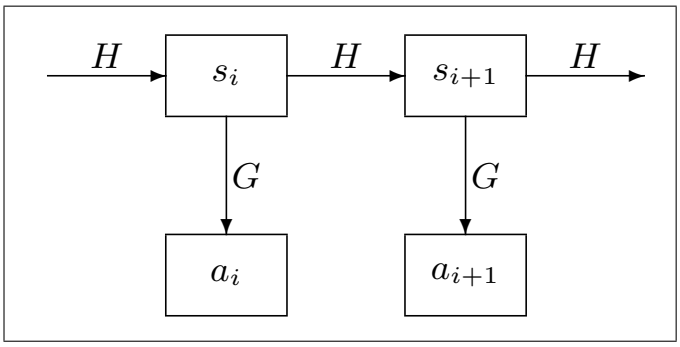


Abbildung 3.1: *Hash-Chain*: Tag berechnet Antwort an Leser und neues Geheimnis [Ohkubo u. a. 2003, Abb. 1].

nach der Entschlüsselung dieselben Daten vorliegen. In der Regel wird diese Veränderung durch Zufallszahlen[81] erreicht.

Grundsätzlich kann man zwischen zwei verschiedenen Arten von Systemen unterscheiden. *Off-Line*-Systeme brauchen für die Authentifikation und Verschlüsselung lediglich den Tag und den Leser. Die Kommunikation geschieht nur dezentral zwischen diesen beiden Komponenten. Bei *On-Line*-Systemen hingegen wird für gewisse Berechnungen oder den Erhalt von Schlüsseln das Backend benötigt. Der Leser muss also während des Lesevorgangs zusätzlich mit dem Backend kommunizieren. Im Folgenden wird für beide Arten stellvertretend jeweils ein Verfahren vorgestellt.

In [Ohkubo u. a. 2003, Kap. 4] wird ein *On-Line*-Verfahren für kostengünstige Tags vorgeschlagen. Dabei werden drei wichtige Ziele verfolgt, die neben dem geringen Preis für die Tags zur Sicherheit beitragen: die Ununterscheidbarkeit zwischen zwei Tags, die Ununterscheidbarkeit zwischen zwei verschiedenen Antworten eines Tags sowie die *Forward-Security*. *Forward-Security* bedeutet, dass vergangene Antworten der Tags nicht mehr konstruiert werden können. Eine Historie, welche beim *Tracking* hilfreich ist, wird somit unmöglich. Erreicht wird dies durch einen *Hash-Chain*-Algorithmus[82] (siehe Abbildung 3.1).

[81] Genau genommen sind die Zufallszahlen nicht wirklich zufällig, sondern sie werden deterministisch durch einen Algorithmus und/oder mit dem Eingangsparameter Uhrzeit berechnet. Deswegen spricht man dann auch von „Pseudo-Zufallszahlen“.

[82] Ein *Hash*-Algorithmus berechnet aus einem Eingabewert ein Ergebnis, von dem man nicht auf den Eingabewert schließen kann. Da diese Algorithmen nur „in eine Richtung“ funktionieren, werden die *One-Way*-Algorithmen genannt. *Chain* bedeutet, dass mehrere Durchläufe dieser Algorithmen hintereinander ausgeführt werden.

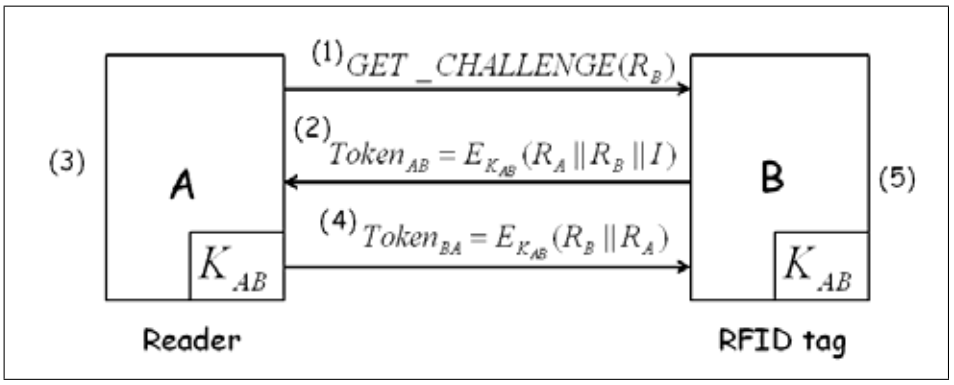


Abbildung 3.2: *Three-pass*-Authentifikation zwischen Tag und Leser [Chang 2005, Abb. 1].

Auf dem Tag werden zwei verschiedene *Hash*-Algorithmen G und H sowie eine initiale Zeichenkette s_1 (*secret*) abgespeichert. Beim i-ten Lesevorgang berechnet der Tag die Antwort $a_i = G(s_i)$ (*answer*) und sendet diese an den Leser. Sofort im Anschluss wird der neue Wert $s_{i+1} = H(s_i)$ berechnet. Dieser ersetzt den alten Wert s_i im Tag. Der Leser sendet die Antwort a_i an das Backend, welches aus allen bekannten Geheimnissen s der Tags mit Hilfe der beiden Funktion G und H die Werte $a'_i = G(H^i(s_1))$ berechnet. Findet das Backend einen Wert a'_i mit $a'_i = a_i$, dann ist der Tag identifiziert und der Leser kann mit der gewünschten ID des Tags versorgt werden.

Grundlage der gegenseitigen Authentifikation ist die beiderseitige Kenntnis der beiden Funktionen G und H sowie der initialen Geheimnisse s_1. In der Praxis wird das Backend aus Performanz-Gründen das letzte s_i speichern, um beim nächsten Lesevorgang nur einen linearen Aufwand zur Berechnung zu haben. Der Tag muss Berechnungen ausführen können und wiederbeschreibbaren Speicher besitzen. Nach einem Lesevorgang (Antwort a_i) kann eine Replay-Attacke ausgeschlossen werden, weil erstens s_{i+1} neu berechnet wird und zweitens ausgehend von einem abgefangenen a_i und der Kenntnis von G und H kein a_{i+1} konstruiert werden kann (*Hash*-Algorithmus).

[Chang 2005] stellt ein kryptographisches Verfahren mit dezentralem Charakter vor. Die Authentifikation wird über ein *Challenge-Response*-Verfahren[83]

[83] Beim *Challenge-Response*-Verfahren wird der zu authentifizierende Kommunikationspartner durch die *Challenge* aufgefordert sich zu authentifizieren. Anschließend antwortet dieser mit der *Response*. Diese Antwort wird ausgewertet und dann wird entscheiden, ob die Authentifizierung erfolgreich war.

nach dem Prinzip der *three-pass mutual*-Authentifikation vorgenommen (siehe Abbildung 3.2). Sowohl Tag als auch Leser besitzen den gleichen Schlüssel K_{AB} und verwenden den identischen Verschlüsselungsalgorithmus $E_{K_{AB}}$. Die Schritte sind im Einzelnen:

1. Der Leser generiert die Zufallszahl R_B und überträgt sie zum Tag.
2. Der Tag erstellt ebenfalls eine Zufallszahl R_A und berechnet das $Token_{AB} = E_{K_{AB}}(R_A \| R_B \| I)$. I ist ein Kontrolldatum, um Replay-Attacken durch mehrere identische *Challenges* zu verhindern.[84]
3. Der Leser empfängt das $Token_{AB}$ und berechnet nach der Entschlüsselung und Verifikation der Zufallszahl R_B den gemeinsamen Schlüssel K_{AB}. Anschließend wird überprüft, ob die Schlüssel von Leser und Tag übereinstimmen.
4. Der Leser berechnet $Token_{BA} = E_{K_{AB}}(R_B \| R_A)$ und sendet es zum Tag.
5. Der Tag entschlüsselt und verifiziert ebenfalls das Token. Somit sind beide Partner gegenseitig authentifiziert.

Die verwendete Verschlüsselung ist die Stromverschlüsselung[85] (*Stream-Cipher*) A5/1. Der Algorithmus kann leicht und mit wenigen Gattern[86] realisiert werden, so dass sich der Einsatz in RFID-Tags anbietet.

Optional schlägt Chang als drittes Sicherheitsmerkmal eine Schlüssel-Diversifikation (*key diversification*) vor. Da alle Tags den identischen Schlüssel K_{AB} besitzen, besteht die Gefahr, dass nach einem erfolgreichen Angriff auf den Schlüssel (z. B. durch eine *Brute Force*-Attacke[87]), alle Tags ausgelesen

[84] Ist der Wertebereich der Zufallszahlen nicht besonders groß, dann ist die Wahrscheinlichkeit, dass der Tag erneut die Zufallszahl R_A generiert, nicht ausreichend gering. Ein Angreifer könnte so lange die *Challenge* R_B an den Tag senden, bis dieser mit der Zufallszahl R_A antwortet. Würde das Kontrolldatum I fehlen, dann müsste der Angreifer nur die Antworten vergleichen und das abgehörte $Token_{BA}$ an den Tag senden. Somit wäre dann die gegenseitige Authentifikation ohne die Kenntnis des Schlüssels gelungen. Bei ausreichend großen Zufallszahlen könnte auf das Kontrolldatum verzichtet werden.

[85] Bei der Stromverschlüsselung wird die Nachricht bitweise durch eine Funktion und anschließendes XOR verschlüsselt.

[86] Ein Gatter ist eine digitale Schaltung, die eine logische Operation ausführen kann, z. B. UND, ODER, NICHT oder XOR.

[87] Bei einer *Brute Force*-Attacke werden nacheinander alle möglichen Zeichenkombinationen ausgetestet. Dieses Vorgehen dauert üblicherweise sehr lange und kann durch lange Schlüssel und ein großes Alphabet erschwert werden

werden können. Aus diesem Grund hat jeder Tag einen eigenen Schlüssel, der mit Hilfe der Tag-ID, eines *Master*-Schlüssels im Leser und einem weiteren Algorithmus berechnet werden kann. Zunächst fragt der Leser nach der Tag-ID, berechnet dann den Schlüssel des Tags und stößt schließlich die bereits erklärte *three pass*-Authentifikation an. Somit wird die Sicherheit der Daten auf dem Tag wesentlich erhöht, jedoch kann die ID des Tags immer ohne Probleme ausgelesen werden.

Die von Chang vorgeschlagene Methode ist von größerer Sicherheit, setzt aber hohe Ansprüche an die zu verwendenden Tags (Speicher, Zufallszahlengenerator, Chip für Authentifikation und Verschlüsselung). Diese hohen Ansprüche machen sich natürlich durch höhere Kosten als bei einfachen Tags bemerkbar. Bei dieser wie auch bei fast jeder anderen Entscheidung bestimmen die Anforderungen der Anwendung den notwendigen und hinreichenden Sicherheitsgrad des RFID-Systems.

Ein weiteres Beispiel für eine Möglichkeit zur Authentifikation ist das Hopper-Blum-Protokoll [Weis 2005, Kap. 4]. Weis stellt das Verfahren, welches auf dem LPN-Problem[88] basiert, als Alternative zu aufwändigen und damit teuren Verfahren vor. Die Tags brauchten lediglich wenig Speicher und müssten nur XOR, AND und Zufallszahlen berechnen. In [Hopper und Blum 2001] wird diese Authentifikation genauer erläutert.

Selbstverständlich ist auch der Einsatz von *Public Key*-Infrastrukturen[89] (PKI) denkbar. Da jedoch dafür relativ viele Anforderungen an die Tags gestellt und damit die Preise für Tags deutlich höher werden, ist die Verbreitung eher gering [Sarma u. a. 2003, S. 466]. Allerdings gibt es im HF-Bereich den Anbieter NTRU[90], der mit GenuID eine komplette Lösung inklusive Tags, Leser und Schlüssel-Verwaltung anbietet.

[88] Das *learning parity with noise* Problem bedarf weniger Rechenschritte und kann ja nach Schlüssellänge im Kopf berechnet werden. Mehr dazu in [Hopper und Blum 2001, Kap. 3.1]

[89] *Public Key*-Infrastrukturen benutzen zur Verschlüsselung einen öffentlichen Schlüssel und einen privaten Schlüssel zum Dekodieren von Informationen (asymmetrische Verschlüsselung). Diese Methode gilt als sehr sicher und wird häufig zur Datenübertragung im Internet verwendet.

[90] http://www.ntru.com

3.2.5 Antennen-Energie-Analyse

In [Fishkin und Roy 2003] wird ein völlig anderer Ansatz verfolgt, um festzustellen, ob ein Leser berechtigt ist, Informationen von einem Tag zu erhalten. Unter der Annahme, dass „gute“ Leser in der Regel näher am Tag sind als „böse“ (*distance implies distrust*), wird die Authentifikation aufgrund verschiedener Messwerte der Felder getroffen. Diese Messwerte sind z. B. *Received Signal Strength*[91] (RSS) oder *Signal/Noise-Ratio*[92] (SNR, S/N). Stellt ein Tag fest, dass ein Leser zu weit weg ist, dann bekommt der Leser gar keine oder nur wenige Informationen gesendet. Zusätzlich schlagen die Autoren vor, eine mehrstufige Einteilung der Abhängigkeit von Informationsausgabe zu Entfernung zu unternehmen. Gepaart mit zusätzlichen Authentifikationsmethoden entscheidet nicht allein die Entfernung des Lesers über die Menge an Daten, die dem Leser zu Verfügung gestellt wird. Allerdings werden auch Vorbehalte gegen diese Methode angeführt. Da die Orientierung des Tags im Raum direkten Einfluss auf die Energieaufnahme hat, verändert eine andere Orientierung auch die Messwerte des Feldes. Weiterhin sind die emittierten Felder nicht perfekt, so dass Schwankungen und äußere Einflüsse die Messungen beeinflussen können.

Diese Methode wurde bis jetzt lediglich im Labor getestet und ist noch keineswegs ausgereift. Die Annahme, dass nähere Leser eher berechtigt sind als entfernte, bedarf sicherlich einer Diskussion, denn dies gilt nicht für jede Anwendung. Da viele Anwender die zu geringe Reichweite als großes Manko ansehen (siehe Kapitel 2.2.1), sollte die Reichweite nicht noch durch die Antennen-Energie-Analyse beschränkt werden.

3.2.6 Richtlinien

Bislang wurden meist technische Lösungen für die Datenschutz-Problematik vorgeschlagen. Inzwischen werden aber auch Stimmen laut, die einen anderen Umgang mit den RFID-Problemen fordern. Seit ca. 1970 werden die Prinzipien des „Fair Information Practices“ (FIP) immer wieder neu aufgelegt. Darin

[91] Die beim Empfänger erreichte Signalstärke des Feldes wird in vielen kabellosen Netzwerken als Indikator für die Auswahl des günstigsten Kanals verwendet. In diesem Fall dient die Größe als ein Indikator für die Entfernung der Feld-Quelle.

[92] Das Signal-Rausch-Verhältnis (oder Signal-Rauschabstand) ist ein Maß für die Qualität eines Signals. Je höher das SNR, desto geringer ist die Fehlerrate. Die Einheit ist Dezibel (dB).

enthaltene, grundlegende Punkte betreffen die Transparenz der Lesevorgänge und Verwendung der Daten [BSI 2004, Kap. 7.7.7], also die Einführung von Gesetzen oder Richtlinien, die den Umgang mit RFID-Systemen einschränken.

Floerkemeier et al. schlagen Modifikationen auf der untersten Ebene der RFID-Protokolle vor, um den Prinzipien der Beschränkung von Datensammlungen, Zweckgebundenheit, Offenheit und Verantwortlichkeit gerecht zu werden. Selbstverständlich können damit unerwünschte Lesevorgänge – und damit potentieller Missbrauch – nicht gänzlich ausgeschlossen werden, aber durch den vorgeschlagenen Einsatz von *Watchdog-Tags* könnten sie besser sichtbar gemacht werden. *Watchdog-Tags* sind erweiterte mit Batterie und Bildschirm ausgestattete Tags, die alle Lesevorgänge registrieren und nicht dem Protokoll entsprechende Operationen anzeigen.

In [Garfinkel u. a. 2005, S. 41 f.] weist der Autor auf seine selbst verfassten *„RFID Bill of Rights“* hin, welche sich hauptsächlich auf die Rechte der Verbraucher beim Kauf von RFID-markierten Produkten konzentrieren. Dies sind im Einzelnen die Rechte: Wissen über Kennzeichnung, Entfernung des Tags, Alternativen zu RFID, Kenntnis über die Inhalte der Tags und Benachrichtigung bei einem Lesevorgang (z. B. Blinken, Piepton).

Ähnliche Ziele, jedoch noch etwas weiter gehend, formuliert [McCullagh 2003]. Er formuliert nicht die Rechte des Verbrauchers, sondern macht vier Vorschläge, wie mit RFID-Tags in der Praxis umzugehen sei. Erstens sollten Verbraucher beim Kauf auf RFID-Tags hingewiesen werden. Zweitens sollten die Tags standardmäßig beim Kauf deaktiviert werden. Drittens sollten Tags an der Verpackung und nicht am Produkt selbst angebracht werden. Viertens sollten Tags gut sichtbar und einfach zu entfernen sein.

Das *Center for Democracy and Technology*[93] (CDT) stellt in seinem Richtlinienkatalog die aktuellste der bereits genannten Sammlungen von Prinzipien und Praxisverfahren vor [CDT 2006]. Dabei werden drei grundlegende Prinzipien herausgearbeitet, die bei der Auseinandersetzung mit den Bedenken gegenüber RFID-Anwendungen helfen könnten. Das Prinzip der Technologie-Neutralität betont, dass Technologie an sich keine Sicherheitsbedrohung sein kann. Das Prinzip der Privatsphäre und des Datenschutzes als grundlegende Entwurfsvoraussetzung soll Entwickler dazu anhalten, mit Beginn jeglicher Entwicklungen immer die Sicherheitsbedürfnisse aller Parteien zu beachten.

[93] http://www.cdt.org

Schließlich wird das Prinzip der Transparenz angeführt, das Verbraucher vor verborgenen Tags oder Lesern schützen soll. Im letzten Teil des Katalogs werden *Best Practice* Vorschläge gemacht, welche konkrete Anhaltspunkte für Hersteller und Betreiber von RFID-Systemen sein sollen. Diese Vorschläge fallen in die Bereiche Kenntnis, Auswahlmöglichkeit und Einwilligung, Datenweitergabe, Zugriff und Sicherheit.

Alle diese Ansätze verfolgen das Ziel verschiedene, beteiligte Parteien für den sorgfältigen Umgang mit RFID-Daten zu sensibilisieren. Hersteller und Betreiber von RFID-Systemen sollen sich dazu verpflichten, die Rechte der Verbraucher nicht zu ignorieren. Verbraucher müssen über die Gefahren und Potentiale von RFID aufgeklärt werden, damit sie für sich individuell entscheiden können, welcher Grad an Freiheit oder Mehrwert für sie in Frage kommt. Jeder dieser Ansätze kann vielleicht in für alle Beteiligten verbindliche Gesetzte gefasst werden. Trotzdem bleibt die schwierige Nachweisbarkeit von ungesetzlichem Umgang mit den Daten. Dies wird Parteien mit geringem Verständnis für den Datenschutz auch nicht davon abhalten, Daten zu sammeln und daraus z. B. individuelle Profile zu erstellen.

3.3 Gefahr von Virenverbreitung

Im März 2006 veröffentlichte die Computer Systems Group der Vrijen Universiteit in Amsterdam einen Artikel, in dem die Gefahr der Verbreitung von Viren über RFID-Tags diskutiert wird [Rieback u. a. 2006, Kap. 4]. In der Dokumentation eines praktischen Feldversuches wurden auf dem Tag nicht nur einfache Daten, sondern auch SQL-Anweisungen[94] abgelegt. Diese Anweisungen wurden an das Backend übertragen und dort ausgeführt. Der Virus war – genauer gesagt – ein Wurm, der seine eigenen SQL-Anweisungen in alle Datensätze der anderen Tags kopierte. Diese *SQL injection attack* sah ebenfalls das unbemerkte Beschreiben von neuen Tags vor, so dass sich der Wurm weiter hätte ausbreiten können.

Anders als die bisherigen Szenarien geht in diesem Fall die Gefahr nicht von der Kommunikation aus, sondern von den auf den Tag abgelegten Daten, also den Inhalten an sich. Daraus schließen die Autoren auf einer Website der

[94] Die *Structured Query Language* ist eine ANSI-standardisierte Datendefinitions- und Datenmanipulationssprache für relationale Datenbanken.

Arbeitsgruppe[95], dass wenn bestimmte Schwachstellen in der RFID-Software bestehen, dann könnten Tags vorsätzlich mit einem Virus infiziert werden. Damit seien auch die Datenbestände des Backends gefährdet.

Bereits am nächsten Tag der Veröffentlichung reagierten verschiedene Hersteller und Mitglieder von RFID-Organisationen. In [Mullen 2006] relativiert der Autor die Bedrohung. Viele Annahmen übersähen eine Anzahl von notwendigen und fundamentalen Entwurfsmerkmalen in Systemen zur Datensammlung und Datenbanken. Mit anderen Worten: die Forscher bauten ein System mit Schwachstellen und zeigten dann, wie man diese Schwachstellen per *Exploit*[96] ausnutzt. Es sei nicht überraschend, wenn schlechte Systementwürfe, unabhängig davon ob die Daten per RFID, Barcodes oder manuelle Eingaben gesammelt werden, Anfälligkeiten zur Folge hätten.

Sicherlich müssen die Ergebnisse des Feldversuchs relativiert werden. In diesem Fall wurden RFID-Tags lediglich als Träger von Code missbraucht. Die Anfälligkeiten des gesamten Systems liegen am Backend. Gewissenhafte Entwickler verwenden nicht jegliche Eingaben ohne vorherige Prüfung. Es gibt eine Vielzahl von Prüfungen, die auch in dem Kapitel 7 des Artikels von Rieback et al. genannt werden.

Abgesehen davon stellt William Colleran (Impinj[97]) in [RFID Update 2006a] fest, dass RFID-Tags per Definition nur Daten enthalten und niemals Anweisungen.[98] Dies sei anders als bei E-Mails, in welche Skripte und Anwendungscode eingefügt werden könne.

Zusammenfassend kann man sagen, dass die Gefahr der Virenverbreitung sehr gering ist. Sollte durch Daten auf RFID-Tags gefährlicher Code auf das Backend gelangen und dort ausgeführt werden, so liegt die Schwachstelle nicht an der RFID-Technik, sondern an der Software auf dem Backend. Dieser Artikel von Rieback sorgte für lebhafte Diskussionen und dürfte lediglich dazu beigetragen haben, dass Hersteller und Betreiber von RFID-Backends ihre Produkte auf Schwachstellen untersuchten.

[95] http://www.rfidvirus.org

[96] Ein *Exploit* ist ein Programm, welches eine Sicherheitslücke in Software ausnutzt. Dies kann ein *Denial of Service* Angriff, das Erlangen von Rechten oder der Absturz des Zielsystems sein.

[97] http://www.impinj.com

[98] In Zukunft wäre eine andere Definition der gespeicherten Daten denkbar. Die Verbreitung von Anweisungen auf Tags könnte eine sinnvolle und gewünschte Funktion werden.

3.4 Umweltbelastung durch falsche Entsorgung

Anders als Barcodes, die nur auf Oberflächen oder Papieretiketten gedruckt werden, bestehen RFID-Tags nicht nur aus dem Trägermaterial, sondern zusätzlich auch aus dem *Inlay*. Das *Inlay* besteht heutzutage aus metallischen Komponenten. In der Regel sind dies die Elemente Silizium, Kupfer, Blei, Aluminium und Silber, welche nicht in den Hausmüll gehören, da sie eine gesonderte Entsorgung, wie z. B. Elektronik-Schrott, benötigen. Ein einzelnes *Inlay* besteht zwar nur aus weniger als einem Gramm metallischer Elemente, aber sollte sich RFID großflächig bei jeglichen Konsumprodukten durchsetzen, dann summiert sich dieser Metall-Anteil auf Größenordnungen von Tonnen.

Ein weiteres Problem ist die Integration von Tags in Verpackungen oder Produkte. In diesen Fällen sind die Tags von außen nicht erkennbar, und es wird schwierig die Tags vom Objekt zu trennen. Weiterhin haben aktive Tags auch eine Batterie zur Stromversorgung, welche dann ebenfalls fälschlicherweise in den normalen Müll geraten könnte. Die amerikanische Umweltbehörde *Office of the Environmental Executive*[99] (OFEE) warnt vor Schäden an Klär- und Müllverbrennungsanlagen [Weiss und Müller 2005], was zur Folge haben könnte, dass Trinkwasser an Qualität verliert. Diese Warnung ist jedoch nicht akut und auch noch nicht belegbar, da noch nicht absehbar ist, welche Materialien in welchen Mengen die Entsorgung beeinflussen werden.

Aus diesem Grund – und auch anderen, wie z. B. geringere Herstellungskosten oder Schaffung neuer Einsatzgebiete – versucht die Forschung und Industrie neue Materialien zu entwickeln, die die Metalle ersetzen könnten. Zurzeit sind Materialien auf Polymerbasis die wahrscheinlichsten Substitute für die metallischen Elemente. Beispielsweise vereinigt das Konsortium PolyApply[100] einige namhafte Hersteller aus der Halbleiter-Branche. Allerdings ist auch die Entsorgung von Polymeren nicht ganz unumstritten. Bei der Verbrennung von Polymeren können giftige Gase oder Dioxine entstehen.

Andererseits kann die RFID-Technologie auch in der Abfallwirtschaft von Nutzen sein [Environmental Studies 2006]. Durch die eindeutige Kennzeichnung können die Objekte schneller und genauer erkannt und damit auch besser recycelt werden.

[99] http://www.ofee.gov
[100] http://www.polyapply.org

3.5 Strahlungseinflüsse

Da RFID eine Funktechnologie ist, werden nicht nur die Tags den elektromagnetischen Feldern ausgesetzt, sondern auch die Menschen in der Reichweite der Leser. Verschiedene Faktoren beeinflussen die Belastung der Strahlung auf den menschlichen Organismus.

Die wichtigste Größe ist die Intensität der Strahlung. Die Intensität[101] von RFID-Strahlung ist relativ gering und gehört somit zu der Gruppe der „nicht ionisierenden Strahlung“[102] (NIS). Weitere Vertreter von NIS sind Funkwellen (Radio, Fernsehen, Mobilfunknetze, Datenfunknetze), Mikrowellen oder Licht. Das Maß für die Exposition[103] von Körpergewebe ist die spezifische Absorptionsrate (SAR) mit der Einheit Watt/Kilogramm (W/kg) [Hilty u. a. 2003, S. 240]. Ist die Exposition hoch, dann wird die Strahlung im Gewebe in Wärme umgewandelt. Durch die Erwärmung können Schädigungen des Gewebes auftreten (bei ca. 100 W/kg), so dass der Grenzwert auf 2 W/kg festgelegt wurde [Hilty u. a. 2003, S. 240]. Dieser Grenzwert gilt sowohl für RFID-Systeme als auch für Mobilfunknetze. Da bei dieser geringen SAR keine thermischen Effekte auftreten, untersucht die Wissenschaft die Risiken der athermischen Effekte [Hilty u. a. 2003, S. 240]. Allerdings konnten bis heute keine Aussagen darüber gemacht werden, ob die in den Studien beobachten Wirkungen auf die Probanden auf die elektromagnetische Strahlung zurückzuführen ist [Hilty u. a. 2003, S. 241].

Eine weitere, die Belastung beeinflussende Größe ist der Abstand des Menschen von der Quelle, da die Intensität mit dem Abstand abnimmt. [Hilty u. a. 2003, S. 240] führt an, dass 50 % der Strahlung vom Gewebe absorbiert wird, wenn der Mensch eine Strahlungsquelle direkt auf der Haut trägt. Bei einem Implantat sind dies dann fast 100 %. Elektromagnetische Felder nehmen quadratisch zum Abstand von der Quelle ab, so dass die Belastung ebenfalls quadratisch abnimmt.

[101] Intensität ist die Energie der Strahlung pro Zeit und Fläche. Sie berechnet sich aus der zeitlich gemittelten Energiefluss multipliziert mit der Geschwindigkeit der Strahlung (elektromagnetische Strahlung hat Lichtgeschwindigkeit).

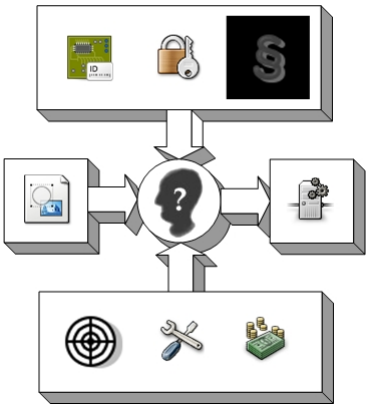
[102] Bei der Ionisierung werden Molekülen durch das Auftreffen von Strahlung Elektronen entrissen, so dass zwei oder mehrere geladene Teilchen (Ionen) entstehen. Zu ionisierender Strahlung gehören Strahlung radioaktiver Stoffe, Röntgenstrahlung und kosmische Strahlung.

[103] Als Exposition bezeichnet man die Aussetzung von Menschen gegenüber gefährlichen oder gesundheitsschädlichen Umweltbedingungen.

Schließlich beeinflusst die Dauer des Aufenthalts innerhalb der elektromagnetischen Strahlung die Belastung des Organismus. Bei RFID-Lesevorgängen werden die Felder nur für kurze Zeit aufgebaut, so dass dann die Exposition nur kurz ist. Bei anderen Funktechnologien, wie z. B. WLAN, werden die Felder konstant aufrechterhalten. Allerdings sind stationäre Leser oft so konfiguriert, dass sie ständig aufeinander folgende Lesevorgänge ausführen, um in Reichweite befindliche Tags zu scannen. Halten sich Menschen ständig in der Umgebung dieser Leser auf, dann sind diese Menschen auch einer höheren Menge an Strahlung ausgesetzt. Beispiele dafür sind Verkäufer an Supermarkt-Kassen oder in Reichweite der Lesern in den Regalen sowie Lageristen auf Gabelstaplern.

Kapitel 4

Standardisierung – Notwendigkeit und Wirklichkeit



Standardisierung ist bei jeglicher Form von Kommunikation zwischen zwei oder mehreren Partnern von enormer Bedeutung. Je nach Ausprägung der Kommunikation ist die Einhaltung von gemeinsamen Regeln die Grundlage für eine erfolgreiche Verständigung. Zwei Menschen können auf verschiedene Arten direkt kommunizieren. In den meisten Fällen geschieht dies durch eine Sprache. Diese Sprachen können bei Menschen verbale oder visuelle Sprachen (z. B. Zeichensprache, Gebärdensprache) sein. Dabei wird zwischen der Syntax[104] und der Semantik[105] von Elementen der Sprache unterschieden. In der Informatik wird eine solche gemeinsame Sprache zwischen zwei Kommunikationspartnern Protokoll genannt.[106] In der Regel werden Protokolle für die elektronische Kommunikation zwischen zwei oder mehreren elektronischen Geräten oder Programmen eingesetzt.

Da RFID als Funktechnologie ebenfalls Kommunikation betreiben muss, erfordert diese Technik ebenfalls Protokolle. Jedes RFID-System hat ein bestimmtes Protokoll nach dem die beteiligten Komponenten kommunizieren.

[104] Syntax beschreibt den formalen Aufbau, die Struktur, die Zusammenstellung oder die Beziehungen von/zwischen verschiedenen Sprachelementen.

[105] Die Semantik ist die Bedeutung oder Interpretation von Sprachelementen.

[106] Zu einem Protokoll gehören zusätzlich zu der Syntax und der Semantik noch Zeit-Bedingungen (*Time Constraints*), z. B. *Timeouts*.

Jeder Hersteller kann für sein Produkt ein eigenes Protokoll entwickeln. Allerdings könnte ein Hersteller auch bereits fertig entwickelte Protokolle benutzen, welche in der Praxis bereits erfolgreich eingesetzt werden. Standardisierungsorganisationen entwickeln z. B. Protokolle und stellen sie der Allgemeinheit zur Benutzung zur Verfügung.[107] Ist ein Protokoll ausgiebig getestet und allgemein anerkannt, dann kann es durch eine Standardisierungsorganisation zu einem Standard[108] erklärt werden. Ob sich dieser Standard langfristig durchsetzt ist allerdings dann noch nicht sichergestellt.

Obwohl RFID schon seit etlichen Jahrzehnten eingesetzt wird, gibt es noch keinen weltweiten eingesetzten Standard, der von allen Parteien akzeptiert und für alle Anwendungen brauchbar ist. Wenn RFID den endgültigen Durchbruch immer noch nicht geschafft hat, wo liegen die Gründe dafür? Worauf warten die Standardisierungsorganisationen, Hersteller und Betreiber? Die technischen Möglichkeiten wurden bereits in Kapitel 2.2 angesprochen, die Kosten werden wahrscheinlich weiter sinken, aber welchen Einfluss haben die bisher fehlenden Standards auf die erst langsam weichende Zurückhaltung der genannten Parteien?

4.1 Aufgabe und Bedeutung von Standards

Die Bedeutung von Standards ist häufig abhängig von der Reichweite der umzusetzenden Anwendung. Soll ein System jeglicher Technik in einem kleinen, abgeschlossenen Rahmen eingesetzt werden, dann spielt der Grad der Standardisierung keine besonders große Rolle. Kommuniziert das System jedoch mit anderen Systemen, gar mit Systemen von externen Parteien, dann gewinnen Standards zunehmend an Bedeutung. In den folgenden Abschnitten werden die wichtigsten, allgemeinen Gründe dafür genannt.

4.1.1 Ökonomische Faktoren

Durch Standardisierung wird eine Vereinheitlichung von verschiedensten Komponenten geschaffen. Sowohl die Komponenten selbst als auch die Kommunikation zwischen den Komponenten wird vereinheitlicht. Die Folge dessen ist ei-

[107] Unter Umständen müssen die Hersteller oder Anwender diese Protokolle käuflich erwerben.
[108] Standards gibt es nicht nur in der Informatik, sondern auch in vielen Bereichen der Technik und Industrie.

ne gewisse Austauschbarkeit zwischen den Produkten verschiedener Hersteller. Dadurch nimmt die Vielfalt der am Markt befindlichen Produkt-Ausprägungen ab, so dass der Markt segmentiert[109] wird. Der resultierende Effekt ist ein steigender Wettbewerb zwischen den Anbietern, was zu sinkenden Preisen und steigender Nachfrage führt. Damit erreichen die Verbraucher eine gewisse Unabhängigkeit und können unter den Herstellern das günstigste Angebot auswählen. Die Hersteller hingegen sprechen einen großen Teil des Marktes an und können in großen Stückzahlen produzieren, was zu den erwünschten Skaleneffekten führen kann.

4.1.2 Investitionssicherheit

Gerade während der Konzeption und vor der Einführung neuer Technologien muss eine Entscheidung für ein bestimmtes Produkt oder eine bestimmte Lösung getroffen werden. Je nach Anwendungsfall ist das Unternehmen gut beraten, wenn das gewählte Produkt einem Standard entspricht, der auch noch in der Zukunft besteht und zusätzlich weit verbreitet ist. Wird ein falscher Standard gewählt, dann ist ein späterer Wechsel auf ein Produkt eines anderen Standards aufwändig und vor allem kostenintensiv. Häufig sind zukünftige Entwicklungen nicht vorhersehbar, so dass bei strategischen Entscheidungen immer ein gewisses Risiko besteht. Dieses Risiko kann einer der Gründe sein, warum ein Entscheidungsträger zunächst einmal die Entwicklung abwartet und vorerst keine Auswahl trifft. Stellt sich im späteren Verlauf heraus, dass die getroffene Entscheidung richtig und wirtschaftlich war, dann war auch die Investition in diesen einen Standard korrekt. Zusammenfassend kann man sagen, dass gute, weit verbreitete und starke Standards als Motivation zur Einführung dienen und zur Investitions- und Zukunftssicherheit beitragen.

4.1.3 Kooperation

Kommunikation und Transaktionen zwischen zwei verschiedenen Parteien werden auf der operativen Ebene einfacher, wenn beide Parteien die gleichen Standards verwenden. Interorganisationale Kooperationen werden somit gefördert. Die verwendeten Komponenten sind im günstigsten Fall selbstständige Module eines ganzen Netzes von kooperierenden Parteien. Definierte Schnittstellen

[109] Mit Segment wird in diesem Fall die Menge von austauschbaren Produkten bezeichnet.

verhelfen somit zu einem hohen Integrationspotential und einem hohen Grad möglicher Wiederverwendung.

4.1.4 Begrifflichkeiten

Durch die Definition und schriftliche Niederlegung der Standards können einfache und präzise Bezeichner gewählt werden. Diese Bezeichner dienen als Grundlage für die persönliche Kommunikation und schriftliche Vereinbarungen (geringere Verhandlungskosten). Zusätzlich werden betriebswirtschaftliche Transaktionen durch die Verwendung von Standards vereinfacht und somit Kosten sparender abgewickelt. Dies verringert die anfallenden Transaktionskosten für alle Beteiligten deutlich.

4.1.5 Betrachtungen in der Praxis

Anzumerken bleibt, dass sich nicht immer der qualitativ beste Standard gegenüber konkurrierenden Standards durchsetzt. Häufig entscheidet der Zeitpunkt der Verabschiedung, das Marketing und die Lobby über den Erfolg eines Standards.

Die in diesem Kapitel bisher angesprochenen Aspekte gelten für viele Anwendungsfelder und Arten von Standards. Im Folgenden wird auf die Situation der Standardisierung im Bereich von RFID genauer eingegangen. Da die in der Einleitung gestellte Frage nach dem Grund der zurückhaltenden Haltung vieler Hersteller und Betreiber offen gelassenen ist, wird an dieser Stelle zunächst auf eine einführende Abbildung 4.1 hingewiesen. In der Abbildung werden die Problemfelder von Unternehmen bei der Einführung von RFID-Systemen grafisch dargestellt. Auffällig ist, dass knapp die Hälfte aller Unternehmen die Standardisierung als Grund für die zögerliche Haltung anführt. Deutlich weniger Nennungen hatten die Problemfelder Kosten, Datenschutz, technische Grenzen und Sicherheit. Erst im zugehörigen Text der Quelle wird deutlich, dass die fehlende Standardisierung gemeint ist [Lange 2005, S. 66].[110]

In [Michael und McCathie 2005, S. 628] führen die Autoren an, dass bisher[111] kein Standard existiere, der den Bedürfnissen aller Beteiligten gerecht werde.

[110] Anstatt der fehlenden Standardisierung hätte der hohe Wert in der Abbildung ebenso eine schlechte Qualität der bestehenden Standards bedeuten können.

[111] Der Artikel erschien im Jahre 2005.

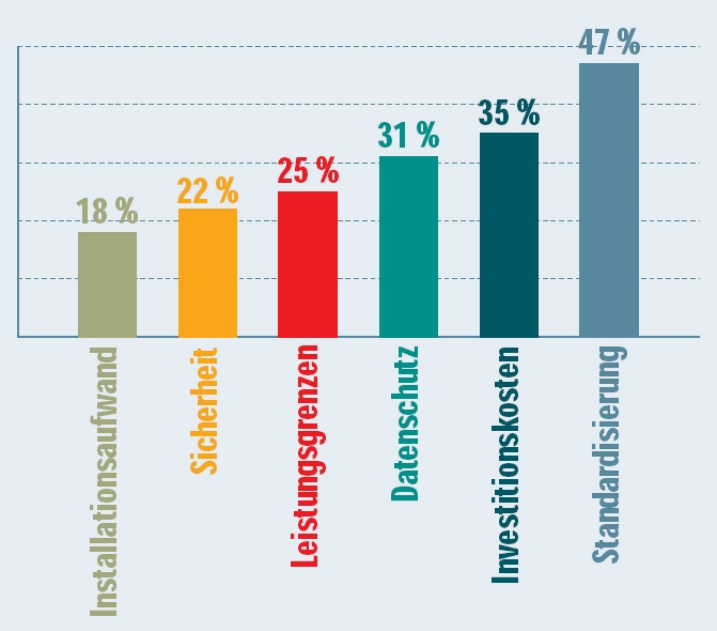


Abbildung 4.1: Fehlende Standardisierung als Hauptproblemfeld von RFID [Lange 2005, S. 66].

Inkompatible Systeme existierten über verschiedene Industrien hinweg, wie Eisenbahn, Lastkraftverkehr, Mauterfassung, Handel und Produktion. Somit sei die Interoperabilität die größte Sorge bei dem nahtlosen Einsatz von RFID in Lieferketten. Schließlich sei der EPC-Standard von höchster Bedeutung für den Erfolg von RFID. Der EPC-Standard wird in Kapitel 4.2.2 detailliert erläutert.

[Sarma u. a. 2003, S. 455] schlägt ebenfalls den EPC-Standard als Lösung für das Problem der fehlenden Standards vor. Ein offener und weit verbreiteter Standard, der einen günstigen Einsatz möglich mache, fehle, so dass bisherige Ansätze zu teuer seien und eine große Herausforderung für Betreiber und Entwickler darstellten. Allerdings muss bei diesem Artikel angemerkt werden, dass er im Jahre 2003 erschienen ist und inzwischen weitere Standards entwickelt wurden, die in den folgenden Abschnitten erläutert werden. Außerdem ist der Artikel im Auto-ID Center entstanden, welches der Vorläufer von EPCglobal war. Aus diesem Grund ist es nicht verwunderlich, dass die Autoren den EPC-Standard als Lösung vorschlagen.

Die meisten Bemühungen der Standardisierungsorganisationen liegen im Bereich der passiven RFID-Tags. Bei aktiven Tags hingegen sind erst seit ca. 2004 ernsthafte Ansätze zur Standardisierung zu beobachten.

In einem Interview mit Mike Marsh von Trolley Scan[112] werden die Aussichten auf den Erfolg derzeitiger Standards diskutiert [News 2005]. Marsh ist nicht der Auffassung, dass die heutigen Standards sich durchsetzen würden. Die Anforderungen der Industrie, bzw. des allgemeinen Marktes, setzten die Standardisierungsorganisationen und Hersteller unter Druck, so schnell wie möglich RFID-Systeme zu entwickeln. Die Gefahr läge darin, dass die Standards nicht ausgereift genug seien, weil sie kaum in der Praxis getestet seien. Langfristige Tests mit einer großen Anzahl von Tags in einer produktiven Umgebung seinen quasi nie durchgeführt worden. Marsh spricht damit das allgemeine Problem an, zu welchem Zeitpunkt ein Standard ratifiziert werden sollte. Bei einer zu frühen Ratifizierung besteht die Gefahr von qualitativ schlechten Standards, bei einer zu späten Ratifizierung kommen vermehrt proprietäre Lösungen auf, welche die Verbreitung von Standards verhindern. Im Falle von RFID scheint dieser Konflikt besonders ausgeprägt zu sein. Da erste RFID-Systeme schon vor über 50 Jahren aufgekommen sind, stellt sich die Frage, warum dann die bis jetzt entstandenen Standards noch nicht ausgereift sein sollen.

Eine ähnliche Meinung vertritt Gilbert, der in [Gilbert 2006] seine zehn RFID-Mythen auflistet. Mythos drei lautet: „Gen 2[113] EPCglobal Standards werden umgehend die Einführung beschleunigen“. Gilbert bemängelt die zu schnelle Umsetzung der Spezifikation in einen Standard, da der Entwurf und die Umsetzung in funktionierende Hardware eine gewisse Zeit dauere. Die Entwicklung sei ein iterativer Prozess mit vielen Tests, um noch versteckte Probleme zu identifizieren. Das eigentliche Ziel von Gen 2 sei die Ermutigung von Halbleiter- und anderen Herstellern RFID-Produkte herzustellen, damit genau ein aufkommender anstatt einem fragmentiertem Markt geschaffen werden könne. Der Nutzen der Betreiber sei vermehrter Wettbewerb und damit auch fallende Preise.

[112] http://trolleyscan.com

[113] Gen 2 ist die Abkürzung eines RFID-Standards und wird in Kapitel 4.2.2 näher erläutert.

4.1.6 Inhalt von RFID-Standards

Die große Diskussion um die Bedeutung von Standards wirft sicherlich die Frage auf, welche Größen und Beschreibungen in den Standards festgehalten sind? Kurz gefragt: Was beinhalten RFID-Standards?

Einen guten Überblick bietet die Präsentation [Harmon 2005]. Danach werden RFID-Standards in vier Kategorien unterteilt: Technik, Dateninhalt, Konformität und Anwendung. Dabei sind die technischen Standards zunächst einmal die wichtigsten für den RFID-Einsatz. Sie bestimmen das *Air-Interface*, also die Kommunikation zwischen Leser und Tag. Die Technik stellt die Basis für jegliche RFID-Systeme dar. Auf diesem Feld sind die meisten Standards entwickelt, so dass sich das nächste Unterkapitel genauer mit den Standards zweier Standardisierungsorganisationen widmet. Daten-Standards beschreiben den Aufbau und die Bedeutung der auf den Tags enthaltenen Daten. Dies sind im Einzelnen die Beschreibungen der IDs, der Syntax bei Transfers zwischen Leser und Anwendung und die Codierung der Daten.[114] Nach [Walk 2006, Kap. 4] bestehen bei den Daten- und Anwendungsstandards noch der größte Standardisierungsbedarf. Die Standards zur Konformität beinhalten Test-Methoden für die Performanz und Konformität von RFID-Geräten.[115] Die Grundlage sind die technischen Standards, so dass Abweichungen zu den Spezifikationen (z. B. nicht eingehaltene Toleranzen) aufgedeckt werden können. Schließlich beschreiben die Anwendungsstandards das Vorgehen der Kennzeichnung der entsprechenden Objekte in dem jeweiligen Anwendungsbereich.[116]

Die technischen Standards beinhalten viele physikalische Größen, welche bereits in Kapitel 2.2 angesprochen wurden. Allerdings werden insgesamt sehr viel mehr Parameter beschrieben. Häufig sind folgende Parameter Inhalt der Technik-Standards: Frequenz, Kanal-Bandbreite, Kanal-Genauigkeit, maximale Energie, störende Emissionen, Modulation, Taktabfolge, Daten-Codierung, Bitrate, Bitraten-Genauigkeit, Reihenfolge der Bitübertragung und ggf.

[114] Eine Auswahl der Dateninhalt-Standards ist: ISO/IEC 15424, ISO/IEC 15418, ISO/IEC 15434, ISO/IEC 15459, ISO/IEC 15961, ISO/IEC 15962 und ISO/IEC 15963 [Harmon 2005, S. 27].

[115] Siehe ISO/IEC 18046 und ISO/IEC 18047 [Harmon 2005, S. 28].

[116] Im Bereich des SCM hat die ISO folgende Standards verabschiedet: ISO 17363, ISO 17364, ISO 17365, ISO 17366, ISO 17367, ISO 10374 und ISO 18185 [Harmon 2005, S. 32]

Frequency Hopping-Rate[117], *Hopping*-Reihenfolge, Frequenzspreizung und das Pseudozufallsrauschen[118].

Im Folgenden wird nicht auf die einzelnen, physikalischen Merkmale jedes Standards eingegangen. Die wichtigsten und am weitesten verbreiteten Standards werden genannt und kurz beschrieben.

4.2 Aktuelle Bemühungen

Zurzeit gibt es zwei Organisationen, die sich im Bereich der Standardisierung von RFID bemühen. Zum einen ist dies die bereits erwähnte *International Organization for Standardization*[119] (ISO), welche ein Netzwerk aus vielen nationalen Standardisierungsorganisationen ist und unter keinem Einfluss einer Regierung steht. Die ISO ist in sehr vielen Bereichen der Standardisierung führend und weltweit anerkannt. Die in der Allgemeinheit wohl bekanntesten Standards sind die ISO 9000 und ISO 14000 Familien, welche sich mit dem Qualitäts- bzw. Umweltmanagement von Unternehmen beschäftigen. Viele Standards werden in Zusammenarbeit mit der *International Electrotechnical Commission*[120] (IEC) verabschiedet, welche die global führende Organisation im Bereich der Standardisierung von elektrischen, elektronischen und deren verwandten Technologien ist. Eine Übersicht über die Zusammenhänge der verschiedenen Organisationen, beteiligten Arbeitsgruppen und den ratifizierten Standards ist in [Harmon 2005, S. 21 f.] zu finden.

Die zweite Standardisierungsorganisation EPCglobal Inc™ beschäftigt sich ausschließlich mit der Standardisierung von RFID. Das Konzept von EPC wurde ursprünglich vom Auto-ID Center, einer wissenschaftlichen Einrichtung von verschiedenen Universitäten, entwickelt und wird seit dem Jahr 2003 in einer neuen Organisation EPCglobal Inc™ weitergeführt. EPC arbeitet stark mit Vertretern aus der Industrie zusammen und fördert hauptsächlich die Standardisierung von RFID für Handelsartikel im SCM. Die Abkürzung „EPC“ steht für *Electronic Product Code* und hat den Anspruch die beiden Barcodes UPC

[117] Beim Frequenzmultiplex-Verfahren kann durch den Wechsel zu einer anderen Frequenz das Signal ungestörter übertragen werden. Diese Technik wird auch häufig bei Mobilfunknetzen (z. B. GSM) eingesetzt

[118] Das Rauschen ist eine Folge von Einsen und Nullen, die dazu dienen bei einer Übertragung Verzögerungen und Verschiebungen zu verhindern (Autokorrelation).

[119] http://www.iso.org

[120] http://www.iec.ch

(*Universal Product Code*) und EAN (*European Article Number*) auf Dauer zu ersetzen. Allerdings müssen die EPC-IDs von EPCglobal erworben werden, so dass die Kosten für den Einsatz eines EPC RFID-Systems durch diese Gebühren deutlich erhöht werden. Anders als die ISO Standards beschreibt das EPC-Netzwerk eine einheitliche Lösung zur Objekt-Identifikation mit Tags, Lesern, Kommunikationssoftware und Integrationsanwendungen.

Neben diesen beiden Standard-Familien regelt das *European Telecommunications Standards Institute*[121] (ETSI) die Funkvorschriften für die Kommunikation zwischen Leser und Tag in Europa [Walk 2006, S. 60 f.]. Dabei werden die zu verwendenden Frequenzen, die maximale Leistung sowie die speziellen Parameter für die jeweiligen Betriebsfrequenzen geregelt. Diese Vorschriften gelten für alle Hersteller von RFID-Geräten und haben damit wesentlichen Einfluss auf die Gestaltung von Tags und Lesern.

Eine kurze Zusammenfassung der RFID-Standards beider Organisationen zu dem Stand im Jahre 2006 findet sich in [Walk 2006].

4.2.1 ISO Standards

Der Standard ISO/IEC 14443 beschreibt die sogenannten *Proximity* Karten. Sie gehören zu der Klasse der *Remote Coupling* Systeme und haben daher eine sehr geringe Reichweite von wenigen Zentimetern. Die Inlays werden häufig in Plastikkarten im Kreditkarten-Format[122] verbaut und arbeiten im HF-Frequenzbereich von 13,56 MHz. Der Standard unterscheidet zwei Varianten mit unterschiedlichen, physikalischen Eigenschaften. Zu erkennen sind die Varianten an dem angehängten „A“ oder „B“ hinter der Zahl „14443“. Die 14443A-Variante ist viel weiter verbreitet. Insgesamt ist der Standard in vier Teile gegliedert, welche den Bereichen „physikalische Eigenschaften“, „Energie und Signal-Schnittstelle“, „Initialisierung und Antikollision“ und „Übertragungsprotokoll“ entsprechen. Bekannteste Hersteller von ISO/IEC 14443 Tags sind Philips[123], Infineon[124], Atmel[125] und STMicroelectronics[126].

[121] http://www.etsi.org
[122] Siehe Standard ISO/IEC 7810 ID-1.
[123] http://www.philips.com. Bekannteste Produktgruppe ist Mifare von Philips, welche für eine Vielzahl von Anwendungen eingesetzt werden kann.
[124] http://www.infineon.com
[125] http://www.atmel.com
[126] http://www.st.com

Der direkte Nachfolger von ISO/IEC 14443 ist ISO/IEC 15693, welcher eine größere Reichweite von bis zu einem Meter erreichen kann (sog. *Vincinity* Karten). ISO/IEC 15693 ist sehr weit verbreitet und ebenfalls ein *Remote Coupling* System bei 13,56 MHz. Die Aufteilung des Standards ist dreiteilig und besteht aus den Bereichen „physikalische Eigenschaften“, „Luftschnittstelle und Initialisierung“ und „Antikollision und Übertragungsprotokoll“. Technischer Hauptunterschied ist die Luftschnittstelle, welche aufgeteilt wurde in die Richtung von Tag zu Leser und in die Richtung von Leser zu Tag. Durch unterschiedliche Codierungen und Modulationen kann so die größere Reichweite erzielt werden. Allerdings wird dadurch die Bandbreite und die Geschwindigkeit gegenüber ISO/IEC 14443 verringert. Eine sehr detaillierte Erklärung der physikalischen Eigenschaften beider Standards findet sich in [Finkenzeller 2002, Kap. 9.2]. Neben Infineon, Philips und STMicroelectronics stellt auch Texas Instruments[127] ISO/IEC 15693 Produkte her.

Die beiden genannten Standards beziehen sich lediglich auf passive Tags. Bis zum Jahre 2004 existierte bei der ISO noch kein Standard für Systeme mit aktiven Tags. Dies änderte sich dann mit der neuen Familie der ISO/IEC 18000 Standards. Die Hersteller von aktiven Tags verwendeten stets eigene, proprietäre Protokolle. Bis zum heutigen Zeitpunkt werden fast ausschließlich proprietäre, aktive Systeme verwendet, da der ISO/IEC Standard noch recht frisch ist und sich noch nicht durchsetzen konnte.

Die im Jahre 2004 ratifizierte ISO/IEC 18000 Familie besteht aus sechs Teilen. Dabei beschreibt ISO/IEC 18000-1 die Referenz-Architektur und die Parameter für alle Frequenzen; die restlichen fünf Teile behandeln die einzelnen Frequenzen. In der Tabelle 4.1 werden alle Teile aufgelistet.

Die einzelnen Teile bestehen aus einem veröffentlichten Standard mit dem Bezeichner „2004“ und einem weiteren Eintrag in der Tabelle mit der Abkürzung „AMD“. Diese *Amendments* sind noch in der Entwicklung befindliche Nachträge oder Revisionen zu den mit der Jahreszahl 2004 versehenen Standards. In den AMDs werden Überarbeitungen der Version 2004 vorgenommen. Zusätzlich ergänzen sie Funktionen zur Unterstützung von Sensoren und batteriegestützten Tags, sowie allgemeinen Verbesserungen [Walk 2006, S. 56].

Anzumerken ist, dass die Standard-Familie einen Teil für jeweils den LF- und HF- und vier Teile für den UHF-Bereich verwendet. ISO/IEC 18000-3 im

[127] http://www.ti.com

Standard	Inhalt
ISO/IEC 18000-1:2004	Luftschnittstellen – Referenz-Architektur und Parameterbeschreibung
/AMD 1	Nachtrag zu ISO/IEC 18000-1:2004
ISO/IEC 18000-2:2004	Luftschnittstellen – Frequenzen $< 135\,\text{kHz}$
/AMD 1	Nachtrag zu ISO/IEC 18000-2:2004
ISO/IEC 18000-3:2004	Luftschnittstellen – 13,56 MHz
/AMD 1	Nachtrag zu ISO/IEC 18000-3:2004
ISO/IEC 18000-4:2004	Luftschnittstellen – 2,45 GHz
/AMD 1	Nachtrag zu ISO/IEC 18000-4:2004
ISO/IEC 18000-5:2004	annulliert (Luftschnittstellen – 5,8 GHz)
ISO/IEC 18000-6:2004	Luftschnittstellen – 860–960 MHz, Typ A & B
/AMD 1	Luftschnittstellen – 860–960 MHz, Typ C
ISO/IEC 18000-7:2004	Luftschnittstellen – 433 MHz
/AMD 1	Nachtrag zu ISO/IEC 18000-7:2004

Tabelle 4.1: Übersicht über die ISO/IEC 18000 Standard-Familie [vgl. Walk 2006, S. 55].

HF-Bereich ist der Nachfolger des weit verbreiteten ISO/IEC 15693 Standards. Ein Teil im UHF-Bereich (ISO/IEC 18000-5) wurde annulliert und wird nicht mehr entwickelt. Der sechste Teil stellt sich als sehr interessant heraus, da er aus drei Typen besteht, von denen der Typ C aus AMD 1 die Aufgabe hat, die Konformität mit einem EPC Standard herzustellen (siehe Kapitel 4.2.2.3). Diese Übereinkunft in der Standardisierung bedeutet einen großen Schritt für die Hersteller und Betreiber von RFID-Systemen. Der siebte Teil beinhaltet den bereits angesprochenen, derzeit einzigen Standard für aktive Tags. Allerdings ist die Frequenz 433 MHz nicht besonders weit verbreitet, so dass es noch eine Weile dauern wird, bis sich dieser Standard flächendeckend in aktiven Systemen durchsetzt. Prominente Ausnahme beim Einsatz von aktiven Tags bei 433 MHz ist das amerikanische Verteidigungsministerium (*Department of Defense*, DoD), welches u. a. auch Produkte von Savi Technology Inc[128] verwendet. Savi verwendet ein eigenes Protokoll[129] für die Luftschnittstelle.

[128] http://www.savi.com
[129] Das Protokoll heißt *Savi EchoPoint Air Protocol*.

Die Standards im HF-Bereich (ISO/IEC 14443, 15693 und 18000-3) sind Nachfolger von Standards der *Smart Cards*, welche durch direkten physischen Kontakt mit dem Leser kommunizieren. Auch *Smart Cards* haben eindeutige IDs, welche nach einer festen Syntax aufgebaut sind. Die ID der *Smart Cards* und RFID-Tags im HF-Bereich nennt sich UID (*Unique Identifier*) und wird im ISO Standard ISO/IEC 7816 definiert. Die Tabelle 4.2[130] zeigt die einzelnen Felder des UID [ST 2006, S. 3]. Im Folgenden werden die Felder genauer erläutert.

Feld	TRC	SMC	PC	USN
Länge	8	8	6	42

Tabelle 4.2: Aufbau der UID der ISO-Tags [ST 2006, S. 3].

- *Tag Registration Category*: acht Bit, bestimmt den Anwendungsbereich, die Codes werden in ISO/IEC 7816-5 definiert (der hexadezimale Wert `0xE0` identifiziert Tags von ISO/IEC 15693),
- *Silicon Manufacturer Code*: acht Bit, identifiziert eindeutig den Halbleiter-Hersteller des Tags, diese Liste der Codes wird in ISO/IEC 7816-6/AM1 geführt (z. B. `0x02` für STMicroelectronics, `0x04` für Philips),
- *Product Code*: sechs Bit, identifiziert die Tag-Produktfamilie des Halbleiter-Herstellers (z. B. Hersteller STMicroelectronics verwendet für die SRI176-Tags den binären Wert `00 0010`) [ST 2006, S. 3],
- *Unique Serial Number*: 42 Bit, identifiziert eindeutig den Tag innerhalb der Produktfamilie.

4.2.2 EPCglobal Inc™

EPC ist nicht nur eine Sammlung von Standards für die Luftschnittstelle, sondern eine ganze Familie von aufeinander abgestimmten Standards in den zusätzlichen Bereichen: Daten, Anwendung, Objektnamenservice (*Object Naming Service*, ONS) und Tag-Datenübersetzung. Insgesamt ergibt sich dadurch eine dreischichtige Struktur, welche in Standards für den Austausch von physischen Objekten, Standards für die unternehmensinterne Infrastruktur und Standards für den Datenaustausch unterteilt ist.

[130] Aus Gründen der Übersicht werden die Feld-Bezeichner in der Tabelle abgekürzt.

4.2.2.1 Class-1 Generation-2 UHF

Die zurzeit wichtigsten EPC-Standards fallen in den Bereich der Luftschnittstelle. In der Tabelle 4.3 werden die sechs Klassen der EPC-Tags aufgelistet und deren Fähigkeiten kurz erläutert. Bisher sind nur die Klasse 0 spezifiziert (Version 1.0) und die Klasse 1 (teilweise) ratifiziert, die restlichen Klassen sind erst einmal zur Spezifikation geplant. Innerhalb der Klasse 1 gibt es zwei verschiedene Betriebsfrequenzen von denen der UHF-Bereich (860–960 MHz) in Version 1.09 ratifiziert ist und der HF-Bereich (13,56 MHz) erst in Version 1.0 spezifiziert ist.

EPC-Tag Klasse	Fähigkeiten
Class 0	Nur lesen (d. h. die EPC-ID wird während der Produktion auf den Tag codiert und kann durch Leser gelesen werden)
Class 1	Lesen, einmaliges Schreiben (d. h. Tags werden ohne ID hergestellt und können später durch einen Leser beschrieben werden)
Class 2	Lesen, Schreiben
Class 3	Class 2 Fähigkeiten plus einer Energiequelle zur Vergrößerung der Reichweite und/oder Funktionalität
Class 4	Class 3 Fähigkeiten plus aktive Kommunikation und der Fähigkeit mit anderen aktiven Tags zu kommunizieren
Class 5	Class 4 Fähigkeiten plus der Fähigkeit auch mit passiven Tags zu kommunizieren

Tabelle 4.3: EPC-Tag Klassen und deren Fähigkeiten [vgl. EPC 2004, S. 14].

Auffällig ist, dass es drei verschiedene Klassen (3–5) aktiver Tags gibt, wobei sie sich in der Kommunikationsfähigkeit deutlich unterscheiden. Allerdings gibt es keine Spezifikationen und damit auch noch keine Bemühungen, dass Hersteller aktive EPC-Tags produzieren.

Die bekannteste Luftschnittstelle ist die Klasse 1 der 2. Generation im UHF-Bereich. In aller Regel werden Komponenten dieser RFID-Systeme mit *Class-1 Generation-2 UHF* RFID bezeichnet. Häufig findet sich auch die einfache Abkürzung *Gen 2*. Diese passiven RFID-Systeme arbeiten mit der Backscatter-Technik zur Kommunikation und im Frequenzbereich von 860–960 MHz, so dass die verschiedenen kontinentalen Vorgaben (Europa 868 MHz, USA 915 MHz, Japan 950–956 MHz) von diesem Standard abgedeckt werden.

Ein Gen 2 Tag ist in vier verschiedene Daten-Abschnitte unterteilt [EPC 2005, S. 35]. Diese Abschnitte heißen Bänke und sind wie folgt bestückt.

- Bank 00 (RESERVED) speichert das *Kill*-Passwort (siehe Kapitel 3.2) und ein *Access*-Passwort.
- Bank 01 (EPC) beinhaltet die 16 Bit lange CRC Prüfsumme, die Längenangabe der EPC-ID (PC) und die EPC-ID selbst.
- Bank 10 (TID) wird mit verschiedenen IDs bestückt, darunter z. B. die *Allocation Class*, welche den verwendeten Standard (EPCglobal) enthält, und Informationen für den Leser, welche Funktionen der Tag unterstützt.
- Bank 11 (USER) darf benutzerdefiniert mit Daten belegt werden.

Die Länge des EPC variiert von 16 bis 496 Bit [Walk 2006, S. 60], wobei jedoch der 96 Bit lange EPC (EPC-96) für den Gen 2 Tag vorgeschlagen wird. Die Syntax (Art und Reihenfolge der Felder) des EPC ist immer identisch, jedoch variiert die Länge der einzelnen Felder mit der Gesamtlänge des EPC. Die Tabelle 4.4[131] beschreibt das für EPC Gen 2 verwendete Format GID-96 (*General Identifier*). Die Felder in den 96 Bit des EPC werden im Folgenden genauer erklärt [EPC 2006a, S. 23 f.].

Feld	H	GMN	OC	SN
Länge	8	28	24	36

Tabelle 4.4: Struktur des EPC Gen 2 Tags im GID-96 Format [vgl. EPC 2006a, S. 23 f.].

- *Header*: acht Bit, binärer Wert `00110101` identifiziert das Format GID-96 für Gen 2,
- *General Manager Number*: 28 Bit, identifiziert eindeutig die Firma oder Organisation, wird von EPCglobal vergeben,
- *Object Class*: 24 Bit, identifiziert das Produkt/die Klasse, also z. B. die Artikelnummer,

[131] Aus Gründen der Übersicht werden die Feld-Bezeichner in der Tabelle abgekürzt.

- *Serial Number*: 36 Bit, identifiziert eindeutig das Objekt innerhalb der Klasse.

Mit Hilfe dieser Felder lassen sich Objekte jeder Art weltweit eindeutig identifizieren. Da die *General Manager Number* von EPCglobal zentral nur einmalig vergeben wird, kann jede Organisation die beiden restlichen Felder selbst bestücken, so dass eine insgesamt drei-stufige Hierarchie des EPC gegeben ist (Organisation – Produkt – Objekt).

Neben der Datenstruktur befinden sich die Gen 2 Tags immer in einem bestimmten Zustand [EPC 2005, S. 39 ff.]. Dieser Zustand ist abhängig von dem vorherigen Zustand und den auf den Tag ausgeführten Operationen (z. B. durch einen Leser). Die Zustände sind *Ready*, *Arbitrate*, *Reply*, *Acknowledged*, *Open*, *Secured* und *Killed* und werden in [EPC 2005, S. 39 ff.] neben einem Zustandsdiagramm detailliert erläutert. Für Gen 2 Tags sind ebenfalls Pseudo-Zufallsgeneratoren vorgesehen. Operationen auf den Tags heißen Befehle und lassen sich in drei Kategorien einteilen: *Select commands*, *Inventory commands* und *Access commands*. Die *Inventory commands* dienen dazu, alle Tags anzusprechen und ggf. abzufragen (*Query*). Abgefragt werden in der Regel das Längenfeld (PC), der EPC und die Prüfsumme. *Select commands* wählen einzelne oder mehrere Tags aus, um Lese- oder Schreib-, Kill- oder Lock-Operationen auszuführen (*Access commands*). Auch diese Befehle sind der Referenz [EPC 2005, S. 45 ff.] dokumentiert.

Die physikalischen Eigenschaften (*Signalling*) von Gen 2 Tags, wie z. B. Modulation, Daten-Darstellung, Datenraten, *Hopping*, usw., sind in [EPC 2005, Kap. 6.3.1] beschrieben.

Ein weiteres Problem wurde mit der Schaffung von Gen 2 gelöst. Die verschiedenen Frequenzen auf den verschiedenen Kontinenten werden alle von dem Standard abgedeckt, da er für Frequenzen von 860 – 960 MHz ausgelegt ist. Damit sollten UHF-Tags jeglicher Frequenz in dem Bereich mit allen Lesern lesbar sein, unabhängig welcher Klasse, Standard oder Frequenz der Tag zugeordnet ist.

Gegenüber älteren UHF-Standards konnte die Erfassungsrate erhöht werden, was sich durch eine schnellere Geschwindigkeit bei Operationen auf Tags bemerkbar macht. Weitere Neuerungen sind eine verbesserte Fehlersicherheit und verschlüsselte Kommunikation zwischen Leser und Tag [Walk 2006, S. 55 f.].

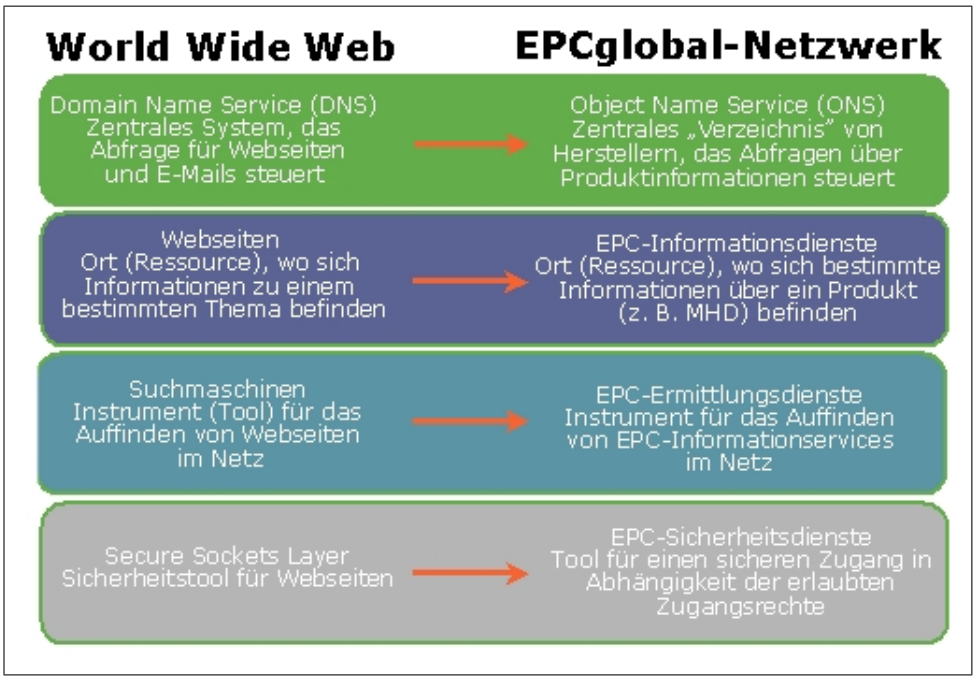


Abbildung 4.2: Komponenten des EPCglobal Inc™-Netzwerkes und die Parallelen zum Internet [EPC 2006b].

4.2.2.2 EPC-Netzwerk

Neben diesen Gen 2 spezifischen Funktionen bietet EPCglobal jedoch mit dem EPC-Netzwerk noch weitaus mehr Funktionen und Möglichkeiten zum Einsatz von RFID. Das EPC-Netzwerk besteht aus den folgenden Komponenten: Objektnamenservice (ONS), Informationsservice (*Information Services*, EPCIS), Ermittlungsservice (*EPC Discovery Services*) und Sicherheitsservice (*EPC Security Services*) (siehe Abbildung 4.2).

Der ONS ist vergleichbar mit dem DNS[132] des Internets. Beim EPC-Netzwerk wird eine gelesene EPC an den ONS gesendet, der die zu dieser EPC gehörende URL[133] an den Absender zurück sendet. Diese verknüpfte URL ist der Ort, der zu dem EPC (und damit zu dem verknüpften Objekt) gehörende

[132] DNS ist die Abkürzung von *Domain Name Service*. DNS ist ein Dienst, der Hostnamen in eine IP-Adresse auflöst, mit der dann eine Verbindung aufgebaut werden kann.

[133] Eine URL (*Uniform Resource Locator*) ist ein Bezeichner einer Ressource (Datei, Webseite, usw.) im Internet. Ein Beispiel ist `http://www.uni-koblenz.de`,

Informationen[134] beherbergt. Mit dieser URL kann dann der Absender – je nach Berechtigung – Daten abfragen oder sogar ändern (z. B. den Ort des Objekts).

Der EPCIS ist die Komponente im EPC-Netzwerk, welche diese Informationen speichert und zur Verfügung stellt. Verwendet ein Unternehmen das EPC-Netzwerk, dann sollte auch ein EPCIS von dem Unternehmen selbst betrieben werden. Auf dem EPCIS werden dann alle Daten zu den eigenen (hergestellten oder mit EPC-Tags versehenen) Objekten gepflegt. Anders der ONS, der zentral für alle im Umlauf befindlichen Tags erreichbar sein muss.

Der Ermittlungsservice ist eine Art Zusatzdienst, der auf Basis der benötigten Informationen über einen bestimmten EPC alle relevanten EPCIS lokalisiert. Dieser Dienst ist vergleichbar mit einer Suchmaschine im Internet. Selbstverständlich müssen sich Benutzer durch Authentifikation und Autorisierung zu der Suche berechtigen. Dies erledigen die Sicherheitsservices, welche Benutzer identifizieren und dann die Berechtigungen überprüfen.

Zu Beginn von Kapitel 3 wurde bereits auf die hohe Bedeutung von Sicherheit im Zusammenhang mit RFID hingewiesen. Auch EPCglobal hat die Notwendigkeit einer sicheren Übertragung von RFID-Daten erkannt. Unterstützung bei der Umsetzung von Sicherheitsmechanismen bieten dabei Unternehmen, die auf diesem Feld bereits vertreten sind. Die Firma VeriSign Inc[135] bietet Infrastruktur-Dienste im Bereich von Sprach- und Datennetzen an. Hauptsächlich stellt VeriSign Zertifikate (SSL, PKI) aus und bestätigt diese auf Anfrage. Im Bereich von RFID weist VeriSign in [VeriSign 2005] auf die Gefahren bei der Benutzung von unsicheren IP-Netzen hin und schlägt Lösungen für die Authentifikation, Datensicherheit (Vertraulichkeit, Integrität) und Zugriffskontrolle vor. Ein Beispiel-Szenario wird in Form einer Skizze anschaulich angeführt. Jede Operation, die über das unsichere Internet zwischen zwei Parteien getätigt wird, wird mit Hilfe von (durch VeriSign beglaubigten) Zertifikaten geschützt.

[134] Objekte werden in PML (*Physical Markup Language*, XML-Derivat) beschrieben und übertragen. Hersteller können die Gestaltung der PML-Objekte selbst vornehmen.
[135] http://www.verisign.com

4.2.2.3 Konformität mit ISO/IEC 18000-6:2004/AMD1

Im Januar 2005 stellte EPCglobal seinen Gen 2 Standard der ISO zur Verfügung, damit die ISO den Gen 2 Standard in ihre ISO/IEC 18000 Familie aufnehmen kann [Weinstein 2005, S. 29]. Schließlich wurde Gen 2 im sechsten Teil, Nachtrag eins[136] aufgenommen, so dass nun eine Interoperabilität[137] zwischen EPC und der ISO/IEC zu Stande gekommen ist. Mit dieser Übereinkunft entsteht nun die Chance, dass sich in bestimmten Bereichen dieser Gen 2 Standard durchsetzen könnte, da ja keine zwei konkurrierenden Standards im passiven UHF-Bereich existieren.

Trotzdem ist diese Konvergenz nicht direkt ein Indikator für die Qualität des Standards. Wie bereits erwähnt, sieht Marsh (siehe Kapitel 4.1) im Gen 2 noch keinen fertig entwickelten Standard. So gesehen bietet die Zusammenarbeit von EPC und der ISO/IEC die Chance den Standard weiter zu entwickeln und damit eine höhere Wahrscheinlichkeit einen guten und anerkannten Standard zu schaffen.

4.2.3 Proprietäre Ansätze

Wie bereits erwähnt, haben viele Hersteller eigene Protokolle entwickelt, um die Kommunikation zwischen Leser und Tag zu realisieren. Die inzwischen stark aufkommenden Standards im Bereich von passiven Tags werden sich wohl in den nächsten Jahren etablieren, wobei bei aktiven Systemen fast ausschließlich proprietäre Lösungen zu finden sind.

Weinstein merkt dazu in [Weinstein 2005, S. 32] an, dass fehlende Standards durch die Hilfe von *Middleware*[138] kompensiert werden könnten. Sollte für die Luftschnittstelle eine nicht-standardisierte Lösung eingesetzt werden, so könnte die *Middleware* die vom Leser kommenden Daten so transformieren, dass das Betriebliche Informationssystem diese weiter verarbeiten kann. Entweder muss dann die *Middleware* vom Betreiber selbst entwickelt werden oder

[136] Die dafür häufig verwendete Abkürzung ISO/IEC 18000-6C oder 18000-6C beinhaltet statt des Nachtrags den Typ des Standards.

[137] Interoperabilität bedeutet die Möglichkeit des gegenseitigen Lesens von Tags des anderen Standards. Bis auf wenige Unterschiede sind die Standards sogar identisch.

[138] *Middleware* ist eine Software-Komponente von vielen Systemen, die mehrschichtig aufgebaut sind. Die *Middleware*-Schicht liegt zwischen der Hardware und den Anwendungen. Ihre Aufgabe ist die Vermittlung zwischen den Schichten, was z. B. Verwaltungs- oder Kommunikationsfunktionen sein können.

es gibt bereits fertige Produkte, die nur noch an die jeweilige Datenstruktur der Leser angepasst werden müssen. Somit wird die *Middleware* zur Schnitt- und Vermittlungsstelle zwischen der Hardware und den vorhandenen Systemen (Anwendungen, Datenbanken) des Betreibers.

4.3 Zukunft der RFID-Standardisierung

Sicherlich ist die Zukunft der Standardisierung noch nicht absehbar. Allerdings gibt es jedoch verschiedene Hinweise, dass aufgrund der großen Nachfrage der Betreiber nach weltweiten Standards auf diesem Feld noch viele Entwicklungen zu beobachten sein werden. Nach [BSI 2004, Abb. 10.2] denken 70 % der befragten Unternehmen, dass bis Ende 2007 die aktuellen Hemmnisse bei der Standardisierung überwunden sein werden.

Die ISO/IEC 18000 Standards sind noch recht jung und bisher wenig verbreitet. Aus diesem Grund wird es interessant sein zu beobachten, ob sich Teile dieser Familie durchsetzen werden. Bei den EPC Standards wird sich der Gen 2/18000-6C Standard zumindest in der SCM erst einmal durchsetzen. Weitere Arbeitsgruppen (z. B. für den *EPC Class-1 Generation-2 HF* Standard) werden zurzeit gebildet, so dass die Arbeit an den angrenzenden Standards nicht ruhen wird.

Für den Einsatz in Unternehmen sind die Standards für die Datenstruktur und die Anwendungen ebenfalls nicht unwichtig, weil erst dadurch eine nahtlose Integration in die bestehenden Systeme möglich ist. Diese Standards werden jedoch wohl erst nach den technischen Standards mit mehr Intensität weiterentwickelt.

Für die Akzeptanz von RFID im privaten Bereich ist eine Regelung der Sicherheitsaspekte unbedingt von Nöten, damit den Sicherheitsbedürfnissen der Allgemeinheit entsprochen werden kann.

4.4 Vergleich mit einer anderen, aktuellen Technik: IP-Telefonie

An dieser Stelle bietet sich der Vergleich der Standardisierungsbemühungen von RFID mit einer anderen Technologie an. Seit einigen Jahren wird die

IP-Telefonie[139] immer populärer und erfreut sich einer wachsenden Benutzerzahl im privaten und im gewerblichen Bereich. Ein anderer, weit verbreiteter Name für IP-Telefonie ist *Voice-over-IP* (VoIP). Grundlegende, benötigte Komponenten sind ein Internetzugang und ein Endgerät, welches die Stimme digitalisieren und versenden kann. Diese Endgeräte sind entweder spezielle Telefon-Apparate oder ein PC mit einem Mikrofon und Lautsprechern[140]. Die klassische Form der IP-Telefonie findet zwischen zwei Partnern statt, die jeweils einen Internetzugang nutzen. Damit nicht zwei Infrastrukturen (herkömmliche Telefonie[141] und VoIP) isoliert voneinander existieren, besteht noch die Möglichkeit zum Aufbau von Gesprächen mit einem Partner mit Internetzugang und einem Partner mit herkömmlichem Telefonzugang. Diese Mischform macht es VoIP-Nutzern möglich auch Gespräche auf herkömmliche Anschlüsse abzusetzen oder sogar von ihnen Gespräche entgegen zu nehmen.

Im VoIP-Bereich gibt es im Grunde vier verschiedene, technische Lösungen, wovon allerdings zwei proprietär und die zwei anderen standardisiert sind. Das proprietäre *InterAsterisk eXchange* (IAX) Protokoll[142] wird von der *Open Source* Telefonanlagen-Software Asterisk[143] verwendet. Es wird zur Kommunikation zwischen den Asterisk-Servern und Endgeräten eingesetzt.

Das H.323-Protokoll ist eine Empfehlung der *International Telecommunication Union*[144] (ITU) und wird in verschiedenen Anwendungen eingesetzt (z. B. Microsoft Netmeeting oder OpenH323). Allerdings werden für die Verwendung Lizenzkosten fällig, so dass andere, frei erhältliche Lösungen dadurch einen klaren Vorteil haben. H.323 benutzt auf der nächst niedrigeren Protokollschicht das *Real-Time Transport Protocol* (RTP).

Auf die beiden anderen Protokolle wird im Folgenden etwas genauer eingegangen, weil sie am weitesten verbreitet und dadurch die zurzeit größten Konkurrenten sind.

[139] Bei der IP-Telefonie wird die Sprache digitalisiert, über Datennetze (*Internet Protocol*) versendet und beim Empfänger wieder in Sprache umgewandelt.
[140] In aller Regel bieten sich *Headsets* dazu an, weil sie einfach zu tragen sind und eigens für solche Zwecke entwickelt worden sind.
[141] Das herkömmliche Telefonnetz wird mit *Public Switched Telephone Network* (PSTN) bezeichnet.
[142] Neben dem IAX-Protokoll gibt es auch eine zweite Version des Protokolls, welches IAX2 genannt wird.
[143] http://www.asterisk.org
[144] http://www.itu.org

4.4.1 SIP

Das *Session Initiation Protocol* (SIP) ist ein *Proposed Standard*[145] der *Internet Engineering Task Force*[146] (IETF) und wird im RFC 3261 spezifiziert [RFC 3261 2002]. SIP wird eingesetzt, um die Verbindung zwischen verschiedenen Partnern zu verwalten. Ist eine Verbindung hergestellt, werden die Pakete mit der digitalisierten Sprache über RTP versendet. Somit ist SIP ein Protokoll der Anwendungsschicht mit den Aufgaben des Session-Managements, der Signalisierung und der Steuerung von Verbindungen [RFC 3261 2002, S. 8]. Die notwendigen Komponenten für eine SIP-Verbindung sind zwei *User Agents* als Endpunkte und *Proxy Server*, an denen sich die *User Agents* anmelden, bevor sie neue Sessions anmelden oder weitere Anfragen senden [RFC 3261 2002, S. 8]. Somit bietet SIP nicht selbst VoIP-Dienste, sondern stellt lediglich Primitive bereit, die zum Anbieten von Diensten genutzt werden können [RFC 3261 2002, S. 9]. In privaten Netzwerken (LAN) sind keine *Proxy Server* notwendig, da dann auch direkte Verbindungen möglich sind. Die Adressierung von Teilnehmern ist durch den Aufbau `sip:user@host.domain` (SIP-URL) recht einfach. SIP-Provider bieten dazu noch Telefonnummern an, damit die Teilnehmer aus dem herkömmlichen Telefonnetz erreichbar sind. Diese Nummernkreise werden von den Providern reserviert und dann den Kunden zur Verfügung gestellt. Für einen Anrufer ist die Umleitung von der Nummer auf die SIP-URL transparent. Die SIP-Nachrichten ähneln denen des HTTP-Protokolls[147], und somit ist SIP ebenfalls ein *Request/Response*-Protokoll[148].

Viele VoIP-Anbieter setzen das SIP-Protokoll ein, da es frei verfügbar und standardisiert ist. Zum Beispiel wird SIP von den großen Providern oder Freemail-Anbietern GMX, freenet, 1&1, AOL, T-Online und Web.de angeboten. In Deutschland ist Sipgate[149] der größte und bekannteste, kostenlose Anbieter von SIP-Internet-Telefonanschlüssen. Man kann sich – sofern die Ortsvorwahl

[145] Die zweite von vier Stufen bis zum offiziellen Internetstandard wird erreicht, wenn eine Spezifikation nach Prüfung eines zuständigen Gremiums dafür würdig erklärt wurde. Der nächste Schritt (*Draft Standard*) wird erreicht, wenn genügend praktische Erfahrungen gesammelt wurden.

[146] http://www.ietf.org

[147] Das *Hypertext Transfer Protocol* ist das im Internet häufig genutzte Protokoll zur Anzeige von Webseiten. HTTP ist von der IETF als *Internet Standard* eingestuft und unter den RFCs 1945 (Version 1.0) und 2616 (Version 1.1) standardisiert.

[148] Ein Kommunikationspartner sendet einen *Request* (Anfrage) an dem Empfänger, der mit der *Response* (Antwort) auf die Anfrage antwortet.

[149] http://www.sipgate.de

unterstützt wird – eine Festnetznummer aus dem eigenen Ortsnetz zuweisen lassen, unter der man dann erreichbar ist. Auch Hardwarehersteller unterstützen SIP bereits. An die AVM Fritz!Box kann man direkt herkömmliche Telefone anschließen und dann VoIP-Telefonie betreiben. Auch Hersteller von großen Telefonanlagen haben das SIP-Protokoll bei ihren Produkten implementiert, z. B. Siemens oder Auerswald[150]. Ein hybrides Telefon wird von Siemens angeboten. Das Gigaset C450 IP kann sowohl an herkömmlichen Telefonanschlüssen als auch an Internetanschlüssen betrieben werden. Die Verbindungsart kann vor jedem Anruf ausgewählt werden.

4.4.2 Skype

Skype heißt die zweite, weit verbreitete VoIP-Lösung. Im Unterschied zu SIP ist das proprietäre Skype-Protokoll nicht öffentlich zugänglich. Die notwendige Software kann jedoch kostenfrei von der Homepage[151] heruntergeladen werden. Skype ist ein *Peer-to-Peer*-Protokoll[152] und wurde von den Gründern der *Filesharing*-Software[153] KaZaa[154] entwickelt [Baset und Schulzrinne 2004, S. 1]. Das Skype-Netzwerk besteht aus den Clients und einem Login-Server, der die einzige zentrale Komponente darstellt [vgl. Baset und Schulzrinne 2004, Abb. 1]. Innerhalb der Menge der Clients werden bestimmte Hosts zu *Super Nodes* erklärt. Diese *Super Nodes* sind eine zweite logische Ebene im Netzwerk. Clients verbinden sich mit diesen *Super Nodes*, bevor sie sich am Login-Server anmelden. Dadurch wird die Anzahl der Verbindungen unter allen Clients verringert, was eine deutliche Minderung des Traffics zu Folge hat. Offiziell werden kaum Informationen über das verwendete Protokoll angeboten, jedoch kann unter [Baset und Schulzrinne 2004] eine Analyse und Interpretation des Netzwerk-Verkehrs eingesehen werden.

Verbindungen zu herkömmlichen Telefonanschlüssen und zu anderen VoIP-Netzwerken kann durch die SkypeIn- und SkypeOut-Funktionen hergestellt werden. Das Anrufen von anderen Teilnehmern über SkypeOut ist natürlich

[150] http://www.auerswald.de
[151] http://www.skype.com
[152] *Peer-to-Peer* ist eine Form der logischen Vernetzung zwischen gleichgestellten Kommunikationspartnern. Jeder Teilnehmer kann gleichzeitig Dienste anbieten und nutzen. Dies ist der grundlegende Unterschied zu *Client-Server*-Netzwerken.
[153] *Filesharing* ist das Tauschen von Dateien über das Internet. Meist werden diese Systeme über *Peer-to-Peer*-Netzwerke realisiert.
[154] http://www.kazaa.com

kostenpflichtig und beginnt bei 1,7 Eurocent pro Minute (Stand Datum der Arbeit). Bei der Nutzung von SkypeIn wird für die Vergabe einer vom Festnetz erreichbaren Nummer eine regelmäßige Gebühr[155] verlangt.

Zusätzlich zu den VoIP-Funktionen bietet die Skype-Software einen *Instant Messenger*[156] und *Buddy*-Listen[157]

4.4.3 Vergleich und Bewertung

Architektur

Es gibt große Unterschiede zwischen den beiden Ansätzen SIP und Skype. SIP hat eine *Client-Server*-Architektur, wobei bei Skype lediglich der Login-Server als zentrale Komponente benötigt wird. Bei der Verwendung von SIP in einem LAN mit einer Firewall und NAT[158] wird für Verbindungen außerhalb des LANs ein STUN-Server[159] benötigt. Bei Skype ist kein zusätzlicher Server notwendig, was die Inbetriebnahme deutlich vereinfacht.

Sprachübertragung

Zusätzlich zu den bereits erwähnten Funktionen neben VoIP soll Skype eine bessere Sprachqualität als SIP leisten können. Dies ist wohl auf die verwendeten *Codecs*[160] zurückzuführen. Der Codec ist für die Kompression der Sprache zuständig und kein direkter Bestandteil des SIP-Protokolls. Also kann die allgemein geltende schlechtere Sprachqualität nicht als Nachlässigkeit von SIP gewertet werden.

[155] Diese Gebühr muss wahlweise alle drei Monate oder ein Mal pro Jahr bezahlt werden.

[156] *Instant Messaging* (IM) ist das Versenden von Text-Nachrichten zwischen zwei Software-Programmen über das Internet. Die Nachrichten erscheinen beim Kommunikationspartner umgehend (*instant*).

[157] In einer *Buddy*-Liste werden die eigenen Kontakte gepflegt. Dieses Adressbuch der *Instant Messenger* liegt oft zentral auf einem Server.

[158] *Network Address Translation* setzt die internen IP-Adressen in öffentliche IP-Adressen um. Damit ist dann die Kommunikation mit Hosts im Internet möglich. Zusätzlich werden die internen Adressen maskiert, was einen erheblichen Schutz vor Angriffen von außen bietet.

[159] STUN ist eine Abkürzung von „*Simple traversal of UDP over NATs*“ und ermöglicht einen transparenten Zugriff von Hosts in einem LAN auf externe Dienste und umgekehrt. STUN ist im RFC 3489 der IETF definiert.

[160] Ein *Codec* ist ein Algorithmus mit dem Daten codiert und decodiert werden können. In diesem Fall wird die Sprache digitalisiert und komprimiert, um die zu übertragende Datenmenge gering zu halten.

Externe Geräte

Da SIP ein offenes Protokoll ist, gibt es inzwischen etliche Anbieter von externen Geräten (Telefon, Telefon-Anlage, Router, usw.), welche die Integration von VoIP in das herkömmliche Telefonnetz unterstützen. Dadurch sind flexible Konfigurationen denkbar. Zusätzlich besteht die Möglichkeit, abhängig von Uhrzeit und Gesprächsart den günstigsten Tarif auszuwählen. Bei Skype ist diese Auswahl nicht gegeben.

Festnetznummer

SIP-Provider bieten eine Festnetznummer kostenlos an, wobei Skype eine Gebühr für diese verlangt. Zurzeit (Stand Datum der Arbeit) ist die SkypeIn-Funktion noch in der Testphase, so dass abzuwarten bleibt, wie Skype die Tarifierung bei der endgültigen Freigabe vornimmt. Bisher sind keine deutschen Festnetznummern erhältlich, sondern lediglich ausländische.

Verschlüsselung

Skype verschlüsselt sämtliche Daten bevor sie den Client verlassen. Bei SIP bieten die Provider in der Regel nur unverschlüsselte Verbindungen an. Die Unterscheidung zwischen Signalisierung und Sprachdaten ist bei SIP zu beachten. Im SIP-Standard (RFC 3261) wird die Verwendung per S/MIME[161] auf Anwendungsebene vorgeschlagen. Die Kommunikation bei SIP könnte auch auf der Transportschicht durch TLS[162] geschützt werden (SIPS). Die Übertragung der RTP-Sprachpakete hingegen könnte durch die Verwendung von SRTP[163] verschlüsselt werden.

Vergleich und Einsatzgebiete

Im Vergleich der beiden Standards steht ein offenes, modulares, standardisiertes Protokoll (SIP) einem proprietären, nicht öffentlichen, ganzheitlichen

[161] *Secure/Multipurpose Internet Mail Extensions* ist eine *Public Key*-Verschlüsselung, die ursprünglich für die Verschlüsselung und Signierung von E-Mails gedacht war. Unter http://www.ietf.org/html.charters/smime-charter.html fasst die IETF etliche Informationen und Links zu RFCs zusammen.

[162] *Transport Layer Security* beschreibt im RFC 3546 der IETF den sicheren Verbindungsaufbau zwischen Client und Server.

[163] Das *Secure Realtime Transport Protocol* ist eine Erweiterung von RTP um die Verschlüsselung durch AES (*Advanced Encryption Standard*). Siehe dazu RFC 3711 der IETF.

Protokoll (Skype) gegenüber. Die Bewertung, welcher Ansatz der richtige ist, ist schwer zu treffen, weil individuelle Präferenzen pro oder contra *Open Source* aufeinander treffen. In diesem Fall sollte der Vergleich der beiden Ansätze hinsichtlich des Einsatzes im gewerblichen Sektor vollzogen werden. Dann können Parallelen oder Unterschiede zu RFID aufgedeckt werden.

Eine große Parallele zu RFID ist das Vorhandensein von zwei verschiedenen Ansätzen bei der Standardisierung. Jeweils ein Ansatz ist dabei offiziell standardisiert (SIP, RFID ISO Standards) und jeweils ein Ansatz ist von einer privaten Unternehmung entwickelt (Skype, EPCglobal). Allerdings ist anzumerken, dass EPCglobal im Gegensatz zu Skype aus einem wissenschaftlichen Umfeld stammt und dass EPCglobal die Standards für die Öffentlichkeit anbietet, jedoch Gebühren für die Verwendung der Nummernkreise erhebt. Durch die Verschmelzung der RFID-Standards für die UHF Frequenz (siehe Kapitel 4.2.2.3) ist im RFID-Bereich allerdings ein erster Schritt in Richtung gegenseitiger Anpassung gemacht. Im VoIP-Bereich hingegen sind solche Bemühungen nicht erkennbar, so dass auch in naher Zukunft zwei getrennte Lösungen für VoIP parallel existieren werden. Der Zusammenschluss der meisten Provider im SIP-Sektor ist absehbar, da sich innerhalb der SIP-Provider immer größer werdende Kooperationen formen (Partnernetze).

Die Segmentierung von zwei vorherrschenden Lösungen im VoIP-Markt kann durch die verschiedenen Nutzer-Kreise erklärt werden. Skype ist kostenlos erhältlich, einfach zu installieren und benutzen, benötigt keine weitere Infrastruktur und enthält weitere Funktionen, wie einen *Instant Messenger*. All diese Eigenschaften bieten sich für den privaten Gebrauch an. SIP allerdings bietet eine Grundlage für den gewerblichen Sektor. Die offenen Standards sind für alle Hersteller erhältlich und in deren Produkte umsetzbar. Eine Integration von SIP in bestehende Telefon-Anlagen und Endgeräte ist denkbar und kann bei der Vernetzung von Zweigstellen über das Internet Kostenvorteile bringen. Skype wäre da sicherlich nur eine schlechte Lösung, da die Skype-Software immer nur in Verbindung mit einem PC oder PDA verwendet werden kann. Anwender von SIP-Geräten jeder Art können zwischen Produkten verschiedener Hersteller auswählen und ggf. den Anbieter wechseln. Dieser Wettbewerb sorgt für niedrige Preise und bietet einen gewissen Investitionsschutz, da Hard- und Software austauschbar sind. Beim Einsatz von Skype ist man auf die Firma Skype angewiesen (Login-Server). Das Problem der meist fehlenden

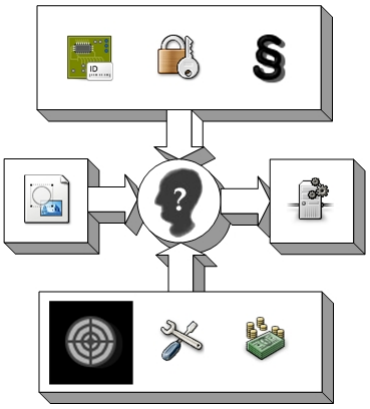
Verschlüsselung bei SIP wird in Zukunft sicherlich behoben werden, wenn die Anwender dies fordern.

Die Qualität und Praxistauglichkeit ist sowohl bei SIP als auch bei Skype schon so gut, dass ein großflächiger Einsatz bereits heute Realität ist. Viele Unternehmen scheuen noch den Einsatz, obwohl die laufenden Kosten durch VoIP deutlich gesenkt werden können. Telefon-Anlagen auf dem jetzigen Stand der Technik enthalten die Unterstützung für SIP, so dass bei den nächsten Neu-Anschaffungen VoIP sicherlich Beachtung findet. Auch für Privatleute ist SIP eine Alternative zu Skype, da deren herkömmliche Telefone mit aktuellen Telefon-Anlagen zu betreiben sind. Die Integration von SIP in DSL-Router[164] könnte ebenfalls die Verbreitung von SIP stärken.

[164] *Digital Subscriber Line* ist eine Übertragungstechnik von Daten über den herkömmlichen Telefonanschluss. Der in Deutschland weit verbreitete Internetzugang ADSL (*Asynchronous Digital Subscriber Line*) ist eine Ausprägung von DSL.

Kapitel 5

Bedeutung von RFID für die Logistik und das SCM



Die Begriffe Logistik und *Supply Chain Management*[165] werden häufig synonym verwendet. An dieser Stelle wird kurz auf die unterschiedliche Bedeutung der beiden Begriffe eingegangen. Logistik (oder auch Logistikmanagement) ist die Planung, Steuerung und Kontrolle von Güter-, Dienstleistungs- und Informationsflüssen zwischen den Punkten des Ursprungs und des Punktes des Konsums mit dem Ziel den Kundenanforderungen gerecht zu werden [vgl. CSCMP 2005]. Dabei sind typische Aktivitäten Transportmanagement, Flottenmanagement, Lagerhaltung, Materialwirtschaft, Auftragserfüllung, Inventarmanagement und das Management von externen Logistik-Dienstleistern [vgl. CSCMP 2005]. Diese Definition beschreibt die Prozesse innerhalb eines Unternehmens mit dem Ziel seine Kunden zu versorgen. Diese Auslegung von Logistik wird von einigen Autoren heute als eine frühe Definition von SCM gesehen [Krcmar 2004, S. 465].

Der Unterschied von Logistik zum heutigen SCM ist die Ausdehnung der Prozesse und Aktivitäten auf alle am Produkt beteiligten Unternehmen. Der wichtige Teil der Definition aus [CSCMP 2005] ist: Wichtig ist, dass ebenfalls Koordination und Kollaboration mit Partnern (Lieferanten, Intermediären, Dienstleistern und Kunden) enthalten ist. Demnach integriert SCM

[165] Eine passende deutsche Übersetzung lässt sich nur schwer finden, jedoch kommt der Begriff Lieferkettenmanagement dem am Nächsten.

das (in der Lieferkette vorgelagerte) Liefer- und (nachgelagerte) Nachfrage-Management innerhalb und jenseits des Unternehmens. Somit ist die Lieferkette als Erweiterung der intraorganisationalen Wertekette nach Porter zu sehen. [Krcmar 2004, S. 465] beschreibt diese Erweiterung mit der Einbeziehung der kompletten Logistikkette vom Rohmaterial bis zum Endkunden des Produkts.

Somit gewinnt das SCM maßgeblich an Bedeutung für alle Unternehmen innerhalb der Lieferkette, da Beschaffung, Produktion und Absatz Einfluss auf andere Glieder in der Kette nehmen. Dabei ist ebenfalls die Betrachtung von beteiligten Gliedern in anderen Unternehmen gefordert. Die interorganisationale Sicht auf die Prozesse schafft Transparenz hinsichtlich der Güter- und Informationsströme [Krcmar 2004, S. 465], so dass viele Vorteile für die beteiligten Unternehmen entstehen. Diese Vorteile können sein: schnellere Reaktion auf Kundenanforderungen oder kürzere Durchlaufzeiten und somit effektivere und effizientere Abläufe, wodurch Kosten gespart werden können. [Fleisch u. a. 2003] führt zusätzlich an, dass durch erhöhte Transparenz nicht nur die Durchlaufzeiten, sondern auch Bestände, *Out-of-stock*-Situationen[166], Diebstähle, Fälschungen und Schäden minimiert werden könnten.

Der Informationsfluss spielt in dieser Arbeit die größte Rolle bei der Betrachtung der Lieferkette. Für den reibungslosen Einsatz von Informationssystemen (IS) zur Unterstützung des SCM sind Vernetzung, Transparenz und Verfügbarkeit der Daten wichtige Voraussetzungen. Ein höherer Grad an Automatisierung und die Vermeidung von Medienbrüchen[167] sind zwei der erreichbaren, unternehmerischen Ziele [vgl. Fleisch u. a. 2002, S. 6]. Auf diese und auf weitere Ziele wird später noch genauer eingegangen.

RFID kann als Auto-ID-Technologie die Lücke zwischen den realen, physischen Gütern und den in den Informationssystemen virtuell abgebildeten Objekten schließen. [Weis 2005, S. 105] bezeichnet RFID als potenzielle Brücke

[166] Eine *Out-of-stock*-Situation entsteht, wenn die für einen Auftrag benötigte Menge eines Artikels der vorhandenen Menge im Lager entspricht oder sie gar übersteigt. Aktuelle oder unmittelbar nachfolgende Aufträge können dann nicht erfüllt werden, so dass Produktion oder Lieferungen verzögert werden. Dies führt zu Planungsänderungen, Mehrkosten und ggf. Lieferverzug.

[167] Ein Medienbruch ist der Übergang von Informationen von einem Medium auf ein anderes bei dem Informationen verloren gehen, die Verarbeitung verlangsamt wird oder Übertragungsfehler entstehen.

zwischen der „*real world*“ und der „*online world*“[168]. RFID wird von [Römer u. a. 2004, S. 689] als Möglichkeit zur Überwindung der Trennung von physischer und virtueller Welt gesehen. All diese Sichten auf die Aufgabe von RFID sind verwandt und lassen sich in das Feld der virtuellen Aktualität[169] einordnen. Aktive, reale Elemente (meist RFID-Leser, aber möglicherweise auch aktive Tags) erfassen bestimmte Vorgänge in der Realität und melden sie an das IS, welches darauf hin Operationen auf den Datenbeständen vornimmt. Diese realen Vorgänge sind z. B. das (Nicht-)Vorhandensein eines Tags oder ein Ereignis eines Sensors. Dabei werden die realen Objekte identifiziert, lokalisiert oder deren Status abgefragt.

In Abbildung 5.1 stellt Fleisch den Zusammenhang zwischen verschiedenen Möglichkeiten der Datenerfassung und der Annäherung von realer und virtueller Welt dar. In der Grafik entspricht die Lücke zwischen beiden Welten den Kosten für die Dateneingabe, die als Folge von Medienbrüchen entstehen [vgl. Fleisch u. a. 2002, Abb. 2]. Mit dem Übergang von Barcodes zu RFID werde ein Grad der Automatisierung erreicht, bei dem kein menschliches Eingreifen notwendig sei. Sicherlich ist diese Annahme kritisch zu betrachten, da in der Praxis immer noch Fehlfunktionen, technische Störungen oder inhaltliche Fehler auftreten können.

Durch den Einsatz von RFID im SCM können Objekte identifiziert und lokalisiert werden. Zusätzlich besteht die Möglichkeit weitere Daten auf dem Tag an dem Objekt (dezentral) zu speichern oder auf einem IS (zentral) abzulegen. Für [Hülsenbeck 2006, S. 10] ist die Trennung des Waren- und Informationsflusses in der Logistik der entscheidende Mehrwert. Durch die Verbindung von physischen Objekten und Informationen durch RFID ergeben sich vier Verbesserungsmöglichkeiten im SCM [Hülsenbeck 2006, S. 10]:

- Vereinfachung von Prozessen: Durch die erhöhte Transparenz können die Prozesse besser überblickt und auf außergewöhnliche Ereignisse effizienter reagiert werden.

[168] Der Semacode (http://semacode.org und http://semacode.com) ist ebenfalls eine Möglichkeit reale Objekte durch die Codierung einer URL mit Online-Informationen zu verknüpfen. Repräsentiert werden die URLs in dem 2D-Barcode DataMatrix.

[169] Virtuelle Aktualität ist ein abgebildeter Teil der wahrnehmbaren Realität [v. Kortzfleisch 2005, 3. Sitzung]. Dies ist vergleichbar mit einer Simulation, die nicht selbstständig abläuft, sondern durch aktuelle Vorgänge in der Realität gesteuert wird.

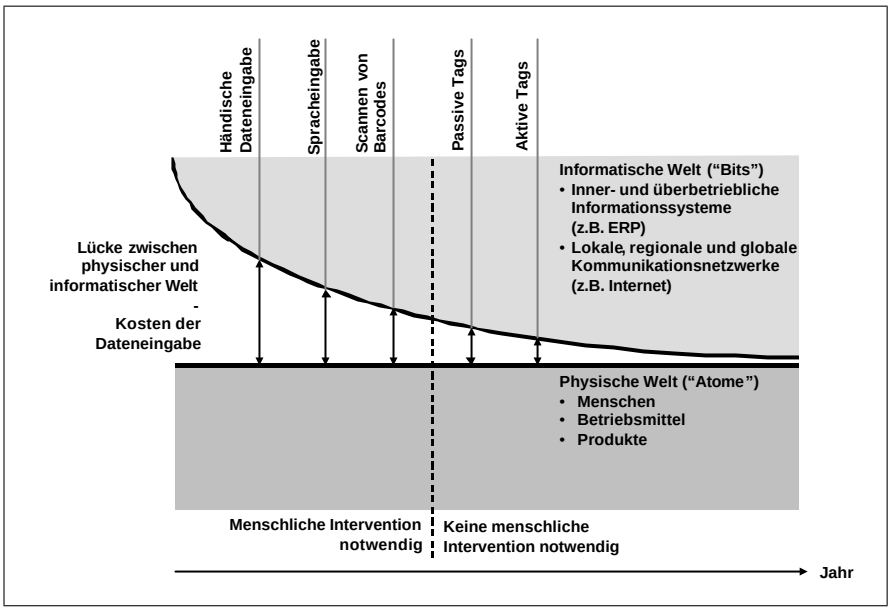


Abbildung 5.1: Annäherung von realer und virtueller Welt hinsichtlich Medienbrüchen und Automatisierung [Fleisch 2001, Abb. 3].

- Erhöhung der Verfügbarkeit und Qualität: Die zu einem Prozess gehörenden Informationen sind vollständiger und mit weniger Fehlern behaftet. Sie stehen den Beteiligten im besten Fall uneingeschränkt zur Verfügung.
- Verkürzung von Reaktionszeiten: Informationen gelangen durch die erhöhte Automatisierung schneller an die beteiligten Parteien. Außerdem kann auch auf Informationen von anderen Unternehmen zugegriffen werden, so dass frühzeitig auf Änderungen reagiert werden kann.
- Reduzierung nicht wertschöpfender Prozesse: Die anfallenden Kosten für Verwaltung, Koordination, Kontrolle, Informationsbeschaffung und -speicherung können reduziert oder aufgeteilt werden. Im Grunde betrifft dies die Transaktionskosten und nicht die Kosten für die Güter.

Bei einer interorganisationalen Zusammenarbeit ist es notwendig, die anfallenden Informationen auszutauschen. Stellen private Netzwerke innerhalb von Unternehmen die Verbindung zu den Informationssystemen her, bedarf es bei unternehmensübergreifender Kommunikation eines zusätzlichen Zugangs von

außen zu den Daten. Dabei bietet sich das Internet als Übertragungsmedium an, weil inzwischen so gut wie jedes Unternehmen einen Internetzugang besitzt. Neben dem technischen Zugriff stellt sich natürlich auch die Frage nach den Berechtigungen und den Sicherheitsaspekten, da das Internet an sich ein unsicheres Medium ist. Zusätzlich zu den stationären Teilnehmern bieten kabellose Funknetzwerke die Möglichkeit zur mobilen Datenerfassung und -verarbeitung. Dabei sind alle IP-basierten Netze denkbar, wie private WLANs oder öffentliche Mobilfunknetze (GSM, UMTS).

Eine weitere Aufgabe neben der Kommunikation ist die Integration der verschiedenen Datenbestände, Anwendungen und Prozesse, so dass für alle Beteiligten ein Mehrwert entsteht. Integration nimmt in dieser Arbeit einen großen Stellenwert ein. In den folgenden Kapiteln wird auf Integration verstärkt eingegangen.

Die Datenbestände und Anwendungen befinden sich an zentraler Stelle in den Informationssystemen. Diese Informationssysteme müssen erweitert werden, wenn sie für RFID im SCM eingesetzt werden (vgl. Kapitel 1 und 2.2). Sind die technischen Anforderungen an die RFID-Tags und Leser erfüllt und ist die technische Infrastruktur für eine erfolgreiche Kommunikation vorhanden, dann müssen die Daten im IS korrekt weiterverarbeitet und gespeichert werden. Wie diese Weiterverarbeitung im Einzelnen aussieht, hängt von dem verwendeten IS und den RFID-Anforderungen ab. Ein Ansatz für eine technische Realisierung eines RFID-Systems (mobiler Client, Kommunikation und Backend) im Behältermanagement wird ab Kapitel 8 vorgestellt.

5.1 Aktuelle Situation in der Praxis

Zurzeit gibt es zwei Branchen, in denen RFID in der Lieferkette produktiv eingesetzt wird. Zum einen ist dies der Handel, zum anderen die Automobilindustrie. Im Handel setzen hauptsächlich große Ketten (Wal-Mart, Metro) RFID ein, um ihre Produkte vom Lieferant bis zur Filiale zu überwachen und zu steuern. Diese Systeme sind geschlossen, da nur direkt beteiligte Parteien partizipieren.

In der Automobilindustrie sind die Bestrebungen weitaus vielfältiger, um von RFID in der Lieferkette zu profitieren. Grund dafür sind die Marktanforderungen an die Hersteller. Permanenter Rationalisierungsbedarf, hö-

here Anforderungen an die Produktzuverlässigkeit, gesetzliche Anforderungen zur besseren Nachhaltigkeit und Automatisierung von ungeführten[170] Prozessen stellen für die Automobilindustrie die größten Verbesserungspotentiale dar [Strassner 2005, S. 2 ff.]. Dadurch ergeben sich zwei verschiedene Systeme des RFID-Einsatzes. Das erste System umfasst die Lieferanten für die Automobil-Hersteller, um die Identifikation und Herkunft von Teilen zu gewährleisten. Das zweite System ist ein internes, geschlossenes System, welches die Verwaltung von Werkzeug und Transportmitteln unterstützen soll [vgl. Strassner 2005, S. 93 f.]. Bei Volkswagen[171] (VW) wurden Spezialgestelle mit RFID-Tags ausgestattet, damit die Behälterverfügbarkeit gesteigert und der Schwund verringert werden kann [Strassner 2005, S. 157 f.].

Im Herbst des Jahres 2000 wurde in den USA der *TREAD Act*[172] erlassen [US Congress 2000]. Das Gesetz verpflichtet die Hersteller von Fahrzeugen oder Fahrzeugteilen dazu, sicherheitsrelevante Mängel an die zuständigen, amerikanischen Behörden zu melden [Strassner 2005, S. 2 f.]. Damit sollen Folgeschäden aus Produktmängeln vermieden und die Sicherheit der Fahrzeuge auf den Straßen verbessert werden. Seit dem Jahr 2005 kommt hinzu, dass bestimmte sicherheitsrelevante Teile eindeutig dem Fahrzeug zugeordnet werden müssen. Somit müssen z. B. die Seriennummern von Autoreifen eindeutig mit der Fahrgestellnummer verknüpft werden [Strassner 2005, S. 182]. Der große Reifenhersteller Continental hat ein Konzept für den RFID-Einsatz entwickelt und prüft, ob RFID auch in der Lieferkette zu einem erhofften Nutzen führt [vgl. Strassner 2005, Kap. 5.6].

In allen genannten Bereichen existieren keine übergreifenden Abkommen über den zu verwendenden Standard, so dass jeder Hersteller seine eigene Wahl des RFID-Systems trifft. Lediglich bei der Kennzeichnung der Reifen erarbeiten zwei Automobil-Verbände Empfehlungen über die Position des Tags, die Frequenz, das Protokoll und die Datenstruktur [Strassner 2005, S. 185].

[170] Ungeführt bedeutet in diesem Zusammenhang eine vorab unbekannte Dynamik innerhalb von Abläufen. Im Transportwesen sind geführte Prozesse z. B. im Schienenverkehr anzutreffen, währenddessen die Bewegungen von Containern ungeführt sind.

[171] http://www.volkswagen.de

[172] TREAD steht für *Transportation Recall Enhancement, Accountability and Documentation.*

5.1.1 Ebene der Kennzeichnung

Im Handel und in der Lieferkette gibt es unterschiedliche Verpackungsmöglichkeiten. Abhängig von der Artikelart (Einzelstück, Massenware, usw.), der Größe oder dem Wert werden Artikel einzeln oder in Verpackungseinheiten verpackt und versendet. Daraus ergeben sich verschiedene Ebenen von Verpackungseinheiten. In der klassischen und am weitesten verbreiteten Einteilung ist die unterste Ebene die Artikel-Ebene (*item level*), die mittlere ist die Karton-Ebene (*box level*) und die oberste ist die Paletten-Ebene (*pallet level*). Diese Einteilung gilt für die meisten Artikel des Handels, wie sie in den Supermärkten angeboten werden.

Eine andere Einteilung wird von der ISO TC 122/104 Joint Working Group (JWG) vorgenommen. In den ISO-Standards 17363–17367 werden fünf Ebenen der RFID-Kennzeichnung in der Logistik spezifiziert, so dass sich insgesamt eine sechsschichtige Einteilung ergibt (siehe Abbildung 5.2). Dabei ergeben sich die Ebenen Artikel, Packung, Transport-Einheiten, Paletten, Container und Fahrzeug. Kennzeichnungen sind nur auf den unteren fünf Ebenen sinnvoll, so dass auch nur für diese Ebenen ein Standard in Arbeit ist.

Allerdings kann es in anderen Branchen weitere mögliche Einteilungen geben. Die Kennzeichnung mit RFID auf den verschiedenen Ebenen ist im Vorfeld einer RFID-Einführung von hoher Bedeutung. Ist die Kennzeichnung von Gütern beim Transport von einem Lager in eine Filiale von Interesse, dann bietet sich die Kennzeichnung auf der Kisten- oder Paletten-Ebene an. Eine Kennzeichnung jedes einzelnen Artikels würde sicherlich auch funktionieren, jedoch stellt sich Frage, ob die dadurch entstehenden Kosten (durch die größere Anzahl von Tags) und die anfallenden Datenmengen vertretbar und angemessen sind.

Im Handel steht die Auszeichnung auf Artikel-Ebene noch nicht zur Diskussion. Die Kosten der Tags sind für einfache Artikel noch zu hoch. Für große Ketten entsteht auch kein Mehrwert oder Nutzen durch die Kennzeichnung auf Artikel-Ebene. Von Interesse ist zurzeit lediglich die Lieferkette bis in die Filiale. Die in der Lieferkette verwendeten Verpackungseinheiten sind mindestens Kartons, wenn nicht sogar ganze Paletten. Aus diesem Grund hat sich die Metro entschieden, auf Karton-Ebene zu kennzeichnen [Kuri 2006].

In der Pharmaindustrie hingegen setzt sich mittlerweile das Kennzeichnen auf Artikel-Ebene durch. Allerdings sind die Gründe nicht die Verfolgung der

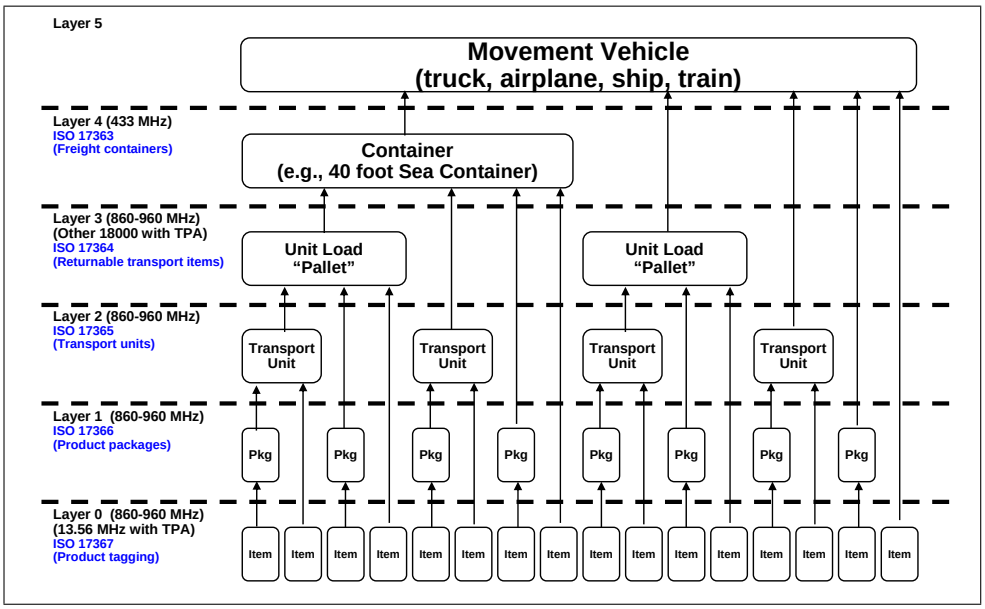


Abbildung 5.2: Einteilung der Ebenen zur Kennzeichnung von RFID-Produkten in der Lieferkette der ISO TC 122/104 JWG [Harmon 2005, S. 30].

Produkte in der Lieferkette, sondern die Fälschungssicherung. Hochwertige Medikamente werden mit Tags ausgezeichnet, damit Händler und Endkunden die Echtheit feststellen können. Massenprodukte, wie z. B. Kopfschmerztabletten, dagegen werden sicherlich nicht ausgestattet, da das Preis-Verhältnis von Produkt zu Tag zu ungünstig ist.

5.1.2 Frequenzen im SCM

Der Preis spielt auch bei der verwendeten Frequenz eine große Rolle. Die Preise im HF- und im UHF-Bereich unterscheiden sich je nach Ausführung des Tags. Auch die Reichweite ist von Bedeutung, da höhere Frequenzen höhere Reichweiten erzielen können. Des Weiteren beeinflussen bestimmte Materialien, wie Wasser und Metalle, die Qualität und Reichweite von RFID-Operationen.

Aus diesem Grunde gehen die Meinungen von Experten und Unternehmen in der Frage der richtigen Frequenz für das SCM weit auseinander. Passive, günstige Tags können für viele SCM-Anwendungen adäquat sein, jedoch muss der Betreiber dann im Einzelfall bereit sein, bestimmte Kompromisse zwischen den

Faktoren Preis, Funktionsumfang und Sicherheitsaspekten einzugehen [Sarma u. a. 2003, S. 456 f.].

Wal-Mart ist zurzeit der führende Betreiber von RFID in der Lieferkette. Das Unternehmen verpflichtet die größten Lieferanten dazu, alle Produkte auf Karton-Ebene zu kennzeichnen. Unter den Lieferanten sind sehr namhafte Firmen, wie z. B. Hewlett-Packard[173], Johnson & Johnson[174], Kimberly-Clark[175], Kraft Foods[176], Nestle[177] und Procter & Gamble[178]. Wal-Mart verwendet die Gen 2 Tags von EPCglobal für die Kennzeichnung aller Produkte auf Paletten- und Karton-Ebene. Bisher ist noch keine offizielle Planung für die Kennzeichnung auf Artikel-Ebene bekannt. Lediglich ein Artikel im „RFID Journal“ gibt Hinweise auf Wal-Marts Absicht auch UHF auf Artikel-Ebene einzusetzen [O'Connor 2006].

Insgesamt spricht vieles für den Einsatz von HF auf Artikel-Ebene. Betreiber und Hersteller beschreiben HF als ideal für die Artikel-Ebene [TRS 2006]. Allerdings müsste für eine gemischte Kennzeichnung von HF und UHF auch eine Infrastruktur geschaffen werden, welche beide Frequenzbereiche erfassen kann. In [Havens 2006] fordert Craig Harmon das Zusammenschmelzen von HF und UHF im SCM. Nicht das Kennzeichnen von Objekten sei das Problem, sondern die Fähigkeiten der Leser seien zu verbessern.

Zusammenfassend kann man sagen, dass mittelfristig erst einmal UHF-Frequenzen im SCM eingesetzt werden (Gen 2, ISO/IEC 18000-6). In geschlossenen Systemen jedoch kann jeder Betreiber die für sich beste Lösung aussuchen.

5.2 Motivation für RFID in SCM

Mit zunehmender Bedeutung des Liefernetzwerkes lassen sich verschiedene Anforderungen an das SCM definieren. Werden diese Anforderungen erfüllt, so steigt die Wahrscheinlichkeit einen Nutzen aus dem Einsatz von zusätzlichen Technologien zu ziehen. RFID kann eine dieser Technologien sein, damit aus einer Menge notwendiger Prozesse in Logistik und Transportwesen ein Wettbewerbsvorteil entstehen kann.

[173] http://www.hp.com
[174] http://www.jnj.com
[175] http://www.kimberly-clark.com
[176] http://www.kraft.com
[177] http://www.nestle.com
[178] http://www.pg.com

Viele Branchen sehen sich einem hohen Preisdruck ausgesetzt, so dass eine Senkung der Kosten bei gleich bleibendem Nutzen erzielt werden sollte. Da die menschliche Arbeitskraft ein gewisser Kostenfaktor ist, kann eine Automatisierung von gewissen Abläufen Kosten einsparen (Substitution). Gleichzeitig haben automatisierte Abläufe ein geringeres Fehlerpotential als Abläufe mit manuellen Tätigkeiten.[179] Dies kann Folgekosten aufgrund von Fehlern einsparen [Strassner 2005, S. 100].

Gleichzeitig besteht die Chance, die Abläufe schneller zu erledigen. Durch den Einsatz von RFID werden Paletten, Kartons oder Artikel gleichzeitig und schnell erfasst. Dies spart kostbare Zeit ein, die dazu aufgebracht werden müsste, manuelle Schritte auszuführen. In einer komplett mit RFID erfassten Lieferkette stehen im idealen Falle alle notwendigen Daten zu jedem Zeitpunkt zur Verfügung. Dies ermöglicht ein unmittelbares Eingreifen bei Änderungen in den Abläufen.

In vielen Branchen (Automobilindustrie, Handel, Industrie) wird das Lager einer Produktion vom Produktionsort auf die Straße verlagert. Das Konzept des *Just in Time* (JIT) hat in der Lieferkette eine große Bedeutung und verhilft Herstellern zu einer allgemeinen Rationalisierung. Da durch die örtliche Verlagerung der benötigten Produkte auf die Straße oder zu den Lieferanten eine gewisse Unsicherheit entsteht, hilft eine bessere Informationsversorgung die verloren gegangene Transparenz wieder zurück zu gewinnen. Da durch RFID die Produkte identifiziert und lokalisiert werden können, hat der Hersteller die Möglichkeit, frühzeitig auf Abweichungen zu reagieren und damit Kosten aufgrund von Produktionsausfällen zu vermeiden. Nicht zu verschweigen ist die größere Belastung der Lieferanten, die neben der Kennzeichnung der Produkte auch die geforderten Informationen zu liefern haben.

In den letzten Jahrzehnten werden immer mehr Anforderungen an die Lieferkette gestellt, weil große Unternehmen weltweit operieren (Globalisierung). Zeitgleich ist die Anforderung der Kundenorientierung immer stärker in den Vordergrund gerückt (z. B. in der Automobilindustrie [Strassner 2005, S. 72 f.]). Diese Kombination stellt eine Herausforderung an das SCM dar, weil schneller weitere Wege zurückzulegen sind. Dies erfordert eine höhere Flexibilität und eine schnellere Reaktion auf kurzfristige Trends.

[179] Diese generelle Aussage kann bei unangemessener Automatisierung auch falsch sein. Spielt das Wissen oder die Erfahrung von Mitarbeitern eine große Rolle, so ist die Substitution durch Technologien und Maschinen zu hinterfragen.

In [Michael und McCathie 2005] werden zusätzliche Aufgaben und Anforderungen von RFID im SCM genannt. Diese lassen sich wie folgt kurz zusammenfassen:

- Identifikation von Retouren und Garantiefällen,
- Qualitätskontrolle (z. B. Temperaturüberwachung),
- Lagermanagement,
- Sicherheitsaspekte und Fälschungssicherheit,
- Zusammenarbeit zwischen verschiedenen Unternehmen und Sparten.

In der Behälter- und Containerlogistik hat RFID das Potential bei drei Aufgaben Unterstützung zu leisten [Hülsenbeck 2006, S. 17]:

1. Segmentierung: Durch die Zuordnung von Objekten zu einem Container kann eine Zusammenfassung von Objekten vorgenommen werden. Die Betrachtung des Containers mit den enthaltenen Objekten bedeutet eine Generalisierung und damit Komplexitätsverminderung. Diese Generalisierung ist eine Form der Abstraktion von einzelnen Objekten.
2. Lokalisierung: Es ergeben sich verschiedene Bezugssysteme, in denen verschiedene Objekte lokalisiert werden können. Der Container kann innerhalb des Bezugssystems Firmengelände lokalisiert werden. Objekte lassen sich innerhalb des Bezugssystems Container lokalisieren, weil die Verknüpfung von Objekt zu Container gegeben ist und die Position des Containers bekannt ist.
3. Controlling: Aufgrund des Ortes von Containern und der Information über die enthaltenen Objekte können Bestände an verschiedenen Orten überwacht und gesteuert werden.

Lokalisierung kann im SCM wie auch im Allgemeinen mit verschiedenen Lösungen geleistet werden. Unter freiem Himmel bietet sich GPS zur Lokalisierung an, weil es außer einem GPS-Empfänger keine weitere Infrastruktur benötigt. Die Genauigkeit von GPS liegt im Bereich von wenigen Metern, was für die meisten Anwendungen ausreichen sollte. Innerhalb von Gebäuden

kann die grobe Position eines Objektes über fest installierte Gates ermittelt werden. Wird ein Objekt durch ein solches Gate befördert, wird dies registriert und gespeichert. Diese Gates sollten dann an markanten Punkten des Geländes positioniert sein, wie z. B. an Toren zwischen Hallen oder an Zugängen zu Sammelplätzen oder Lagern. Schließlich existieren weitere Systeme zur Lokalisierung, die auf RFID basieren. Die Firma RFind[180] bietet ein System an, welches aktive Tags lokalisiert. Verschiedene Leser innerhalb der Gebäude registrieren einen bestimmten RFID-Tag. Aufgrund der Laufzeit und Signalstärke des elektromagnetischen Feldes und den damit übermittelten Informationen berechnet die dazugehörige Software die Position des Tags. Leider werden keine näheren Angaben über die Genauigkeit der berechneten Position gemacht.

5.3 Ziele zum Einsatz von RFID

Im vorangegangenen Kapitel wurden mögliche Beweggründe für den RFID-Einsatz im SCM genannt. Durch den Einsatz neuer Technologien können möglichen Optimierungen verwirklicht werden. Dabei sollte nicht die zur Verfügung stehende Technik diese Optimierungen auslösen, sondern der richtige Ausgangspunkt für eine Umstellung von IT-Systemen und Prozessen sind die konkreten Absichten und Ziele eines Betreibers. Ein Betreiber sollte die Schwachstellen in seinem Unternehmen identifizieren und benennen können, damit er daraus seine zu erreichenden Ziele ableiten kann. Ausgehend von den zu erreichenden Zielen sollen dann weitere Planungen folgen.

Zunächst sind die langfristigen Ziele eines Unternehmens von größter Bedeutung. Was möchte der Betreiber erreichen? Wo sind langfristig die größten Verbesserungspotentiale? Welche allgemeine Ausrichtung der Unternehmung ist von Bedeutung? Aus diesen allgemeinen Zielen lassen sich dann die operativen Anforderungen an die Systeme ableiten. Welche Prozesse sind betroffen? Welche mögliche Reorganisation von Prozessen ist denkbar? Schließlich bieten sich für diese Anforderungen bestimmte Alternativen für die technische Umsetzung an. Welche Alternativen sind möglich? Welche sind sinnvoll? Welche wird ausgewählt?

[180] http://www.rfind.com

5.3.1 Strategische Ziele

Die strategischen Ziele eines Unternehmens bestimmen die Ausrichtung des aktuellen und zukünftigen Handelns. Diese Ziele werden von den Stellen im oberen Management definiert, also von der Führung und den Verantwortlichen einer Unternehmung. Dabei ist zu beachten, dass strategische Ziele auf langfristige Zeiträume ausgelegt sind. Sie bestimmen maßgeblich zukünftige Entscheidungen und damit die Zukunft des Unternehmens. Vereinbart ein Unternehmen Ziele, die nicht adäquat sind oder das Unternehmen in die falsche Richtung lenken, dann kann dies von leichten Problemen bis hin zur Schließung des Betriebs führen.

Diese Ziele sind oft in der Anzahl stark begrenzt und inhaltlich eher allgemein gehalten. Über die Vorgehensweise zum Erreichen der Ziele werden keine Aussagen gemacht. Beispiele für typische Ziele sind Gewinnmaximierung, Erhalt der Arbeitsplätze oder Marktdominanz. Häufig bestimmen die Produktpolitik und damit auch das Marketing zu großen Teilen diese Ziele, weil die Produkte ein Unternehmen definieren und meist das Kerngeschäft darstellen.

Es gibt jedoch auch strategische Ziele, die weniger allgemein sind und sich auf Teile eines Unternehmens beziehen, z. B. Produktion, Lagerhaltung oder Lieferkette. Dabei könnten folgende Ziele von Bedeutung sein: höhere Transparenz in der Wertschöpfungskette, höhere Automatisierung beim Informationsaustausch, bessere Kontrolle über Mengen und Zustände oder Minimierung von Störungen in der Lieferkette [vgl. Kroll 2005, S. 6].

Schließlich diktieren neu geschaffene Gesetze die Ziele eines Unternehmens. Wird ein neues Gesetz zur Rückverfolgung von Gütern gültig, dann muss das Unternehmen diesem Gesetz gerecht werden und ggf. Ziele neu definieren oder neue Ziele aussprechen.

5.3.2 Operative Anforderungen

Aus diesen Zielen ergeben sich Anhaltspunkte für das obere und mittlere Management zur Umsetzung. Dabei wird hauptsächlich die aktuelle Situation der Aufbau- und Ablauforganisation innerhalb des Unternehmens betrachtet, sowie die interorganisationalen Verknüpfungen. Die aktuellen Prozesse sollten

dafür dokumentiert sein, so dass diese Modelle[181] der Prozesse als Grundlage für Verbesserungen genommen werden können.

Innerhalb der Menge aller Prozesse eines Unternehmens werden die betroffenen Prozesse identifiziert. Dabei ist zu beachten, dass Abhängigkeiten und Wechselwirkungen zwischen Prozessen bestehen können. Dabei spielen die Qualität der Modelle und die Fähigkeiten der bearbeiteten Verantwortlichen eine wichtige Rolle. Sind die Prozesse identifiziert, stellt sich die Frage nach der Modifikation der Prozesse. Wie können die Prozesse angeordnet werden, damit die Ziele erreicht werden? Dabei können unterschiedliche Ergebnisse erzielt werden. Führt die Modifikation einzelner Prozesse zu dem gewünschten Ergebnis, bedeutet dies tendenziell einen geringen Aufwand für den Modellierer. Müssen mehrere Prozesse von Grund auf neu modelliert werden, dann spricht man *Business Process Reengineering* (BPR). Diese Neugestaltung von Prozessen ist sehr aufwändig und bedeutet ein gewisses Risiko für die Unternehmung, weil die theoretische Planung in der Theorie häufig zu unvorhergesehenen Problemen führen kann. Im ungünstigsten Fall besteht keine Möglichkeit die Prozesse so anzupassen, dass die Ziele erreicht werden. Dann muss im Einzelfall das weitere Vorgehen mit dem oberen Management abgestimmt werden. Eventuell bieten sich weitere Alternativen, wie z. B. *Outsourcing*[182], an.

Neben den Prozessen müssen weitere Entscheidungen getroffen werden, die eine technische Umsetzung definieren. Wie sieht bei einer Einbeziehung von Partnern die Informationspolitik aus? Darf jeder Teilnehmer alle Daten einsehen? Wie sieht das Berechtigungskonzept aus?

Sind die beteiligten Partner alle bekannt oder kann jede Firma partizipieren? Diese Frage bestimmt die Reichweite des RFID-Systems. Verlassen die gekennzeichneten Objekte bestimmte Wege oder Gelände nicht, dann nennt man dies einen geschlossenen Kreislauf. Alle Partner und Lokationen sind bekannt, so dass Unternehmen außerhalb dieses Kreislaufes keinen Kontakt mit den Objekten haben. Werden die Objekte jedoch auf unbekannten Pfaden und zu unbekannten Unternehmen geführt, wie etwa den Verkauf an nachgelagerte Kunden, dann spricht man von einem geschlossenen Kreislauf. Der Begriff

[181] Ein Modell ist ein verkürztes Abbild der Realität. Es beinhaltet die wesentlichen Eigenschaften und Verhaltensweisen und abstrahiert von den restlichen Aspekten.

[182] *Outsourcing* ist das Auslagern von Prozessen oder Teilen der Produktion zu anderen, externen Unternehmen. Häufig werden Abteilungen außerhalb des Kerngeschäfts ausgelagert. Bei Verwaltungsarbeiten könnte dies die Buch- oder Lohnbuchhaltung sein, in der Produktion die Herstellung von Halbfertigprodukten.

„Kreislauf“ wird in der Praxis auch oft dann verwendet, wenn die Objekte gar keine Rückkehr zu einer Produktionsstätte oder sonstiger, vorher besuchter Lokation vornehmen. Bei genauer Bezeichnung kann ein offener Kreislauf auch als offener Pfad bezeichnet werden, um die fehlende Rückkehr zu betonen. Im Folgenden wird jedoch bei der Teilnahme von unbekannten Partnern stets die Bezeichnung offener Kreislauf verwendet.

Neben diesen organisatorischen Maßnahmen, sind im Einzelfall deutlich mehr Aspekte zu beachten. Im Speziellen bei RFID kommen zusätzlich weitere Faktoren hinzu. Auch technische Eigenschaften sollten bei operativen Überlegungen einbezogen werden. Wenn sich z. B. der Einsatz von elektromagnetischer Strahlung verbietet, ist dies ein Kriterium gegen den Einsatz von RFID. Ebenfalls sollte bei dem Ziel der Kennzeichnung und Identifikation von Objekten die Ebene der Kennzeichnung definiert werden (vgl. Kapitel 5.1.1).

5.3.3 Technische Möglichkeiten

Sind alle operativen Eigenschaften festgelegt, dann kann im darauf folgenden Schritt die Liste der Anforderungen für das einzuführende System erstellt werden. Dabei stellt sich stets die Frage, ob es neben RFID auch andere Technologien gibt, die die Aufgabe der Kennzeichnung und Identifikation lösen können. Im Grunde kommen prinzipiell alle Auto-ID-Technologien in Frage (siehe Kapitel 2.1).

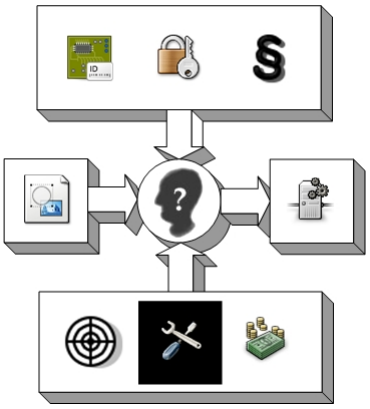
Die Unterschiede von RFID zu der am meisten verbreiteten Auto-ID-Lösung – dem Barcode – wurden bereits in Kapitel 2.4 behandelt. In den vorherigen Kapiteln wurde bereits häufig auf die technischen Eigenschaften eingegangen. Diese Eigenschaften dienen als Grundlage für die Auswahl der richtigen Kombination von Tags, Leser und Software.

Wichtige Größen im SCM sind die Lesereichweite und die Frequenz. Diese beiden physikalischen Eigenschaften wurden bereits in Kapitel 2.2 detailliert behandelt. Ebenfalls wurde in Kapitel 2.2.3 die Problematik von RFID im Zusammenspiel mit Flüssigkeiten und Metallen behandelt. Im SCM werden selbstverständlich auch Güter transportiert, welche aus Metall bestehen, mit metallischen Verpackungen versehen sind oder Flüssigkeiten enthalten. Bei Getränkedosen sind sogar Kombinationen aus den kritischen Materialien anzutreffen.

Die operative Vorgabe der Anwendungsreichweite entscheidet über die Notwendigkeit eines offenen und für alle Partner einsetzbaren Standard. Bei offenen Kreisläufen spielt die Luftschnittstelle eine wichtige Rolle. Da Standards auch für eine gewisse Zukunftssicherheit sorgen, ist ein breit anerkannter Standard tendenziell die sicherere Variante.

Kapitel 6

Handlungsmuster beim Einsatz von RFID im SCM



Dieses Kapitel baut inhaltlich direkt auf dem vorherigen Kapitel auf. Die ermittelten Ziele und Anforderungen eines Unternehmens dienen als Motivation für die Planung und anschließende Umsetzung. Das Kapitel behandelt zum einen drei Instrumente für die Realisierung von RFID-Systemen und zum anderen drei mögliche, resultierende Effekte.

Bei einer immer größer werdenden Anzahl von Informationssystemen und immer mehr anfallenden Daten bieten neue Technologien eine Möglichkeit zur notwendigen, besseren Koordination. RFID ist eine potentielle Lösung für die Verbesserung dieser Koordination.

Die Vorgehensweise ist in der Praxis auf die jeweilige Anwendung anzupassen. Jedoch lassen sich bestimmte, immer wieder kehrende Aspekte herausarbeiten. Diese Aspekte werden im ersten Teil dieses Kapitels behandelt. Daraus ergeben sich dann verschiedene Möglichkeiten zur Optimierung. Der zweite Teil des Kapitels besteht aus der Auseinandersetzung mit drei resultierenden Effekten aus diesen Optimierungen.

Die hier genannten Aspekte gelten sowohl für stationäre als auch für mobile RFID-Lösungen, da sowohl die Instrumente als auch die Effekte einen allgemeingültigen Charakter besitzen. Wenn wesentliche Unterschiede zwischen stationären und mobilen Systemen von Bedeutung sind, werden sie explizit angeführt.

6.1 Instrumente zur Koordination

Koordination ist in der Lieferkette ein entscheidender Faktor für eine effektive und effiziente Planung und Steuerung. Man kann ein SCM-System in verschiedene Komponenten unterteilen [Strassner 2005, S. 99]. Die zentralen SCM-Komponenten haben zur Aufgabe die globalen Prozesse zu planen und kontrollieren. Lokale, dezentrale Anwendungen hingegen sammeln die notwendigen Daten an den Gliedern der Lieferkette, an denen die Güter wesentliche Stellen passieren, Status-Änderungen erfahren oder übergeordnete Entscheidungen benötigen. Diese lokalen Anwendungen können z. B. in PPS oder WMS (*Warehouse Management System*) enthalten sein und sind Teil des großen, übergreifenden SCM-Prozesses. Koordination ist nicht nur zwischen diesen zentralen und dezentralen Komponenten des SCM-Systems notwendig, sondern auch an der Schnittstelle zwischen den lokalen Anwendungen und den realen Objekten. Gerade diese Schnittstelle kann mit Hilfe von RFID durch die drei folgenden Instrumente überwunden werden.

Die Eigenschaften und Funktionen von RFID sind als mögliche Lösung für eine bessere Koordination innerhalb der Lieferkette zu sehen. Von sonstigen Problemen innerhalb der Prozesse oder von mangelnder Kommunikation zwischen verschiedenen Unternehmen wird im Folgenden abstrahiert. Bestehende, unternehmensübergreifende Zusammenarbeit kann durch Integration, Automatisierung sowie Dezentralisierung verbessert werden und damit auch durch den Einsatz von RFID [vgl. Strassner 2005, S. 100].

6.1.1 Integration

Integration zielt auf die dauerhafte Verbindung von Systemen zu einem übergeordneten Gesamtsystem [Strassner 2005, S.23]. Dies bedeutet die Eingliederung in ein größeres Ganzes, wobei die von außen wahrgenommene Identität der eingebundenen Systeme zugunsten der Identität des übergeordneten Systems zurücktritt [Strassner 2005, S.23]. Auf diese Weise werden koordinatorische Probleme dauerhaft behoben. Es gibt verschiedene Sichten auf Integration. Eine technische Sicht auf Integration kann z. B. bei Kommunikationsprotokollen beobachtet werden. TCP/IP[183] ist inzwischen vollständig in viele andere

[183] Die Protokolle *Transmission Control Protocol* und *Internet Protocol* sind in den RFCs 793 und 791 der IETF definiert.

Protokolle und Anwendungen integriert. In der Betriebswirtschaftslehre hingegen ist die Sicht auf Integration eine andere. Sie bezieht sich auf organisatorische Elemente, wie Prozesse, Stellen oder sonstige Ressourcen [Strassner 2005, S. 23]. Für diese Arbeit ist die Sicht der Wirtschaftsinformatik gültig, welche sich auf die Integration von Betrieblichen Informationssystemen konzentriert. Dabei werden sowohl Prozesse, aber auch Menschen und Technik beachtet.

Strassner unterscheidet weiterhin zwischen zwei Arten der Integration [Strassner 2005, S. 24 ff.]. Zum einen gilt es verschiedene BIS zu integrieren, so dass die Informationsverarbeitung schnell und ohne Medienbrüche geleistet werden kann. Zum anderen stellt sich die Integration zwischen IT-Systemen und der realen Welt als große Aufgabe heraus, weil bisher nicht beachtete Prozesse und Objekte in das Gesamtsystem integriert werden müssen. Durch die Schnittstellen von Mensch-zu-Maschine (Eingabegeräte, Bildschirme) und Maschine-zu-Maschine (Sensoren, Aktoren) kann diese Aufgabe gelöst werden [Strassner 2005, S. 26]. RFID als Auto-ID-Technologie kann durch automatisierte Datenerfassung bei dieser Art der Integration wertvolle Dienste leisten. In Kapitel 5 wurde auf die Bedeutung von RFID als Brücke zwischen der wirklichen und virtuellen Welt bereits hingewiesen.

Wichtige Begriffe bei der Diskussion über Integration und RFID sind Integrationstiefe und Integrationsreichweite. Die Tiefe der Integration beschreibt den Grad der Detaillierung. Mit Detaillierung kann dabei sowohl die Anzahl der integrierten Produkte als auch die Kennzeichnungsebene gemeint sein. Die klassische Einteilung von verschiedenen Produkten eines Unternehmens ist die Einteilung in A-, B- und C-Ressourcen. Dabei sind die A-Ressourcen die wichtigen oder hochwertigen Produkte. Somit steigt die Integrationstiefe mit der Einbeziehung der B- und C-Ressourcen. Die Ebene der Kennzeichnung ist bereits aus Kapitel 5.1.1 bekannt und beschreibt die Kennzeichnung von Palette, Karton oder Artikel. Die Artikel-Ebene ist dabei die detaillierteste Stufe, so dass dann die Integrationstiefe am größten ist. Die größte denkbare Integrationstiefe ist dann folglich die Kennzeichnung aller Produkte auf Artikelebene. Ob die Maximierung der Integrationstiefe ein gewünschtes Ziel ist, darf dabei in Frage gestellt werden. Je nach Anwendungsfall bringt die maximale Integrationstiefe andere Probleme mit sich, z. B. eine zu große Datenflut oder zu hohe Kosten.

Mit Integrationsreichweite bezeichnet man die Menge der einbezogenen Parteien in der Lieferkette. Ist ein System nur lokal an einem Standort eines Unternehmens gültig oder gar nur in einer Abteilung, dann ist die Integrationsreichweite eher gering. Sie steigt mit der Ausweitung des Systems auf angrenzende Standorte oder gar externe Partner. Sind alle Partner einer Lieferkette integriert, dann ist die Integrationsreichweite maximal. Eine andere, verwandte Sicht auf die Integrationsreichweite ist die Anzahl der einbezogenen Prozesse [Strassner 2005, S. 126 f.].

Integrierte Systeme haben noch eine weitere Eigenschaft, die mit der Integrationsreichweite sehr verwandt ist. In dieser Arbeit wurden schon häufig offene und geschlossene Systeme[184] erwähnt. Geschlossene Systeme (*Closed loop*) beteiligen nur eine begrenzte Anzahl von Partnern. Im äußersten Fall besteht ein geschlossenes System aus lediglich einem Teil eines Unternehmens.[185] Die teilnehmenden Partner stimmen sich untereinander auf die technischen und organisatorischen Einzelheiten ab und agieren dann unabhängig von weiteren Einflussfaktoren. Bei offenen Systemen (*Open loop*) hingegen bewegen sich die logistischen Objekte außerhalb von vorher bekannten Pfaden. Eine Rückkehr zu einem bestimmten Ort ist dabei nicht unbedingt gegeben. Die beteiligten Parteien können sich vorher nicht auf Einzelheiten des Systems einigen, was einen Einsatz von Standards erforderlich macht. Eine Mischform von Systemen ist das kollaborative System (siehe Abbildung 6.1). Strassner definiert das kollaborative System als ein geschlossenes System, in dem aber externe Partner beteiligt sind [Strassner 2005, S. 126]. Allerdings definiert er die reinen geschlossenen Systeme immer als lokale Systeme, also ohne eine Einbeziehung eines externen Partners. Strassner sieht kollaborative Systeme als einen Zwischenschritt zu offenen Systemen. Ob in der Realität wirklich diese Vorgehensweise von geschlossenen zu offenen Systemen möglich ist, hängt von der Anwendung und deren Anforderungen ab. Eine kritische Hinterfragung dieses Vorgehens ist angebracht, da z. B. die Festlegung auf ein nicht standardisiertes System im offenen Betrieb Probleme bringt.

Koordination durch Integration kann sich in folgenden Punkten äußern [Strassner 2005, S. 105 f.]:

[184] Neben dem Begriff „System“ wird auch häufig von „Kreisläufen“ gesprochen.

[185] Ein Beispiel sei die Verwendung von Spezialbehältern in einem Fertigungswerk der Automobilindustrie [Strassner 2005, S. 157 ff.].

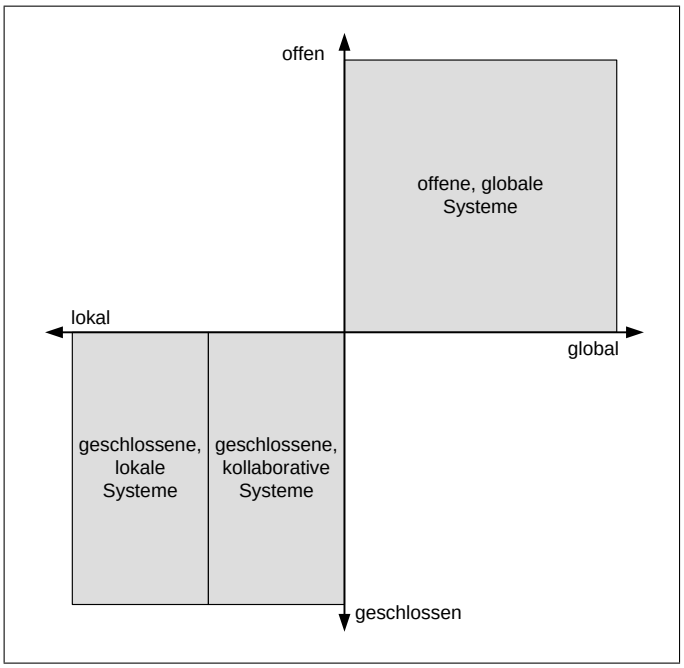


Abbildung 6.1: Eigenschaften verschiedener RFID-Systeme hinsichtlich ihrer Reichweite nach der Definition von Strassner.

- Sinkender Kommunikationsbedarf: Integration vermindert Schnittstellen und somit Medienbrüche.
- Bessere Qualität der Planung: Durch die größere Anzahl und bessere Qualität der Daten können Planungs- und Koordinationsverfahren vorab Probleme erkennen und schneller reagieren.
- Aktualität: Häufige Aktualisierung der Daten schafft eine höhere Genauigkeit der Statusangaben.
- Zuverlässigkeit der Erfassung: Durch die Verknüpfung von verschiedenen Systemen können erfasste Daten mit bestehenden verglichen werden. Zusätzliche Plausibilitätsprüfungen erkennen Fehler und können auf manuelle Eingriffe hinweisen.

Die unternehmensübergreifende Integration birgt für die Partner aber auch gewisse Gefahren. Unternehmen könnten ihre Kunden oder Lieferanten durch

die Einführung eines bestimmten Systems an sich binden. Die Partner müssten dann in die notwendige Infrastruktur investieren. Ein Wechsel zu dem System eines Konkurrenten wird dadurch allerdings erschwert. Die Mitbewerber haben dann ebenfalls erschwerte Bedingungen, in diesem Markt Partner zu finden. Diese Situationen werden *Lock-In* bei Abhängigkeit von einem Partner und *Lock-Out* bei Ausgrenzung von Mitbewerbern genannt. Somit könnte ein Partner seine Marktdominanz ausnutzen und sogar weiter ausbauen.

6.1.2 Automatisierung

Allgemein macht sich Automatisierung durch die Unterstützung von Maschinen in Prozessen bemerkbar [Strassner 2005, S. 106]. Dabei ist zwischen der Teil- und Vollautomatisierung zu unterscheiden.

Bei der Automatisierung ist die Rationalisierung der ursprünglichste und offensichtlichste Vorteil. Durch den Einsatz von Maschinen oder der Informationstechnologie werden Arbeitsschritte automatisiert und somit manuelle Arbeiten eingespart. Monotone Arbeiten werden zuverlässiger und kostengünstiger erledigt. Jedoch ist Rationalisierung nicht der einzige Vorteil. Durch die Automatisierung kann den Wünschen des Kunden flexibel entsprochen werden. Ein Beispiel dafür ist die Fertigung von Autos. Ein in einer Zweigstelle konfiguriertes und bestelltes Auto wird anschließend in der Fabrik nach diesen individuellen Vorgaben gefertigt.

Auch in der Verarbeitung von Daten kann die Automatisierung durch den Einsatz von WfMS (*Workflow Management System*) gesteigert werden. Prozesse werden von diesem System kontrolliert und somit manuelle Arbeiten reduziert. Bei notwendigen, manuellen Eingriffen wird der zuständige Mitarbeiter benachrichtigt, bevor die Verarbeitung fortgeführt wird. RFID kann in diese *Workflows*[186] eingebunden werden, da die automatische Erfassung von Daten ein Startpunkt eines Workflows sein kann. *Workflows* sind eine Menge von Regeln, die aus Sequenzen, Entscheidungen und Wiederholungen von Operationen auf Daten bestehen.

[186] Ein *Workflow* ist ein Prozess oder Arbeitsablauf, der aus einer Menge von verschiedenen Aufgaben besteht. Teilweise können diese Aufgaben automatisiert werden (auch z. B. bestimmte Entscheidungen), jedoch müssen manche Arbeiten manuell ausgeführt werden. Jeder *Workflow* in einem WfMS muss vor Benutzung definiert und konfiguriert werden.

Automatisierung bedeutet eine direkt nutzbare Steigerung der Effizienz der Prozesse, wobei die Einrichtung der *Workflows* und der Betrieblichen Informationssysteme zunächst einmal geleistet werden muss [Strassner 2005, S. 108]. Trotz dieses gesteigerten Aufwands verhilft Automatisierung zu einem verringerten Koordinationsaufwand [Strassner 2005, S. 109]:

- Vermeidung von Verzögerungen: Die vordefinierten Regeln zur Verarbeitung von Daten werden einmalig angelegt und dann automatisch ausgeführt. Dies bedeutet einen Zeitgewinn gegenüber der menschlichen Ausführung.
- Vermeidung menschlicher Entscheidungen: So weit es geht, sollen die Entscheidungen in den Regeln ohne das menschliche Eingreifen ausgeführt werden. Dadurch werden die automatisierbaren Entscheidungen schnell und korrekt[187] ausgeführt.
- Vermeidung von Folgeproblemen: Beim Auftreten von Problemen oder bei der Abweichung von erwarteten Ergebnissen (Plausibilitätsprüfung) stoppt die Verarbeitung, so dass eventuelle Fehler nicht weitergereicht werden, was einen erhöhten Aufwand für die Berichtigung zur Folge haben würde.
- Eliminierung von Prozessschritten: Die Prozesse werden im Einzelfall durch das Entfallen bestimmter Schritte effizienter. Diese Schritte sind z. B. Verwaltungsarbeiten oder das Suchen nach Lösungen.

Durch den Einsatz von mobilen RFID-Geräten kann die Automatisierung ausgeweitet werden. Neben der stationären Erfassung können mobile Geräte an sich bewegenden Objekten (Gabelstapler, Container) montiert werden, so dass eine ständige Erfassung unabhängig von der Position möglich ist. Zusätzlich besteht die Möglichkeit der Erfassung von Daten durch mobile Leser, wie PDAs, wodurch die manuelle Erfassung teilautomatisiert wird.

[187] Vorausgesetzt ist, dass die Regeln korrekt definiert wurden und dann stets korrekte Ergebnisse liefern.

6.1.3 Dezentralisierung

Dezentralisierung bedeutet die Verlagerung von Daten, Aufgaben und Entscheidungen auf niedrigere Ebenen. Diese Ebenen können sowohl durch die Aufbauorganisation[188] als auch durch die Architektur integrierter BIS definiert werden. Durch die RFID-Kennzeichnung bekommt jedes Objekt eine Identität und optional sogar Speicher- und Rechenkapazität. Somit entsteht die Alternative, Daten dezentral an den Objekten abzulegen, die sonst zentral im BIS gespeichert worden wären.[189] Ebenso können Aufgaben und Entscheidungen dezentral ausgeführt werden, da die notwendigen Daten und Rechenkapazitäten vorliegen. Dabei sind einfache Daten-Aktualisierungen bis hin zu Entscheidungen über den nächsten Schritt im Prozess denkbar.

Ausführende Einheiten der Aufgaben oder Entscheidungen können dabei die stationären oder mobilen RFID-Leser, die Tags an den Objekten oder die zuständigen Arbeiter an den jeweiligen Stellen sein. Durch die Verlagerung von Kompetenz auf niedrigere Ebenen erhalten die Arbeiter mehr Verantwortung und Entscheidungsgewalt, benötigen jedoch auch mehr Fähigkeiten und Legitimation durch die Vorgesetzten (*Empowerment*) [Strassner 2005, S. 109].

Die Dezentralisierung ist kein Widerspruch zu Automatisierung durch z. B. *Workflows*. Obwohl die zentrale Steuerung durch *Workflows* auf den ersten Blick orthogonal zu der Dezentralisierung steht, ist eine nebenläufige Zusammenarbeit sehr wohl möglich. Eine zentrale Steuerung der einzelnen Arbeitsschritte verbietet nicht das Ausführen von Aufgaben oder Entscheidungen an anderen räumlichen Stellen. Durch eine sinnvolle Kombination von dezentralen Entscheidungen und automatisierter Verarbeitung mit Hilfe von *Workflows* lässt sich eine flexible und dynamische Verarbeitung der Daten entlang der Lieferkette schaffen. Die entstehenden Freiräume sind dabei nicht als koordinationsfreie Inseln zu sehen, sondern eher als autonome, verantwortungsbewusste Stellen in der Lieferkette, die innerhalb der Koordination fungieren [Strassner 2005, S. 109].

[188] Die Aufbauorganisation beschreibt die Anordnung der Stellen und Abteilungen eines Unternehmens. Dabei entstehen verschiedene Anordnungen, die eher hierarchisch oder flach sein können.

[189] Ob die Speicherung von Daten dezentral am Objekt sinnvoll ist, kann nicht allgemein beantwortet werden. An dieser Stelle werden die Möglichkeiten und eventuelle Vorteilen gegenüber der zentralen Speicherung diskutiert. Für diese Arbeit wird die entsprechende Diskussion in Kapitel 9.2.6 geführt.

Durch eine erhöhte Entscheidungsgewalt auf den unteren Ebenen werden die oberen Ebenen des Systems entlastet, was zu einer Verringerung der Komplexität der zentralen Komponenten führen kann. Die Informationsversorgung der dezentralen Einheiten muss dabei jedoch immer gewährleistet sein [Strassner 2005, S. 110], denn Entscheidungen können häufig nicht nur mit den dezentral vorliegenden Daten getroffen werden, sondern benötigen ggf. auch zentral abgelegte Daten[190]. Der Zusammenhang zwischen Organisation und Informationstechnologie wird bei der Dezentralisierung besonders deutlich. RFID kann bei der Dezentralisierung und gleichzeitiger Informationsverarbeitung wertvolle Dienste leisten.

Die Voraussetzungen für eine erfolgreiche Dezentralisierung sind die Kenntnis der genauen Anforderungen an die Anwendungen, die ausreichende Kompetenz der dezentralen Entscheidungsträger und die Anpassung der Betrieblichen Informationssysteme an die neuen Anforderungen. Tendenziell bieten sich dynamische Prozesse für eine dezentrale Koordination an, da dann die Flexibilität ausgenutzt werden kann [Strassner 2005, S. 111]:

- Entlastung zentraler Steuerungsinstanzen: Durch die Verlagerung von Entscheidungen und Aufgaben auf niedrigere Ebenen werden andere Systeme entlastet.
- Anpassungsflexibilität: Auf Veränderungen innerhalb des Zuständigkeitsbereichs von dezentralen Einheiten kann schnell und unkompliziert reagiert werden. Eine Änderung des Ortes der Einheit verursacht keine Probleme.

Gerade die mobile Erfassung und Verarbeitung von RFID-Daten bietet enormes Potential die Dezentralisierung voran zu treiben. Mobile RFID-Leser und auch aktive RFID-Tags mit Sensoren oder Aktoren können Aufgaben und Entscheidungen übernehmen mit denen zentrale Systeme entlastet werden. Damit können Daten dezentral ausgefiltert oder bereits verarbeitet werden, bevor sie wieder auf dem Tag oder im BIS abgelegt werden. Nicht jeder Anwendungsfall profitiert von Dezentralisierung, jedoch können mobile Leser bei der Unterstützung von stationären Prozessen hilfreich sein, z. B. bei der Ausnahmebehandlung oder Fehlersuche.

[190] Zentral abgelegte Daten haben den Vorteil für alle Beteiligten erreichbar und aktuell zu sein.

Es gibt jedoch auch Anwendungen bei denen mobile RFID-Leser ohne eine andere, sinnvolle Alternative erforderlich sind. Verschiedene Prozesse in der Logistik und im SCM bieten sich deswegen für die mobile Erfassung an. Diese Prozesse können die Erfassung von Warenein- und -ausgängen, die Inventur, das Tracking oder Suchen von Objekten (auf einem LKW oder in einem Regal) sein [Michael und McCathie 2005]. Auch [Sarma u. a. 2003] betont den Logistik-Einsatz mobiler RFID-Erfassung in den Bereichen der Inventarisierung auf Artikel-Ebene, im SCM, bei der Inventar-Überwachung, beim automatisierten Qualitätsmanagement und beim automatischen Warenein- und -ausgang. Ein Beispiel für einen dezentralen RFID-Ansatz aus der Forschung ist das Projekt „Sm@rt Logistics“[191] eines Konsortiums bestehend aus der RWTH Aachen, TU Dresden, TCS, simcron und intellion. Ziel ist die dezentrale Unterstützung der Mitarbeiter durch eine dynamische Steuerung der Prozesse. Zum Einsatz kommen sowohl mobile Geräte, RFID- als auch Funk-Technologie.

Bei einer dezentralen Verarbeitung kann der Ort eines Gegenstands oder einer Operation von Bedeutung sein. GPS ist eine Technologie, die außerhalb von Gebäuden die Position eines Objektes bestimmt (siehe Kapitel 2.3 und 5.2). Dabei sind zwei verschiedene Methoden zur Positionsbestimmung denkbar. Die erste Methode ist die Ausstattung des Objekts mit einem GPS-Empfänger, damit die Position jederzeit zu kontrollieren ist (*Real Time Location Services*). Die zweite Methode ist das Aktualisieren der Objekt-Position nach jeder Positionsänderung. Transportmittel (Gabelstapler, LKW) werden mit einem GPS-Empfänger versehen und können beim Abstellen des Objekts (Container, Behälter, Palette) die neue Position mit der ID des Objekts verknüpfen und im Betrieblichen Informationssystem aktualisieren.

6.2 Resultierende Effekte

Im Folgenden werden nun drei mögliche Effekte erläutert, die beim Einsatz von RFID erzielt werden können. Durch die drei Instrumente Integration, Automatisierung und Dezentralisierung ergeben sich neue Möglichkeiten für die Gestaltung der beteiligten Prozesse, für die Zusammenarbeit mit anderen Partnern der Lieferkette und den Einsatz von neuen Technologien.

[191] Es gibt keine gemeinsame Homepage des Projekts, jedoch finden sich etliche Informationen dazu unter http://www.wzl.rwth-aachen.de/de/de918e3a8accdcacc125711d00521c9c.htm.

Die folgenden Effekte können unabhängig voneinander umgesetzt werden, jedoch unterscheidet sich die Reichweite der organisatorischen und technischen Änderungen bei den drei Effekten. Ähnlich wie in den Unterkapiteln zuvor stammen große Teile des Inhalts aus [Strassner 2005]. Zusätzlich werden die für diese Arbeit wichtigen Inhalte, z. B. die mobilen Aspekte, behandelt.

6.2.1 Substitution durch Technologie

Herkömmliche Abläufe innerhalb von Prozessen können durch den Einsatz von neuen Technologien ersetzt werden. Durch Automatisierung und Integration können damit die Effektivität und Effizienz der Prozesse gesteigert werden.

Effizienz ist eines der wichtigsten Ziele heutiger Industrie- oder Logistik-Unternehmen. Effiziente Prozesse haben ein gewisses Einsparpotential [Strassner 2005, S. 112]. Aus diesem Grund können Technologien, die eine erhöhte Automatisierung versprechen, vorhandene Lösung ersetzen oder unterstützen. Manuelle Abläufe bieten sich als Ansatzpunkt zur Automatisierung und Substitution an. Sollten bereits andere Technologien eingesetzt werden, muss im Einzelfall entschieden werden, ob eine Einführung von, z. B. RFID, lohnt. Wird die Charge eines Produktes hinreichend durch einen aufgedruckten Barcode auf der Verpackung identifiziert, so bringt die Substitution durch RFID keinen signifikanten Mehrwert. Im Gegenteil: Die Einführung und Umstellung auf ein RFID-System würde höhere Kosten verursachen als Nutzen einbringen. In anderen Fällen können bestehende Systeme zwar funktionieren, aber durch gesetzliche Vorschriften oder die eigenen Unternehmensziele zu wenig Funktionen bieten. Dann muss jedoch für jede Anwendung gesondert entschieden werden, ob eine neue Technologie eingeführt werden sollte.

Ein weiterer Vorteil bei der Substitution durch RFID kann die Sicherung der Qualität des Angebots sein [Strassner 2005, S. 114]. Dabei spielen sowohl die Qualität des Produktes selbst als auch die Einhaltung von Terminen eine große Rolle. Durch die Vermeidung von Fehlern (Automatisierung) und eine schnellere Verarbeitung (Integration verschiedener IS) kann also die Prozess-Effektivität gesteigert werden. Jegliche Planungen (Prozesse, Produktionsmittel) werden zuverlässiger, so dass insgesamt das allgemeine Risiko von Fehlern vermindert werden kann.[192]

[192] Ausgenommen sind dabei die Test-, Einführungs- und Übergangsphasen, in denen mit einer erhöhten Fehlerrate zu rechnen ist.

RFID-Systeme sorgen für eine bessere Informationsversorgung und bilden damit die Basis für eine bessere Prozess-Planung. Während der Umsetzung dieser Planung kann dann fortwährend der Status der Objekte kontrolliert werden, was bei manuellen Abläufen mit einem deutlichen Mehraufwand verbunden wäre.

6.2.2 Reorganisation von Geschäftsprozessen

Die Reorganisation von Geschäftsprozessen fällt in das in Kapitel 5.3.2 bereits erwähnte Feld von BPR. Ein oder mehrere Prozesse werden von Grund auf neu modelliert und anschließend umgesetzt. Dieser Effekt kann einem Unternehmen dazu verhelfen, durch geänderte Anforderungen und neue Technologien mit Hilfe der verschiedenen Instrumente bestehende Prozesse zu optimierten oder neue zu schaffen.

Dieser Schritt ist für ein Unternehmen gewagter als die reine Ersetzung von Lösungen durch neue Technologien. Der Vorteil der Reorganisation ist nicht mehr adäquate Prozesse zu verwerfen und nur die brauchbaren Eigenschaften mit den neuen Technologien zu verschmelzen. Diese Neugestaltung ist sicherlich nicht trivial und ex ante schwer zu bewerten, jedoch steckt großes Potential in ihr. Koordinationsprobleme können von Grunde auf gelöst werden ohne den alten Prozessen Beachtung schenken zu müssen.

RFID kann dabei in der Produktion und im SCM für neue Prozesse über die gesamte Lieferkette sorgen. Neben den grundlegenden Anforderungen an die Produktion oder das SCM entsteht die Möglichkeit, neue Prozesse zu entwickeln, die neue Produkte schaffen oder neue Dienstleistungen anbieten. Gerade im SCM bietet sich die Unterstützung von IT, RFID und Lokalisierungstechnologien an, um neue Möglichkeiten in der Lagerhaltung, im Transport und in der Kundenorientierung zu schaffen. Ein möglicher neuer Prozess ist ein Online-Dienst, der es Kunden ermöglicht Informationen über den Status und den Ort seiner erworbenen Produkte zu erhalten. Dabei ist es unerheblich, ob sich das Produkt noch in Planung, in der Produktion oder schon in der Auslieferung befindet, da die Daten über die gesamte Lieferkette vorhanden sind. Gerade Internet-Dienste verhelfen aufgrund ihrer weltweiten Erreichbarkeit den anbietenden Unternehmen zu einer Chance neue Prozesse zu schaffen.

Individualisierte Angebote und Produkte können mit Hilfe von RFID einfacher erstellt werden, so dass den Kundenwünschen entsprochen werden kann.

Im Kapitel 6.1.2 wurde die Konfiguration eines Autos beim Kauf bereits angesprochen. Dieser Dienst ist ein weiteres Beispiel für einen neu geschaffenen Prozess innerhalb eines Automobil-Unternehmens. Dabei lassen sich alle drei beschriebenen Instrumente wiederfinden. In diesem Prozess sind mehrere Informationssysteme beteiligt, die integriert werden müssen. In dem Autohaus muss der Verkäufer ein System zur Verfügung haben, mit dem er für den Kunden das Fahrzeug konfiguriert. Dabei kommt es auf eine ansprechende Oberfläche und einfache Bedienung an. Die Ergebnisse dieser Konfiguration müssen dann in PPS in die verschiedenen Planungen von Ressourcen eingebunden werden. Anschließend müssen die Systeme der Fertigung das Fahrzeug erstellen, und letztlich sorgt die Verwaltung für die Auslieferung und Fakturierung. Während der Produktion entsteht durch Automatisierung die notwendige Rationalisierung und fehlerfreie Fertigung. Dieses Beispiel zeigt, dass an vielen, verschiedenen Stellen dieses Prozesses dezentrale Entscheidungen getroffen werden, die unter keinem Einfluss der zentralen Planung stehen. Dabei kann RFID das fehlende Glied zwischen den verschiedenen Abschnitten der Lieferkette sein.

Für die Lagerhaltung bietet RFID ebenfalls neue Prozesse. Durch RTLS kann der Status eines Lagers zu jedem beliebigen Zeitpunkt abgefragt werden. Anstatt der Erfassung jeder Lager-Bewegung parallel zu der Realität, kann auf eine fehleranfällige Bestandsführung komplett verzichtet werden. Wird der Bestand eines oder mehrerer Artikel benötigt, so kann das zuständige RFID-System diese Artikel „rufen“ (vgl. *Broadcast*). Die Artikel, die den geforderten Kriterien entsprechen, „melden sich“ durch eine Antwort dem System. Diese Lagersysteme werden *Roll Call* genannt, da jedes Produkt seine Anwesenheit wie bei einem Appell meldet. Im Deutschen wird manchmal auch der Begriff des Echtzeitlagers verwendet.

6.2.3 Interorganisationaler Einsatz

Der dritte Effekt beim Einsatz von RFID im SCM ist der Einsatz von unternehmensübergreifenden Systemen. Nicht nur ein Unternehmen betreibt ein RFID-System in der Lieferkette, sondern es beteiligt vor- und nachgelagerte Unternehmen daran. Das Ziel ist, so viele Informationen wie möglich[193] über den

[193] Selbstverständlich ist nicht die reine Menge an Daten das angestrebte Ziel, sondern die wesentlichen und nützlichen Daten sind von Interesse.

Status aller Produkte in der Lieferkette zu erhalten. Diese Art von Zusammenarbeit ist eine Organisationsform, die gelegentlich auch *C-Business* (*Collaborative Business*, *Corporate Business*) genannt wird [Heinemann und Rau 2003, S. 15]. Dem Instrument der Integration kommt dabei die gewichtigste Rolle zu, da die Integration der Schlüssel zu der unternehmensübergreifenden Nutzung des RFID-Systems ist. Bisherige Kooperationen zwischen verschiedenen Unternehmen sind sicherlich nicht eine Neuerung. Herkömmliche Kooperationen können sich in einem Datenaustausch per EDI[194] oder in Zusammenarbeit einer anderen Form äußern. Bei interorganisationaler Zusammenarbeit kommt hinzu, dass auch die organisatorischen und Daten verarbeitenden Vorgänge zwischen den Unternehmen integriert sind. Sie operieren also auf denselben Datenbeständen und nutzen dieselben Anwendungen. Insgesamt besteht die Vision, ein ganzes Netzwerk von Lieferketten der Unternehmen aufzubauen, unter denen dann ein reibungsloser Datenaustausch möglich ist. Diese Art der Kooperation muss nicht auf die Lieferkette beschränkt sein, sondern kann auch auf andere Felder übertragen werden.

[Yang und Jarvenpaa 2005] halten RFID-Systeme für eine neue Form von interorganisationalen Systemen (IOS). Durch ihre Fähigkeit zur Echtzeit-Identifikation und zum *Tracking* über große Distanzen, glaubten Manche, dass RFID-Systeme grundlegend die Art und Weise der Geschäfte von Unternehmen verändern werden. Allerdings führen die Autoren gleichzeitig Unsicherheiten und Probleme bei einer solchen Zusammenarbeit an. Zunächst einmal müssten die beteiligten Parteien fast gleichzeitig RFID entlang der Lieferketten einführen. Weiterhin könne sich ein einzelnes Unternehmen nicht sicher sein, dass sich alle anderen Unternehmen ebenfalls gleich stark an der Einführung beteiligten. Aus diesem Grund sei Vertrauen eine wichtige Größe bei kollaborativen Aktivitäten. Die drei größten Unsicherheiten sind laut [Yang und Jarvenpaa 2005] die folgenden:

- Wenn sich ein Unternehmen dazu entschließt RFID einzuführen, dann könne es sich nicht sicher sein, dass andere Unternehmen dies erwidern. Bei einer größeren Anzahl von Gegnern einer Einführung könne der erwartete Nutzen nicht erreicht werden.

[194] *Electronic Data Interchange* ist ein Sammelbegriff für den elektronischen Datenaustausch zwischen Organisationen. Dabei wurde ehemals das Telefonnetz zur Übertragung verwendet, heute hingegen das Internet. Die EDI-Formate sind sehr vielfältig und reicht vom bekannten EDIFACT bis zu dem offenen XML (*Extensible Markup Language*)

- Die durch die Produktivitätsverbesserungen erzielten Gewinne seinen vorab nicht den Unternehmen zuteilbar. Ebenso sei die Höhe der Gewinne nicht bekannt. Unklarheit bestehe auch, ob Gewinn erzielende Unternehmen bereit seien, den Gewinn mit anderen zu teilen.
- Die RFID-Technologie sei noch in der Entwicklung. RFID könnte in manchen Anwendungen nicht so funktionieren, wie die einführenden Unternehmen es erwarteten.

Aufgrund dieser Unsicherheiten und unterschiedlichen Vorstellungen könnten Unternehmen verunsichert werden. Dabei sei das Vertrauen in die Partner jedoch unbedingt notwendig. Vertragliche Allianzen seien ein Ansatz, um eine Vertrauensbasis zu schaffen, die weiter ausgebaut werden könne.

Eine weitere Möglichkeit ist nicht auf die zu erwartenden Gewinne zu hoffen, sondern vor der Einführung die Kosten aufzuteilen. Diese Kosten sind zwar vorab nicht zu 100 % vorherzusagen, jedoch könnte ein Teil der Unsicherheit verringert werden. Im Gegensatz zu den Kosten für die Umstellung der Organisation und der Software-Entwicklung lassen sich die Kosten für die Hardware recht genau vorab bestimmen. Dies sind im Grunde die Kosten für die Tags und die Kosten für die Infrastruktur, welche hauptsächlich aus RFID-Lesern und den Kommunikationseinrichtungen bestehen. Für diese Kosten könnten Gebührenmodelle entwickelt werden, in denen die Belastungen auf alle Beteiligten verteilt werden. Dabei sind viele verschiedene Modelle denkbar, wie die direkte Beteiligung, die Vermietung von Komponenten oder Nachlässe für Produkte. Lieferanten könnten sich dazu bereit erklären, die Kosten für die Tags zu übernehmen, wenn sie die Infrastruktur der Kunden nutzen können. Unternehmen, die auf eine Einführung drängen, könnten durch eine Form des *Sponsorings* die ersten, großen Partner für eine Zusammenarbeit belohnen und damit auch das geforderte Vertrauen entgegenbringen. Die Größe oder Marktdominanz eines Unternehmens sowie die relative Zuordnung der Kosten sind einige Faktoren, die über das verwendete Modell entscheiden können.

6.3 Strategische und operative Bedrohungen

Die in diesem Kapitel genannten Instrumente und dadurch entstehenden Effekte begünstigen den Einsatz von RFID im SCM. Jedoch existieren für po-

tentielle Betreiber einige Gefahren, auf die im Folgenden eingegangen wird. Dabei kann man die Bedrohungen in drei verschiedene Arten unterteilen. Die strategischen Fehler werden während der Planungs- und Vorbereitungsphase gemacht und sind Folge von ungenügender Auseinandersetzung mit den verschiedenen Themen. Operative Fehler hingegen entstehen bei der Umsetzung der strategischen Planung. Bei der Realisierung werden dann organisatorische oder technische Lösungen gewählt, die nicht den erhofften Nutzen bringen. Die dritte Form von Bedrohungen sind Sicherheitsbedenken.

Für viele Unternehmen ist vor der Einführung von RFID-Systemen die fehlende Wirtschaftlichkeit ein großes Problem [Strassner 2005, S. 96].[195] Gerade bei offenen Systemen und der Beteiligung von vielen Partnern in der Lieferkette sind die Kosten und vor allem der zu erwartende Nutzen vorab nur schwer zu berechnen. Des Weiteren wird diese Schwierigkeit durch eventuelles Misstrauen gegenüber den Partnern gesteigert (vgl. Kapitel 6.2.3). Schließlich könnte die Einführung von RFID-Systemen überhaupt unnötig sein, da bereits Lösungen eingesetzt werden, die den gestellten Anforderungen entsprechen. Der Barcode ist häufig vollkommen ausreichend und sollte dann nicht ohne zwingende Gründe abgelöst werden.

Bei der Umsetzung der Ergebnisse der Planung kann die Auswahl der falschen RFID-Komponenten den Einsatz erschweren oder gar unbrauchbar machen. Viele technische Eigenschaften (siehe Kapitel 2.2) können bei falscher Auswahl die Funktion des Gesamtsystems beeinträchtigen. Häufig werden falsche Tags, Systeme mit zu kurzen Reichweiten oder Systeme mit zu hohen Fehlerraten gewählt [Strassner 2005, S. 97.]. Bereits häufig wurde in dieser Arbeit auf die Bedeutung von Standards hingewiesen. Bei der Wahl des falschen Standards könnten hohe Kosten entstehen oder gar Kooperationen scheitern.

Im SCM ist die Wahrung der Privatsphäre innerhalb der Lieferkette von keiner großen Bedeutung. Am Ende der Lieferkette jedoch erwerben Kunden die Produkte, was bei einer Kennzeichnung auf Artikel-Ebene zu Problemen führen könnte. Kunden könnten durch die mögliche Identifikation durch die Produkte abgeschreckt werden und deswegen die gekennzeichneten Produkte meiden. Aus diesem Grund müssen Hersteller und Händler eine geeignete Lösung für

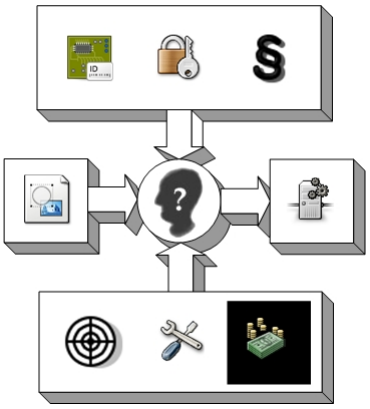
[195] Die entsprechende Diskussion um den richtigen Zeitpunkt zur Einführung neuer Technologien und der damit verbundenen Investitionsunsicherheit wurde bereits in den Kapiteln 4.1.1, 4.1.2 und 4.1.5 im Zusammenhang mit Standards geführt. Diese Diskussion ist auf RFID und die Überlegungen innerhalb von Unternehmen übertragbar.

dieses Problem finden. In Kapitel 3.1 wurden bereits einige Sicherheitsbedrohungen für Unternehmen aufgeführt. Dabei sind vorrangig die Firmenspionage (Daten für das Marketing der Mitbewerber), die Fälschungssicherheit, Angriffe auf die Infrastruktur (*Denial of service*) und die Datensicherheit zu nennen.

Kapitel 7

Auswirkung neuer Geschäftsmodelle auf die Wirtschaftlichkeit

In diesem Kapitel werden die Auswirkungen eines RFID-Systems auf die Wirtschaftlichkeit eines Unternehmens erörtert. Für viele Unternehmen ist der fehlende Nachweis der Wirtschaftlichkeit ein entscheidendes Problem vor der Einführung von RFID (vgl. Kapitel 6.3). Aus diesem Grund werden die fundamentalen Aspekte zur Betrachtung der Wirtschaftlichkeit genannt und erläutert.



7.1 Bestimmung der Ausgangslage

Die folgenden Unterkapitel betrachten die Einführung von RFID unter allgemeinen Gesichtspunkten. In der Praxis muss für jeden Anwendungsfall im Einzelnen eine Betrachtung aller wirtschaftlichen Aspekte vorgenommen werden. Viele Entscheidungen während der Konzeptionalisierung haben großen Einfluss auf das Ergebnis der Wirtschaftlichkeitsanalyse. Eine große Rolle z. B. spielt die Integrationsreichweite eines Systems. Eine Substitution einer bestehenden, lokalen Lösung durch RFID lässt sich einfacher berechnen als ein interorganisationales System für die gesamte Lieferkette. Neben der Integrationsreichweite existieren noch deutlich mehr Faktoren, von denen im Folgenden nur die wesentlichen angeführt werden.

Die Wirtschaftlich ist jedoch nicht nur aufgrund unterschiedlicher Anwendungsfälle schwer zu berechnen, sondern auch wegen der ungewissen Vorhersagbarkeit verschiedenster Einflüsse und des Verhaltens der Beteiligten. Die Fragen nach den Zielen der Unternehmung, den beteiligten Partnern, den betroffenen Prozessen und den technischen Lösungen müssen vor einer Berechnung von Kosten und Nutzen beantwortet sein. Dabei sind die anfallenden Kosten häufig besser zu berechnen als der zu erwartende Nutzen. Der Nutzen ist meist in den strategischen Zielen ausgedrückt und schwer zu quantifizieren. Die Steigerung der Kundenzufriedenheit ist sicherlich nutzbringend, aber fast unmöglich in Zahlen zu fassen. Nach einer Einführung lässt sich durch Marketing-Analysen die Kundenzufriedenheit messen und näherungsweise beziffern, aber die Entwicklung der Kundenzufriedenheit vor der Einführung zu quantifizieren ist mit einem hohen Maß an Unsicherheit behaftet.

Im Folgenden werden ausgehend von den Zielen einer Unternehmung die Kosten verursachenden und die Nutzen erbringenden Faktoren identifiziert. Dabei werden sowohl die quantitativen als auch die qualitativen Elemente genannt.

7.2 Ökonomische Faktoren

Ein RFID-System setzt sich aus vielen einzelnen Komponenten zusammen, die nicht nur aus elektronischen Bestandteilen sondern auch aus Software und Organisation bestehen. Im Folgenden wird somit eine Einteilung der ökonomischen Faktoren in die drei Kategorien Hard-, Soft- und Orgware[196] sowie einer Kategorie Nutzen vorgenommen.

7.2.1 Hardware

- RFID-Tags: Die Kosten für Tags können sehr stark variieren. Dabei entscheiden viele physikalische Faktoren über den Tag-Preis. Bei einer Anzahl von einer Million Tags kosten die günstigsten circa 20 Eurocent pro Tag und andere – mit vielen Funktionen ausgestattete Tags – bis zu 20 Euro. Dabei entscheidet nicht nur der absolute Preis über die Wahl, sondern auch das Verhältnis des Tag-Preises zum Produkt-Preis.

[196] In diesem Fall werden mit Orgware nicht nur die organisatorischen Aufgaben innerhalb von IT-Projekten beschrieben, sondern auch die Aufgaben des Managements und des Marketings.

Bei einer Bestellung von einer großen Menge sind hohe Rabatte möglich, so dass die Berechnung der benötigten Anzahl Einfluss auf die Kosten hat. RFID-Tags sind in der Regel teurer als Barcodes. Deswegen ist der Einsatz in offenen Systemen mit einer vorab unbekannten Anzahl von Tags mit einem gewissen Risiko behaftet.

- RFID-Leser: Ein RFID-Leser kann verschiedene Ausprägungen haben, die zu unterschiedlichen Zwecken dienen und auch unterschiedliche Preise kosten. Leser an Gates bestehen oft aus mehreren Antennen und einer Kommunikationseinheit. Die Anzahl dieser Gates sollte dem Betreiber genau bekannt sein, so dass diese Kosten exakt zu berechnen sind. Des Weiteren fallen Anschaffungskosten für weitere Leser an, die eine Kombination aus Antennen und Kommunikationseinheiten sind. Diese sind meist kleiner und decken dadurch einen geringeren Bereich ab. Diese Leser sind für die Montage an bestimmten Lokationen (Tür, Gabelstapler) gedacht, deren Lesereichweite eingeschränkt sein soll. Zusätzlich gibt es mobile Leser, die entweder an einen Rechner oder ein mobiles Gerät angeschlossen werden. Mobile Geräte sind tendenziell teurer, so dass eine gute Schätzung der benötigten Anzahl sinnvoll ist.

- Backend: Das Backend kann bei jedem RFID-System aus unterschiedlichen Komponenten bestehen. In aller Regel bilden jedoch ein oder mehrere Server das gesamte Backend. Dabei ist vorab die Verteilung der Dienste auf die verschiedenen Server zu beachten (Datenbank-Server, Web-Server, *Middleware*, Kommunikationseinrichtungen, BIS). Eventuell können bestehende Systeme genutzt werden, jedoch sollte beachtet werden, dass bei einer späteren Neuverteilung der Dienste erneut Kosten (Mehraufwand) anfallen. Längere Antwort- oder Ausführungszeiten aufgrund einer zu hohen Auslastung können ebenfalls Probleme verursachen. Zusätzlich zu den Servern muss das notwendige Zubehör beachtet werden, was zum Betrieb notwendig ist. Dies können Unterbrechungsfreie Stromversorgungen[197] (USV), Geräte für die Datensicherung (Laufwerke,

[197] Eine USV ist ein minimaler Rechner mit Akkus hoher Kapazität. Die USV wird zwischen den Server und der Stromversorgung geschaltet, damit im Falle eines Stromausfalls der Server weiter laufen kann. Ansonsten besteht die Gefahr von Datenverlust oder auch Hardware-Defekten.

Medien) oder Komponenten auf Lager für den Austausch im Falle eines Defektes sein.

- Interne Infrastruktur: Die Infrastruktur besteht hauptsächlich aus Einrichtungen zur Kommunikation der Komponenten untereinander. Manche RFID-Leser benötigen einen Rechner für die Kommunikation mit Servern oder der *Middleware*. Neben diesen Rechnern oder vielleicht sogar PDAs sind natürlich Netzwerk-Komponenten notwendig. Dazu gehören Switches, Router, die notwendige Verkabelung von Netzwerk und Strom, WLAN-*Access-Points*[198] und eventuell WLAN-Antennen. Sicherlich existieren bereits solche Komponenten in einem Unternehmen, jedoch müssen diese je nach der Anzahl der Leser zusätzlich angeschafft werden.

- Öffentliche Infrastruktur: Die Nutzung von öffentlichen Einrichtungen kostet während des Betriebs Gebühren oder Miete (GSM, UMTS). Außerdem fallen Kosten für die Geräte zur Nutzung der Infrastruktur an (Mobiltelefone, Erweiterungskarten).

- Bauliche Maßnahmen: Für die Errichtung von Gates oder anderen RFID-Lesern können verschiedenste bauliche Maßnahmen notwendig sein. Für die Einrichtung der Kommunikation müssen eventuell Maste für WLAN-Antennen aufgestellt werden. In der Produktion ist der Umbau von Bändern für die Fertigung denkbar. Gabelstapler brauchen eine Vorrichtung für die Montage eines Lesers.

- Optionale Hardware: Zusätzlich ist die Anschaffung von GPS-Empfängern denkbar.[199] Für eine präzisere Lokalisierung ist die Installation von eigenen GPS-Antennen eine kostenintensive Anschaffung. Manche Anwendungen benötigen den Einsatz von Sensoren oder Aktoren in Verbindung mit RFID-Tags. Diese Sensoren treiben die Kosten für RFID-Tags auf Artikel-Ebene deutlich in die Höhe.

[198] Ein *Access-Point* (AP) ist ein Netzwerk-Knoten, der den Endpunkt für die Funk-Verbindung der WLAN-Clients darstellt. Vom AP zur restlichen Infrastruktur wird die Kommunikation über ein Kabel hergestellt.

[199] Durch den Aufbau von eigenen Antennen kann die Genauigkeit des GPS-Signals von den Satelliten für die Empfänger deutlich erhöht werden. Dieses Verfahren wird *Differential Global Positioning System* (DGPS) genannt und kann ungefähr auf der Fläche eines Firmengeländes eingesetzt werden.

7.2.2 Software

- Middleware: Die *Middleware* hat eine bedeutende Aufgabe in einem RFID-System und bedarf deswegen besonderer Aufmerksamkeit. Die Aufgaben der *Middleware* sind die Geräte-Verwaltung, die Filterung von Daten und der Verbindung zu verschiedenen Servern im Backend. Inzwischen besteht ein Angebot von verschiedenen Software-Herstellern aus der ERP- und der Datenbank-Branche für den Erwerb einer fertigen *Middleware*-Lösung. Alternativ kann diese Komponente auch von dem Unternehmen selbst entwickelt werden. Diese *Make-or-Buy*-Entscheidung muss im Einzelfall getroffen werden, weil die eingesetzten Systeme, die Anforderungen und die verfügbaren Ressourcen in jedem Unternehmen unterschiedlich sind.

- Backend: Das Backend besteht neben dem BIS aus verschiedenen Servern. Dabei dürfte minimal ein Datenbank- und ein Web-Server eingesetzt werden. Viele Standard-Produkte sind kostenlos erhältlich (*Open-Source*), jedoch kann die Auswahl des richtigen Produkts von der Systemumgebung diktiert werden. Die *Middleware* und nachgelagerte Betriebliche Informationssysteme können aufgrund fehlender Unterstützung bestimmter Lösungen die Auswahlmöglichkeiten stark einschränken. Neben der Server-Software müssen eventuell Anwendungen, die auf dem Server ausgeführt werden, entwickelt werden. Diese Anwendungen können ebenfalls durch die eigenen Mitarbeiter oder externe Dienstleister realisiert werden.

- BIS: Letztendlich werden die RFID-Daten im BIS verarbeitet. Die Anbindung der Komponenten kann durch verschiedene Möglichkeiten realisiert werden. Bei einem universellen ERP-System ist die Wahrscheinlichkeit, dass der ERP-Hersteller selbst eine RFID-Anbindung anbietet, relativ hoch. Somit stellt sich dann die Frage, ob dieses ERP-Modul erworben wird oder ob eine Eigenentwicklung günstiger ist.

- Clients: Je nach Ausführung der RFID-Leser und der *Middleware* werden Rechner oder mobile Geräte benötigt. Auf diesen dezentralen Geräten

wird dann ein Software-Client der Herstellerfirma oder eine eigene Entwicklung eingesetzt. Die Aufgabe der Software ist die Verbindung der dezentralen Leser mit der *Middleware*.

7.2.3 Orgware

- Planung der Integration: Die Ermittlung der Ziele, die Planung der Umsetzung und die Identifikation der verschiedenen, benötigten Ressourcen (Hardware, Software, Datenstruktur) benötigt im Vorfeld überwiegend gedankliche Arbeit und somit menschliche Arbeitskraft. Diese Personalkosten fallen dabei in den oberen und mittleren Ebenen des Managements an. Eventuell müssen externe Ressourcen bei der Planung einbezogen werden. Dies könnten Beratungsunternehmen oder Hersteller von Hard- oder Softwarelösungen sein.

- Realisierung der Integration: Die Realisierung der geplanten Maßnahmen beteiligt sehr viele verschiedene Parteien. Der Aufbau und die anschließende Inbetriebnahme der Komponenten und der Infrastruktur beschäftigt dabei sowohl handwerkliche (Elektriker, Schlosser, Bauarbeiter) als auch technische (Netzwerk, IT, Fachabteilungen) Abteilungen oder externe Dienstleister. Diese Kosten sind vorab schwer zu schätzen, so dass hier Erfahrungswerte hilfreich sein können. Diese Erfahrung kann durch externe Mitarbeiter gewonnen werden, die bereits RFID-Systeme eingeführt haben. Dabei müssen alle Komponenten des Systems eingerichtet und betriebsbereit gemacht werden. Dies fängt bei der Verfügbarkeit von Tags an und geht bis zur Einrichtung von eigenen GPS-Antennen.

- Schulung: Vor der Inbetriebnahme müssen die beteiligten Parteien ausreichend geschult werden. Dies betrifft hauptsächlich die Anwender des Systems (Lageristen, LKW-Fahrer, Arbeiter in der Produktion), die Sachbearbeiter in der Verwaltung (Einkauf, Logistik, Vertrieb) und die Verantwortlichen der Instandhaltung (IT, Elektriker).

- Allgemeine Wartung und Pflege: Während des Einsatzes des RFID-Systems muss ein entsprechender Aufwand geleistet werden, um die Betriebsbereitschaft sicher zu stellen. Dabei müssen die entsprechenden

Geräte gewartet und ggf. repariert oder ausgetauscht werden, die anfallenden Daten müssen gesichert und archiviert werden und das ganze System muss einer allgemeinen, vorbeugenden Wartung und Kontrolle unterliegen.

- Kooperation: Vereinbarungen unter den Partnern müssen bei einer unternehmensübergreifenden Kooperation getroffen werden. Dabei sind vertragliche Allianzen über die Verteilung der Kosten und Gewinne, sowie den zu leistenden Aufgaben (Bereitstellung von Daten, Kennzeichnung), denkbar.

- Test: Das Testen des Systems zu jedem Zeitpunkt bis zur produktiven Inbetriebnahme ist ein erheblicher Kostenfaktor, da das Testen ein mühsamer und zeitintensiver Prozess ist. Jede getroffene Entscheidung muss durch das Testen validiert und gerechtfertigt werden. Dabei gibt es verschiedene Testarten, die von einfachen Tests im Kleinen bis hin zu einem Pilotversuch oder einem vollständigen Systemtest reichen können. Tests binden Ressourcen wie Mitarbeiter oder Maschinen und kosten deshalb viel Zeit und Geld. Eventuell müssen alle Partner der Lieferkette in die Tests eingebunden werden, so dass beim Testen ein erhöhter Koordinationsbedarf notwendig ist.

- Kommunikation: Für eine reibungslose Planung, Realisierung und den anschließenden Einsatz sind zwischen Schnittstellen Vereinbarungen und Absprachen notwendig. Diese Schnittstellen bestehen zwischen den Mitarbeitern, Abteilungen und Unternehmen. Bestimmte Stellen übernehmen innerhalb eines Unternehmens die Koordination der Arbeiten und die Abstimmungen der Vorgehensweise. Diese Personen sind ausschließlich mit der Koordination beschäftigt und verantwortlich für die reibungslose Einführung. Für die Kommunikation zwischen den Unternehmen muss im Einzelfall die entsprechende Stelle ausfindig gemacht werden. Die Kommunikation mit potentiellen Kunden oder Lieferanten übernimmt die Marketing-Abteilung oder die Geschäftsleitung. Dazu gehören auch die Versorgung mit Informationsmaterial (Broschüren, Internet-Auftritt) und die Werbung.

7.2.4 Erwarteter Nutzen

- Rationalisierung: Von der RFID-Einführung wird hauptsächlich erwartet, dass Prozesskosten gesenkt werden können [Strassner 2005, S. 146]. Durch Automatisierung wird sowohl die Effektivität als auch die Effizienz gesteigert, was sich durch weniger Kosten bei gleicher Leistung oder mehr Leistung bei gleichen Kosten bemerkbar macht. Die Neuorganisation der Prozesse durch BPR oder die Schaffung neuer Prozesse und Dienstleistungen hingegen zielt auch auf eine Steigerung der Leistung. Der allgemeine Nutzen ist vorab schwer zu bestimmen. Daher ist die allgemeine Rationalisierung nur qualitativ vorherzusagen.

- Weniger Arbeitsaufwand: Eine Form der Kosteneinsparung ist die Verminderung von manueller Arbeit. Personalkosten machen einen großen Teil der Kosten im SCM aus, so dass dort enormes Potential vorhanden ist. Bestimmte Abläufe können schneller und fehlerfreier erledigt werden. Durch die Vermeidung von Fehlern werden zusätzlich die sonst notwendigen Kosten zu deren Behebung sowie den Kosten der Folgefehlern eingespart. Sowohl die Personal- als auch die Fehlerfolgekosten lassen sich annähernd vor der Einführung berechnen, da sowohl der Grad der Automatisierung als auch statistische Werte über die auftretenden Fehler vorhanden sein könnten.

- Senkung der Lagerkosten: Im SCM ist neben dem Transport die Lagerung von Gütern ein wichtiger Prozess. Durch die Versorgung der BIS und der Mitarbeiter mit genaueren Daten werden geringere Bestände, genauere Lieferdaten und eine bessere Planung möglich. Zusätzlich kann die Reduzierung von Schwund angestrebt werden.

- Kundenzufriedenheit: Ein qualitativer Nutzen ist die Steigerung der Kundenzufriedenheit. Dies gilt sowohl für private als auch für geschäftliche Kunden. Durch erhöhte Pünktlichkeit, ausgebauten Service, eingehaltene Lieferzeiten und mehr Transparenz in der Lieferkette werden Vertrauen und Leistung gesteigert. Dies kann vorhandene Kontakte festigen und somit langfristig Umsätze sichern.

- Kommunikation: Durch die verbesserte Kommunikation kann die Qualität der Daten und Informationen gesteigert werden, wodurch weniger

Datenfehler und Medienbrüche auftreten. Dieser nicht messbare Nutzen bedeutet eine deutliche Verbesserung der Prozesse im SCM.

7.3 Metriken zur Erfolgsmessung

Nach einer Einführung des RFID-Systems kann man den wirklichen Erfolg durch verschiedene Arten messen. Zum einen besteht die Möglichkeit, ein rechnerisches Ergebnis basierend auf den wirtschaftlichen Ergebnissen zu erhalten (*hard benefits*). Zum anderen lassen sich nicht-monetäre, qualitative Resultate (*soft benefits*) erkennen.

Wirtschaftliche Kennzahlen geben Auskünfte über den Erfolg der Investition. Die Kapitalströme sind vorab nicht bekannt, jedoch ist eine nachträgliche Berechnung des Kapitalwertes oder des internen Zinsfußes denkbar. Das Problem dabei ist – wie bereits erwähnt – die Bewertung des Nutzens. Eine verwandte Methode ist die Kosten-Nutzen-Analyse, jedoch wird dabei die Verzinsung des Kapitals in der Regel ignoriert.

Weitere mögliche Methoden sind die Berechnung der *Total Cost of Ownership* (TCO), welche jedoch lediglich die direkten und indirekten Kosten eines IT-Systems berechnet und den Erfolg auslässt, und die Methode des *Return on Investment* (ROI), welche die Abschreibungsdauer der Investition als Betrachtungszeitraum ansieht. Für diese Methoden dürfte ein aussagekräftiges Ergebnis jedoch nicht zu erwarten sein, da entweder zu vage oder gar keine sinnvollen Daten ermittelt werden können.

Effizienz-Steigerungen innerhalb von Prozessen lassen sich durch Vergleiche zu den Zahlen vor der Einführung messen, so dass ein Teil des Erfolgs oder Misserfolgs näherungsweise berechnet werden kann. Ob das Ergebnis aussagekräftig genug ist, hängt von der Anwendung und dem RFID-System ab, so dass eine allgemeine Beurteilung durch Effizienz-Steigerungen nicht möglich ist.

Typische *soft benefits* sind Verbesserungen in den Bereichen der Flexibilität, des Services und der Kundenzufriedenheit. Durch Marketing-Statistiken, Umfragen oder sonstige Erhebungen lassen sich solche Größen messen. Beispiel für Kennzahlen sind z. B. das Verhältnis von gewonnen Kunden zu verlorenen Kunden, die Entwicklung von Reklamationen, die Einhaltung von Lieferzeiten,

die Ergebnisse direkter Kundenbefragungen oder ähnliche Indikatoren. Langjährige Mitarbeiter können durch ihre Erfahrungswerte die Situation am Markt und den Kontakt zu den Kunden oder Lieferanten einschätzen und bewerten.

7.4 Verwandte Beispiele aus der Praxis

An dieser Stelle werden kurz zwei Beispiele aus der Praxis angeführt, welche einen Nachweis der Wirtschaftlichkeit erbringen. Das erste Beispiel ist ein Konzept zur Identifikation und Verfolgung von Behältern bei Volkswagen, das zweite ist ein Vergleich zu einer ähnlichen Situation in den siebziger Jahren, der UPC-Barcode-Einführung.

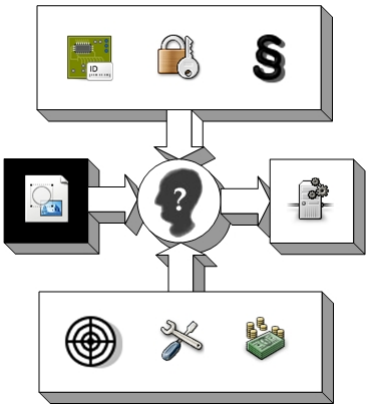
VW möchte bestimmte Standardbehälter mit RFID-Tags ausstatten, um das Management der Behälter effektiver und effizienter gestalten zu können [Strassner 2005, S. 163 ff.]. Die Ziele sind den Schwund zu verringern, die Prozesse zu automatisieren und die Kontrolle beim Versand zu vereinfachen. Zukünftig sollen externe Partner die Behälter auf Mietbasis nutzen können. Durch den RFID-Einsatz werden verschiedene Effekte erzielt: Der Umlauf der Behälter wird beschleunigt, verschwundene Behälter werden berechnet, die Anzahl der Behälter wird reduziert, manuelle Vorgänge werden ersetzt und Fehler beim Versand werden vermieden [Strassner 2005, S. 168 f.]. Das Ergebnis des Konzepts ist ein jährliches Einsparungspotential von knapp sechs Millionen Euro bei einer Abschreibungsfrist von drei Jahren. Allerdings ist diese Zahl eine Schätzung und kann durch verschiedene Risiken verringert werden. Diese Risiken sind fehlende Zuverlässigkeit, die fehlende Erfassung bei Versendungen nach Übersee und die allgemeine Entwicklung von RFID im Behältermanagement [Strassner 2005, S. 169].

Anfang der siebziger Jahre wurde der UPC-Barcode standardisiert und eingeführt. Zu Beginn der Einführung waren die Kosten und der Nutzen von Barcodes ebenso unbekannt wie die wirtschaftlichen Zahlen von RFID heute. In [Rindle 2006, S. 10] wird angeführt, dass sich die Kosten für eine Einführung eines Barcode-Systems innerhalb von 22 Jahren halbiert haben und dass der Nutzen um den Faktor sechs gestiegen ist. Zu Erkenntnissen aus den Erfahrungen der damals neuen Auto-ID-Technologie kann man erst heute gelangen. Zu der schnellen Entwicklung der Barcodes verhalfen die Schaffung globaler Standards, die offene Kommunikation unter Partnern, die Zusammenarbeit bei

der Veränderung von Geschäftsprozessen und die Anpassung an den jeweiligen Anwendungsfall. Aus diesen Erfahrungen könnte man Rückschlüsse auf die Entwicklung der RFID-Technologie ziehen. Die genannten Erkenntnisse ähneln stark den Forderungen an RFID, z. B. die Schaffung globaler Standards. Das Motiv der Anpassung der Lösung an den speziellen Anwendungsfall wurde in dieser Arbeit bereits häufig gefordert. Im folgenden Kapitel wird ein Anwendungsfall als Beispiel für die Entwicklung eines RFID-Systems beschrieben.

Kapitel 8

Beispiel: Hersteller von Containern



Dieses und die beiden folgenden Kapitel bilden den dritten Teil dieser Arbeit, der sich mit der praktischen Konzeption und Realisierung eines RFID-Prototyps beschäftigt. Zunächst wird in diesem Kapitel der betroffene Geschäftsprozess beschrieben, anschließend werden dann die daraus abgeleiteten Ziele und Anforderungen aufgelistet. Die beschriebenen Konzepte beziehen sich nicht auf ein konkretes Unternehmen, basieren aber auf realen Anwendungsfällen der produzierenden Industrie. Zu dem hier vorgestellten, exemplarischen Szenario wurden ergänzend Informationen aus einem konkreten Unternehmen eingeholt, dass hier aber aus Vertraulichkeitsgründen nicht genannt werden soll. Der Kernbereich dieses konkreten Unternehmens ist die Herstellung, der Vertrieb und die Rekonditionierung[200] von Industrie-Containern.

Im folgenden Unterkapitel wird zunächst der zu optimierende Geschäftsprozess detailliert beschrieben (Ist-Situation). Anschließend werden die angestrebten Änderungen in dem Prozess aufgeführt (Soll-Situation). Aus diesen Beschreibungen lassen sich dann die angestrebten Ziele und resultierenden Anforderungen an das RFID-System ableiten.

[200] Rekonditionierung ist das Recycling, die Reinigung, das Wiederaufbereiten oder das Entsorgen von Produkten.

8.1 Beschreibung Geschäftsprozess

Ein Hersteller von Containern für die Industrie und Lebensmittelbranche produziert nicht nur die Container, sondern vertreibt diese und nimmt sie nach der Entleerung wieder zurück, um sie wiederaufzubereiten oder zu entsorgen.

Die Container sind in verschiedenen Ausführungen erhältlich, die von wenigen hundert bis hin zu 1500 Litern reichen. Sie bestehen immer aus einem Innenbehälter aus Kunststoff und entweder einem Gitterrohrrahmen oder einer Stahlummantelung als Außenhülle. Die Container können wahlweise auf Holz- oder Stahlpaletten montiert werden, so dass sie mit einem Gabelstapler zu transportieren sind. Mögliche Füllgüter sind Flüssigkeiten jeglicher Art oder bestimmte feste Stoffe, wie z. B. Granulate oder Pulver. In hochwertigen Ausführungen können Gefahrgüter[201] oder Lebensmittel abgefüllt werden.

Die Nutzung der Container findet in einem Kreislauf statt, da sie von dem herstellenden Unternehmen rekonditioniert und anschließend wieder vertrieben werden. Für dieses Beispiel wird dieser Kreislauf als Lieferkette behandelt. Vorgelagerte Lieferanten (Hersteller von Stahlrohren oder Kunststoffen) werden nicht betrachtet. Innerhalb dieses Kreislaufes gibt es verschiedene Arten beteiligter Unternehmen, die sich in fünf Rollen einteilen lassen:

- Hersteller: Der alleinige Hersteller der Container ist das betroffene Unternehmen, welches das RFID-System einführen möchte.
- Abfüller: Ein Abfüller ist Kunde des Herstellers und erwirbt die Container. Sie werden mit einem Füllgut gefüllt und anschließend verkauft oder intern transportiert oder verwendet.
- Entleerer: Ein Entleerer kann Kunde des Abfüllers sein oder selbst der Abfüller, wenn die Container innerhalb eines Unternehmens gefüllt und entleert werden.
- Rekonditionierer: Ein Rekonditionierer recycelt den Container für eine erneute Benutzung. Diese Behandlung kann eine Reinigung, eine Reparatur oder ein teilweiser Austausch von Teilen des Containers sein. Ist der Container zu stark verschmutzt oder beschädigt, dann wird er entsorgt. Häufig ist der Hersteller gleichzeitig auch der Rekonditionierer.

[201] Gefahrgüter sind explosive, entzündbare, gasförmige (komprimiert, verflüssigt oder gelöst), oxidierende, giftige, ansteckungsgefährliche, radioaktive oder ätzende Stoffe.

- Spediteur: Für den Transport der Container zwischen den genannten Parteien ist eine oder mehrere Speditionen zuständig. Dabei können verschiedene Parteien diese Rolle gleichzeitig übernehmen, wenn sie einen eigenen Fuhrpark für den Transport haben.

Im einfachsten Falle gibt es zwei Unternehmen, die jeweils zwei oder drei der fünf Rollen einnehmen. Der Hersteller ist gleichzeitig der Rekonditionierer und der Kunde des Herstellers ist sowohl Abfüller und Entleerer. Für den Transport sorgen eigene LKW. Der Kunde könnte ein Industrie-Unternehmen sein, welches an einem Standort Betriebsmittel herstellt und an einem anderen Standort verbraucht. Die Container werden also lediglich für den internen Umschlag von Zwischen- oder Hilfsprodukten benötigt. Ein weiterer Fall ist die Verteilung von Abfüller und Entleerer auf zwei verschiedene Unternehmen. Der Abfüller befüllt die Container mit seinen Endprodukten und verkauft diese weiter an seine Kunden. Der Entleerer hingegen kauft den Container nicht nur für den Transport, sondern primär als Verpackung eines Produktes. Für die Betrachtung des Prozesses dieser Arbeit wird dieser zweite Fall angenommen. Der Hersteller ist wiederum gleichzeitig Rekonditionierer, so dass drei Unternehmen an der Lieferkette beteiligt sind.

Der allgemeine Kreislauf des Containers lässt sich durch die Grafik in Abbildung 8.1 darstellen. Die blau gekennzeichneten Stellen des Kreislaufs sind Vorgänge innerhalb der Lieferkette, wobei die Lagerung ein notwendiger aber für die Beschreibung des Geschäftsprozesses nebensächlicher Vorgang ist. Die Transporte zwischen den Parteien sind grün eingefärbt. Abweichungen von dem normalen Lauf der Container oder Störungen in der Lieferkette sind rot gekennzeichnet. Die Zeichen an den Pfeilen, die die Richtung des Kreislaufes anzeigen, sind einfache Kardinalitäten[202], die die Anzahl der Durchläufe eines Containers entlang des Weges beschreiben. Die fünf aufgelisteten Rollen lassen sich den blau (Hersteller, Abfüller, Entleerer, Rekonditionierer) und grün (Spediteur) gekennzeichneten Stellen der Abbildung zuordnen. Eine Ausnahme bildet der Vorgang der Lagerung, weil davon ausgegangen wird, dass die Lagerung beim Hersteller oder Rekonditionierer vorgenommen wird.

[202] In der Datenbank-Modellierung und objektorientierten Softwareentwicklung werden Beziehungen zwischen zwei Relationen oder Klassen mit Kardinalitäten versehen, die den Grad einer Beziehung beschreiben. Sie drücken die Anzahl der in Beziehung stehenden Entitäten zwischen den beteiligten Relationen oder Klassen aus. Das „n“ oder der Asterisk „∗“ stehen für beliebig viele Beziehungen.

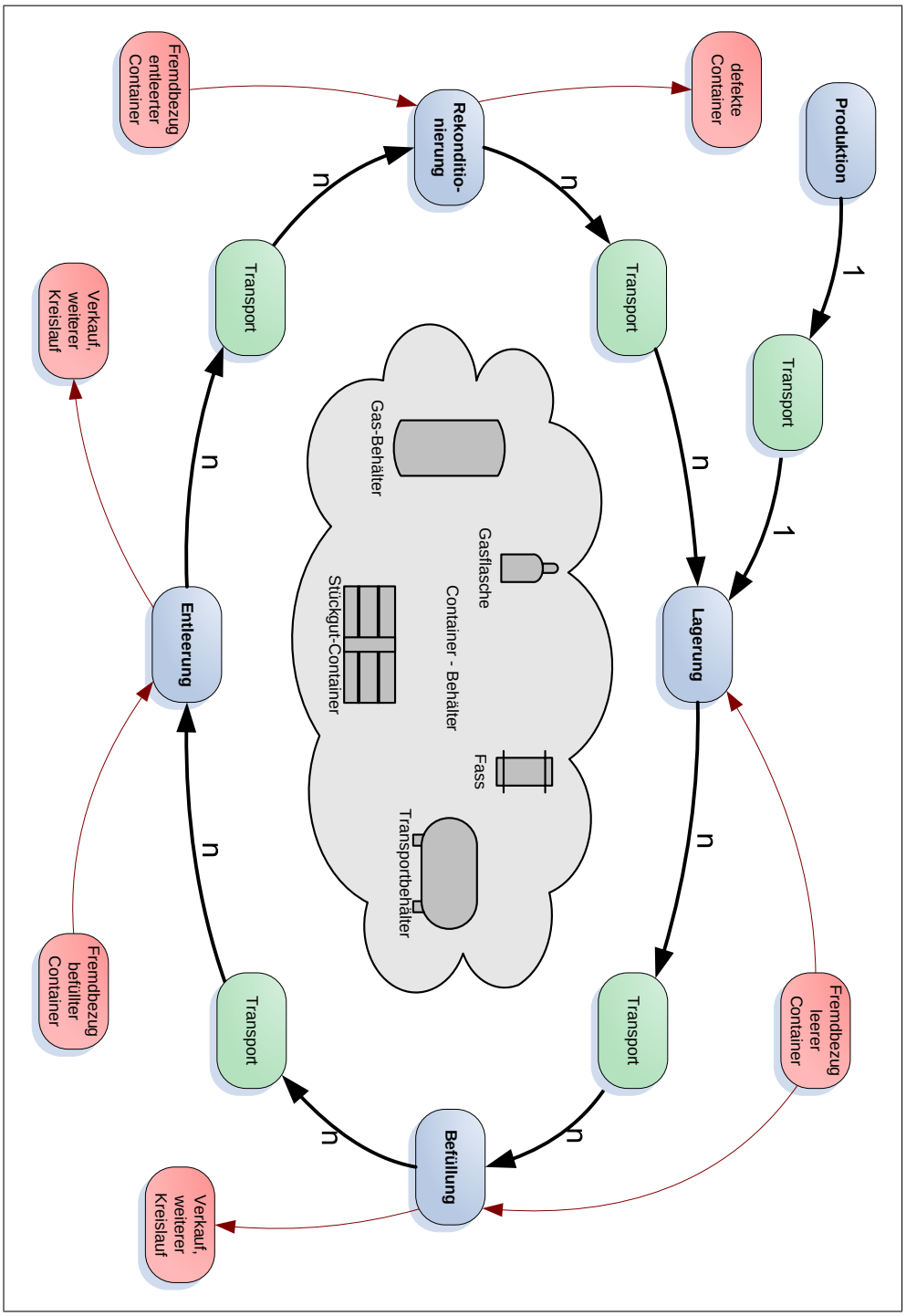


Abbildung 8.1: Kreislauf der Container mit den beteiligten Parteien und eventuellen Störungen.

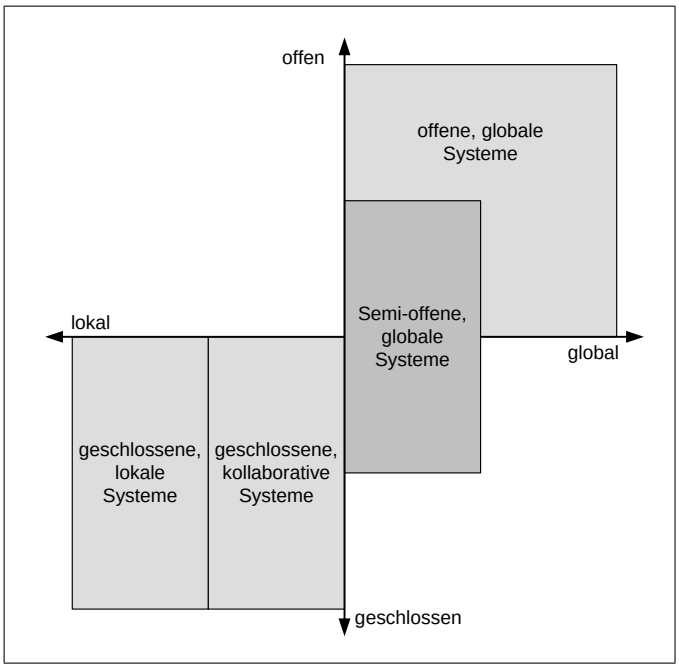


Abbildung 8.2: Eigenschaften verschiedener RFID-Systeme hinsichtlich ihrer Reichweite mit der Einteilung des RFID-Systems dieser Arbeit.

Dieser Kreislauf kann selbstverständlich auch auf ähnliche Produkte und Rollen angewendet werden. In dieser Arbeit stehen die Container stellvertretend für Behälter aller Art. Weitere Vertreter dieser Behälter könnten Gasflaschen, Stahlfässer, Stückgut-Container oder Wechselbrücken sein.

Eine Einteilung des Kreislaufes in die beiden, bereits angesprochenen Kategorien von offenen und geschlossenen Kreisläufen ist nicht ohne weiteres möglich. Der Kreislauf ist weder geschlossen noch lokal, da er sich dynamisch mit den externen Partnern verändert. An offenen Kreisläufen kann jedes Unternehmen teilnehmen. In diesem Fall jedoch können nur Kunden des Herstellers – und ggf. dessen Kunden – teilnehmen, so dass der Kreislauf nicht als offen zu bezeichnen ist. Eine mögliche Bezeichnung dieses Kreislaufs ist semi-offen oder kooperativ und global (siehe Abbildung 8.2). Weiterhin besteht die unerwünschte Möglichkeit, dass Container den Kreislauf verlassen. Abfüller oder Entleerer geben den Container an nicht beteiligte Partner außerhalb der Lieferkette weiter. Tritt ein Container eines fremden Herstellers in den Kreislauf,

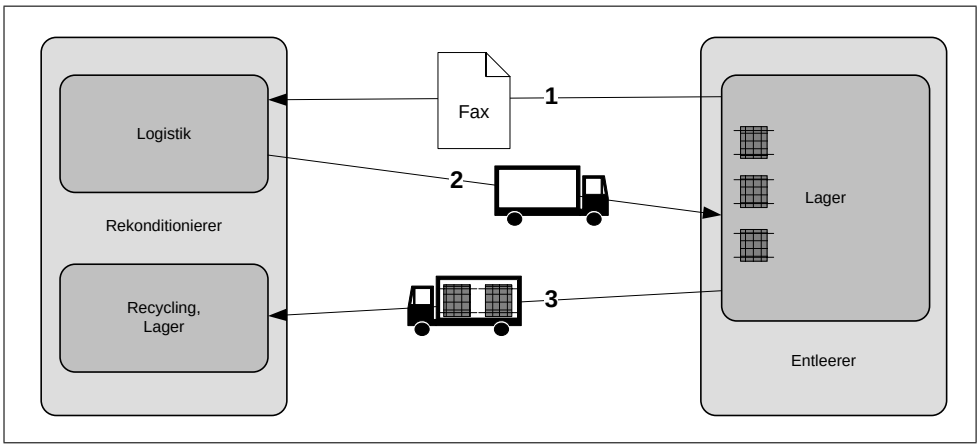


Abbildung 8.3: Avisierung und Abholung leerer Container.

so erhält der Rekonditionierer einen unbekannten Container, der nicht den eigenen Spezifikationen oder Qualitätsansprüchen genügt und unbrauchbar ist. Diese beiden Ausnahmefälle werden in der Arbeit beachtet, da der Hersteller und Rekonditionierer dadurch einen Schaden erleiden kann (Verlust von Containern in der Lieferkette und Kosten für die Entsorgung fremder Container).

Der Kreislauf besteht aus vielen Prozessen, die in der Produktion, dem Transport, der Lagerhaltung, usw. angesiedelt sind. In der Praxis tritt zum Beispiel das Problem auf, dass ein Entleerer eine gewisse Anzahl von Containern sammelt, bevor er den Hersteller bittet, die Container für die Rekonditionierung abzuholen (Avisierung, siehe Abbildung 8.3). Das Abholen der benutzen Container ist ein kostenloser Service des Herstellers. Der Entleerer teilt dem Hersteller die Anzahl und den Typ der leeren Container durch das Ausfüllen und Versenden eines Fax-Vordruckes mit. Darauf hin werden die Container innerhalb weniger Tage abgeholt. Jedoch treten zwei große Probleme auf, die den reibungslosen Ablauf behindern. Zum einen sammeln sich in der Zwischenzeit mehr Container beim Entleerer an, als zunächst per Fax gemeldet waren. In den meisten Fällen wird vom Entleerer keine Avisierung dieser zusätzlichen Container vorgenommen. Zum anderen werden die Faxe oft falsch oder unvollständig ausgefüllt. Die Container sind nicht eindeutig identifizierbar. Sie sind lediglich mit einem Aufkleber versehen, auf dem die Auftragsnummer in Klarschrift und als Barcode codiert aufgedruckt ist.

Eine wünschenswerte Verbesserung des Geschäftsprozesses wäre der Wegfall des manuellen Ausfüllens des Fax-Vordrucks. Das manuelle Ausfüllen ist feh-

leranfällig, weil Daten falsch eingetragen werden oder nach der Übertragung schlecht lesbar sind. Da die Entleerer oft vergessen Daten zu notieren, sind diese zudem häufig unvollständig. Für den anschließenden Prozess der Rekonditionierung ist die Information über das ehemalige Füllgut enorm wichtig, da die weitere Behandlung abhängig von den in den Containern befindlichen Füllgut-Resten ist. Des Weiteren kann eine höhere Automatisierung erreicht werden, wenn Medienbrüche (Fax) vermieden werden können.

Zusätzlich zu diesem Prozess können noch weitere Prozesse und andersartige Probleme gelöst werden. Eine alleinige Lösung für den beschriebenen Prozess ist nicht sinnvoll, da das RFID-System in der ganzen Lieferkette sinnvoll eingesetzt werden kann. Dabei sind die Prozesse Produktion, Transport, Qualitätsmanagement und Warenannahme denkbar.

8.2 Ziele

In diesem Anschnitt werden die fünf zentralen Ziele zur Optimierung des genannten Prozesses und dem Management der Container in der Lieferkette aufgeführt. Die Reihenfolge der Ziele beschreibt den Verlauf von allgemeinen zu speziellen Zielen. Jedes Ziel wird kurz erläutert, so dass dessen Sinn und Zweck deutlich wird.

1. Eindeutige Identifikation der Container

Container werden bisher nur durch eine eindeutige Auftragsnummer identifiziert. Da ein Auftrag jedoch viele Container beinhaltet, kann ein einzelner Container nicht identifiziert werden. Die eindeutige Identifikation ist die Grundvoraussetzung für eine Datenerfassung bei der Avisierung leerer Container.

Ein weiterer Nutzen ist eine bessere Rückverfolgbarkeit innerhalb der Lieferkette. Da Abfüller die Container möglicherweise an verschiedene Kunden verkaufen und verschiedene Füllgüter abfüllen, ist eine Identifikation durch die Auftragsnummer nicht ausreichend. Mit einer Identifikation jeden Containers kann diese Rückverfolgung exakt durchgeführt werden.

Container fremder Hersteller können nicht mehr in die Lieferkette des Herstellers gelangen. Nur identifizierte Container dürfen in der Lieferkette bewegt werden und schließlich rekonditioniert werden. Das Entsorgen von fremden

Containern auf Kosten des Rekonditionierers oder des Herstellers wird somit verhindert.

Gesetze verpflichten bestimmte Unternehmen aus der Industrie und Lebensmittelbranche ihre Produkte eindeutig zu kennzeichnen, wenn Aspekte der Sicherheit oder Qualität im Vordergrund stehen. Bereits im Jahr 2002 hat die EU eine Verordnung erlassen, in der Unternehmen der Lebensmittelindustrie die Rückverfolgbarkeit ihrer Produkte sicherzustellen haben [EU 2002, Art. 18]. Dabei ist die gesamte Lieferkette in die Rückverfolgbarkeit einbezogen. Die Unternehmen müssen Systeme einrichten, die die Daten vorhalten und den Behörden auf Aufforderung zur Verfügung stellen. Ein denkbares, zukünftiges Gesetz könnte die Rückverfolgbarkeit und Identifikation von Containern mit Gefahrgütern regeln.

2. Elektronische Erfassung

Manuelle Erfassungen innerhalb des betreffenden Prozesses sollen verringert werden. Aufgrund der dadurch zunehmenden Automatisierung werden Medienbrüche und Fehler verringert, was zu einer höheren Effizienz und schnelleren Verarbeitung führen soll.

Des Weiteren wird durch die elektronische Erfassung der Container die Integration in die vorhandenen IS gefördert. Dabei ist sowohl die stationäre Erfassung (Produktion, Lager) als auch die mobile, dezentrale Erfassung (Avisierung, Warenannahme) notwendig. Ein weiterer Prozess für die mobile Erfassung ist neben der Avisierung die Warenannahme beim Entleerer. Ein Fahrer der Spedition könnte mit Hilfe eines mobilen RFID-Lesers die Container erfassen und gleichzeitig als Wareneingang für die Rekonditionierung buchen.

3. Verknüpfung mit zusätzlichen Daten

Neben der Identifikation der Container mit eindeutigen IDs ist die Verknüpfung mit zusätzlichen Daten anzustreben. Die Daten müssen auch bei dezentralen Abläufen verfügbar sein. Da sich bestimmte Daten eines Containers (Füllgut) häufig ändern können, muss der Speicherplatz wiederbeschreibbar sein.

Dabei muss beachtet werden, dass sowohl die Möglichkeit der Ablage am Container als auch auf zentralen Informationssystemen möglich ist. Je nach

Sicherheitsanforderungen müssen die Daten mit Zugangsbeschränkungen geschützt werden können.

4. Steigerung der Transparenz

Die Wege der Container innerhalb der Lieferkette sollen deutlicher werden. Dadurch wird das Austreten von Containern aus der Lieferkette sichtbar, so dass Maßnahmen zur Vermeidung des Verlusts von Containern getroffen werden können.

Des Weiteren können alle Partner mit mehr Informationen über die Historie, den Aufenthaltsort und das Füllgut der Container versorgt werden.

5. Höhere Qualität der Produkte

Durch die höhere Menge an Daten über die Container und die eindeutige Identifikation kann die Qualitätssicherung mehr Anregungen zur Verbesserung der Produkte erhalten. Bisher versteckte Probleme mit bestimmten Füllgütern oder anderen Variablen können aufgedeckt und behoben werden. Des Weiteren kann die Anzahl der Umläufe eines Containers im Kreislauf ermittelt werden, was eine bessere Planung der Produktion ermöglicht und ein Indikator der Produktqualität für zukünftige Änderungen sein kann.

Durch Statistiken über den Status des Containers beim Empfang nach der Avisierung können Abfüller, Entleerer und Speditionen ausfindig gemacht werden, die nicht ordnungsgemäß mit den Containern umgehen.

8.3 Anforderungen

Aus diesen Zielen ergeben sich die folgenden Anforderungen, die im vorherigen Abschnitt bereits genannt wurden und an dieser Stelle zusammengefasst werden:

- Entwicklung eines RFID-Systems für das Container-Management,
- Merkmal zur Identifizierung an jedem Container[203],

[203] Somit wird eine Kennzeichnung auf Artikel-Ebene angestrebt. Diese Sicht gilt jedoch nur für den Hersteller und Rekonditionierer. Für Abfüller und Entleerer ist der Container eine Verpackung (vgl. mit einer Kennzeichnung auf Karton-Ebene).

- Funktionsfähigkeit des Tags auch auf Metall und in der Nähe von Wasser,
- Mobile und stationäre Erfassung,
- ID elektronisch lesbar,
- Zusätzliche Daten auf Tag oder Backend,
- Mehrfachverwendung der Container und des Datenspeichers,
- Kommunikation mit dem IT-System (Backend),
- Zugriff zu jeder Zeit und jedem Ort,
- Zugriffsbeschränkungen der Daten,
- Integration in bestehende Systemlandschaft,
- Speicherung der Historie eines Containers,
- Test auf Originalität der Container,
- Backend greift auf Stammdaten der BIS zu,
- Verknüpfung von ID zu Auftrag oder Kunde.

Neben diesen direkt abgeleiteten Anforderungen gibt es weitere, die sich nach einer gedanklichen Vorwegnahme des Systems erschließen. Diese Anforderungen sind nicht unwichtig, aber auch nicht immer umsetzbar. Sie beschreiben hauptsächlich technische Details:

- Verwendung günstiger und verbreiteter Hardware,
- Austauschbarkeit von Hardware-Komponenten,
- Verwendung freier, offener Software[204],
- Modularisierung der Software,
- Abstraktion von speziellen Kommunikationsarten (z. B. WLAN, GSM, UMTS),

[204] Diese Anforderung ist nicht allgemein umsetzbar, da viele kommerzielle BIS die Verwendung von offener Software nicht unterstützen. Aus diesem Grund ist die Forderung nach nach freier, offener Software nicht vorgeschrieben.

- Möglichkeit zur Anbindung eines GPS-Gerätes zur Positionsbestimmung,
- Ermittlung eines geeigneten Daten-Schemas,
- Verwaltung von Berechtigungen an den gespeicherten Daten,
- Verlagerung des größten Teils des Rechenaufwand auf das Backend (Entlastung des Clients),
- Intuitive und leicht zu erlernende Bedienung.

8.4 Herausforderungen und Abhängigkeiten

Diese Ziele und die daraus resultierenden Anforderungen an das RFID-System sind allerdings nicht ohne bestimmte Voraussetzungen zu erreichen und umzusetzen. Die größte Herausforderung ist die Beteiligung aller Parteien der Lieferkette. Da an jeder Stelle der Lieferkette der Einsatz von RFID notwendig ist, müssen auch alle Partner das RFID-System benutzen. Nach der Kennzeichnung der produzierten Container und der Einrichtung der dazugehörigen Daten-Strukturen beim Hersteller, müssen die Abfüller die Container-ID mit dem Füllgut verknüpfen, sei es auf dem Tag oder in einer zentralen Datenbank. Die Entleerer brauchen für die Avisierung der leeren Container die notwendigen Leser, damit die notwendigen Daten zum Rekonditionierer übertragen werden können. Im Idealfall benutzen alle Parteien RFID nicht nur für die Avisierung, sondern setzen RFID auch innerhalb eigener Prozesse (Produktion) ein.

Eine weitere Herausforderung ist die Frage nach der Speicherung der Daten. Werden die Daten zentral abgelegt, dann entstehen Kosten für die Anschaffung und Wartung der Infrastruktur. Des Weiteren kann es sein, dass Parteien nicht gewillt sind, ihre Daten auf Informationssysteme anderer Unternehmen abzulegen, weil sie fürchten, sie geben wichtige Daten preis. Dieses Vertrauen in die Datensicherheit und -vertraulichkeit muss gegeben sein.

Neben den Kosten für die gemeinsam benutzten Komponenten ist die Frage nach der Gewinn-Aufteilung zu beantworten. Wie bereits in Kapitel 6.2.3 erwähnt, muss auch eine Regelung für die Verteilung gemeinsam erzielter Gewinne geschaffen werden.

Ein wichtiger Aspekt bei Investitionen aller Art ist die Zukunftssicherheit. Natürlich ist diese Frage nicht eindeutig zu beantworten, weil niemand abschätzen kann, wie sich RFID in den nächsten Jahren entwickelt. Jedoch ist die Beachtung von weltweiten Standards und damit kompatiblen Komponenten nicht zu unterschätzen (siehe Kapitel 4).

Zusammenfassend kann man daraus die vier folgenden Fragen ableiten:

- Können alle Partner in der Lieferkette zur Teilnahme motiviert werden?
- Wie werden die gemeinsam benutzten Daten sicher verwaltet?
- Kann eine Übereinkunft bei der Verteilung der Kosten und Gewinne gefunden werden?
- Kann durch die Auswahl eines offenen und weltweiten Standard Zukunftssicherheit geschaffen werden?

Die Antworten auf diese allgemeinen Fragen sind im Einzelfall vorab zu klären. Sicherlich gibt es bei anderen Anwendungen weitere Fragen, die beantwortet sein müssen, bevor man ein RFID-System plant und einführt. Auf die beiden Fragen der Daten-Sicherheit und der Nutzung offener Standards wird im folgenden Kapitel erneut eingegangen. Die beiden anderen Fragen werden nicht weiter behandelt, weil der Prozess der Avisierung nicht auf einer realen Einführung basiert.

Ein spezifisches Problem beim Einsatz dieses RFID-Systems ist die Aktualität der Füllgut-Information. Sollte ein Container nach einer Befüllung den Kreislauf verlassen (siehe Abbildung 8.1) und die nachfolgenden Parteien nach Entleerung, fremder Rekonditionierung und erneuter Befüllung mit einem anderen Füllgut keine Aktualisierungen der Angaben des Containers in der Datenbank vornehmen, dann besteht die Gefahr einer falschen Behandlung des Containers, wodurch gefährliche Situationen für beteiligte Arbeiter und Maschinen entstehen können. Dieses Problem entsteht nicht erst durch den RFID-Einsatz, da auch im herkömmlichen Prozess der Container mit dem Füllgut gekennzeichnet werden muss, jedoch besteht die Gefahr, dass sich Anwender zu stark auf die RFID-Informationen verlassen. In der Praxis muss dann im Einzelfall entschieden werden, wie diese Situationen vermieden werden können. Das Einführen von Plausibilitätsprüfungen kann dabei ein automatisierter Teil einer Lösung sein.

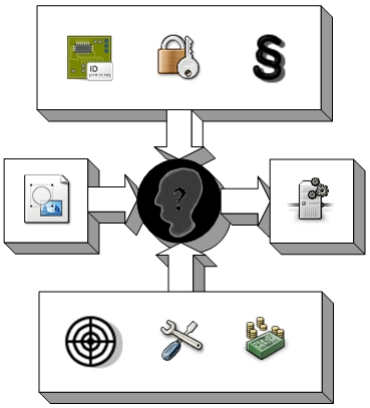
8.5 Weitere denkbare Anwendungen

Der Prototyp implementiert lediglich Funktionen, die die Avisierung von leeren Containern ermöglichen. Dabei lässt sich der Web-Service und die Client-Anwendung noch um weitere Funktionen erweitern, damit zusätzliche Prozesse unterstützt werden können. Im Folgenden werden einige, mögliche Prozesse aufgeführt, die ein Hersteller von Containern für die Industrie ebenfalls mit dem RFID-System unterstützen könnte:

- Produktion: Durch die Nutzung von RFID-Lesern an den Fertigungsbändern kann die Steuerung und Kontrolle der Prozesse übernommen werden. Dabei können sowohl neu produzierte als auch rekonditionierte Container in die Verwaltung aufgenommen werden.
- Warenannahme und -ausgabe: Durch die Nutzung von RFID-Gates an den Eingangs- oder Ausgangstoren der Produktions- oder Lagerstätten können die internen und externen Warenumschläge gebucht werden. Die Pulkerfassung bietet hier einen erheblichen Zeitvorteil und vermindert manuellen Arbeitsaufwand. Im Einzelfall ist die entfernte Warenannahme durch eigene oder fremde LKW-Fahrer denkbar, welche einen mobilen Client benutzen, um die gesammelten Daten an die zentralen Server zu senden.
- *Tracking & Tracing*: Durch die Kopplung von GPS oder anderen Techniken zur Lokalisierung kann der Standort von Containern auf dem eigenen Firmengelände oder gar in der gesamten Lieferkette festgestellt werden.

Kapitel 9

Konzeption eines RFID-Systems



Dieses Kapitel beschäftigt sich mit der Planung eines RFID-Systems. Die hier vorgestellte Vorgehensweise ist ein möglicher Vorschlag für aufeinander folgende Schritte von der Zielsetzung bis hin zur praktischen Umsetzung. Dieses Vorgehen kann nicht nur auf diesen speziellen Anwendungsfall der „Avisierung von leeren Containern“ angewendet werden, sondern kann nach notwendigen Anpassungen auch für andere Szenarien eingesetzt werden.

Die beschriebenen Schritte wurden hauptsächlich bei der Erstellung dieser Arbeit entwickelt, jedoch sind auch Gemeinsamkeiten zu den Handlungsempfehlungen von [Strassner 2005, Kap. 6.3] erkennbar. Teilweise wurden diese Empfehlungen auch in abgewandelter Form übernommen. Zum Beispiel ist die Ermittlung des notwendigen Informationsbedarfs die erste seiner sechs Handlungsempfehlungen [Strassner 2005, S. 207 f.]. Auf die Bedeutung der benötigten Daten und Informationen ist bereits in den drei vorherigen Kapiteln eingegangen worden, so dass an dieser Stelle keine erneute Diskussion darüber geführt wird. Für den Prozess der Avisierung sind folgende Informationen von Bedeutung: Container-ID[205], Ort der Avisierung oder Abholung[206] und die Füllgut-Information vom Tag oder aus der Datenbank.

[205] Mit der ID der Container sind auch Typ, Füllvolumen, Produktionsdatum, usw. bekannt.
[206] Die Lokation wird entweder durch GPS übermittelt oder durch die Stammdaten des Entleerers.

Die Konzeption des Systems lässt sich in zwei große Abschnitte einteilen. Zunächst werden die notwendigen Funktionalitäten und die physischen Voraussetzungen der Tags und Leser herausgearbeitet. Das Ergebnis ist dann eine bestimmte Anzahl von Alternativen aus denen eine als Empfehlung für dieses System gewählt wird. Anschließend wird im zweiten großen Teil des Kapitels das IT-System geplant. Dieses System besteht aus mehreren Komponenten, die aufeinander abgestimmt sein müssen. Schließlich wird auf die Bedeutung von organisatorischen und wirtschaftlichen Überlegungen während der Planung eingegangen, sowie weiterer möglicher Geschäftsprozesse oder Szenarien.

Das Ziel bei der Entwicklung des Prototyps ist die Prüfung der technischen Machbarkeit und den damit verbundenen Möglichkeiten oder Schwierigkeiten. Das Ziel ist nicht eine vollständige Implementierung mit allen Funktionen eines RFID-Systems, eine hohe Performanz oder Robustheit.

9.1 RFID-Technik

Die Auswahl der RFID-Komponenten hängt von vielen Faktoren ab, die von Anwendung zu Anwendung verschieden sind. In den Anforderungen sind bereits einige Funktionen genannt worden.

Zunächst sind die Anforderungen an den RFID-Tag zu beachten. Er wird direkt am Container befestigt und muss sowohl auf metallischen Oberflächen als auch in der Nähe von Flüssigkeiten funktionieren. Die Bauform ist dabei so zu wählen, dass Beschädigungen aufgrund äußerer Einflüsse[207] so weit wie möglich vermieden werden können. Dabei spielt neben der Bauform auch die Position des Tags am Container eine Rolle. Allerdings muss der Tag auch von einem Lageristen zu sehen sein, damit die manuelle Erfassung mit einem mobilen Gerät möglich ist. In Kapitel 2.2.3 wurden zwei mögliche Lösungen für den Einsatz auf metallischen Oberflächen vorgestellt. Der *FlagTag* ist für diese Anwendung nicht geeignet, weil er einfach von den Containern entfernbar wäre. Die *Mount-on-Metal*-Tags mit Ferritkern hingegen lassen sich relativ einfach in einer Mulde eines Bleches versenken und damit vor Kanten anderer Container oder Gabeln von Gabelstaplern schützen (siehe Abbildung 9.1).

[207] Äußere Einflüsse wie das Wetter, Sonneneinstrahlung, Hitze oder Stöße durch Gabelstapler können bei verschiedenen Bauformen zu Lese-Problemen führen, weil die Materialien beschädigt oder verformt werden können.

Abbildung 9.1: *Mount-on-Metal*-Tag versenkt in ein Blech eines Containers.

Die Verwendung von aktiven Tags verbietet sich wegen Sicherheitsbedenken bei der Befüllung mit Gefahrgut. Es gibt keine aktiven RFID-Tags, die explosionsgeschützt sind[208]. Die Dicke der passiven, metallgängigen Tags beträgt ungefähr einen Millimeter.

Ein weiterer wichtiger Faktor bei der Auswahl des Tags sind die Frequenz und der verwendete Standard. UHF-Frequenzen werden von Flüssigkeiten (Wasser) stark absorbiert, haben jedoch eine größere Reichweite als HF-Frequenzen. An dieser Stelle ist nun abzuwägen, welcher Nachteil für diese Anwendung größer ist. Weiterhin ist zu beachten, dass der UHF ISO/IEC 18000-6C-Standard im SCM eine deutlich weitere Verbreitung als alle HF-Standards hat. Die Verfügbarkeit von austauschbarer Hardware und die Zukunftssicherheit von UHF im SCM sind ausschlaggebende Faktoren für die Entscheidung zu Gunsten eines UHF-Systems. Sollte die Nähe von Flüssigkeiten in anderen Anwendungen eine größere Bedeutung haben, so kann dies den Ausschlag für ein HF-System geben.

[208] Im Allgemeinen spricht man von der Eigenschaft „Ex-Schutz“ bei elektrischen Geräten.

Abbildung 9.2: RFID-Leser als Erweiterungskarte mit CF-Schnittstelle [ACG 2003].

Unabhängig von der verwendeten Frequenz ist die Forderung nach wiederbeschreibbarem Speicherplatz auf dem Tag selbst. Jeder Hersteller von Tags stattet seine Tags mit einer bestimmten Menge an Speicher aus. In dem Anwendungsfall „Avisierung von leeren Containern“ kann lediglich die Angabe des Füllgutes auf dem Tag von Interesse sein, so dass ein wiederbeschreibbarer Speicher von 1024 Bit ausreichend ist.

Ist die Entscheidung für ein Tag-Produkt gefallen, dann bietet sich eine Menge an kompatiblen Lesern zur Verwendung an. Dabei sind verschiedene Typen zu wählen, die für die Prozesse notwendig sind. Für die Avisierung leerer Container werden hauptsächlich mobile Leser benötigt, da die Entleerer die Anmeldung vornehmen und an den Rekonditionierer senden. Man kann zwei Arten mobiler Leser unterscheiden: *All-in-One*-Geräte und RFID-Leser in Form von Erweiterungskarten. *All-in-One*-Geräte bestehen aus einem mobilen Rechner (PDA) und integrierten RFID-Lesern. Zusätzlich besitzen diese Geräte Schnittstellen für die Kommunikation mit nachgelagerten Komponenten. Diese Geräte sind sofort einsetzbar, aber die Komponenten sind selten erweiterbar oder austauschbar. Die RFID-Leser in Form von Erweiterungskar-

ten haben standardisierte Schnittstellen[209] für die Verwendung mit Rechnern, Notebooks oder PDAs. Damit kann günstige und weit verbreitete Hardware verwendet werden, da nahezu jeder PDA eine CF-Schnittstelle besitzt. Des Weiteren können dann eigene Anwendungen entwickelt werden, die dann auf dem mobilen Gerät (PDA und RFID-Leser) zur Verwendung kommen. Aus diesen Gründen kommen bei dem Prototyp ein PDA und eine CF-Karte als RFID-Leser zum Einsatz (siehe Abbildung 9.2). Inzwischen sind CF-Karten für die gängigsten Frequenzen (HF, UHF) erhältlich. Der Preis für einen PDA und die CF-Karte liegt dabei deutlich unter dem Preis für ein *All-in-One*-Gerät (bis zu dem Faktor fünf).

Neben den mobilen Geräten bieten sich so genannte *Desktop*-Leser an, die nur aus einer Antenne und der Steuereinheit bestehen und selbst keine Daten verarbeiten können. Sie werden über Kommunikationskomponenten (z. B. LAN oder WLAN) an weiterverarbeitende Systeme angeschlossen. Diese kleinen, stationären Leser werden häufig an Türen oder an Gabelstaplern eingesetzt, weil sie trotz dem stationären Charakters leicht und handlich sind. Schließlich könnte in der Produktion oder im Lager über die Anschaffung von *Gates* nachgedacht werden, die aus einer Steuereinheit und verschiedenen Antennen bestehen.

Diese Vorschläge für die Auswahl der verwendeten Geräte muss in jedem Anwendungsfall unbedingt durch einen Test[210] unter echten Bedingungen überprüft werden. Insbesondere die Lesbarkeit, Reichweite und äußere Einflüsse bestimmen über den Erfolg einer Kombination aus verschiedener Hardware. Zusätzlich können Metalle und Flüssigkeiten die Fehlerrate enorm steigern, so dass sich bestimmte Systeme bei dem Test als unbrauchbar herausstellen.

Obwohl ein UHF-System mit metallgängigen Tags die empfehlenswerte Lösung ist, kommt bei dem verwendeten Prototyp ein HF-System zum Einsatz. Der Grund dafür ist die bereits vorhandene RFID-Hardware, so dass keine Kosten für die Anschaffung anderer, neuer UHF-Geräte anfallen mussten. Dabei

[209] Die verbreitetsten Schnittstellen sind PCMCIA (*Personal Computer Memory Card International Association*), CF (*CompactFlash*), SD Memory Card (*Secure Digital Memory Card*) oder MMC (*Multimedia Card*). SD und MMC werden hauptsächlich für die Erweiterung mit Speicher verwendet. RFID-Leser sind mit den Schnittstellen PCMCIA und CF erhältlich.

[210] Diese umfangreichen Tests werden häufig als „Pilot“ oder „Feldtest“ bezeichnet.

Abbildung 9.3: Einsatz eines PDA zur Erfassung von RFID-Daten eines Containers.

kamen ((rfid))-onMetal-Tags (siehe Abbildung 9.1) von Schreiner LogiData[211] und der RF PC Handheld Reader (CF-Karte) von ACG[212] zum Einsatz.

9.2 IT-Gesamtsystem

Nach der Auswahl der entsprechenden Technik können die restlichen Komponenten des Systems definiert werden. Die eigentliche RFID-Erfassung geschieht lediglich zwischen Tag und Leser. Die nachgelagerten Komponenten hingegen haben die Aufgabe, die erfassten Daten zu sammeln, zu versenden und weiter zu verarbeiten. Die Architektur und die Kommunikationswege des Systems werden im direkt folgenden Unterkapitel behandelt. Anschließend wird auf die technischen Möglichkeiten und Alternativen eingegangen. Aus diesen Alternativen wird die geeignetste gewählt und im Backend und Client umgesetzt. Die Aspekte der Kommunikation und die Orte der Datenspeicherung werden

[211] http://www.schreiner-group.de
[212] http://www.acg.de

während der Konzeption ebenfalls diskutiert, damit ein ausreichendes Maß an Sicherheit der Daten erreicht werden kann.

9.2.1 Schematischer Aufbau

Der schematische Aufbau des Prototyps wurde bereits kurz in Kapitel 1.2 erläutert. Die Abbildung 1.2 zeigt den Aufbau aller beteiligten Komponenten. Neben den RFID-Komponenten, die bereits im vorherigen Kapitel behandelt wurden, existieren noch etliche andere Komponenten, auf die im Folgenden eingegangen wird. Dabei kann man Hard- und Software-Komponenten unterscheiden, wobei die Hardware in diesem Prototyp nur eine geringe Rolle spielt, da nur austauschbare Standard-Komponenten zum Einsatz kommen.

Der Begriff Architektur wurde bereits in vorherigen Kapiteln erwähnt, jedoch bisher nicht definiert. Dies wird an dieser Stelle nachgeholt, weil dadurch die getroffenen Entscheidungen und der resultierende Aufbau besser verstanden werden kann. [Fowler 2002, S. 2] versucht Systeme in verschiedene Schichten (*Layer*) zu unterteilen und durch die Einteilung und den Aufbau der Schichten die Architektur von Systemen zu definieren. Es gibt viele verschiedene Definitionen von Architektur, jedoch sind zwei Elemente üblicherweise in den Definitionen enthalten: Zum einen ist dies die Aufteilung des Gesamtsystems in seine einzelnen Teile und zum anderen sind dies die schwer zu ändernden, getroffenen Entscheidungen [Fowler 2002, S. 1]. Ein weiterer Versuch zur Definition stammt von Ralph Johnson, der Architektur als subjektiv und als gemeinsames Verstehen von Entwicklern auf das Design eines Systems versteht, also die Form der Haupt-Komponenten und wie sie interagieren [Fowler 2002, S. 1 f.]. Schließlich reduziere sich Architektur auf das „wichtige Zeug“. Für diese Arbeit wird keine spezielle Definition von Architektur benötigt. Die in diesem Absatz genannten Eigenschaften von Architektur lassen sich im RFID-Prototyp wieder finden.

In der Literatur wird die Architektur eines RFID-Systems häufig mit drei Haupt-Schichten dargestellt. Die Schichten sind Tag, Leser und das Daten verarbeitende Subsystem [Sarma u. a. 2003, S. 455 f.]. Diese Schichten lassen sich in allen RFID-Systemen wieder finden, da alle Schichten für den Betrieb notwendig sind. Variationen innerhalb einer Schicht, z. B. unterschiedliche Tag-Typen oder Daten-Strukturen, sind dabei nicht nur möglich sondern fast unvermeidbar. Da jede Anwendung andere Anforderungen hat, ergeben sich au-

tomatisch verschiedenste Ausprägungen. Zwischen jeder Schicht existiert eine oder mehrere Schnittstellen. Zwischen Tag und Leser regelt das *Air-Interface* die Kommunikation, wobei zwischen Leser und Backend verschiedene Kommunikationswege möglich sind (siehe Kapitel 9.2.5). Der Hauptunterschied von Systemen mit stationären Lesern zu Systemen mit mobilen Lesern ist diese Schnittstelle zwischen Leser und Backend.[213] Alle anderen Komponenten sind nahezu identisch.

Die verschiedenen Ausprägungen der Tags und Leser wurden bereits häufig diskutiert. Der mobile Client und das Backend jedoch wurden bisher nur in Ansätzen behandelt. Aus diesem Grund wird nun auf die Software des Clients und des Backend verstärkt eingegangen. Auf jedem Rechner des Systems wird eine bestimmte Software benötigt, damit die Daten weiter verarbeitet werden können. Der Client hat die Aufgaben der Datenerfassung, -vorfilterung und -versendung. In aller Regel haben mobile Clients zusätzlich eine grafische Oberfläche (GUI, *Graphical User Interface*) zur Bedienung der Anwendung. Stationäre Leser hingeben arbeiten oft ohne manuelle Eingriffe und bieten lediglich eine Statusanzeige oder ein Protokoll. Die nächste Komponente des Backends wird allgemein *Middleware* genannt und ist der Endpunkt der Kommunikation mit dem Client. Der Begriff *Middleware* wird häufig für die verschiedensten Komponenten in einem RFID-System benutzt. Im Allgemeinen ist die Middleware zuständig für die Kommunikation mit Clients, die Identifikation der Clients, die Filterung und das Ablegen oder Weiterleiten von Daten an nachgelagerte Systeme. Eventuell stößt die Middleware durch das Versenden von Ereignissen neue Prozesse zur Weiterverarbeitung an. Die empfangenen Daten werden in einer Datenbank abgelegt, damit das BIS die Daten zu einem geeigneten Zeitpunkt lesen und verarbeiten kann. Eventuell liegt die Datenbank sogar innerhalb des BIS, so dass eine zusätzliche Datenbank unnötig wird. Anzumerken ist, dass nicht notwendigerweise alle empfangenen Daten direkt ins BIS gelangen sollen. Je nach Anwendung und Sicherheitsaspekten ist die separate Speicherung der Daten sinnvoll. Das BIS kann aus einer Vielzahl verschiedener Systeme bestehen, die auch ohne die RFID-Komponenten be-

[213] Bei Systemen mit mobilen Lesern können dies PDAs oder Gabelstapler sein, die über die verschiedensten Kommunikationswege – teilweise nur temporär – angebunden werden. Bei stationären Lesern hingegen sind die Geräte fest installiert und haben in der Regel eine ständige Anbindung an das IT-System.

stehen, weil sie für die täglichen Prozesse (Beschaffung, Produktion, Vertrieb, Buchhaltung, usw.) verwendet werden.

Die Anbindung an die bestehenden Systeme (Integration) ist eine Herausforderung, die in jedem Unternehmen verschieden schwer und aufwändig sein kann. Eventuell müssen auch innerhalb des BIS neue Software-Module oder -Komponenten entwickelt werden, damit die RFID-Daten verarbeitet werden können. Diese Anbindung ist im Prototyp nicht implementiert, da es kein allgemein gültiges Vorgehen zur Integration in Betriebliche Informationssysteme gibt. Diese Integration ist für diese Arbeit auch nicht notwendig, weil die hier vorgestellten Konzepte als Demonstration eines RFID-Prototyps ausreichen.

9.2.2 Einsetzbare Techniken

Die Software-Komponenten auf den verschiedenen Rechnern müssen problemlos miteinander kommunizieren können. Deswegen können entweder Lösungen eines Herstellers oder Standards verwendet werden, um eine reibungslose Kommunikation zu gewährleisten. Der Einsatz von kompletten, fertigen Lösungen von verschiedenen Software-Herstellern ist nicht immer möglich, weil dann die Kompatibilität nicht immer gewährleistet ist. Viele ERP-Hersteller bieten für ihre Systeme RFID-Module an, die verwendet werden können, aber es existieren keine allgemeinen Lösungen für alle Anwendungsfälle. Der Prototyp verwendet selbst entwickelte Programme und offene Schnittstellen. Er erfüllt die grundlegenden Funktionalitäten und bietet nachgelagerten BIS offene Schnittstellen für den Zugriff auf die Daten.

Es gibt verschiedene Konzepte zur Integration verschiedener Anwendungen und Parteien. Die Begrifflichkeiten verschiedenster Konzepte werden dabei häufig falsch benutzt. Aus diesem Grund wird zunächst eine kurze Unterscheidung der Bedeutungen der Begriffe getroffen. Im Allgemeinen kann Integration auf drei verschiedenen Ebenen geschehen. Diese Ebenen sind Datenintegration, Anwendungsintegration und Prozessintegration.

Bei der *Enterprise Application Integration* (EAI) werden Anwendungen verschiedener Unternehmen verbunden, die unabhängig voneinander arbeiten und lediglich durch gemeinsame Prozesse verbunden sind. In aller Regel ist EAI

eine Prozessintegration, die sich durch die Schaffung von *E-Business*-Anwendungen[214] realisieren lässt.

Eine Serviceorientierte Architektur (SOA, *Service Oriented Architecture*) hingegen zielt nicht primär auf die Verbindung von verteilten Anwendungen in verschiedenen Unternehmen, sondern eher auf die Verbindung zweier Anwendungen, welche aus Client und Server bestehen. Dadurch wird eine direkte Kommunikation zwischen zwei Anwendungen erreicht. Ein Client stellt eine Anfrage an einen Dienst eines Servers und erhält darauf hin eine Antwort. Web-Services[215] sind eine mögliche Umsetzung der Serviceorientierten Architektur. Weitere dienstbasierte Vertreter sind *Common Object Request Broker Architecture*[216] (CORBA) oder *Distributed Component Object Model*[217] (DCOM). Da DCOM eine proprietäre Lösung ist und CORBA einen sehr großen Overhead an Verwaltung und Software-Komponenten mit sich bringt, bieten sich Web-Services als schlanke und standardisierte Schnittstelle für die Kommunikation zwischen Client und Server an. Bei Web-Services werden die bekannten Protokolle TCP/IP und HTTP verwendet sowie SOAP[218] für die Strukturierung der Daten auf der Anwendungsschicht. Sie sind eine der möglichen Lösungen für die Realisierung von *Remote Procedure Calls*[219] (RPC) über das Internet. Vorteile von Web-Services sind ihre Plattformunabhängigkeit, sie benötigen keine weitere Software auf dem Client und lassen sich über die Standard-Ports des Internets[220] ausführen. Um Verbindungen zu Web-Services von anderen HTTP-Verbindungen zu unterscheiden, z. B. aus sicherheitstechnischen oder systembedingten Gründen, können die Web-Services aber auch so konfiguriert

[214] *E-Business* sind Geschäftsprozesse zwischen Unternehmen, die mit Hilfe von Internet-Technologien (oder andere elektronischen Technologien) durchgeführt werden.

[215] In der Literatur wird „Web-Service“ häufig anders geschrieben. Zum Beispiel finden sich häufig die Schreibweisen „Web Service“ oder „Webservice“.

[216] CORBA ist eine objektorientierte Anwendungsschicht für den Einsatz von verteilten Anwendungen. Sie wurde von der Object Management Group (OMG, `http://www.omg.org`) entwickelt.

[217] DCOM ist ein Protokoll von Microsoft (`http://www.microsoft.com`) zur Kommunikation von Anwendungen innerhalb eines Netzwerkes.

[218] Das *Simple Object Access Protocol* ist eine Spezifikation des W3C (`http://www.w3.org`) und wird zum Datenaustausch zwischen zwei Systemen verwendet. Die Daten werden in Form von XML *Extensible Markup Language* repräsentiert.

[219] Ein *Remote Procedure Call* ist der Aufruf einer Operation (Methode, Prozedur, Funktion) einer Anwendung (Objekt) auf einem anderen Host in einem Netzwerk (auch Internet). Gibt die Operation einen Rückgabewert zurück, dann wird dieser an den Client gesendet.

[220] Web-Services benutzen die HTTP-und HTTPS-Ports der Web-Server, welche standardmäßig auf 80 und 443 eingestellt sind. Diese Ports der Web-Server sind in der Regel nicht von Firewalls geblockt.

werden, dass sie auf anderen als den Standard-Ports laufen. Jedoch kann das Parsen der XML-Nachrichten im Einzelfall die Performanz verschlechtern. Die verwendeten Programmiersprachen müssen die Web-Services mit Hilfe von speziellen Erweiterungen unterstützen. Web-Services sind dabei nur eine Schnittstelle für die Kommunikation zu dem Backend. Die funktionalen Teile des Backends sind dabei herkömmliche Anwendungen, für die die aufrufenden Instanzen – lokal oder entfernt – transparent sind.

Ein weiterer Ansatz für die Kommunikation zwischen Client und Server ist neben EAI und SOA der Architekturstil *Representational State Transfer* (REST), welcher in einer Dissertation von Fielding bekannt wurde [Fielding 2000]. Dabei stellt ein Client eine Anfrage in Form eines HTTP-GET-Requests, worauf der Server dann mit einer HTTP-Response antwortet. Bei der Anfrage können Parameter für den Aufruf der Operation übergeben werden. REST und HTTP werden beim *Browsen* im Internet verwendet, jedoch ist REST weniger mächtig als Web-Services. Einfache Web-Services können durch REST-Implementierungen ersetzt werden, jedoch ist die Übermittlung komplexer Datenstrukturen mit REST nicht möglich. Ursprünglich war REST für die Abfrage von einfachen Ressourcen im Internet gedacht und nicht – wie Web-Services – für den komplexen Nachrichtenaustausch zwischen Systemen [Mintert 2005].

Aus den oben genannten Gründen werden für diesen Prototyp Web-Services verwendet. In den folgenden Kapiteln werden die beteiligten Komponenten näher erläutert.

9.2.3 Backend

Das Backend besteht aus den verschiedenen Servern an zentraler Stelle des Unternehmens. Neben der Schnittstelle zu den mobilen Clients, die mit Hilfe von Web-Services realisiert wird, müssen die Anwendungen mit dem BIS verbunden werden, damit die Daten weiterverarbeitet werden. Aus diesen beiden Schnittstellen und den benötigten funktionalen Anwendungen wird das Backend aufgebaut.

9.2.3.1 Alternativen zur Implementierung von Web-Services

Für die Anbindung der mobilen Clients werden Web-Services eingesetzt. Für die Implementierung von Web-Services bieten sich verschiedene Kombinationen

von Software-Komponenten an. Im Folgenden werden verschiedene Komponenten genannt, und anschließend wird eine Alternative ausgewählt. Da Web-Services standardisierte Schnittstellen zu den mobilen Geräten sind, kann eine Auswahl unter den verschiedenen am Markt erhältlichen Produkten getroffen werden.

IBM bietet ein Web-Services-Gateway innerhalb seiner WebSphere-Suite an. Diese Lösung ist ein kommerzielles Produkt und wird mit dem WebSphere Application Server eingesetzt. Die verwendete Programmiersprache ist Java. Da die WebSphere-Suite ein großes, komplexes und dazu kostenpflichtiges Paket ist, wird es nicht in die engere Auswahl genommen. Für Unternehmen mit IBM-Produkten im produktiven Einsatz oder einer WebSphere-Installation kann diese Alternative eine günstige und geeignete Lösung sein.

Der Software-Hersteller SAP[221] hat das Produkt Web Application Server als Teil der NetWeaver-Plattform im Angebot. Ein auf Java und ABAP[222] basierender Web-Server kann als Basis für Web-Services und eigene Anwendungen benutzt werden. Obwohl SAP hauptsächlich als ERP-Softwarehersteller bekannt geworden ist, bieten sie NetWeaver-Komponenten inzwischen auch ohne die ERP-Software an, so dass auch Unternehmen ohne die ERP-Software von SAP den Web Application Server einsetzen können. Jedoch ist auch diese Lösung nicht kostenlos erhältlich, so dass der SAP Web Application Server nicht ausgewählt wurde. In Zukunft könnte die Kombination der SAP Auto-ID Infrastructure mit dem Web Application Server interessant sein, da damit gleichzeitig eine Verwaltung von RFID-Hardware möglich ist. Allerdings entfalten diese Komponenten ihren größten Nutzen erst mit dem Einsatz der kompletten ERP-Software, da die Schnittstellen der Auto-ID Infrastructure auf die restlichen SAP-Module abgestimmt sind.

Es gibt zwei weitere Alternativen, die für den Einsatz im Prototyp zur Avisierung von leeren Containern geeignet sind. Zum einen ist die Kombination aus dem Tomcat-Server und Axis2-Engine von dem *Apache Software Foundation*[223] denkbar. Zum anderen kann der *Internet Information Server* (IIS) mit dem

[221] http://www.sap.com

[222] ABAP steht für *Advanced Business Application Programming* und ist die SAP-eigene Programmiersprache. ABAP bildet die Grundlage des SAP-Systems und wird schrittweise – aber sicherlich nie komplett – durch Java ersetzt.

[223] http://www.apache.org

Microsoft XML SDK[224] verwendet werden, um Web-Services zu implementieren. Alle diese Software-Produkte sind kostenlos, wenn man die Lizenzkosten für Microsoft Windows, in dem der IIS integriert ist, außer Acht lässt. Bei den Apache-Produkten kann man Eclipse[225] als Entwicklungsumgebung (*Integrated Development Environment*, IDE) einsetzen und die erstellten Anwendungen mit Web-Service-Schnittstelle als Java-Servlets[226] auf dem Tomcat-Server ablegen. Die Programmiersprache für die Web-Service-Implementierung auf dem IIS hingegen ist Microsoft .NET (C++, C#, Basic, usw.), so dass verschiedene IDEs eingesetzt werden können. Es gibt verschiedene, freie IDEs für C++ und .NET, jedoch bietet Microsoft Visual Studio den größten Funktionsumfang und unkomplizierte Bedienung im Zusammenspiel mit dem IIS. Allerdings ist Visual Studio nicht kostenlos erhältlich. Eine weitere, benötigte Komponente ist eine Datenbank für die Ablage der empfangenen Daten. Es gibt freie Datenbanken wie MySQL[227] und PostgreSQL[228], sowie den SQL Server von Microsoft. Wichtig für eine Plattform übergreifende Benutzung ist eine offene Datenbank-Schnittstelle. Die drei genannten Datenbanken sind SQL-fähig und für sie existieren ODBC-Treiber[229].

Der Prototyp verwendet die Lösung mit den Microsoft-Komponenten, weil sie der Universität Koblenz-Landau kostenlos zur Verfügung stehen und in Visual Studio 2005 vollständig enthalten sind (IDE, SQL Server, IIS bei Windows XP Professional, XML SDK als kostenloser Download). Dadurch ist der Aufbau und die Nutzung aufeinander abgestimmter Komponenten möglich. Der Funktionsumfang ist durch die Integration der IDE in den IIS umfassend und die Bedienung komfortabel. Dies wird auch in Kapitel 9.2.4.1 deutlich. Das Konzept der Programmiersprache .NET ähnelt stark dem Java-Konzept. In der Version 2.0 ist .NET um viele Funktionen erweitert worden, die die Entwicklung von Web-Services erleichtern.

[224] Ein *Software Development Kit* ist eine Menge von Programmen, Werkzeugen und Dokumentationen für die Entwicklung von Programmen. Ein SDK gehört immer zu einer bestimmten Programmiersprache und wird von dem Hersteller bereitgestellt.

[225] Eclipse ist *Open Source* und unter http://www.eclipse.org erhältlich.

[226] Servlets sind Java-Anwendungen, die auf einem Web-Server ausgeführt werden. Dabei können dynamische Inhalte auf dem Web-Server generiert werden.

[227] http://www.mysql.de

[228] http://www.postgresql.org

[229] *Open Database Connectivity* ist eine API für die Verwendung verschiedener Datenbanken. Sie verwendet SQL als Datenbanksprache.

Der Nachteil der Microsoft-Lösung ist, dass die Komponenten nicht Plattform übergreifend einsetzbar sind. Zum einen benötigen der IIS und Visual Studio als Betriebssystem Microsoft Windows und zum anderen unterstützt .NET nur Programmiersprachen von Microsoft. Es gibt Bestrebungen für .NET kompatible Laufzeitumgebungen zu schaffen[230], jedoch gilt dies lediglich für herkömmliche Anwendungen und nicht für Web-Services innerhalb Web-Servern.

Die wichtigste Eigenschaft des Prototyps ist die Beachtung von Standards bei der Kommunikation. In diesem Fall sind das Web-Services, die SOAP und HTTP verwenden. Das ermöglicht einen eventuell notwendigen Austausch der Software eines Web-Services. Dies kann der Fall sein, wenn Teile der Systemlandschaft migriert werden müssen, z. B. im Zuge eines Wechsels des ERP-Systems. Die Nutzer der Dienste bemerken im besten Fall nichts von dieser Umstellung und können so ohne Unterbrechung oder Störungen ihre Daten erfassen.

9.2.3.2 Integration in bestehende Systeme

Die Integration des Prototyps in bestehende Systeme wird nicht implementiert. Erstens steht kein BIS zur Verfügung und zweitens liegt der Fokus der Arbeit nicht auf der Integration in Betriebliche Informationssysteme, sondern auf der Entwicklung des Prototyps.

Aus diesem Grund werden lediglich zwei mögliche Lösungen angeboten, die einem BIS die Datenübernahme ermöglichen. Der Prototyp kann nach dem Empfang von Daten eine E-Mail versenden oder stellt die Daten in einer eigenen Datenbank über offene Schnittstellen zur Verfügung. Der Versand einer E-Mail wird in einem produktiven System wohl nicht zum Einsatz kommen, sondern stellt lediglich einen Stellvertreter für das *Pushen*[231] von Daten dar. Die im Produktivbetrieb empfohlene *Push*-Methode ist der Aufruf einer entfernten Prozedur (RPC, *Remote Procedure Call*). Da jedoch dieser Aufruf von dem verwendeten BIS abhängt, wird im Prototyp kein RPC implementiert.

[230] Novell (http://www.novell.com) betreibt das *Open Source* Projekt Mono für die Betriebssysteme Windows, Linux und Mac OS X. Microsoft hat eine .NET-Umgebung namens Rotor für BSD-Varianten zur kostenlosen Benutzung freigegeben.

[231] Mit dem *Pushen* von Daten wird das sofortige Weiterleiten der Daten oder die Benachrichtigung von nachgelagerten Systemen über das Eintreffen von neuen Daten bezeichnet. Eine Alternative ist die *Pull*-Methode, welche die Daten ablegt. Anschließend werden die Daten dann – meist periodisch – von anderen Systemen abgeholt.

Die empfangenen Daten werden immer in einer eigenen Datenbank abgelegt. Nachgelagerte Systeme können dann auf diese Daten per SQL zugreifen, so dass die notwendige Weiterverarbeitung möglich ist. Es gibt eine Vielzahl von möglichen Datenbank-Produkten, die zum Einsatz kommen können, da fast jede Datenbank SQL-fähig ist. Die Auswahl der Datenbank hängt von den bereits eingesetzten Lösungen und den gewünschten Datenbank-Funktionen (Transaktionssicherheit, *Constraints*, *Stored Procedures*, *Trigger*, usw.) ab. Der Prototyp verwendet die Microsoft SQL Datenbank, weil diese bereits in dem Paket von Visual Studio 2005 enthalten ist.

In der Praxis ist eine Kombination von *Push*- und *Pull*-Methode denkbar. Beim Empfang werden die Daten in der Datenbank des Backends abgelegt und im Anschluss wird das entsprechende BIS durch den Aufruf einer Methode von dem Eintreffen neuer Daten benachrichtigt. Der Vorteil dieser Vorgehensweise ist die Entlastung der Datenbanken des BIS durch die Speicherung in einer getrennten Datenbank und keine nennenswerte Verzögerung der Verarbeitung aufgrund der Benachrichtigung. Periodische Abfragen der Datenbank nach neu eingetroffenen Daten können entfallen und entlasten somit Server und Netzwerke.

9.2.3.3 Aufbau des Web-Services

Der Prototyp implementiert einen Web-Service mit genau einem Dienst[232]. Dieser Dienst ist die Anmeldung zur Abholung (Avisierung) von entleerten Containern, wie sie in Kapitel 8 bereits ausführlich beschrieben wird. Die per RFID gesammelten Daten werden entgegengenommen und den nachgelagerten Informationssystemen zur Verfügung gestellt. An dieser Stelle werden kurz die einzelnen Aufgaben des Dienstes erwähnt:

1. Der Datensatz wird entgegengenommen. Aus den Inhalten der SOAP-Nachricht wird ein lokales Objekt erstellt.

2. Die Angaben für die Authentifikation (Benutzername/Passwort) werden mit den Werten aus der zuständigen Datenbank verglichen.

[232] Ein Web-Service („Web-Dienst“) ist eine Sammlung von vielen einzelnen Diensten unter einer URL. Der benötigte Dienst wird durch die Übergabe von Parametern ausgewählt und angefragt. Ein Web-Service ist vergleichbar mit einer Objekt orientierten Schnittstelle und ein Dienst mit einer Operation der Schnittstelle

3. Die restlichen Inhalte werden validiert und ggf. in das korrekte Format umgewandelt.
4. Die übertragene Container-ID wird überprüft (Existenz, Gültigkeit, Status).
5. Der Datensatz wird in der Datenbank persistent gemacht.
6. Zur Benachrichtigung wird eine E-Mail versendet.

Aus diesem kurzen Ablauf werden einige wichtige Eigenschaften des RFID-Systems deutlich. Aus Gründen der Sicherheit werden nur authentifizierte Benutzer zu dem Web-Service zugelassen. Dies ist einer der ersten Schritte der Filterung der eingehenden Daten. Anschließend werden die anderen Angaben auf gültige Wertebereiche und Vollständigkeit überprüft. Dies verringert falsche oder fehlende Angaben. Schließlich wird der bereits existierende Stamm-Datensatz des betroffenen Containers gesucht. Erlauben die hinterlegten Daten eine Avisierung zur Abholung des Containers, dann kann diese Avisierung gespeichert und weiterverarbeitet werden. Das Ziel der sorgfältigen Prüfung der eingehenden Daten ist die Entlastung der nachfolgenden Anwendungen, so dass nicht zu bearbeitende Datensätze so früh wie möglich ausgefiltert werden. Andererseits soll auf dem Client so wenig wie notwendig berechnet werden, da die mobilen Clients in der Regel deutlich schwächer ausgestattet sind[233]. Eine große Belastung der PDAs könnte mit langen Wartezeiten verbunden sein und die Arbeit des Anwenders unnötig verzögern. Durch die Prüfung der Container-ID werden nicht zugelassene (fremde) Container abgelehnt, so dass schon bei der Avisierung unnötige Folgekosten vermieden werden können.

9.2.4 Client

Der mobile Client sammelt die anfallenden RFID-Daten und sendet sie an den Web-Service des Backends. Der Client hat die Aufgaben, die notwendige Hardware für die Erfassung von RFID- und Positionsdaten einzubinden, die Daten

[233] Die Ausstattung von mobilen Clients ist wegen der Miniaturisierung, dem Gewicht und dem niedrigeren Energieverbrauch deutlich schwächer. Dies betrifft den Prozessor (CPU, *Central Processing Unit*), den Arbeitsspeicher (RAM) und die Speicher-Kapazität (Flash-Speicher, Erweiterungskarten).

für den Versand aufzubereiten und die Verbindung zum Backend aufzubauen. In den folgenden Abschnitten wird die Auswahl der geeigneten Komponenten für einen mobilen Client zur Kommunikation mit dem Backend getroffen und begründet.

9.2.4.1 Auswahl des Betriebssystems und der Entwicklungsumgebung

Es gibt zwei vorherrschende Betriebssystem-Familien bei mobilen Geräten (z. B. PDAs). Zum einen bietet Microsoft mit seinem Windows CE Betriebssystem-Kern die Basis für die Betriebssysteme Pocket PC und Windows Mobile[234]. Zum anderen stellt Palm[235] PDAs mit dem Betriebssystem Palm OS her, welches lange Zeit das vorherrschende Betriebssystem war. Microsoft gewann in den letzten Jahren jedoch immer mehr Marktanteile und war schon Mitte 2005 mit ca. 50 % Marktanteil Marktführer [Kuri 2005]. Da beide Betriebssysteme auf der ARM-Architektur[236] laufen und Palm OS ständig an Marktanteilen verliert, hat sich Palm dazu entschlossen, auch das Microsoft Betriebssystem auf ihren Geräten zu verwenden [Ziegler 2005].

Weitere Betriebssysteme für mobile Geräte sind Symbian und Linux. Symbian wird hauptsächlich für *Smartphones*[237] und Mobiltelefone verwendet, so dass es für den Einsatz in PDAs nicht geeignet ist. Linux weckt auch im PDA-Bereich immer mehr das Interesse von großen Herstellern [Kaps 2006]. Bis zur Marktreife und den möglichen Einsatz im gewerblichen Umfeld wird jedoch noch das ein oder andere Jahr vergehen.

Aufgrund der großen Verbreitung, guter Erhältlichkeit und bekannter Bedienungselemente aus dem PC-Bereich bietet sich ein Pocket PC oder Windows Mobile Gerät für die Verwendung als mobilen RFID-Client an.

Ein weiterer, großer Vorteil ist die Möglichkeit zur Verwendung der gleichen Programmiersprache (C#) für die Client-Software wie für den Web-Service. Microsoft bietet für die mobilen Betriebssysteme das .NET Compact Framework für den kostenlosen Einsatz zum Download an. Des Weiteren können Anwendungen für mobile Geräte mit Microsoft Visual Studio 2005 erstellt werden,

[234] Je nach Version des Betriebssystems unterscheiden sich die Bezeichnung der mobilen Betriebssysteme. Nach dem anfänglichen Namen Windows CE und Pocket PC ist zurzeit die Bezeichnung Windows Mobile aktuell.

[235] http://www.palm.com

[236] ARM ist eine Prozessor-Architektur für mobile Geräte, die ein gutes Verhältnis zwischen Leistung und Stromaufnahme bietet.

[237] Ein *Smartphone* ist eine Kombination von einem Mobiltelefon und einem PDA.

Abbildung 9.4: PDA HP iPAQ hx4700 als mobiles Gerät für den Prototyp [MA-1 Datori 2005].

so dass nicht nur die gleiche Programmiersprache für Client und Web-Service, sondern auch eine ähnliche API (.NET Framework) und die gleiche IDE zur Entwicklung, benutzt werden kann.

Durch die Verwendung von weit verbreiteten Komponenten steigt die Wahrscheinlichkeit für eine gute Unterstützung der einzubindenden Hardware-Komponenten. Unter diesen Komponenten ist die wichtigste Komponenten der RFID-Leser.

9.2.4.2 Hardware für die Erfassung

Die für den Client verwendete Hardware zur RFID-Erfassung setzt sich aus drei Komponenten zusammen. Das mobile Gerät ist ein gut erhältlicher Standard-PDA, der RFID-Leser ist eine Erweiterungskarte im CF-Format und der GPS-Empfänger ist eine GPS-Maus[238] mit Bluetooth-Schnittstelle.

[238] Eine GPS-Maus ist ein kleines, elektronisches Gerät für den Empfang der GPS-Signale. Durch die entfernte Ähnlichkeit zu einer Computer-Maus hat sich die Bezeichnung Maus weit verbreitet.

Die Anforderungen an den PDA sind nicht sehr hoch. Aufgrund der Anforderungen nach Austauschbarkeit und Preisgünstigkeit wurde der Hewlett-Packard iPAQ hx4700 ausgewählt (siehe Abbildung 9.4). Der PDA hat das Betriebssystem Pocket PC 2003, den notwendigen CF-Slot, die Bluetooth-Schnittstelle für die Kommunikation mit dem GPS-Empfänger und WLAN für die Kommunikation. Diese Komponenten reichen für den Test-Betrieb des mobilen Clients aus. Der ausgewählte PDA stammt aus der Business-Linie von HP, so dass für den produktiven Einsatz im industriellen Umfeld die Auswahl eines robusteren Modells oder ein zusätzliches Gehäuse zum Schutz vor Staub, Feuchtigkeit und Stößen ratsam ist.

Wie bereits in Kapitel 9.1 angekündigt wird für den Prototyp eine CF-Karte als RFID-Leser verwendet. Unter extremen, äußeren Bedingungen mag ein Handheld-Gerät mit integrierter Leser sinnvoll sein, jedoch ist auch eine CF-Karte für den Einsatz außerhalb von Gebäuden geeignet. Für viele PDAs gibt es Gehäuse für den Außeneinsatz, die Staub und Spritzwasser abhalten können.

Die CF-Karte muss für den HF-Frequenzbereich ausgelegt sein und den ISO/IEC 15693 Standard unterstützen, da die Schreiner ((rfid))-onMetal-Tags nur diesen Standard unterstützen. Des Weiteren muss für die Karte eine API erhältlich sein, damit die C#-Anwendung über diese Schnittstelle auf die Funktionen der Karte und damit die RFID-Daten zugreifen kann. Jedoch wird die API von verschiedenen Herstellern zu hohen Preisen angeboten. Die Firma Socket[239] bietet zusätzlich ihrer CompactFlash RFID Reader Card 6E das passende SDK für 1.000 US-Dollar an. Das SDK beinhaltet Online-Support und Updates für ein Jahr. Man benötigt das SDK nur einmalig und kann dann so viele Anwendungen wie gewünscht ohne Zahlung weiterer Lizenzgebühren entwickeln. Die Socket Karte bietet sich somit für Software-Hersteller an, die ihre Produkte verkaufen möchten, oder für Abnehmer großer Mengen der Karten, so dass die Kosten für das SDK im Verhältnis nicht so stark ins Gewicht fallen.

Neben dem Anbieter mit kostenpflichtiger API gibt es drei bekannte RFID-Hardware-Hersteller, die die APIs kostenlos zu den CF-Karten ausliefern. Dies sind MeshedSystems[240] (Hand-IT 13,56 MHz CF Slot RFID Schreib-/Leseeinheit), microsensys[241] (CFC reader PRO) und ACG (RF PC Handheld Reader).

[239] http://www.socketstore.com
[240] http://www.meshedsystems.com
[241] http://www.microsensys.de

Abbildung 9.5: GPS-Empfänger mit Bluetooth-Schnittstelle [Navilock 2005].

Alle drei Produkte sind für den Einsatz im mobilen Client geeignet, jedoch fiel die Wahl auf die ACG-Karte, weil der Support sehr gut[242] und das Produkt weit verbreitet ist.

Dieser Prototyp verwendet eine Frequenz im HF-Bereich. Sollte bei anderen Anforderungen an die Anwendung der UHF-Bereich gewählt werden, dann gibt es auch CF-Karten im UHF-Bereich für den Einsatz in PDAs. Identec[243] bietet beispielsweise seit ca. Ende 2005 die i-CARD CF Karte an, welche aber lediglich über eine von Identec geschaffene, proprietäre Luftschnittstelle verfügt. Somit sind nur Tags von Identec benutzbar, was die Auswahl von einer geeigneten Kombination aus Tag und Leser deutlich einschränkt.

Da der PDA keinen internen GPS-Empfänger hat, wird ein externer eingesetzt (siehe Abbildung 9.5). Die GPS-Maus wird per Bluetooth-Funkverbindung an den PDA angeschlossen, um die GPS-Daten vom Empfänger in der Anwendung zu nutzen. Dabei werden nur die Informationen für die aktuelle Position in der Anwendung benötigt (geographische Länge und Breite). Für das Auslesen der Daten wird keine API des Herstellers benötigt, da so gut wie alle GPS-Empfänger das NMEA-0183-Protokoll[244] beherrschen. Die NMEA-Datensätze sind einfach aufgebaut und deswegen auch leicht auszulesen. Es wird lediglich einer der Datensatz-Typen mit den Positionsdaten benötigt (GPRMC-Datensatz). Wegen der geringen Anforderungen an den

[242] Vor dem Kauf konnten der ACG-Vertrieb und die Techniker bereits alle Fragen zu den Funktionen und der möglichen Einbindung in C#-Anwendungen Auskunft geben. Dieser Eindruck hat sich im Verlauf der Implementierung bestätigt.

[243] http://www.identecsolutions.com

[244] Der Standard zur Übertragung von Positionsdaten wurde von der amerikanischen *National Marine Electronics Association* verfasst und ist heute in der Version 0183 weit verbreitet.

GPS-Empfänger gibt es eine Vielzahl von verschiedenen Anbietern und Produkten, die problemlos verwendet werden können. Für diese Arbeit wurde von Navilock der Bluetooth GPS-Empfänger BT-308 verwendet.

Somit werden die drei Hardware-Komponenten verwendet, die zusammen einen den Anforderungen gerecht werdenden mobilen Client ergeben. Die Kosten für diese Komponenten belaufen sich insgesamt auf ca. 700 Euro. Für erhöhten Komfort – wie z. B. integrierte GPS-Empfänger oder RFID-Leser – oder robuste Ausführung der Gehäuse sind deutliche Mehrkosten notwendig. Geräte mit integrierten RFID-Lesern sind für deutlich über 1000 Euro erhältlich.[245]

9.2.5 Kommunikation

Die Kommunikation spielt eine der wichtigsten Rollen beim Einsatz von mobilen RFID-Clients. Dabei werden verschiedene Schnittstellen und Protokolle eingesetzt (siehe auch Abbildung 1.2):

- RFID-Tag – RFID-Leser: Luftschnittstelle ISO/IEC 15693,
- GPS-Satelliten – GPS-Empfänger: Signale im UHF-Bereich,
- RFID-Leser – PDA: CF-Slot, serieller Anschluss, Hersteller-API,
- GPS-Empfänger – PDA: Bluetooth, serieller Anschluss, NMEA-Protokoll,
- PDA – Netzwerk: WLAN (LAN), GPRS/UMTS,
- Client-Software – Web-Service: SOAP (XML, HTTP),
- Web-Service – Server-Anwendung: .NET Framework,
- Server-Anwendung – Datenbank: SQL, ODBC,
- Server-Anwendung – BIS: RPC, E-Mail,
- BIS – Datenbank: ODBC, SQL.

[245] Zum Beispiel wird auf http://www.identware.de/html/PSION-Teklogix-7535.html für den Outdoor-Handheld Psion Teklogix 7535 mit RFID-Leser die Preis-Klasse von 2500 Euro angegeben (Stand Juli 2006).

Die wichtigste Schnittstelle ist die Kommunikation zwischen der Client-Anwendung und dem Web-Service, also die Kommunikation zwischen Client und Backend. Dabei sind nicht nur die Inhalte der Nachrichten von Bedeutung, sondern vor allem die Aspekte der Sicherheit. Da die SOAP-Nachrichten nicht nur innerhalb privater Netze übermittelt werden, sondern auch über öffentliche Transportnetze (GPRS, UMTS) und das Internet, werden hohe Anforderungen an die Identifikation und Authentifikation des mobilen Clients sowie die Integrität der übertragenen Daten gestellt.

Zur Kommunikation über WLAN besitzt der PDA einen integrierten WLAN-Adapter, der den Standard IEEE 802.11b (bis 11 Mbit/s) unterstützt. Die gängigen Verschlüsselungsmethoden WEP[246] und WPA[247] werden unterstützt.

Da der PDA keine GPRS- oder UMTS-Funktionen besitzt, muss für den Einsatz außerhalb von WLANs ein zusätzliches Gerät den Verbindungsaufbau übernehmen. Diese Aufgabe kann ein Mobiltelefon mit Bluetooth-Funktion für den PDA übernehmen. Nach der Bluetooth-Kopplung der beiden Geräte kann auf dem PDA eine neue Verbindung zu dem jeweiligen Mobilfunk-Provider aufgebaut werden. Die Bandbreite bei GPRS-Verbindungen ist natürlich nicht so groß wie bei WLAN-Verbindungen, jedoch reicht sie für diese Anwendung aus, da nur kleine SOAP-Nachrichten versendet werden.

9.2.6 Benötigte Daten und Speicherort

Im Geschäftsprozess „Avisierung von leeren Containern“ werden bestimmte Daten vom Entleerer zum Hersteller übermittelt, damit dieser eine Abholung planen kann. Dafür benötigt er bestimmte Daten über den Entleerer und den Container. Jeder Entleerer und Container ist dem Hersteller bekannt und wird durch einen entsprechenden Datensatz in einer Datenbank des BIS abgebildet. Identifiziert werden die Container durch die eindeutige ID auf dem RFID-Tag und die Entleerer durch einen Benutzernamen[248]. Für die Lokalisierung des Lesevorgangs per GPS wird lediglich die geographische Länge und

[246] *Wired Equivalent Privacy* ist einer der ersten Standards zur Verschlüsselung der WLAN-Funkverbindung. Aufgrund bestimmter Sicherheitsmängel ist diese Methode nicht mehr ratsam.

[247] *Wi-Fi Protected Access* ist der Nachfolger von WEP und verspricht durch längere und dynamische Schlüssel eine erhöhte Sicherheit.

[248] Damit die Benutzer eindeutig zu identifizieren sind, ist die Kundennummer des Entleerers nicht geeignet, da ein Entleerer mehrere Benutzer mit unterschiedlichen Berechtigungen oder Anwendungen haben kann.

Breite benötigt. Zusätzlich steht in den Stammdaten des Entleerers die postalische Adresse, so dass bei einer Verwendung ohne GPS eine Ortsinformation vorhanden ist. Ist diese Angabe aber zu ungenau, weil z. B. der Entleerer mehrere Standorte hat, dann bleibt noch die Möglichkeit, die Adresse manuell in den PDA einzugeben[249]. Selbstverständlich muss die wichtigste Angabe, die RFID-ID des Containers, sowie das Datum der Erfassung übermittelt werden. Optionale Felder neben der bereits erwähnten Adresse können Angaben über den Zustand des Containers oder ein Text-Feld für Bemerkungen jeglicher Art sein. Im Folgenden werden die im Prototyp übermittelten Daten zusammenfassend aufgelistet:

- Authentifikation Web-Server IIS: Benutzername und Passwort,
- Authentifikation Web-Service: Benutzername und Passwort,
- Lokalisierung: geographische Länge und Breite,
- Container-ID,
- Erfassungsdatum,
- Zustand Container OK (ja/nein),
- Bemerkungen.

Durch die Möglichkeit zur Speicherung von zusätzlichen Daten auf dem Tag selbst, stellt sich bei der Entwicklung eines RFID-Systems die Frage, wo weitere Daten über den Container gespeichert werden. Bei der Avisierung eines Containers werden keine weiteren Daten benötigt, jedoch sollte beachtet werden, dass der Container-Typ und das Füllgut für die Rekonditionierung von großer Bedeutung sind. Anhand des Füllgutes lässt sich sehr gut erkennen, warum diese Entscheidung großen Einfluss auf die verschiedensten Prozesse hat. Der Hersteller benötigt die Füllgut-Information bei der Rekonditionierung, damit er den Container dementsprechend behandeln kann.[250] Ob der Hersteller diese Information aus einer Datenbank ausliest oder ob die Information vom Tag

[249] Die Felder für die Eingabe einer Adresse sind im Prototyp nicht vorgesehen. Eine nachträgliche Implementierung ist jedoch keine problematische Erweiterung.

[250] Beispielsweise stellt die Behandlung von Containern mit Wasser oder Salzsäure als Füllgut verschiedene Anforderungen an die zu verwendenden Maschinen und Reinigungsmittel.

gelesen wird macht keinen Unterschied. Wichtiger ist die Frage nach der Verfügbarkeit der Daten für andere Parteien. Wenn die Füllgut-Information häufig gelesen werden muss, dann bietet sich eine Speicherung auf dem Tag an. Der Vorteil ist, dass keine Netzwerkverbindung zu dem Web-Service aufgebaut werden muss, der diese Information bietet. Allerdings müssen die auf dem Tag gespeicherten Daten dann entsprechend gesichert werden. Sie sollten dann nicht ohne ausreichende Berechtigung änderbar oder sogar auslesbar sein. Ein Entleerer könnte nicht wollen, dass die Füllgut-Information für andere Parteien sichtbar ist. Dies könnte der Fall sein, wenn sich sehr wertvolle oder geheime[251] Inhalte in einem Container befinden. Ein weiterer Nachteil bei der dezentralen Speicherung sind die Mehrkosten bei den Tags, damit diese überhaupt Daten speichern und ggf. verschlüsseln können.

Aus diesen Gründen wurde für den Prototyp eine Speicherung aller Daten eines Containers in der zentralen Datenbank und nicht auf dem Tag gewählt. Der dadurch entstehende Nachteil der vermehrten Kommunikation wird in Kauf genommen. Durch das vermehrt aufkommende Angebot an Flatrates[252] zur Datenübertragung über öffentliche Mobilfunk-Netze sind auch die Kosten für die Kommunikation gut kalkulierbar. Selbstverständlich wäre auch eine Speicherung von Daten auf dem Tag und in der Datenbank denkbar, was jedoch wegen der Redundanz erhöhte Anforderungen an die Daten-Verwaltung stellen würde, um die Konsistenz zu erhalten.

9.2.7 Sicherung vor unbefugtem Zugriff

Viele in Kapitel 9.2.5 genannten Schnittstellen werden mit der Hilfe von Funktechnologien überbrückt. Tendenziell sind Funkverbindungen unsicherer als Kabelverbindungen, weil die Funksignale sich nicht nur in dem Kabel ausbreiten, sondern sich gerichtet oder ungerichtet durch die Luft ausbreiten. Dies ermöglicht Angreifern, die die übertragenen Daten abhören wollen, bessere Chancen, weil sie mit Hilfe einer Antenne diese Signale einfach abfangen können. Aus diesem Grund werden in der Regel Funkverbindungen verschlüsselt,

[251] Coca-Cola benutzt für den Transport des geheimen Coca-Cola-Konzentrats (Sirup) industrielle Container oder Tankwagen [vgl. McDonald's 2004].

[252] Eine Flatrate ist ein Tarif für einen Dienst, der einen festen Preis hat und dafür keine Begrenzungen der Zeit oder des Volumens bietet.

so dass der Inhalt der übertragenen Daten durch Angreifer nicht rekonstruiert werden kann. Die Methode der Verschlüsselung ist auch bei der RFID-Luftschnittstelle eine mögliche Lösung zur Sicherung der Daten gegen das Abhören von Verbindungen (siehe Kapitel 3.2).

Aber nicht nur das Abhören von Verbindungen stellt eine potentielle Gefahr für die Daten eines Tags dar, sondern auch das unberechtigte, direkte Auslesen der ID oder der zusätzlichen Daten. Aus diesem Grund kann das Auslesen von Tags durch eine gegenseitige Authentifikation von Tag und Leser geschützt werden. Einige Ansätze für eine Authentifikation wurden in Kapitel 3.2 beschrieben. Je nach Anwendung lässt sich das Auslesen der ID oder der zusätzlichen Daten getrennt schützen. Dabei könnte der Tag die Leser-ID als Authentifikationsmerkmal überprüfen oder den Zugriff aufgrund des Ergebnisses des verwendeten Algorithmus gestatten oder verweigern.

Der Zugriff auf die Daten des Tags ist in dem Prototyp nicht geschützt. Jeder Leser darf alle Daten des Tags lesen oder schreiben. Da der Tag jedoch keine dezentralen Daten für den Prozess „Avisierung von leeren Containern“ speichern muss, können auch keine relevanten Daten ausgelesen oder gar verfälscht werden. Somit ist lediglich die ID auf den Tags eine brauchbare Information. Der Grund für die fehlende Absicherung der Luftschnittstelle ist die Tatsache, dass alle Daten des Containers in der zentralen Datenbank gespeichert werden. Die Verknüpfung zu diesen Daten ist die ID, die in jeder Abfrage des Web-Services enthalten sein muss. Des Weiteren stehen für den Prototyp nur einfache Tags zur Verfügung, die keine Funktionen zur Authentifikation und Verschlüsselung haben.

Die in der Datenbank abgelegten Daten werden selbstverständlich nicht bei allen Anfragen zurückgegeben. Nur Anfragen von berechtigten Benutzern dürfen diese Daten erhalten. Dabei kommen zwei Stufen der Authentifikation zum Einsatz. Die erste Stufe ist die Anmeldung an dem Web-Server, der den Web-Service beherbergt. Die zweite Stufe ist dann die Anmeldung an dem Web-Service (die eigentliche Anwendung), der die Berechtigungen an den einzelnen Funktionen regelt. Diese beiden Stufen ermöglichen die Ablehnung unberechtigter Benutzer schon beim ersten Zugriff auf den Web-Server und eine anschließende feingranulare Vergabe von Berechtigungen innerhalb den Anwendungen. Nur durch diese Berechtigungen wird der Zugriff auf die Daten

der Datenbank geregelt, so dass der alleinige Besitz einer ID keinen Nutzen bietet.

Schließlich bleibt noch ein weiterer, möglicher Angriffspunkt bei der Kommunikation zwischen dem mobilen Client und dem Backend: die HTTP-Verbindung. Da SOAP-Nachrichten in Klartext über HTTP versendet werden, könnte ein Angreifer diese Nachrichten abfangen und lesen. Im Prototyp wird aus diesem Grund eine HTTPS-Verbindung zwischen Client und Backend aufgebaut. HTTP-Verbindungen ohne SSL-Verschlüsselung werden vom Web-Server gar nicht erst zugelassen. SSL-Verschlüsselung gilt im Allgemeinen als eine ausreichende Sicherung von HTTP-Verbindungen, wenn ausreichend lange Schlüssel verwendet werden [Völker u. a. 2003, S. 48]. Bei dem Prototyp wird ein X.509-Zertifikat in der Version 1 mit RSA-Verschlüsselung[253] verwendet. Der Schlüssel zur Verschlüsselung ist 128 Bit lang. Der öffentliche RSA-Schlüssel ist 1024 Bit lang.

Zur Steigerung der Sicherheit wird neben der Verschlüsselung eine Server-Authentifizierung für die Verbindung benötigt. Das SSL-Zertifikat auf dem Web-Server wird durch die Client-Software auf Gültigkeit überprüft. Zur Überprüfung des Zertifikats kann der Fingerabdruck verwendet werden. Auf die Authentifikation des Clients per SSL-Zertifikat wird verzichtet, weil sich der Client am Web-Server authentifizieren muss.

Bei der Verwendung einer WLAN-Verbindung des Clients zu dem entsprechenden *Access-Point* kann ebenfalls eine Verschlüsselung eingesetzt werden. Diese Verschlüsselung (WEP, WPA) wird dann auf der Sicherungsschicht[254] (*Data Link Layer*) vorgenommen und verhindert das Abhören der Netzwerk-Pakete durch andere WLAN-Clients.

9.3 Organisatorische und wirtschaftliche Faktoren

Bei dem Einsatz des RFID-Systems ist nicht nur der Prozess „Avisierung von leeren Containern“ betroffen, sondern auch Prozesse der Produktion und der

[253] RSA ist ein asymmetrisches Verfahren für die Verschlüsselung von elektronischen Daten. Die Abkürzung RSA steht für die ersten Buchstaben der Nachnamen der Erfinder des Algorithmus: Ronald L. Rivest, Adi Shamir und Leonard Adleman.

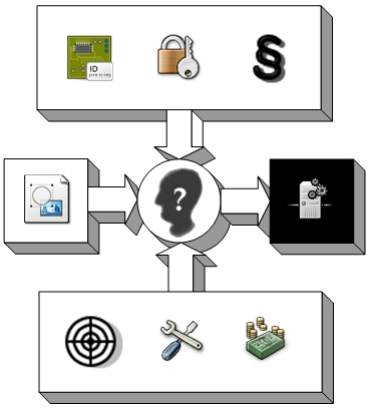
[254] Die Sicherungsschicht ist die zweite Schicht in dem OSI-Referenzmodell der ISO.

Logistik. Die in der Lieferkette beteiligten Partner müssen ebenfalls das RFID-System nutzen, damit der Prozess der Avisierung in dieser Form funktioniert. Zum einen müssen die Abfüller die für die Rekonditionierung notwendige Füllgut-Information in der Datenbank hinterlegen und zum anderen müssen die Entleerer die Avisierung in der beschrieben Form durchführen. Alle Parteien brauchen dazu eine eigene RFID-Infrastruktur, unabhängig davon, ob diese stationär oder mobil ist.

Diese anderen Prozesse sind kein Bestandteil dieser Arbeit. Jedoch müssen solche Überlegungen unbedingt bei der strategischen und operativen Planung in Betracht gezogen werden (siehe Kapitel 6.2.3). Können die beiden genannten Voraussetzungen (Füllgut-Information, RFID-Infrastruktur bei anderen Parteien) nicht erfüllt werden, dann ist die Einführung eines RFID-Systems nicht sinnvoll. In diesem Fall wird sich sicherlich auch kein wirtschaftlicher Erfolg erzielen lassen, weil die gewünschten Optimierungen in den Prozessen nicht zum Tragen kommen können. Die wirtschaftliche Unsicherheit eines solchen Systems bleibt vor der Einführung bestehen und ist nur schwer zu berechnen.

Kapitel 10

Umsetzung Prototyp



Dieses Kapitel beschreibt die Entwicklung des RFID-Prototyps und setzt damit die in den vorherigen Kapiteln erarbeiteten Anforderungen und Konzepte um. Mit diesem System ist die Avisierung von leeren Containern möglich. Eine denkbare Erweiterung für die Unterstützung von weiteren Geschäftsprozessen ist dabei beachtet worden.

Das Kapitel ist in drei Unterkapitel aufgeteilt. Zunächst wird kurz die Einrichtung der Entwicklungsumgebung Visual Studio 2005 beschrieben. Die beiden nächsten Kapitel beschäftigen sich dann mit der Entwicklung des Backends und des mobilen Clients.

Der Geschäftsprozess „Avisierung von leeren Containern“ ist ein Prozess innerhalb einer ganzen Anzahl von verschiedenen anderen. Ein Container durchläuft von der Produktion bis zu seiner Entsorgung verschiedene Zustände. Diese Zustände werden in der Abbildung 10.1 in Form eines UML-Zustandsdiagramms[255] aufgelistet. Nach der Produktion und Lagerung erfolgt die Befüllung und Entleerung. Der Rekonditionierer entscheidet dann, ob der Container weiterhin zu verwenden ist oder ob er entsorgt wird. Nach der Rekonditionierung wird ein Container wieder für die nächste Befüllung gelagert. Die Avisierung des Containers findet statt, wenn der Container den Zustand „entleert“ angenommen hat.

[255] UML ist eine Abkürzung für *Unified Modeling Language* und ist eine Modellierungssprache für die Software- und Systementwicklung. Es gibt verschiedene Diagrammarten für die Struktur und das Verhalten von Software.

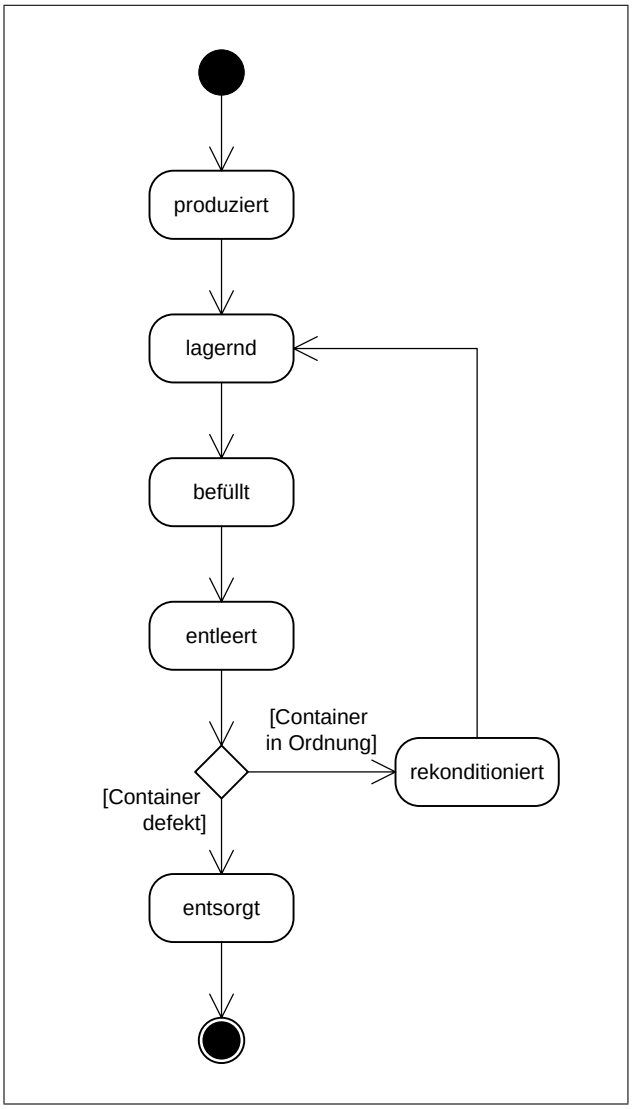


Abbildung 10.1: Zustandsdiagramm eines Containers im Kreislauf.

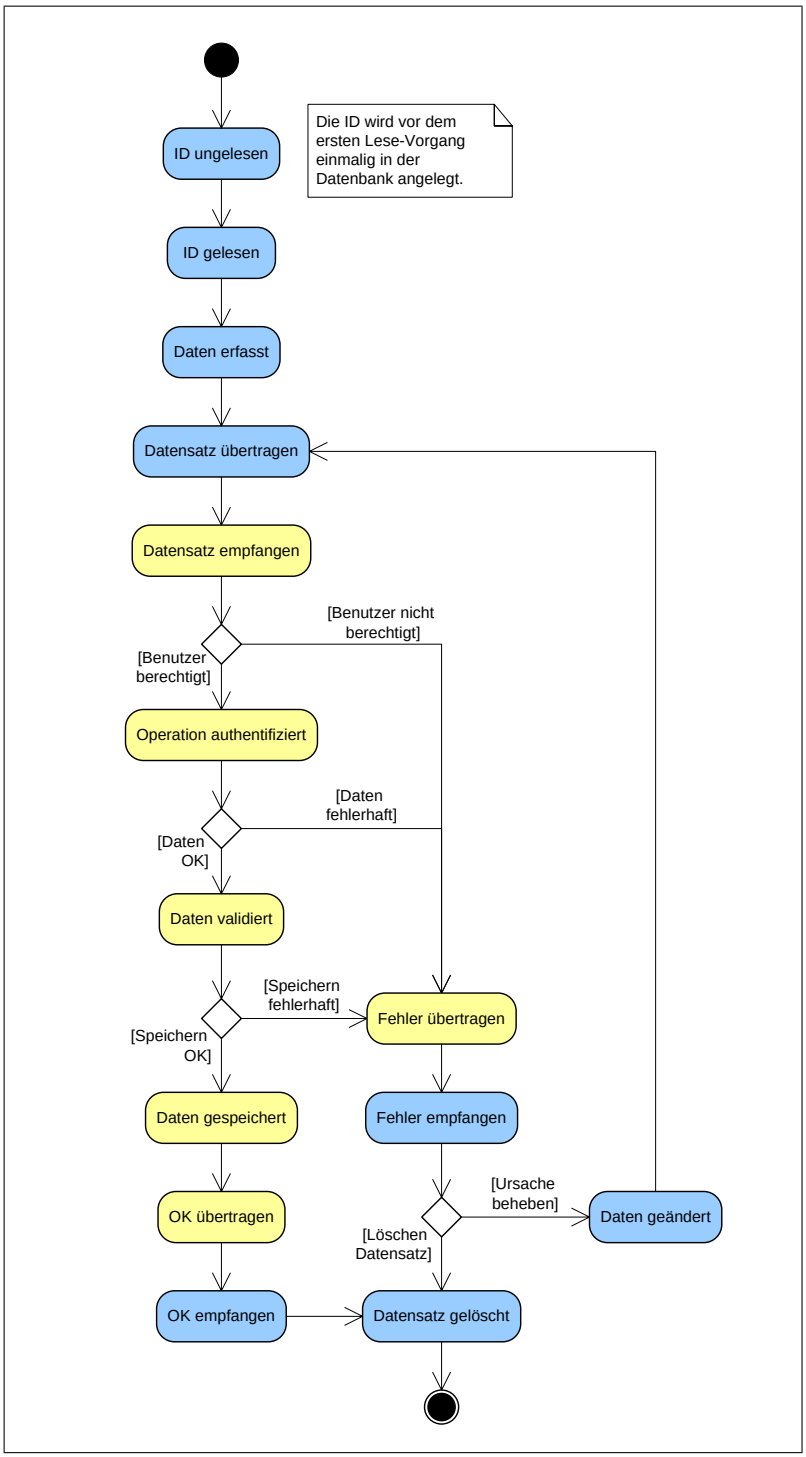


Abbildung 10.2: Zustandsdiagramm der gesamten Anwendung zur Avisierung leerer Container.

In diesem Zustand des Containers wird die entwickelte Anwendung ausgeführt. Die gesamte Anwendung besteht aus verschiedenen Schritten, die sowohl auf dem mobilen Client als auch auf dem Backend ausgeführt werden. Wie für den Container wurde ebenfalls für die Anwendung ein UML-Zustandsdiagramm (Abbildung 10.2) erstellt, welches einen Überblick über die erstellte Anwendung gibt. Die wichtigsten Pfade und Entscheidungen werden dargestellt, wobei von vielen Details des Ablaufs abstrahiert wurde. Da das Zustandsdiagramm auf verschiedenen Systemen ausgeführt wird, sind zur besseren Lesbarkeit die Zustände des mobilen Clients blau und die Zustände des Backends gelb eingefärbt. Anzumerken ist, dass die Anwendung zwischen dem Zustand „Datensatz übertragen“ und den Zuständen „OK empfangen“ und „Fehler empfangen“ blockiert ist. Während der Verarbeitung auf dem Backend wartet die Client-Anwendung auf eine Antwort und kann in dieser Zeit keine anderen Funktionen ausführen.[256] Die in dieser Abbildung nicht enthaltenen Details werden in den folgenden Kapiteln näher erläutert.

10.1 Einrichtung Entwicklungsumgebung

Die Anwendungen wurden unter dem Betriebssystem Microsoft Windows XP entwickelt und getestet. Sowohl die IDE als auch die Datenbank SQL Server laufen unter Windows XP. Im produktiven Betrieb sind jedoch die Server-Versionen von Windows die bessere Alternative, da sie für solche Zwecke speziell entwickelt wurden.[257] Selbstverständlich müssen der Web-Server und die Datenbank nicht auf einem Host laufen. Je nach bestehender Systemlandschaft ist die Trennung von Anwendungsserver (Web-Server) und Datenbank-Server gewollt und sinnvoll.

Die IDE Visual Studio 2005 beinhaltet bereits alle notwendigen Komponenten, so dass das System nach der Installation keine weiteren Software-Pakete benötigt. Eventuell können jedoch verschiedene Dokumentationen oder Werkzeuge zur effizienteren Entwicklung hinzugefügt werden. Mit Visual Studio 2005 werden die folgenden Komponenten installiert:

[256] Der Aufruf des Web-Services ist synchron und kann mit einem RPC verglichen werden. Im Gegensatz dazu ist das Senden von asynchronen Nachrichten nicht blockierend.

[257] Die Server-Versionen sind den Desktop-Versionen in verschiedenen Funktionen überlegen: Performanz, Hintergrund-Verarbeitung (*Batch*), adressierbarer Speicher, Anzahl CPUs.

- Programmiersprache Visual C#,
- Visual Web Developer (Web-Service Programmierung),
- MSXML 6.0 Parser (XML-Implementierung),
- .NET Framework 2.0,
- .NET Framework 2.0 SDK,
- .NET Compact Framework 2.0,
- SQL Server Express 2005.

Ratsam ist die zusätzliche Installation von Microsoft SQL Server Management Express [Microsoft 2006a] und der dazugehörigen SQL Server 2005 Onlinedokumentation [Microsoft 2006b]. SQL Management Express erlaubt die Verwaltung von Datenbanken und Tabellen, sowie den darin enthaltenen Daten. Somit können die durch die Anwendung in die Datenbank geschriebenen Daten manuell überprüft werden. Ebenso ist das Hinzufügen von Test-Daten in einzelne Tabellen sinnvoll, um vorgelagerte Geschäftsprozesse zu simulieren oder Fehlerfälle zu provozieren.

Nach der Installation der Onlinedokumentation startete die Anwendung SQL Management Express nicht mehr. Keine Fehlermeldung deutete auf eine Problem und damit einen möglichen Lösungsansatz hin. Auf den Support-Seiten von Microsoft ließ sich zu dem Zeitpunkt der Installation (April 2006) kein Hinweis finden. Allerdings hatten bereits andere Anwender ebenfalls dieses Problem und konnten es durch das Umbenennen oder Löschen eines *Registry*-Schlüssels[258] lösen [Erickson 2005]. Nach dem Löschen von `HKEY_LOCAL_MACHINE \Software\Microsoft\Microsoft SQL Server\90\Tools\Shell` startete dann SQL Management Express einwandfrei. Inzwischen ist eine aktuellere Version der Onlinedokumentation verfügbar, in der das Problem behoben sein könnte.

Für die Benutzung der Datenbank MySQL wird eine DLL-Datei benötigt, die in dem Treiber-Paket MySQL-Connector/NET enthalten ist. Dieser Connector muss installiert sein, damit Visual Studio 2005 die MySQL-Methoden benutzen kann. Die Dokumentation der API befindet sich unter [MySQL 2006].

[258] Die *Registry* ist eine Datenbank von Microsoft Windows, in der verschiedene Einstellungen des Betriebssystems und installierter Anwendungen abgelegt werden.

Ist die Entwicklungsumgebung vollständig eingerichtet, dann kann mit der praktischen Entwicklung begonnen werden. In den beiden nächsten Kapiteln werden das Backend und der Client entworfen und implementiert.

10.2 Backend

Aus gutem Grund wird zunächst die Implementierung des Backends erklärt. Da der Client den Dienst des Backends nutzt, kann der Client erst dann vollständig entwickelt werden, wenn die aufzurufende Methode auf dem Backend fertig gestellt ist. Ist die Methode bereits implementiert und aufrufbar, dann kann der Client entwickelt werden. Die Entwicklung von Backend und Client verlief iterativ, so dass diese vereinfachte, kausale Zweiteilung der Entwicklung in Backend und Client verwischt wird.

Das Backend besteht aus dem Web-Server, der den Web-Service anbietet und den dazugehörigen Anwendungen, die die Daten verarbeiten. Sie werden in der Datenbank abgelegt, damit nachgelagerte Anwendungen darauf zugreifen können. In Abbildung 10.3 wird der Aufbau der Schichten des Backends deutlich, wobei der mobile Client nur am oberen Rand angedeutet ist. Die einzelnen Schichten haben die Aufgaben, die Daten entgegen zu nehmen („Service“), zu filtern („Validierung“), zu verarbeiten („Verarbeitung“), zu sichern („Persistenz“) und nachgelagerte Systeme zu benachrichtigen („Ereignisbehandlung “).

Jeder Dienst hat einen entsprechenden Software-Client, der mit ihm kommunizieren kann. Hinter jedem Dienst arbeiten dann verschiedene Anwendungen, die die entsprechenden Funktionen ausführen. Durch diesen modularen Aufbau ist eine flexible Wartung und Erweiterbarkeit gewährleistet.

Aufbauend auf diese Schichten des Backends lässt sich als nächster Schritt ein UML-Klassendiagramm[259] erstellen (siehe Abbildung 10.4). Die Schichten „Service“ und „Validierung“ aus Abbildung 10.3 werden beide innerhalb der Methode `entleerung1()` der Klasse `Dienst01` implementiert. „Verarbeitung“ hingegen ist in diesem Geschäftsprozess kaum notwendig, weil das Speichern des empfangenen Datensatzes keine spezielle, rechenintensive Verarbeitung benötigt. Da lediglich Typ-Umwandlungen und Ausnahmebehandlungen dieser

[259] Ein UML-Klassendiagramm ist ein statischer Diagrammtyp und beschreibt die betroffenen Mengen von Entitäten, bzw. Objekten. Objekte haben Attribute und Methoden. Verbunden werden Klassen durch Assoziationen.

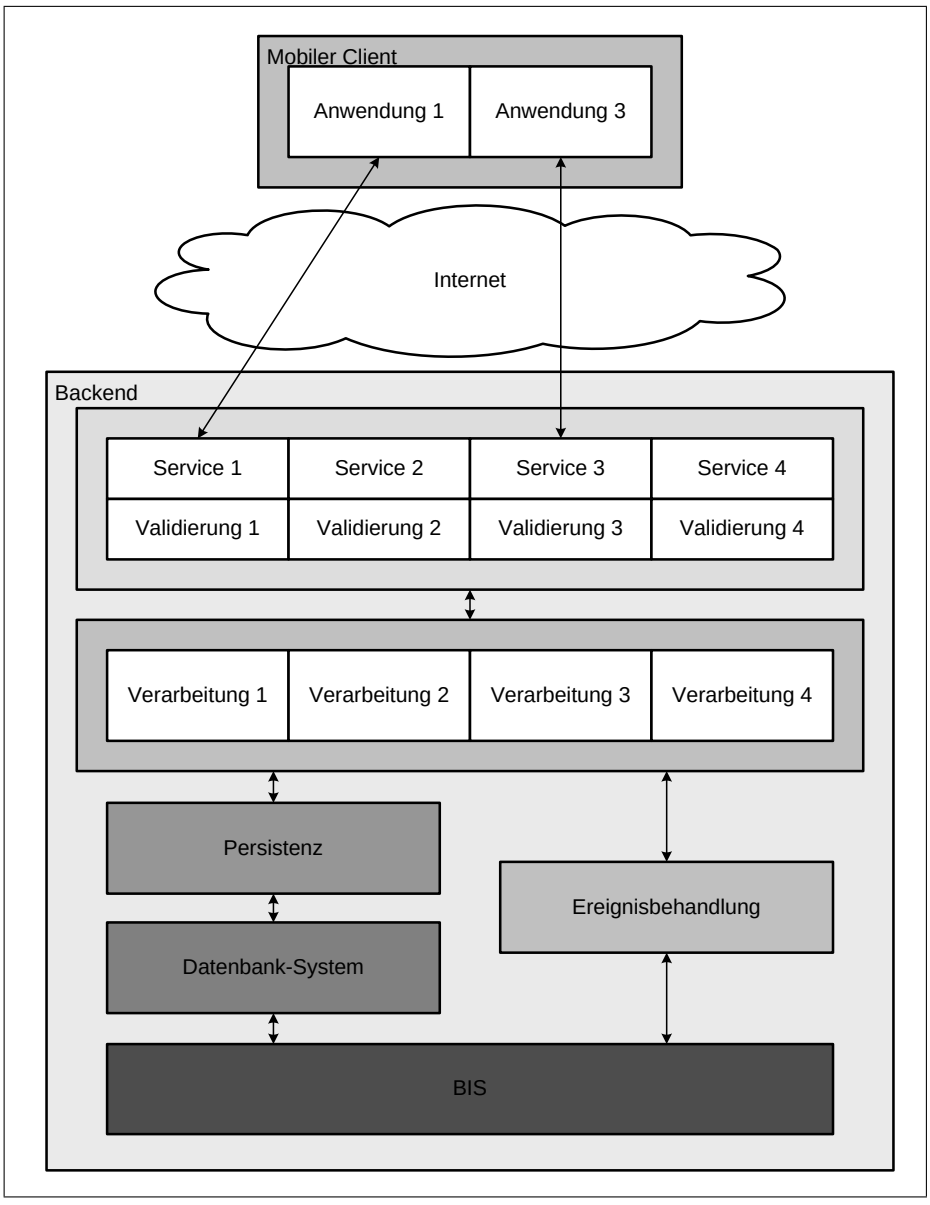


Abbildung 10.3: Schematischer Aufbau des Backends.

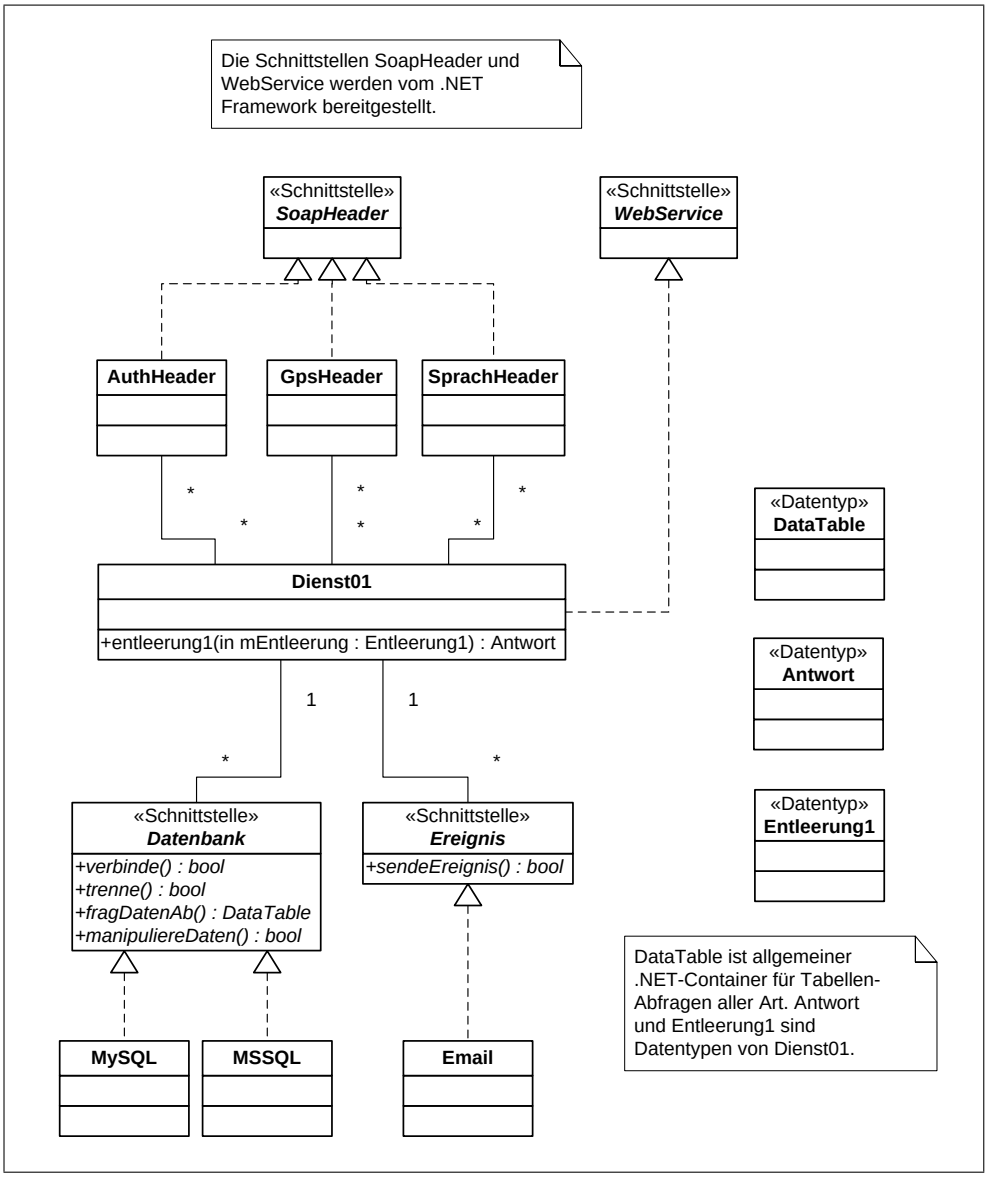


Abbildung 10.4: Klassendiagramm des Backends.

Schicht zuzuordnen sind, macht eine Auslagerung in separate Klassen aus softwaretechnischen Gründen keinen Sinn. Das Ablegen der Daten in die Datenbank („Persistenz“) wird von den implementierten Klassen der Schnittstelle `Datenbank` übernommen. Die „Ereignisbehandlung“ wird analog dazu von der Klasse `Email` der Schnittstelle `Ereignis` geleistet. Auffällig in dem Klassendiagramm ist die Implementierung von drei `SoapHeader`-Schnittstellen in den Klassen `AuthHeader`, `GpsHeader` und `SprachHeader`. Diese speziellen Klassen erweitern die SOAP-Nachrichten um weitere XML-Felder, die bei jedem Web-Service-Aufruf hinzugefügt werden. Da bei jeder Nachricht eine Authentifikation notwendig ist und immer GPS-Koordinaten übergeben werden, bedeutet die Verwendung von SOAP-Headern eine deutliche Vereinfachung für die Erstellung und das Parsen der Nachrichten. Der `SprachHeader` beinhaltet die verwendete Sprache des Clients, die für die Auswahl der Sprache von Fehlermeldungen benutzt wird (siehe auch Kapitel 10.2.2).

10.2.1 Installationen und Konfiguration

Die Installation der Datenbank für das Backend wurde bereits in Kapitel 10.1 beschrieben. Soll die Datenbank auf einem anderen Host eingesetzt werden, dann kann sie auch ohne Visual Studio 2005 installiert werden. Die Express-Version der MS SQL Datenbank kann bei Microsoft kostenlos heruntergeladen werden.

Für den Web-Server kann sowohl der IIS Version 5.1 von Windows XP als auch die Version 6.0 von Windows Server 2003 zum Einsatz kommen. Beide Versionen unterstützen die ASP.NET-Technologie[260] von Microsoft für die Ausführung von .NET-Anwendungen. Die Grundlage für ASP.NET ist das .NET Framework, welches verschiedene Sprachen unterstützt, z. B. C#. Die C#-Anwendungen werden dann in einem ASP.NET-Container ausgeführt und per Web-Service für die Clients verfügbar gemacht. Der Web-Service erhält die Anfragen von dem Web-Server, der die HTTP-Requests von dem Browser oder der Client-Anwendung empfängt. Der Aufbau des IIS und die benötigten Komponenten sind in Abbildung 10.5 schematisch zusammengefasst. Anfragen von Browsern auf statische Dateien (HTML) im Dateisystem werden vom IIS direkt durch die Rückgabe der Datei beantwortet.

[260] ASP ist die Abkürzung von *Active Server Pages* und ist eine Entwicklung von Microsoft für die Erstellung und Benutzung von serverseitigen Anwendungen.

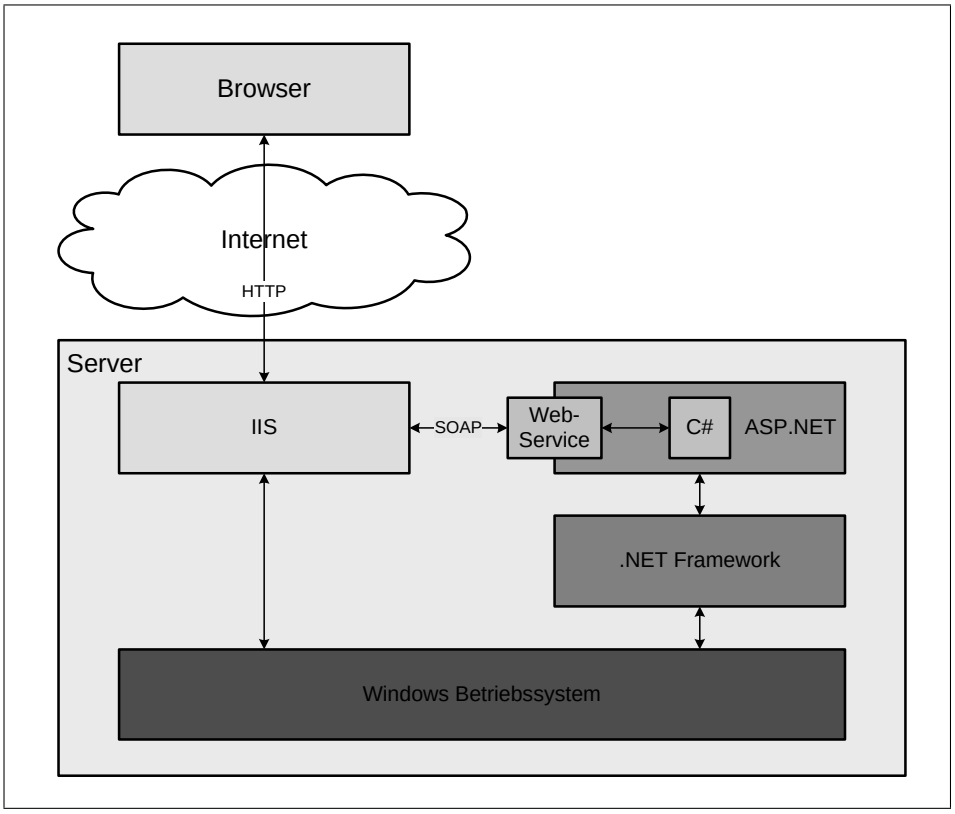


Abbildung 10.5: Aufbau der Komponenten des Microsoft Web-Servers.

Sollen auf dem Host mit dem IIS lediglich Anwendungen angeboten werden, dann reicht die Installation von .NET Framework Redistributeable, welches keine zusätzlichen Bibliotheken oder Werkzeuge für die Entwicklung, sondern lediglich die Komponenten für die Ausführung von ASP.NET-Anwendungen, beinhaltet. Des Weiteren wird die Installation der MDAC[261] in der aktuellen Version 2.7 für den Datenzugriff vorausgesetzt, welche bei Windows XP und Server 2003 bereits enthalten sind. Eine weitere, benötigte Komponente ist der MSXML 6.0 Parser für die Konvertierung der SOAP-Nachrichten.

Der Web-Server erlaubt standardmäßig auch unverschlüsselte Verbindungen über HTTP. Unser System soll jedoch keine HTTP-Verbindungen in den geschützten Verzeichnissen erlauben, sondern nur verschlüsselte HTTPS-Verbindungen zulassen. Dazu ist dem Web-Server ein globales SSL-Zertifikat hinzuzufügen (`Verwaltung IIS`, `Website`, `Einstellungen`, Reiter `Verzeichnissicherheit`, Button `Server-Zertifikat`). Die Verzeichnisse, die die Dateien der Web-Services und der Anwendungen aufnehmen, müssen ebenfalls konfiguriert werden. Bei den Verzeichnissen des Web-Servers wird dazu unter `Verzeichnis sicherheit`, `Sichere Kommunikation`, `Bearbeiten` die Option `Sicheren Kanal verlangen` aktiviert. Ab diesem Zeitpunkt werden dann für die Ressourcen in den Verzeichnissen nur HTTPS-Verbindungen zugelassen. Für die Ausführung von Anwendungen muss noch eine weitere Einstellung vorgenommen werden. Unter `Eigenschaften`, `Verzeichnis`, `Anwendungseinstellungen` muss die Option `Erstellen` gewählt werden. Bei der Verwendung von Web-Services benötigt der IIS noch eine letzte Einstellung in der Konfigurationsdatei `web.config`. Erst nach dem Hinzufügen des folgenden `protocols`-Abschnitts können Web-Services mit SOAP-Nachrichten, GET- und POST-Methoden verwendet werden:

```
<configuration>
    <system.web>
    <webServices>
        <protocols>
            <add name="HttpGet"/>
            <add name="HttpPost"/>
        </protocols>
    </webServices>
```

[261] Die *Microsoft Data Access Components* sind ein Framework für den Zugriff auf Daten in verschiedenen Datenspeichern, z. B. Datenbanken.

```
    </system.web>
</configuration>
```

Nach dem Erstellen einer ersten ASP.NET-Anwendung zum Test der Installation konnte Visual Studio 2005 die Dateien nicht in die vorbereiteten Verzeichnisse ablegen. Die Fehlermeldung

```
Visual Studio .NET hat ermittelt, dass auf dem angegebenen
   Webserver nicht ASP.NET, Version 1.1, ausgeführt wird.
   ASP.NET-Webanwendungen und -dienste können daher nicht
   ausgeführt werden.
```

wurde trotz installiertem .NET in der Version 2.0 angezeigt. Unter [Microsoft 2005b] wird die Lösung des Problems beschrieben. Der IIS verwendete eine alte .NET Version und musste erst durch eine erneute Registrierung von .NET 2.0 neu konfiguriert werden. Beim Testen einer ersten ASP.NET-Anwendung erschien dann im Browser die Fehlermeldung:

```
Die Serveranwendung ist nicht verfügbar.
```

Die Ursache war ein Berechtigungsproblem des Benutzerkontos `ASPNET`. Die Lösung wird in dem Microsoft Knowledgebase-Eintrag [Microsoft 2005a] erklärt. Die ursprüngliche Ursache für die Einstellungen und Fehler ist die Reihenfolge der Installation der Komponenten. Auf dem Test-System wurde der IIS 5.1 erst nach Visual Studio .NET installiert. Der IIS verwendet dann nicht die aktuellste .NET Version, sondern die Version 1.1. Durch die Installation des IIS vor Visual Studio 2005 oder vor dem .NET 2.0 Framework werden diese Fehler vermieden.

Aber auch bei der Benutzung der MS SQL Server Datenbank kann es zu Problemen bei der Anmeldung kommen. Standardmäßig ist die Datenbank auf `Windows Authentication Mode (Windows Authentication)` eingestellt. In diesem Modus versucht sie die Kombination aus Benutzername und Passwort mit den Windows-Benutzerkonten zu vergleichen. Sind die Benutzer jedoch in der datenbankeigenen Benutzerverwaltung selbst angelegt, dann erhält man die Fehlermeldung

```
Anmeldung schlug für Benutzer 'Benutzername' fehl. Der
   Benutzer ist einer vertrauenswürdigen SQL Server-
   Verbindung nicht zugeordnet. (Microsoft SQL Server,
   Fehler: 18452).
```

Zur Lösung stellt man den Modus auf den `Mixed Mode (Windows Authentication and SQL Server Authentication)`, so dass die Authentifikation auch gegen den SQL Server erfolgt [Microsoft 2005c]. Der Zugriff über das Netzwerk auf die Datenbank muss erst explizit freigegeben werden. In der `Netzwerk-Konfiguration` des `SQL Server Configuration Managers` müssen die Einträge `Named Pipes` und `TCP/IP` mit der rechten Maustaste aktiviert werden. Zur Sicherheit sollte unter den Einstellungen von `TCP/IP` der Port 1433 kontrolliert werden.

10.2.2 Beschreibung des Dienstes und der Anwendung

Die Anwendung auf dem Server hat die Aufgabe, die empfangenen Daten zu überprüfen und anschließend in der Datenbank abzulegen. Allerdings sind insgesamt etliche weitere Schritte notwendig, damit die Anwendung robust und fehlerfrei funktioniert. In Abbildung 10.6 wird das Flussdiagramm[262] des Backends dargestellt. Aus Gründen der Übersicht sind nicht alle Pfade und alle Entscheidungen in der Abbildung enthalten.

Die Authentifikation am Web-Server ist nicht in dem Diagramm enthalten, weil sie kein Bestandteil der .NET-Anwendung ist. Bei dem IIS geschieht dies durch die Standard- oder Windows-Authentifizierung; bei anderen Web-Servern kann dies auch durch Konfigurationsdateien in den geschützten Verzeichnissen realisiert werden (`.htaccess` bei Apache HTTPD).

Die zweite Authentifizierung geschieht an dem Web-Service selbst. Durch die Übergabe von Benutzername und Passwort in dem `SoapHeader` kann die Anwendung prüfen, ob der Request zur Ausführung berechtigt ist. Die Benutzerdaten können bei der Übertragung nicht ausgelesen werden, weil die SOAP-Nachricht mit SSL verschlüsselt ist. Der aufrufende Benutzer wird durch den Benutzernamen eindeutig identifiziert. Ist der Benutzer angelegt und das Passwort korrekt, dann wird geprüft, ob der Benutzer zu einer Benutzergruppe gehört, die an der Anwendung berechtigt ist. Sind diese Überprüfungen positiv ausgefallen, so werden die übertragenen Inhalte auf Gültigkeit überprüft. Diese Überprüfungen hängen natürlich von dem realisierten Geschäftsprozess und den organisatorischen Richtlinien ab. Anschließend wird die Speicherung der Daten in der Datenbank vorbereitet. Der Datensatz kann nur hinzugefügt

[262] Ein Flussdiagramm (PAP, Programmablaufplan) ist ein Diagramm für die Beschreibung des Verhaltens einer Anwendung. Die verwendeten Symbole sind in der DIN 66001 definiert.

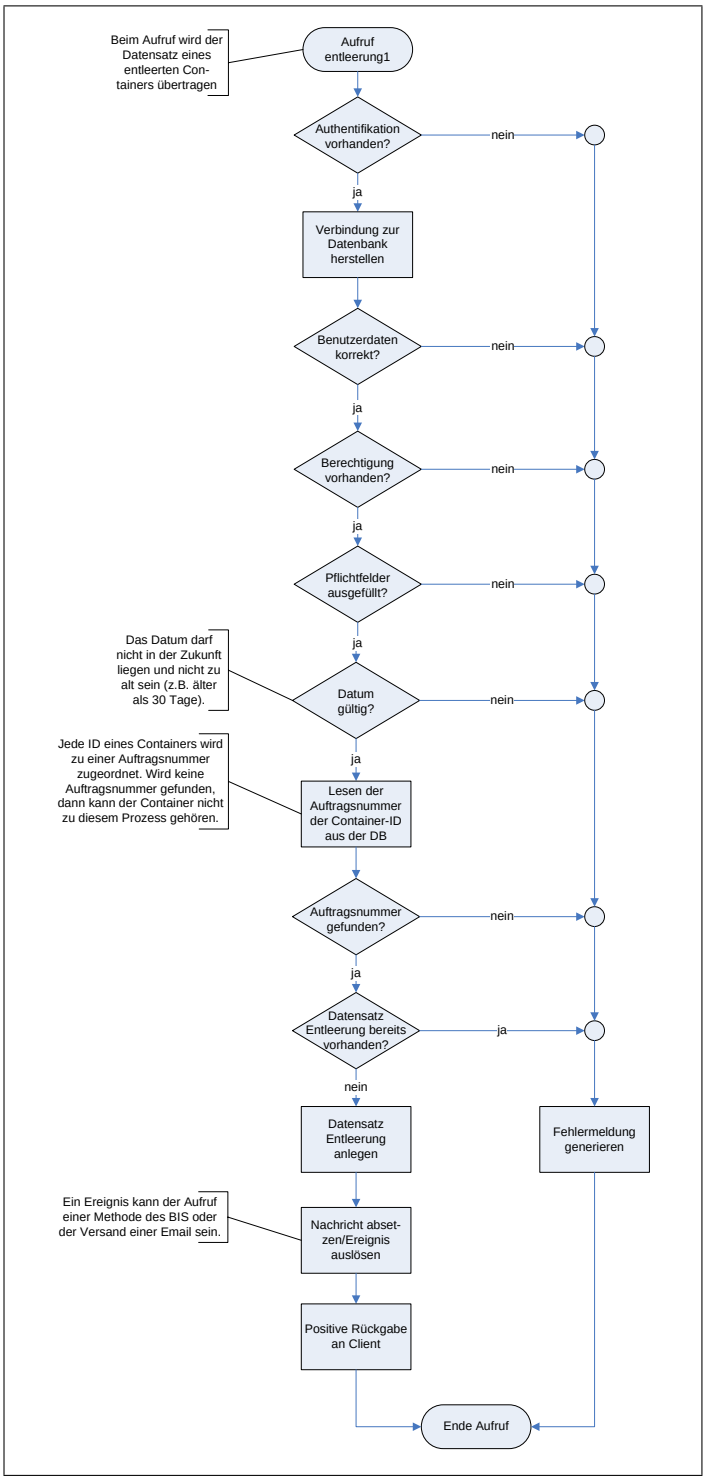


Abbildung 10.6: Flussdiagramm des Backends.

werden, falls ein Stamm-Datensatz zu dem Container existiert. Dabei kann es aufgrund der mehrfachen Verwendung von Containern vorkommen, dass eine Container-ID mit mehreren Aufträgen verknüpft ist. Ein Auftrag ist gleich zu setzen mit einer Umrundung des Kreislaufs aus Abbildung 10.1. Ist dem Container eine aktuelle Auftragsnummer zugewiesen, dann kann der Container auch zur Entleerung angemeldet werden, ansonsten wird der Datensatz abgewiesen. Ist bereits eine Meldung zur Entleerung vorhanden, dann wird diese nicht überschrieben, damit keine Daten verloren gehen können. Wird eine Aktualisierung von vorhandenen Daten gewünscht, dann bietet sich ein zweiter Web-Service für diese Aufgabe an.

Die aufgerufenen Methoden des Web-Service haben Bezeichner, die einem bestimmten Aufbau folgen: Nach einem beschreibenden Substantiv folgt eine oder mehrere Ziffern. Das Substantiv ist für Methoden eines Dienstes gleicher Aufgabe identisch. Die Ziffern beschreiben die Version der Methode. So ist eine Unterscheidung zwischen verschiedenen Versionen von Methoden möglich. Eine Alternative wäre ein zusätzliches Versionsfeld innerhalb des Datensatzes selbst[263], jedoch lässt sich dadurch der Aufbau des Web-Service deutlicher gliedern, da schon beim Aufruf die Version erkannt werden kann und nicht erst nach der Inspektion des übergebenen Datensatzes. Außerdem verursacht das Versionsfeld unnötigen – zugegeben wenigen – Datenverkehr. Die Wartung der Methoden ist einfacher als bei der Verwendung des Versionsfeldes, da die Fehlersuche und -behebung in vielen einzelnen Methoden schneller erfolgen kann als in wenigen großen. Durch die Verteilung der Funktionen auf mehrere Methoden steigt der Grad der Wiederverwendbarkeit (Möglichkeit der Generalisierung und Spezialisierung).

Die Übertragung eines Datensatzes erfolgt durch Parameterübergabe einer Datenstruktur (`struct`) von dem Client an die ausführende Methode des Backends. Die `structs` werden auf dem Backend angelegt und haben die Sichtbarkeit `public`, so dass sie auch von der mobilen Anwendung nutzbar sind.[264] Die Datenstrukturen könnten auch als Klassen implementiert werden, jedoch benötigen sie weder selbst Methoden noch Generalisierung oder Spezialisierung

[263] In vielen Netzwerk-Protokollen wird das Versionsfeld in jedem Paket übertragen, siehe das Internet-Protokoll (IP).

[264] Die mobile Anwendung kann neben den Methoden auch auf die öffentlichen Datenstrukturen und Klassen zugreifen. Der Web-Service ist somit nicht nur mit einem RPC vergleichbar, sondern eher mit einer Klasse im Web.

zwischen den verschiedenen Datenstrukturen. Deswegen reichen `structs` als Datenstruktur vollkommen aus. Somit kann jeder Methode genau ein `struct` zugeordnet werden, was zu einer klaren und übersichtlichen Struktur führt.

Wird in der Zukunft der Web-Service um einen Dienst erweitert, dann genügt das Hinzufügen einer neuen Methode und dem dazugehörigen `struct`. Durch diesen Aufbau der Schnittstelle des Web-Services und der Datenstrukturen wird Flexibilität erreicht, die Wartbarkeit vereinfacht und eine mögliche Abwärtskompatibilität gesichert.

Der Rückgabewert von Methoden ist häufig ähnlich, so dass eine allgemeine Struktur gewählt werden kann. Dieser allgemeine `struct` besteht aus den Attributen Rückgabe-Code, Fehlertext, Rückgabe-Array[265]. Bei erfolgreicher Ausführung wird der Rückgabe-Code 0 zurückgegeben. Jeder andere Wert bedeutet eine fehlerhafte Verarbeitung, die dann im Fehlertext näher beschrieben wird. Das Rückgabe-Array kann benutzerdefinierte Daten enthalten, die je nach Methode und Fehler von dem Programm-Entwickler wählbar sind.

Die Anwendung implementiert die zwei globalen Schnittstellen (*Interfaces*) `Datenbank` und `Ereignis`. Die Klassen `MSSQL` und `MySQL` implementieren die Schnittstelle `Datenbank` und ermöglichen den Zugriff auf die gleichnamigen Datenbanken. Implementiert werden die wichtigen Methoden für den Verbindungsaufbau zur Datenbank, die Durchführung von Abfragen und Manipulationen auf den Daten, sowie die Trennung der Verbindung. Die Klasse `Email` implementiert die Schnittstelle `Ereignis` und ist für das Pushen von empfangenen Nachrichten zuständig. Hier kann eine weitere Klasse für eventuelle, weitere Arten von Benachrichtigungen implementiert werden.

Die Verwendung von Schnittstellen für diese beiden Aufgaben ist nicht nur aus softwaretechnischen Gründen sinnvoll, sondern auch aus praktischen. Objekte können von implementierten Klassen der Schnittstellen `Datenbank` oder `Ereignis` erstellt werden. Abhängig von den vom Betreiber gewählten Einstellungen kann zur Laufzeit entschieden werden, von welcher implementierten Klasse das Objekt instanziert wird. Da die Schnittstellen der implementierten Klassen identisch sind – aufgrund der gemeinsamen Oberklasse – ist für die Anwendung die Benutzung der Klassen transparent. Für den Entwickler bedeutet

[265] Mit *Array* wird in einer Programmiersprache typischerweise ein Feld aus Werten eines Datentyps bezeichnet. Häufig ist das *Array* zweidimensional und dient als Datenspeicher für verschiedenste Matrizen oder Tabellen.

dies, dass er die verwendete Konfiguration nicht kennen und beachten muss. Er kann von den verwendeten Klassen in der Anwendung abstrahieren.[266]

Bei der Entwicklung der `Email`-Klasse ist zu beachten, dass ab der Version 2.0 von .NET neue Namensräume (*Namespaces*) existieren, die die Klassen für die E-Mail-Versendung enthalten. Noch in .NET Version 1.1 waren dafür Klassen aus `System.Web.Mail` zuständig. Ab Version 2.0 sind diese (leicht modifizierten) Klassen in `System.Net.Mail` zu finden. Für die eigentliche Versendung sind nur wenige Zeilen Code notwendig:

```
1 System.Net.Mail.MailMessage message = new System.Net.Mail.
    MailMessage(sender, receiver, subject, body);
2 message.BodyEncoding = System.Text.Encoding.UTF8;
3 System.Net.Mail.SmtpClient client = new System.Net.Mail.
    SmtpClient(server, port);
4 client.Credentials = new System.Net.NetworkCredential(user,
     password);
```

Die grau gedruckten Parameter in den Methoden müssen vom Benutzer definiert werden. In der ersten Code-Zeile wird ein neues `Email`-Objekt angelegt. Die übergebenen Parameter sind die typischen, notwendigen Elemente einer E-Mail: Absender, Empfänger, Betreff und Body[267]. Anschließend wird die Kodierung für diese E-Mail festgelegt. Ausgewählt wird die Codepage UTF-8 (Unicode), weil sonst die Standard-Kodierung ASCII (7 Bit) verwendet wird. Dies könnte zu Problemen bei der Kodierung von Sonderzeichen oder Umlauten führen. In der dritten Zeile wird der zu verwendende Mail-Server und Port für ausgehende E-Mails[268] angegeben. Schließlich wird in Zeile vier die Authentifizierung an dem Server für den Versand der E-Mail übergeben. Die meisten SMTP-Server verlangen heute von den Absendern eine Authentifikation, um den anonymen Versand zu verhindern und somit *Spam* einzudämmen.[269] An-

[266] Schnittstellen, Vererbung und Abstraktion sind bekannte und hilfreiche Motive der objektorientierten Programmierung und damit keine Errungenschaften dieser Arbeit. Diese Motive werden lediglich effektiv und vorteilhaft angewendet.

[267] Der Begriff „Body“ lässt sich nur schwer sinnvoll in die deutsche Sprache übersetzen. Meist wird die englische Bezeichnung auch im Deutschen benutzt. Allerdings sind auch manchmal die deutschen Begriffen Inhalt, Hauptteil oder Text anzutreffen.

[268] Das Protokoll für das Versenden von E-Mails ist SMTP (*Simple Mail Transfer Protocol*). Dieses Protokoll war eines der ersten Internet-Protokolle und wird heute bis auf einige Modifikationen (ESMTP, *Extended SMTP*) unverändert benutzt. SMTP wird im RFC 821 und ESMTP im RFC 1869 der IETF spezifiziert.

[269] Verlangt ein SMTP-Server im Internet keine Authentifizierung, dann spricht man von einem *Open Relay*.

zumerken bleibt, dass .NET bei der Wahl von UTF-8 als Zeichen-Kodierung automatisch die Kodierung `Base64` für die Übertragung (*TransferEncoding*) einstellt.

Da der Einsatz von mobilem Client und Backend nicht notwendigerweise in einem Land stattfinden muss, wurde in dem Prototyp eine Variable eingeführt, die bei jedem Aufruf des Web-Service übergeben wird. Diese Variable ist das Länderkennzeichen, das für den mobilen Client gilt. Gültige Länderkennzeichen sind `de-DE`, `en-GB` und `en-US`. Es gibt zwei Gründe für die Einführung dieser Variablen. Ein in .NET-Anwendungen angezeigtes Datum wird standardmäßig in dem Datumsformat angezeigt, das von dem zu Grunde liegenden Betriebssystem vorgeschlagen wird. Durch diese Variable kann nun innerhalb der Anwendung unabhängig von der Sprachversion des Betriebssystems entschieden werden, in welchem Format das Datum angezeigt werden soll. Manche Formatierungen des Datums könnten Benutzer verwirren: Das amerikanische Datum hat das Format `MM/TT/JJJJ`[270]. Das deutsche Datum wird laut DIN 5008 im Format `JJJJ-MM-TT` angegeben: Häufiger anzutreffen ist jedoch das ebenfalls gültige Format `TT.MM.JJJJ`. Um diesem Problem vorzubeugen, wird das Format verwendet, das in der konfigurierbaren Einstellung der Anwendung hinterlegt ist. Der zweite Grund hat ebenfalls mit der Darstellung zu tun. Die zurückgegebenen Fehlermeldungen an den mobilen Client können in der korrekten Sprache verfasst werden, so dass der Benutzer diese auch verstehen kann.

In Verbindung mit dem Datum tritt jedoch noch ein zusätzliches Problem auf. Wenn sich Clients in verschiedenen Zeitzonen befinden, dann kann es zu Fehlern bei der Interpretation des Datums und der Uhrzeit kommen. Aus diesem Grund werden alle übertragenen Daten und Uhrzeiten in das UTC-Format[271] umgewandelt. Dadurch werden Verschiebungen durch die Verwendung der lokalen Uhrzeit in anderen Zeitzonen vermieden, sofern in den Einstellungen des Betriebssystems die Zeitzone korrekt gepflegt wird. Auf dem Backend kann dann entweder die UTC-Zeit verwendet und in der Datenbank abgelegt oder die empfangene Zeit in die lokale Zeit umgewandelt werden. In

[270] `M` ist die Abkürzung für Monat, `T` für Tag und `J` für Jahr.

[271] UTC steht für die koordinierte Weltzeit. UTC ist keine Abkürzung, die für ein Begriff steht der mit den Anfangsbuchstaben U, T und C beginnt. UTC wird als Referenzzeit für verschiedene Bereiche benutzt, z. B. für die Luftfahrt, den Funk oder das Internet.

dem Prototyp wird aus Gründen der besseren Testbarkeit die Uhrzeit in die lokale Zeit umgewandelt.

Nach der Erstellung oder nach Änderungen des Web-Service muss die in der IDE aktualisierte Version auf dem Web-Server veröffentlicht werden. Dies ist bei Visual Studio 2005 elegant gelöst. Im `Solution Explorer` kann mit der rechten Maustaste auf die *Solution*[272] der Punkt `Publish Web Site` auswählt werden. In dem folgenden Dialog muss dann der Pfad zu dem Verzeichnis des Web-Service angegeben werden. Dies kann entweder ein lokaler Pfad, falls der Web-Server auf dem gleichen Host installiert ist, oder eine URL zu dem Verzeichnis auf dem Web-Server sein. Nach Bestätigung wird mit der Veröffentlichung begonnen. Die *Solution* wird kompiliert und – sofern keine syntaktischen Fehler entdeckt werden – erscheint die Frage, ob die ggf. bereits vorhandenen Dateien in dem Verzeichnis überschrieben werden sollen. Anschließend werden die Dateien aktualisiert und die Veröffentlichung wird mit einem Hinweis in der Statuszeile abgeschlossen. Unter dem angegebenen Pfad sind dann Dateien mit den folgenden Endungen zu finden: `asmx` (Web-Service in .NET), `dll` (*Dynamic Link Library* mit den C#-Klassen) und `config` (Konfiguration des Web-Service).

10.2.3 Datenbank-Schema

Neben den funktionalen Komponenten spielt die zu Grunde liegende Datenstruktur eine wichtige Rolle. Die Datenbank ist der Datenspeicher des Systems und deswegen von hoher Bedeutung. Die Entwicklung des Datenbank-Schemas ist vor der Entwicklung der Anwendung zu treffen, da die Anwendung auf die Struktur der Daten zugreifen muss. Der Geschäftsprozess „Avisierung von leeren Containern“ wurde bereits in den vorherigen Kapiteln beschrieben (siehe Kapitel 8). Nach der Erfassung der Anforderungen und dem schematischen Aufbau des Systems wurden in Kapitel 9.2.6 die zu übertragenden Daten identifiziert. Aus diesen Informationen lässt sich dann ein Datenmodell erstellen und in ein Datenbank-Schema (siehe Abbildung 10.7) überführen. Dieses Schema ist nur für den entwickelten Prototyp gültig. In einem Unternehmen mit

[272] Eine *Solution* ist der Begriff für ein Projekt in Visual Studio 2005. In aller Regel wird aus einer *Solution* eine Anwendung erstellt.

bestehenden Datenbanken und Strukturen könnte eine Daten-Integration anders aussehen. Da jedoch für diese Arbeit keine bestehende Struktur vorliegt, wurde eine neue für diese Arbeit entwickelt.

Die Tabellen der Datenbank lassen sich grob in drei Kategorien einteilen. Die erste Kategorie besteht aus den Stammdaten der verkauften Artikel, also den Containern. Jeder Container hat einen Stamm-Datensatz in der Datenbank `Container`, der die eindeutige Container-ID und die entsprechenden, zusätzlichen Informationen enthält. Für jedem Kreislauf, den der Container durchläuft, wird ein neuer Datensatz in der Tabelle `Produktion` angelegt. Der Primärschlüssel dieser Tabelle ist ein kombinierter Primärschlüssel aus den Attributen `id` und `auftragsnummer`. Die Auftragsnummer wird von einer Anwendung des Vertriebs vergeben und dem Container zugeteilt. Auf diese Vertriebsanwendung wird nicht weiter eingegangen, weil sie kein Bestandteil dieser Arbeit ist. Nach der Produktion und nach jeder Rekonditionierung wird ein neuer Datensatz angelegt. Auf diese Weise wird nicht nur die aktuelle Zuordnung von ID zu Auftragsnummer festgehalten, sondern auch die Historie eines Containers mit seiner ID.

Die zweite Kategorie der Tabellen sind die Bewegungsdaten der Container. Für den Prototyp reicht lediglich eine Tabelle in dieser Kategorie aus. Die Tabelle `Entleerung1` speichert die Daten, die von dem Web-Service und der Methode `entleerung1()` empfangen werden. Neben den benötigten Informationen über den Sender (`benutzername`) und das Erfassungsdatum sind die Felder `inspektion`, `bemerkung`, `gpsbreite` und `gpslaenge` als optionale Informationen vorhanden.

In die dritte Kategorie fallen die Tabellen für die Benutzerverwaltung und Berechtigungen. Jeder Benutzer gehört zu einer Firma, die eine Adresse hat. Da eine Firma mehrere Benutzer mit verschiedenen Berechtigungen haben kann, sind diese Entitäten in verschiedenen Tabellen untergebracht. Jeder Benutzer gehört zu einer Gruppe. Diese Gruppe hat dann bestimmte Berechtigungen, die in der Tabelle `Gruppenberechtigung` zusammengefasst werden. Dort werden die erlaubten Operationen an bestimmten Tabellen festgehalten. Die Tabelle `Berechtigung` enthält die Definitionen für die jeweiligen Berechtigungen. Möglich ist hier das Hinzufügen von zusätzlichen Attributen, wie in diesem Fall `Bemerkung`. Das Feld `operation` enthält die Werte `R` oder `W`, die für lesenden oder schreibenden Zugriff stehen. Diese Zugriffe können dann direkt

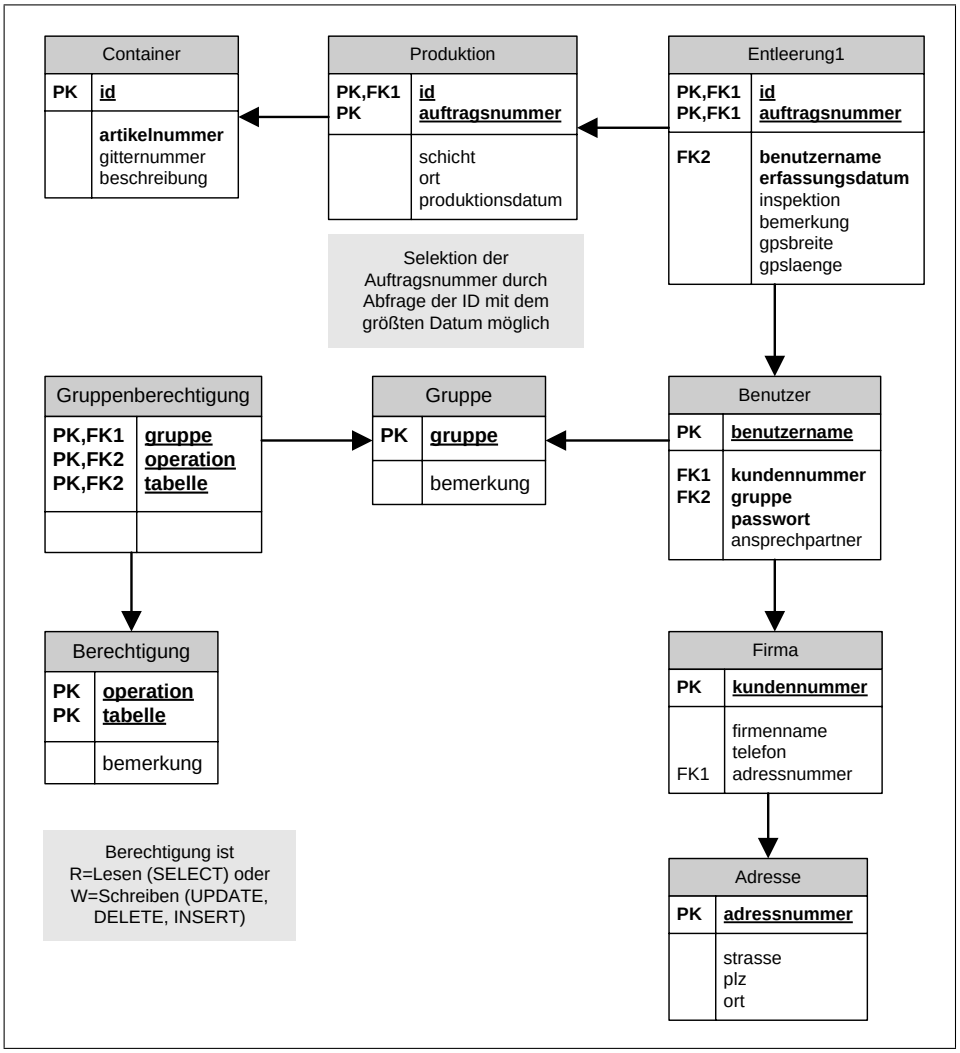


Abbildung 10.7: Datenbank-Schema des Backends.

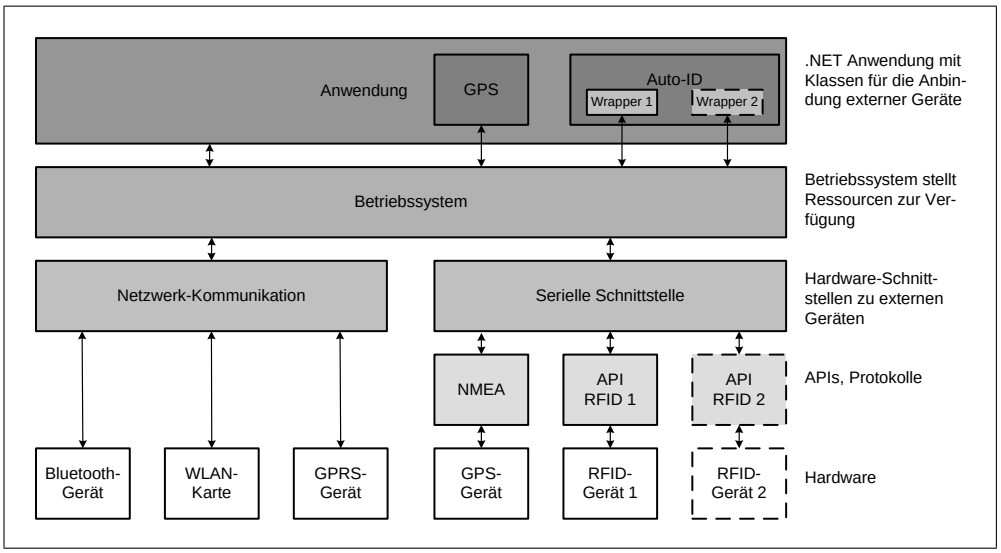


Abbildung 10.8: Schematischer Aufbau des mobilen Clients.

auf SQL-Anweisungen übertragen werden. Lesen bedeutet die Berechtigung für `SELECT`-Abfragen und Schreiben erlaubt die Anweisungen `UPDATE`, `DELETE` und `INSERT`.

In diesem Datenbank-Schema ist lediglich eine Tabelle mit Bewegungsdaten enthalten. Diese Daten sind die empfangenen Informationen nach der Entleerung eines Containers. In der Abbildung 10.1 ist erkennbar, dass der Container nicht nur den Zustand „entleert“ haben kann. Für eine vollständige Menge an Tabellen von Bewegungsdaten sind deswegen weitere Tabellen notwendig, die z. B. `Befuellung1`, `Rekonditionierung1` und `Transport1` heißen könnten. Diese Tabellen hätten ebenfalls den kombinierten Primärschlüssel aus den Attributen `id` und `auftragsnummer` sowie weiterer, benötigter Attribute.

10.3 Client

Der Client ist ein mobiles Gerät (PDA) mit entsprechender Zusatz-Hardware (RFID, GPS) und der notwendigen Client-Anwendung zur Kommunikation mit dem Backend. Ein schematischer Aufbau des Clients zeigt Abbildung 10.8.

Die .NET-Anwendung enthält verschiedene Klassen für die Anbindung der Hardware. Dabei müssen die in der Abbildung ganz unten aufgeführten Geräte

nutzbar gemacht werden. Innerhalb der Auto-ID-Schnittstelle können verschiedene Implementierungen („Wrapper“) für die RFID-Geräte entwickelt werden. Die Klasse `Wrapper 2` ist mit einer gestrichelten Linie versehen, weil diese Klasse im nicht Prototyp implementiert ist. Die Einbindung dieser zweiten Klasse ist jedoch durchaus machbar. Das Betriebssystem stellt den Anwendungen verschiedene Schnittstellen zur Verfügung. An diesen Schnittstellen können Geräte betrieben werden, die mit Hilfe der passenden Treiber nutzbar gemacht werden. Der Datenaustausch zwischen Anwendung und Gerät erfolgt dann über die mitgelieferten, spezifischen APIs und Protokolle. Das zu der Klasse `Wrapper 2` gehörende `RFID-Gerät 2` ist ebenfalls nicht im Prototyp enthalten und deswegen mit gestrichelter Linie versehen.

10.3.1 Einrichtung PDA

Für die Anbindung des PDA an den Rechner liefert HP – ähnlich wie andere Hersteller – eine *Docking-Station*[273] mit dem Gerät. Für die Kommunikationsverbindung zu dem PDA wird dann noch die Microsoft-Software ActiveSync benötigt. Die Software liegt entweder dem PDA bei oder kann von dem Microsoft Download-Bereich heruntergeladen werden. Bei diesem Prototyp wurde die aktuellste Version 4.1 verwendet. Nach dem Einsetzen des PDA in die Docking-Station wird das Gerät automatisch erkannt und in das System eingebunden.

Für die Benutzung der Anwendung muss auf dem PDA ebenso wie auf dem Web-Server das .NET-Framework installiert werden. Für das Betriebssystem Pocket PC 2003 kann jedoch nicht das gleiche .NET-Framework installiert werden. Für Pocket PC wird das .NET Compact Framework 2.0 benötigt, welches mit der IDE Microsoft Visual Studio 2005 geliefert wird oder im Internet kostenlos von dem Microsoft Download-Bereich heruntergeladen werden kann. Das Framework wird auf dem PC installiert und kann dann von dort auf die mobilen Geräte (z. B. PDA) verteilt werden. Bei dem ersten Einsetzen des PDA in die *Docking-Station* nach der Installation des .NET Compact Framework 2.0 erkennt ActiveSync, dass noch kein Framework auf dem PDA

[273] Eine *Docking-Station* ist ein Ständer für einen PDA, der gleichzeitig eine Schnittstelle zu dem mobilen Gerät und einen Anschluss an einen Rechner (USB) hat. Teilweise wird auch der Bezeichner *Cradle* verwendet.

installiert ist und schlägt die Installation vor. Alternativ kann die Installation für Pocket PC 2003 durch das Aufrufen der Datei `NETCFv2.ppc.armv4.cab` aus dem Verzeichnis `<Installationspfad .NET Compact Framework>\WindowsCE \wce400\armv4\` angestoßen werden. Ist das Framework installiert und sind alle notwendigen Schnittstellen nutzbar (seriell, Bluetooth, WLAN, siehe Kapitel 10.3.6), dann ist der PDA ausreichend vorbereitet.

10.3.2 Anwendungsmodellierung

Analog zu der Vorgehensweise beim Backend wurde zunächst ein UML-Klassendiagramm entwickelt, welches als Grundlage für die Entwicklung der Client-Anwendung diente (siehe Abbildung 10.9). Die vier wichtigsten Klassen werden von der .NET-Schnittstelle `Form` abgeleitet. Sie repräsentieren die vier Fenster der Anwendung, die die GUI für den Anwender sind. Die Klasse `FrmHaupt` enthält dabei die meisten Funktionen, weil sie die zentrale Klasse ist, von der alle anderen Instanzen gestartet werden. Die Klasse `Program` wird bei der Anlage einer neuen *Solution* von Visual Studio 2005 automatisch generiert. Sie instanziert lediglich eine von `Form` abgeleitete Klasse und hat sonst keine weiteren Aufgaben. Die Methode `addiereEntleere1()` der Klasse `FrmHaupt` sorgt für das Hinzufügen neuer, zu sendender Datensätze zu den internen Datenstrukturen.

Die Klasse `XMLEinstellungen` sorgt für die Verwaltung der Anwendungseinstellungen. Diese Einstellungen sind die Stammdaten für den Zugang zum Web-Service, die Proxy-Konfiguration sowie den Hardware-Einstellungen für RFID und GPS. Beim Start wird die Datei `config.xml` mit den entsprechenden Werten ausgelesen. Bei Veränderungen wird diese Datei aktualisiert, so dass die Werte dauerhaft gespeichert werden.

Die Schnittstelle `IRFIDLeser` bietet den Rahmen für die Anbindung und Benutzung von RFID-Hardware. Die Klasse `ACGHandheldLeser` implementiert diese Schnittstelle und bindet die gleichnamige CF-Karte über die spezifische API ein. Diese Einbindung wird in Kapitel 10.3.6 genau beschrieben. GPS-Empfänger hingegen benötigen im Allgemeinen keine eigene API, so dass nur eine Klasse `GPS` für die Nutzung vieler verschiedener GPS-Geräte implementiert wird. Auch auf die GPS-Anbindung wird im Verlauf dieses Kapitel eingegangen.

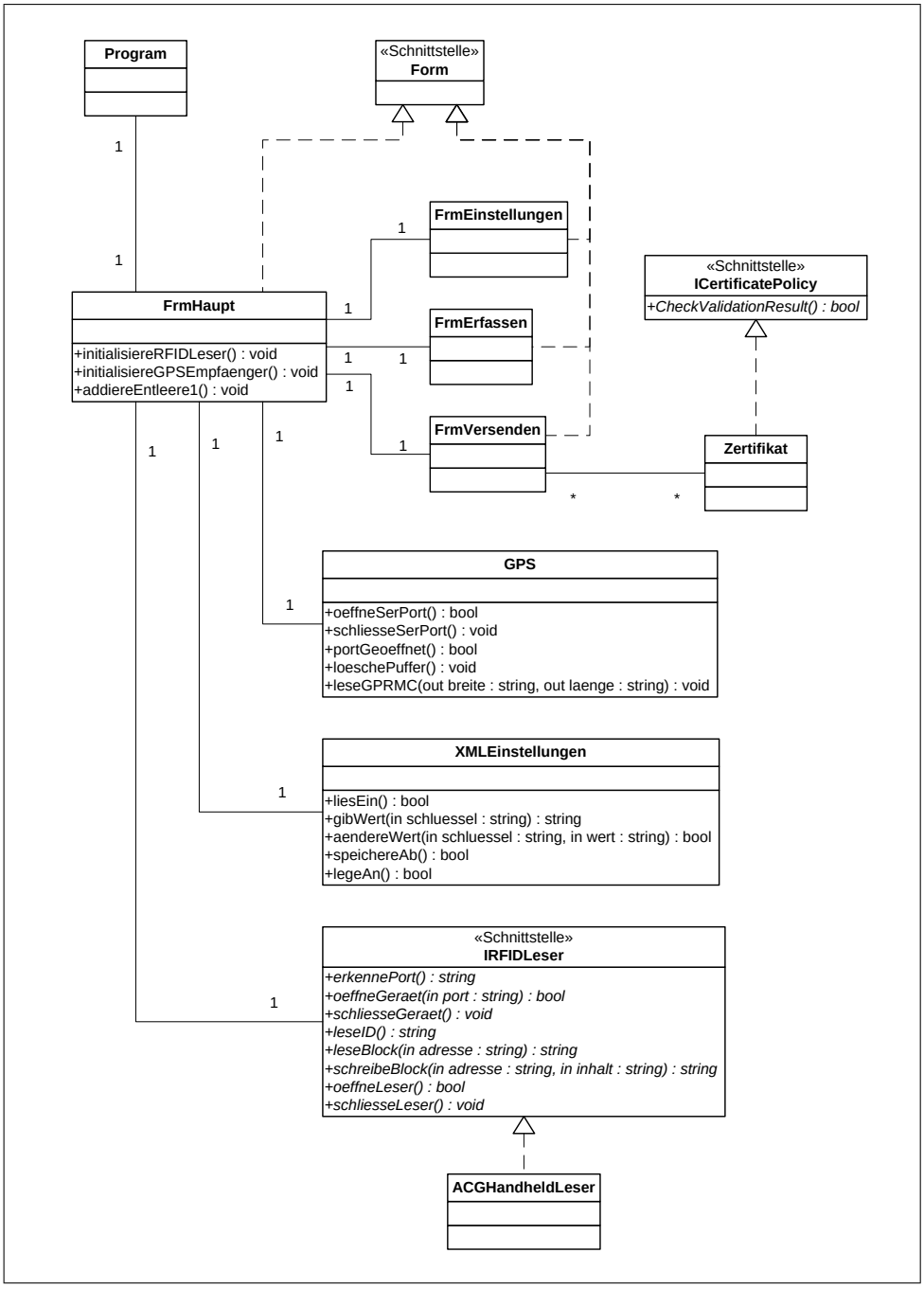


Abbildung 10.9: Klassendiagramm des mobilen Clients.

Beim Versenden der Datensätze wird das SSL-Zertifikat des Web-Servers überprüft. Dafür stellt .NET die Klasse `ICertificatePolicy` zur Verfügung. Die abgeleitete Klasse `Zertifikat` erlaubt einen Verbindungsaufbau nur dann, wenn das Server-Zertifikat korrekt ist.

Neben der statischen Struktur der Anwendungen in Form des UML-Klassendiagramms wurde ebenfalls ein Flussdiagramm entwickelt, welches ein Vertreter der dynamischen UML-Diagrammtypen ist. Das Flussdiagramm besteht aus den folgenden, drei Abbildungen 10.10, 10.11 und 10.12. Die Anwendung beginnt mit dem Start-Ereignis in der Abbildung 10.10. Zunächst wird versucht, die Einstellungen der Anwendung aus der Datei `config.xml` auszulesen. Ist diese Datei vorhanden, werden folgende Daten als globale Einstellungen übernommen.

- Stammdaten: Benutzer Web-Server, Passwort Web-Server, Benutzer-Anwendung, Passwort-Anwendung, Sprache,
- Verbindungen: Proxy-URI, Benutzer Proxy, Passwort Proxy,
- RFID-Einstellungen: RFID-Gerät, RFID COM-Port,
- GPS-Einstellungen: GPS COM-Port, GPS Baudrate.

Ist die Datei nicht vorhanden, werden die Standard-Einstellungen benutzt. Ein erfolgreicher Zugang zu dem Web-Service ist mit den Standard-Einstellungen jedoch nicht ratsam.[274] Im Anschluss werden interne Datenstrukturen aufgebaut, die für die Speicherung und Verwaltung der erfassten RFID-Daten notwendig sind, sowie die weiteren Fenster der Anwendung. Nach dem Auslesen der Einstellungen können ebenfalls die externen Geräte initialisiert werden. Zuerst wird der RFID-Leser mit der Methode `initialisiereRFIDLeser()` für die Benutzung eingebunden. Dazu wird ein neues Objekt geschaffen, welches von einer von `IRFIDLeser` abgeleiteten Klasse instanziert wird. Über den COM-Port wird der Leser verbunden und geöffnet. Eine detaillierte Beschreibung dazu findet sich in Kapitel 10.3.6. Schließlich wird der GPS-Empfänger

[274] Für die Zugangsdaten gibt es keine vernünftigen Standard-Einstellungen. Ein Standard-Zugang (z. B. Benutzer `gast` mit Passwort `gast`) würde jegliche Form von Sicherheit untergraben. Ein Löschen der Datei `config.xml` würde durch die Verwendung der Standard-Einstellungen den Zugang zum Web-Service ermöglichen. Diese Lösung wäre selbstverständlich technisch umsetzbar, ist aber in dieser Anwendung nicht gewünscht.

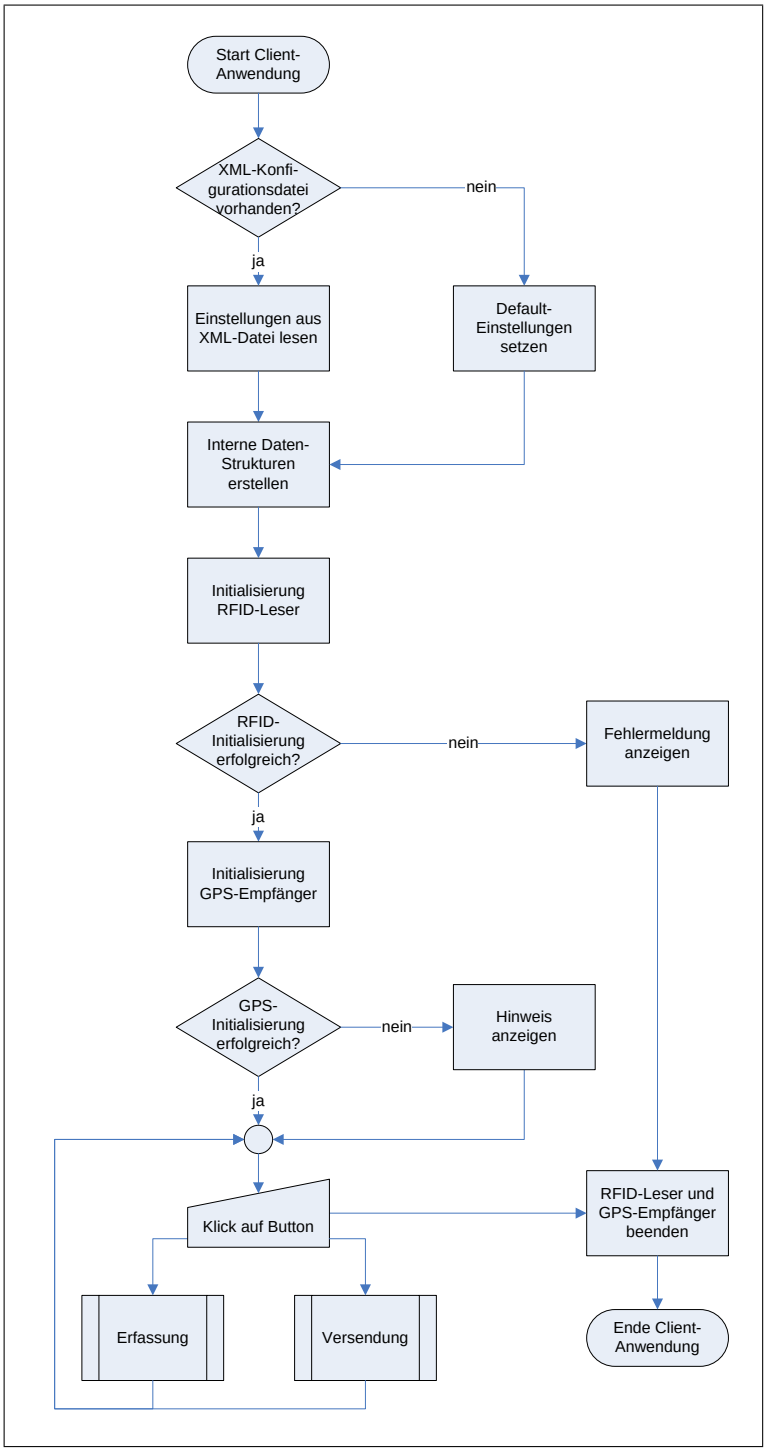


Abbildung 10.10: Flussdiagramm des Clients (Rahmenanwendung).

nutzbar gemacht, indem ebenfalls ein neues Objekt instanziert, die Baudrate für die Kommunikation eingestellt und das Gerät geöffnet wird.

Sofern die Initialisierung der Geräte erfolgreich war, hat der Benutzer die Möglichkeit zur Eingabe der gewünschten Funktion. Der Benutzer kann durch einen Klick auf einen Button die Erfassung oder die Versendung starten oder das Programm verlassen.[275] Vor dem Beenden der Anwendung werden die Verbindungen zu den beiden Geräten ordnungsgemäß getrennt.

Hat der Benutzer den Button `Erfassung` angeklickt, dann wird das Fenster `Erfassung` gestartet. Der Ablauf innerhalb dieses Teils der Anwendung wird im Flussdiagramm 10.11 beschrieben. Der Benutzer kann durch einen Klick auf einen weiteren Button einen Lesevorgang starten, der die RFID-ID eines Tags vom Leser an die Anwendung überträgt. Zur Überprüfung des Vorgangs wird die ID ausgegeben. Zur Ortung des Lesevorgangs werden die GPS-Koordinaten der aktuellen Position in dem gleichen Datensatz gespeichert. Ist kein GPS-Empfänger angeschlossen, so werden die Standard-Werte von 0° nördlicher Breite und 0° östliche Länge verwendet. Schließlich ist neben dem Ort noch das aktuelle Datum und die Uhrzeit von Interesse. Diese Daten werden innerhalb eines neuen Datensatzes in einer internen Datenstruktur gespeichert. Der Benutzer kann dann entweder einen neuen Lesevorgang starten oder das Fenster verlassen. In dem Flussdiagramm wird nicht die Möglichkeit deutlich, dass der Benutzer zwischen zwei Modi der Erfassung wählen kann. Zum einen kann der Benutzer durch einen Klick auf den Button `Lesen` einen manuellen Lesevorgang starten. Zum anderen kann ein periodisches Lesen eingestellt werden, welches automatisch in Reichweite befindliche Tags liest. Dies ist in dem Diagramm nicht erkennbar, weil .NET einen `Timer` zur Verfügung stellt, welcher den Klick auf den Button aus der Anwendung vornimmt und somit eine Benutzer-Eingabe ersetzt. Für die Methode mit dem Code zur Erfassung ist dieser Unterschied nicht erkennbar. Weiterhin spielt diese Funktion für die technische Machbarkeit keine große Rolle, da die Funktion des Timers keine RFID-spezifische ist. Verlässt der Benutzer das Fenster `Erfassung`, dann gelangt er wieder zu dem Haupt-Fenster.

Nach der Erfassung kann der Benutzer die Datensätze versenden. Durch die Auswahl des Buttons `Versendung` gelangt er in das entsprechende Fenster. Dem

[275] Die Möglichkeit des Benutzers, die Einstellungen der Anwendungen zu ändern, wurde in der Abbildung 10.10 nicht hinzugefügt, weil sich das Flussdiagramm auf die Erfassung und Versendung von RFID-Daten konzentriert.

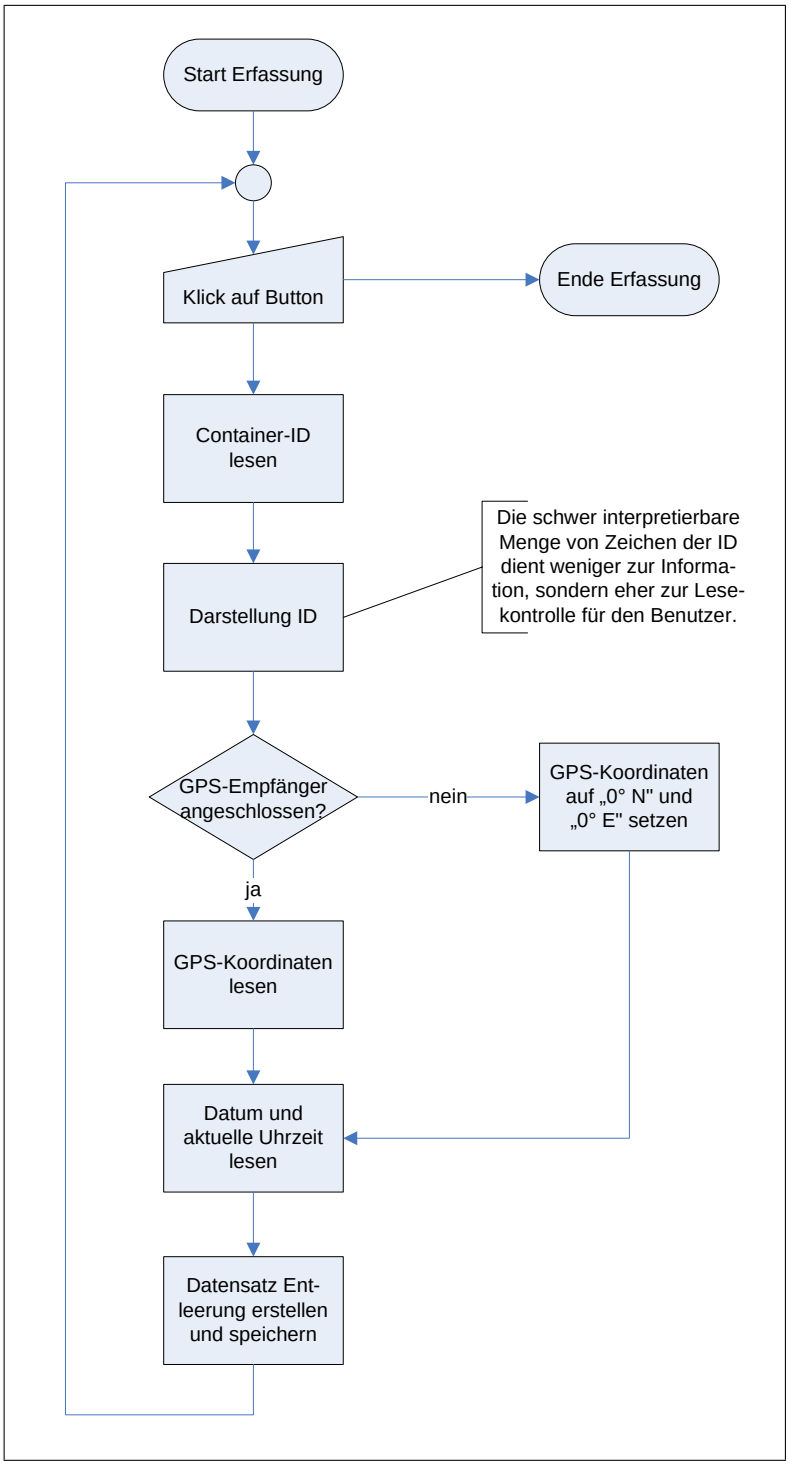


Abbildung 10.11: Flussdiagramm des Clients (Erfassung).

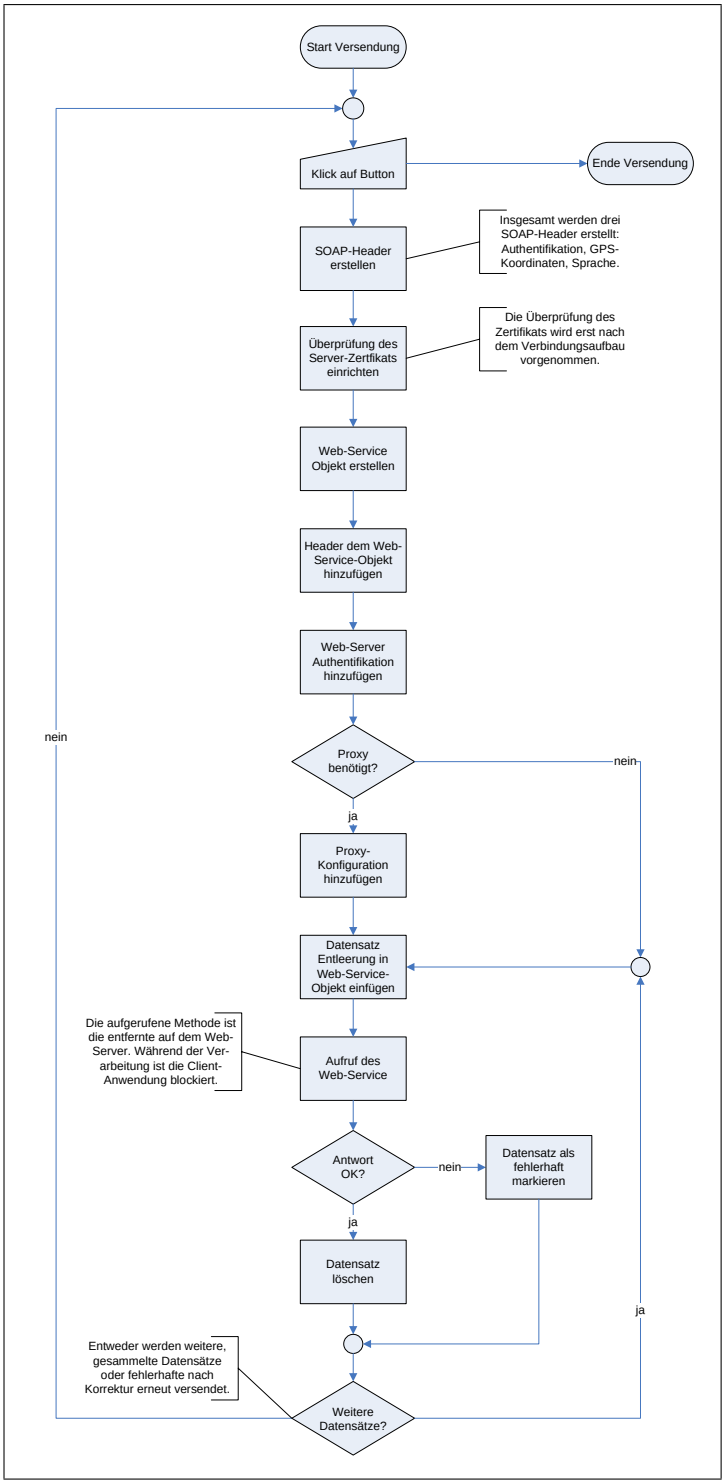


Abbildung 10.12: Flussdiagramm des Clients (Versendung).

Benutzer werden die gesammelten Datensätze zur Kontrolle in einer Tabelle angezeigt. Durch einen Klick auf den Button `Senden` werden diese nacheinander versendet. Zunächst werden die bereits angesprochenen SOAP-Header (`AuthHeader`, `GpsHeader`, `SprachHeader`) erstellt. Anschließend werden die notwendigen Schritte für die Kommunikation mit dem Web-Server durchgeführt. Diese sind im Einzelnen die Überprüfung des Server-Zertifikats, die Erstellung des Web-Service-Objekts, das Hinzufügen der erstellten Header zu dem Web-Service-Objekt und die Einrichtung der Authentifikation am Web-Server. Ist in der Konfiguration der Anwendung ein Proxy-Server für die Verbindung zu einem Web-Server außerhalb eines LANs hinterlegt, dann wird diese Konfiguration zur Laufzeit hinzugefügt. Die Datensätze aus der Tabelle werden nun ausgelesen und in das `Struct Entleerung1` des Web-Services geschrieben. Schließlich ruft das Web-Service-Objekt mit dem Parameter `Struct Entleerung1` den Web-Service auf. Ist die Übertragung und die Verarbeitung ohne Fehler, dann gibt die Anwendung auf dem Backend den Antwort-Code `0` zurück und der aktuelle Datensatz auf dem Client kann gelöscht werden. Anderenfalls wird ein Fehler-Code ungleich `0` empfangen, so dass der Datensatz nicht gelöscht und die Fehlermeldung in der Tabelle als Rückmeldung an den Benutzer hinzugefügt wird.

10.3.3 Einstellungen und Benutzung

Die in den vorherigen Kapiteln vorgestellten Diagramme werden im Feld der Softwaretechnik eingesetzt. Dieses Kapitel erklärt Teile der Anwendung aus der Benutzersicht. Im Folgenden werden Screenshots vom PDA mit den verschiedenen Fenstern gezeigt und erläutert. Die Screenshots wurden mit dem frei erhältlichen XnViewPocket[276] für Pocket PC erstellt.

Nach dem Start der Anwendung wird das Haupt-Fenster (Abbildung 10.13) angezeigt, in dem der Benutzer auswählen kann, welche Funktion er ausführen möchte. Grundsätzlich sind dies die Erfassung und Versendung von RFID-Daten, die Einstellungen sowie das Beenden der Anwendung durch einen Klick auf den `OK` Button rechts oben neben der Uhrzeit. Ebenfalls in der oberen, blauen Statuszeile sind die Status-Symbole für die WLAN-Netzwerkverbindung und die Lautstärke-Einstellungen zu erkennen. Unten rechts auf dem Schirm

[276] http://www.xnviewpocket.org

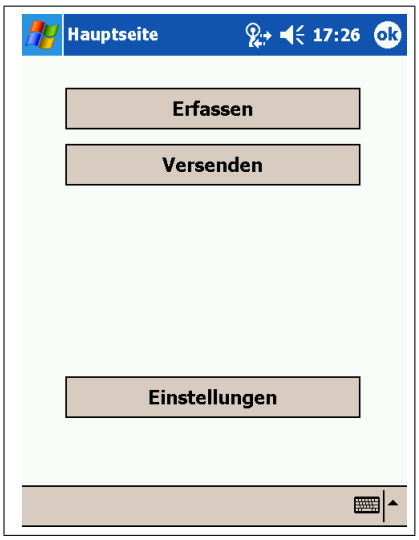


Abbildung 10.13: Screenshot: Hauptseite der Client-Anwendung.

ist eine Tastatur zu erkennen, die für die Eingabe von Zeichen benutzt werden kann.

Beim ersten Start sollte der Benutzer unter „`Einstellungen`“ seine individuelle Konfiguration hinterlegen. Durch einen Klick auf „`Einstellungen`“ gelangt man in das Fenster der Abbildung 10.14. Das Fenster besteht aus vier verschiedenen Reitern (*Tabs*, `TabPage`). Jeder Reiter enthält Einstellungen zu einem Bereich der Anwendung. Zunächst können die Zugangsdaten und die Sprache eingestellt werden. Die Benutzernamen werden in Klartext eingeben, die Zeichen der Passwörter hingegen werden durch den Asterisk („`*`“) maskiert. Die zu verwendende Sprache kann aus den möglichen Werten „`de-DE`“, „`en-GB`“ und „`en-US`“ ausgewählt werden. Sind Änderungen an den Einstellungen auf einem Reiter vorgenommen worden, dann muss jeweils der Button „`Speichern`“ angeklickt werden, damit die Einstellungen dauerhaft gespeichert bleiben. Die Passwörter werden nicht in Klartext sondern mit dem Rijndael-Algorithmus[277] verschlüsselt in der Datei `config.xml` abgelegt.

Auf dem nächsten Reiter „`Verbindungen`“ werden die Proxy-Einstellungen vorgenommen (Abbildung 10.15). Wenn die Anwendung innerhalb eines LAN benutzt und der Zugang nach Außen durch einen Proxy gesteuert und geschützt wird, dann muss auf diesem Reiter der Haken bei „`Proxy benutzen`“ gesetzt und

[277] Rijndael ist eine andere Bezeichnung für den symmetrischen Verschlüsselungsalgorithmus *Advanced Encryption Standard* (AES).

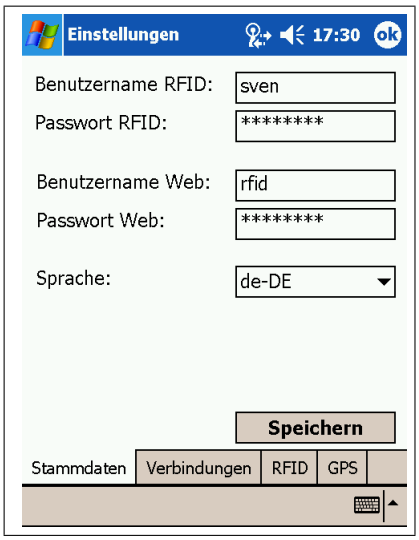


Abb. 10.14: Screenshot: Einstellungen Stammdaten

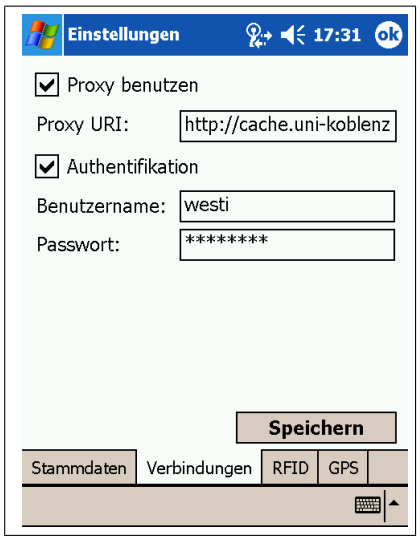


Abb. 10.15: Screenshot: Einstellungen Proxy

das Textfeld „`Proxy URI`“ mit der entsprechenden URI gefüllt werden. Eine URI ist wie folgt aufgebaut: `http://<host>:<port>` und lautet im Falle der Universität Koblenz `http://cache.uni-koblenz.de:3128`. Je nach Konfiguration des Proxy kann eine Authentifikation verlangt werden, deren Werte in den beiden Textfeldern eingetragen werden können.

Die letzten beiden Reiter enthalten Einstellungen, die für die Nutzung der Hardware notwendig sind. Zunächst kann der Typ der verwendeten RFID-Karte ausgewählt werden. Im Falle des Prototyps ist dies lediglich die Karte „`ACG RF Handheld Reader`“. Der Standard-Port dieser Karte ist „`COM6:`“, welcher auch bei der Anwendung eingestellt werden sollte. Auf dem Reiter „`GPS`“ braucht wegen der Verwendung des NMEA-Protokolls kein spezielles Gerät ausgewählt werden. Ebenso wie bei der RFID-Karte muss jedoch der COM-Port ausgewählt werden, an dem das Gerät angeschlossen ist. Ein zusätzlicher Parameter ist die Baudrate der seriellen Verbindung. GPS-Empfänger unterstützen verschiedene Baudraten, so dass hier eine feste Einstellung notwendig ist. Entweder kann man eine funktionierende Baudrate durch Testen herausfinden oder man informiert sich in der Dokumentation des Empfängers über einen unterstützten Wert. Bei RFID-Karten wird in der Regel diese Über-

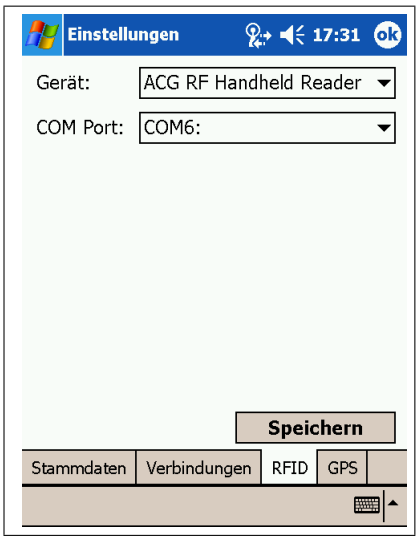


Abb. 10.16: Screenshot: Einstellungen RFID

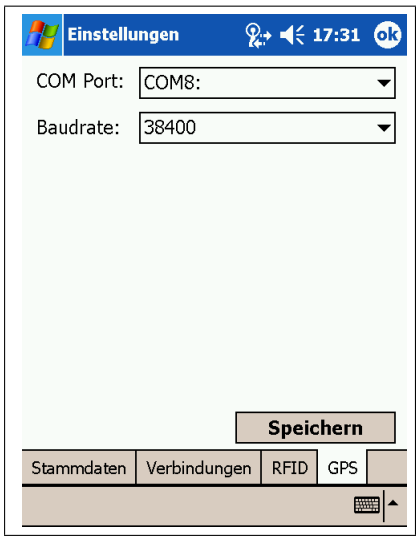


Abb. 10.17: Screenshot: Einstellungen GPS

tragungsgeschwindigkeit automatisch festgestellt. Aus diesem Grund fehlt die Einstellung „`Baudrate`“ auf dem RFID-Reiter.

Nach den Grundeinstellungen ist die Anwendung für die Erfassung und Versendung von RFID-Daten vorbereitet. Durch einen Klick auf „`Erfassen`“ gelangt man in das Fenster „`Erfassung`“, in dem man Tag-IDs lesen kann. Unter „`Lesevorgang`“ stellt der Benutzer ein, ob er mit einem manuellen Lesevorgang Tags lesen möchte oder ob ununterbrochen gelesen werden soll. Im zweiten Fall wird dann periodisch der Lesevorgang von der Anwendung ausgelöst. Wird eine ID gelesen, dann wird diese in der Mitte des Fensters angezeigt. Die Elemente „`Inspektion`“ und „`Bemerkung`“ sind nicht unbedingt notwendig. Sie dienen lediglich für zusätzliche Informationen an den Rekonditionierer und können ggf. weggelassen oder geändert werden. Die gelesenen IDs werden in den internen Datenstrukturen abgespeichert und bleiben natürlich innerhalb der Anwendung verfügbar. Während des Lesevorgangs werden auch die aktuellen GPS-Koordinaten abgelegt. Voraussetzung ist jedoch, dass der GPS-Empfänger eingeschaltet ist, die Verbindung hergestellt ist (z. B. über Bluetooth), und dass der GPS-Empfänger genügend Signale der GPS-Satelliten empfangen kann.

Man kann sich die erfassten Daten nach einem Klick auf „`Versenden`“ des Haupt-Fensters anzeigen lassen, bevor man die Daten an den Web-Service sen-

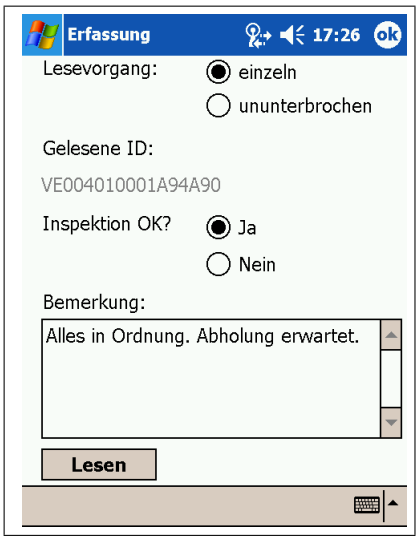


Abb. 10.18: Screenshot: Erfassung

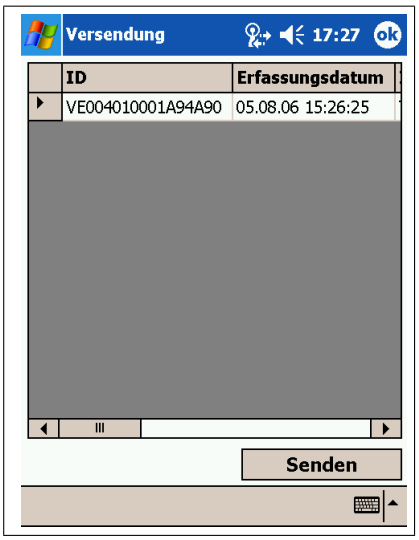


Abb. 10.19: Screenshot: Versendung

det. Die Datensätze werden in einer Tabelle angezeigt, die für die Anzeige auf dem PDA zu breit ist. Um alle Felder der Datensätze zu sehen, muss man in der Tabelle nach rechts scrollen. Bei einem Klick auf den Button „`Versenden`“ kann man alle Datensätze an den Web-Service versenden. Der aktuelle zu sendende Datensatz wird in der Tabelle blau markiert. Kann ein Datensatz nicht erfolgreich versendet und verarbeitet werden, dann wird die zurückgegebene Fehlermeldung in der Tabelle ganz rechts angezeigt. Anderenfalls wird der Datensatz aus der Tabelle und den internen Datenstrukturen gelöscht.

Sind alle gewünschten Funktionen ausgeführt worden, dann kann man die geöffneten Fenster durch das „`OK`“ oben rechts schließen. Zu beachten ist, dass in dem Prototyp gelesene aber nicht versendete Datensätze nicht im Dateisystem abgespeichert werden. Beim Verlassen der Anwendung gehen diese Daten verloren. Die Einstellungen der Anwendung bleiben jedoch erhalten.

10.3.4 Implementierungsdetails und Alternativen

In diesem Kapitel werden verschiedene Eigenschaften der Client-Anwendung diskutiert. An etlichen Stellen im Quellcode sind erwähnenswerte Details erkennbar oder es existieren Alternativen zu den getroffenen Entscheidungen. Diese Details und die getroffenen Entscheidungen werden im Folgenden erklärt und begründet.

Die globalen Einstellungen der Anwendung können unter dem Punkt `Einstellungen` konfiguriert werden. Durch das Speichern werden sie in der `config.xml` abgelegt und beim nächsten Neustart eingelesen. Diese Einstellungen sind Paare aus dem Parameternamen und dem Parameterwert. Das Ablegen dieser Paare in einer einfachen Text-Datei wäre eine ausreichende Lösung, jedoch müsste dann das Speichern und Auslesen der Text-Datei mit einem aufwändigen Parsen implementiert werden. XML hingegen bietet eine Strukturierung durch die Verwendung von *Tags* und den dazugehörigen Werten. Zusätzlich ist eine Hierarchisierung denkbar, welche jedoch für die Anwendung nicht benötigt wird. .NET bietet für die Verwaltung von XML-Dateien einen eigenen *Namespace* `System.Xml` an, so dass das Erstellen, Verändern und das Auslesen einer XML-Datei für den Programmierer vereinfacht wird. Die XML-Datei wird zunächst mit einem `XmlDocument`-Objekt verknüpft. Diese kann anschließend mit den Methoden der `XmlReader`-Klasse ausgelesen und mit den Methoden der Klasse `XmlNodeList` verändert werden. Das Speichern der Datei übernimmt die Methode `Save` der Klasse `XmlDocument`.

Wie bereits erwähnt, wird der RFID-Leser durch von `IRFIDLeser` abgeleitete Klassen eingebunden. Diese Modellierung erlaubt eine einfache Erweiterung von unterstützter Hardware durch das Hinzufügen von neuen Klassen. Die Implementierungsdetails der verwendeten Hardware werden in Kapitel 10.3.6 erläutert.

Der Benutzer hat die Möglichkeit, zwischen zwei Modi bei der Erfassung zu wählen. Entweder wird jeder Lesevorgang mit einem Klick auf einen Button eingeleitet oder einmalig die periodische Erfassung auswählt, welche in bestimmten Zeitabständen einen Lesevorgang vornimmt. Wenn die ID eines Tags bei der periodischen Erfassung mehr als ein Mal gelesen wird, dann stellt sich die Frage, welcher der beiden erstellten Datensätze gespeichert wird[278]. Wenn mehrere Male der selbe Tag gelesen wird, dann muss diese Entscheidung von der Anwendung getroffen werden und nicht vom Benutzer, weil dieser bei mehreren Erfassungen pro Sekunde nicht schnell genug reagieren könnte. Denkbar ist auch die unbeaufsichtigte Erfassung[279] von Tags, bei der ein ma-

[278] Es kann nur ein Datensatz eines Tags gespeichert werden, weil die eindeutige ID des Tags als Primärschlüssel in den lokalen Datenstrukturen und in der Datenbank des Backends dient.

[279] In der Regel werden mobile Geräte (PDA) nicht unbeaufsichtigt Daten erfassen. Jedoch ist dieses Problem auch auf stationäre Leser übertragbar.

nuelles Eingreifen nicht möglich ist. In der Anwendung wird daher immer die letzte Erfassung gespeichert. Zuvor erfasste Datensätze der gleichen ID werden überschrieben, so dass eine Aktualisierung von bestimmten Daten des Containers möglich ist (z. B. der Ort oder der Zustand). Der Nachteil bei diesem Vorgehen ist, dass unbeabsichtigte Lesevorgänge die korrekten, älteren Datensätze überschreiben und dass damit die Gefahr von Datenverlust steigt. Bei der Avisierung von leeren Containern wird diese Gefahr in Kauf genommen, weil keine wichtigen Daten überschrieben werden können und der Vorteil der Aktualität der Daten diesen Nachteil übertrifft.

Die bereits häufig erwähnte, intern verwendete Datenstruktur ist der .NET Datentyp `DataTable`. In der Instanz `dataEntleere1` dieses `DataTable` werden die erfassten Daten abgelegt. `dataEntleere1` ist ein globales Attribut und deswegen von allen anderen Klassen der Anwendung erreichbar. Das Suchen, Hinzufügen und Löschen von Datensätzen wird durch die .NET-Methoden `Find()`, `Add()` und `Remove()` ermöglicht.

Datums- und Uhrzeitangaben können in dem Datentyp `DateTime` gespeichert werden. Bei der Erfassung werden das aktuelle Datum und die lokale Uhrzeit gespeichert und in das UTC-Format konvertiert. Das Datum wird dann in dem Datensatz der erfassten ID abgelegt. Die folgenden beiden Zeilen Code zeigen das Auslesen des aktuellen Datums und das Konvertieren in UTC.

```
1 System.DateTime lokalesDatum = System.DateTime.SpecifyKind(
    System.DateTime.Now, System.DateTimeKind.Local);
2 System.DateTime erfassungsdatum = lokalesDatum.
    ToUniversalTime();
```

In der implementierten Client-Anwendung werden die Daten zunächst gesammelt und in einem getrennten, zweiten Schritt versendet. Eine Alternative wäre dazu die Versendung sofort nach der Erfassung, so dass der Benutzer bei Problemen sofort aufmerksam gemacht wird. Dies könnte durch die temporäre Schaffung eines Threads[280] in dem gleichen Prozess realisiert werden. Dieser Thread läuft für den Benutzer unsichtbar im Hintergrund ab. Da der Aufruf eines Web-Service blockierend ist, wird dieser zweite Thread blockiert, aber die Anwendung mit der GUI ist für die nächste Erfassung sofort wieder frei. .NET

[280] Ein Thread ist ein Unterprozess innerhalb eines Prozesses. Ein Prozess kann aus mehrere Threads bestehen. Threads werden auch als leichtgewichtige Prozesse bezeichnet.

bietet für die Schaffung von benutzerdefinierten Threads die Klasse `System.Threading.Thread` an. Der Vorteil dieser Lösung ist, dass kein zweiter Schritt für den Benutzer zum Versenden nötig wäre. Bei einer fehlgeschlagenen Versendung könnte vor Ort die Ursache identifiziert werden. Jedoch gibt es auch Nachteile dieser Alternative. Notwendig dafür wäre eine ständige Netzwerk-Verbindung. Außerdem hat dann der Benutzer weniger Kontrolle über die zu übermittelnden Daten, da er bei der implementierten Lösung eine Übersicht aller Datensätze vor der Kommunikation mit dem Web-Service geboten bekommt. Für den Programmierer stellt der Einsatz von Threads eine weitere Fehlerquelle dar, da parallele Threads[281] auf gemeinsame Daten zugreifen könnten. Die Gefahr von Programmfehlern durch *Deadlocks*[282] und falschen Berechnungen[283] steigt dadurch enorm.

Die Tabelle mit den Datensätzen in dem Fenster `Versendung` ist ein *Control* vom Typ `DataGrid`. Dieses Control wird in dem *Namespace* `System.Web.UI.WebControls` zum Anzeigen von Datenstrukturen in einer Tabelle benutzt. Dem Attribut `DataSource` kann z. B. ein `DataTable` zugewiesen werden. Zusätzlich muss dem `DataGrid` ein `Style` zugeordnet werden, damit in der Tabelle die richtigen Felder in der richtigen Formatierung angezeigt werden. Die Möglichkeiten des `DataGrid` sind in dem .NET Compact Framework jedoch stark beschnitten, so dass nur grundlegende Elemente des *Controls* konfigurierbar sind. Beispielsweise ist das Einfärben von Zeilen, Spalten oder Zellen mit den .NET Compact Methoden nicht möglich.

Die Klasse `Zertifikat` wird von der .NET-Schnittstelle `ICertificatePolicy` abgeleitet. Sie dient der Überprüfung von Zertifikaten und wird in der Client-Anwendung benutzt, weil sichergestellt werden soll, dass der Server, an den die Daten gesendet werden, auch der richtige Server ist. Dadurch werden *Man-In-The-Middle*-Attacken vermieden und Schäden als Folge von *DNS-Spoofing*[284]

[281] Threads auf Systemen mit einem Prozessor (CPU) werden nur scheinbar parallel ausgeführt. In Wirklichkeit wechseln sich Threads in der Verarbeitung ab.

[282] Ein *Deadlock* (Verklemmung) ist ein Zustand eines Programms, in dem zwei Threads auf Betriebsmittel warten, die von anderen Threads benutzt werden, die ebenfalls auf Betriebsmittel warten. Dadurch entsteht eine zyklische Abhängigkeit, die nicht mehr aufgelöst werden kann. Das Programm „hängt“.

[283] Durch die Schaffung von Kritischen Gebieten können falsche Berechnungen beim Einsatz mehrerer Threads verhindert werden

[284] Beim *DNS-Spoofing* fälscht der Angreifer die Zuordnung von IP-Adresse zu Hostname, so dass ein Client nicht auf den gewünschten Server, sondern auf einen Server des Angreifers, gelangt.

verringert. Beim Aufbau der HTTPS-Verbindung zu dem Web-Service übermittelt der Web-Server der Client-Anwendung das SSL-Zertifikat. Mit der Methode `CheckValidationResult()` kann dann in der Klasse `Zertifikat` das empfangene Zertifikat auf Gültigkeit überprüft werden. Das Zertifikat ist in der .NET-Anwendung ein Objekt und bietet über verschiedene Attribute Zugriff auf die Zertifikat-Eigenschaften. In der Anwendung wird lediglich der Fingerabdruck des SSL-Schlüssels überprüft (Attribut `GetCertHashString()`). Selbstverständlich können auch weitere Eigenschaften des Zertifikats überprüft werden, wie z. B. Aussteller und Gültigkeitszeitraum.

Die beiden Authentifikationen an dem Web-Server und Web-Service werden in der Klasse `Versenden` implementiert. Für die Web-Server-Authentifikation wird eine Instanz der Klasse `System.Net.NetworkCredential` erstellt. Dieses Objekt wird dann der `WebService`-Eigenschaft `Credentials` zugewiesen.

```
1 webService.Credentials = new System.Net.NetworkCredential(
    benutzer, passwort);
```

Die Authentifikation an dem Web-Service geschieht durch den Benutzernamen und das Passwort in dem `SoapHeader`. Die XML-Header sind .NET-Objekte, die Attribute und Methoden haben können. Der `SoapHeader` hat lediglich die beiden Attribute `benutzername` und `passwort`, welche von der Anwendung auf dem Backend ausgewertet werden. Die Authentifikation an einem eventuell eingesetzten Proxy-Server wird ebenfalls durch die Klasse `System.Net.NetworkCredential` geleistet. In diesem Fall wird ein zusätzliches Objekt von der Klasse `System.Net.WebProxy` erstellt. Dieses Objekt hat ebenfalls ein `Credentials`-Attribut und wird schließlich dem `WebService`-Objekt zugewiesen, so dass bei dem Verbindungsaufbau der angegebene Proxy benutzt wird.

```
1 System.Net.WebProxy webProxy = new System.Net.WebProxy(
    proxyUri, true);
2 webProxy.Credentials = new System.Net.NetworkCredential(
    benutzer, passwort);
3 webService.Proxy = webProxy;
```

Die Versendung der Datensätze geschieht in einer Schleife, die jeden Datensatz einzeln an den Web-Service sendet. Wenn ein Datensatz erfolgreich verarbeitet wurde (Antwort-Code `0`), dann wird der Datensatz aus dem `DataGrid` und damit auch gleichzeitig aus dem `DataTable` gelöscht (Methode `RemoveAt()`).

Fehlerhafte Datensätze werden nicht gelöscht, sondern bleiben mit der entsprechenden Fehlermeldung in der Tabelle gelistet.

10.3.5 Nutzung Web-Service

Die Client-Anwendung ruft Methoden des Web-Service auf dem Web-Server im Backend auf. Für die Benutzung der Methoden während der Erstellung der Anwendung – also während dem Codieren – ist erforderlich, dass der Web-Service bereits auf dem Web-Server zur Verfügung steht. Der Grund dafür ist, dass die Klassen, Methoden und Datentypen in das Client-Projekt (*Solution*) von Visual Studio 2005 importiert werden müssen. Dieser Import ist technisch eine Referenz auf den Web-Service und seine Dienste.

Die Referenz wird angelegt durch die Auswahl von `Add Web Reference` in dem Menü `Projekt`. In dem folgenden Dialog kann dann die URL des Web-Service in der Form `https://host/pfad/dienst.asmx` angegeben werden.[285] Nach dem Hinzufügen erscheint der Web-Service unter dem Punkt `Web Reference` im `Solution Explorer` und kann innerhalb des Codes mit Hilfe eines Bezeichners (*Folder-Name*) benutzt werden. Während der Entwicklung ist dabei folgendes Problem aufgetreten. Ist auf dem Web-Server die Anonyme Authentifikation für das entsprechende Verzeichnis nicht eingeschaltet, dann kann die *Web Reference* nicht hinzugefügt werden. Beim Zugriff auf die URL wird der Entwickler zwar aufgefordert sich an dem Web-Server zu authentifizieren, aber anschließend wird der Zugriff trotz korrekter Anmeldung verweigert. Erst wenn die Anonyme Authentifikation eingeschaltet ist, kann die *Web Reference* erfolgreich hinzugefügt werden. Dieses Verhalten war nur während der Benutzung des Web-Service mit Visual Studio zu beobachten. Bei der erstellten Client-Anwendung konnte die Anmeldung an dem Web-Server erfolgreich durchgeführt werden. Die Ursache für dieses Verhalten konnte nicht eindeutig geklärt werden.

Ist der Web-Service erfolgreich hinzugefügt, dann können die öffentlichen Objekte[286] des Web-Service wie lokale benutzt werden. Alle Objekte des Web-Service sind unter dem bei der Referenz vergebenen Bezeichner erreichbar. Während der Entwicklung muss dann nicht notwendigerweise eine Verbindung

[285] Auch lokal laufende Web-Services sind durch die Angabe des lokalen Datei-Pfades importierbar. Gleiches gilt für Web-Services innerhalb der *Solution*.

[286] Öffentliche Objekt sind diejenigen Objekte, die bei der Programmierung des Web-Service mit dem Modifier `public` erstellt wurden.

zum Web-Service bestehen. Wird die Schnittstelle des Web-Service jedoch zwischenzeitlich verändert, dann ist unbedingt ein Update der *Web Reference* notwendig.

Auffällig bei dem Testen der Anwendung war, dass der erste Aufruf eines Web-Service sehr viel länger dauerte als identische, nachfolgende Aufrufe. Man kann davon ausgehen, dass nach einem Neustart des Hosts oder des Web-Servers erst Dateien vom Dateisystem geladen werden müssen, die beim zweiten Versuch dann bereits im Speicher oder Cache des Servers liegen und somit schneller verarbeitet werden können. Auswirkungen auf die Ergebnisse der Aufrufe waren nicht zu beobachten.

10.3.6 Anbindung Hardware

Bei dem Prototyp werden verschiedene Hardware-Schnittstellen zur Nutzung von externen Geräten verwendet. Die CF-Schnittstelle des PDA wird durch das Betriebssystem Pocket PC 2003 bereits erkannt und nutzbar gemacht. Bei dem Einsetzen einer CF-Karte weist das Betriebssystem der seriellen Schnittstellen eine Adresse (COM1: bis COM8:) zu, so dass Kommunikation zwischen Anwendungen und der Karte möglich ist. Die zweite, benötigte Schnittstelle ist die Bluetooth-Schnittstelle, welche bei Pocket PC 2003 durch Treiber des Herstellers eingebunden werden muss. Bei dem HP iPAQ hx4700 hat Hewlett-Packard bereits mit der Auslieferung des PDA die Treiber installiert. Der WLAN-Adapter des PDA wird ebenso bereits mit HP-Treiber versehen, so dass nur noch die spezifische Konfiguration des WLAN-Netzes notwendig ist.

RFID-Leser

Der RFID-Leser von ACG wird mit einer API für die Benutzung in eigenen Anwendungen ausgeliefert. Diese API kann in .NET-Anwendungen der Sprache C# verwendet werden. Sie wird von ACG sehr detailliert dokumentiert [ACG 2005], was für den Entwickler von großem Nutzen ist, weil die exakte Reihenfolge der Befehle sehr wichtig ist. Im Folgenden wird die Einbindung der Karte in die Client-Anwendung beschrieben.

Die API besteht aus der Datei `CFReader.dll` und einem Wrapper[287] `CFReader DLLWrapper.dll` für C#, der erst seit der Version 3.2.0 enthalten ist [ACG 2005, S. 96]. Der Wrapper muss für die Nutzung der enthaltenen Objekte in Visual Studio eingebunden werden. Der Ablauf ist vergleichbar mit dem Importieren des Web-Service. Die Datei `CFReaderDLLWrapper.dll` wird durch das Hinzufügen einer *Reference* eingebunden. Anschließend muss der neue *Namespace* `CFReaderDLLWrapper` mit dem C#-Schlüsselwort `using` deklariert werden.

Das neue Objekt für den verwendeten RFID-Leser wird mit dem Konstruktor `ACG_CFReader()` erstellt. Anschließend stehen verschiedene Befehle für die Kommunikation mit dem Leser zur Verfügung. Der Auf- und Abbau der Verbindung ist in Abbildung 10.20 erklärt. Zunächst wird der Port des Lesers benötigt. Ist der Port nicht in der Konfiguration der Anwendung eingestellt, dann wird er automatisch erkannt (Methode `RDR_DetectSerialPort()`). Anschließend muss die Kommunikation zu dem Gerät aufgebaut werden (Methode `RDR_OpenComm()`) bevor der eigentliche RFID-Leser des Geräts mit der Methode `RDR_OpenReader()` initialisiert wird. Dabei wird ein Parameter übergeben, der den Typ der Karte angibt, denn der ACG-Treiber ist nicht nur für diese CF-Karte zu benutzen, sondern auch für weitere Produkte des Herstellers. Der Parameter-Wert `0` steht für die automatische Erkennung der verwendeten Karte. Zu beachten ist, dass direkt nach dem Einsetzen der CF-Karte von der Firmware automatisch auf den Modus `Continuous Read` geschaltet wird. In diesem Modus wird ständig nach RFID-Tags in Reichweite gescannt. Wird in diesem Modus ein Befehl an das Gerät gesendet, dann wird das Zeichen `S` als Fehlercode zurückgegeben. Aus diesem Grund sollte nach dem Einschalten die Methode `RDR_AbortContinuousRead()` aufgerufen werden. Diese beendet den Modus und ermöglicht das manuelle Erfassen von RFID-Daten, bei dem das Senden von Befehlen an die Karte notwendig ist. Anschließend kann der Leser für bestimmte RFID-Protokolle konfiguriert werden. Mit der Methode `RDR_SendCommandGetData()` kann man verschiedene Befehle an den Leser senden. Diese Befehle sind unabhängig von der verwendeten Programmiersprache und werden von der API direkt an die Firmware des Lesers gesendet. Die

[287] Ein Wrapper ist eine API, welche eine andere API für die Benutzung mit anderen Programmiersprachen erweitert. Im Grunde werden die Anfragen an die API von dem Wrapper umgewandelt und weitergeleitet. Ebenso werden die Antworten, die von der API kommen, vom Wrapper für die Anwendung nutzbar gemacht.

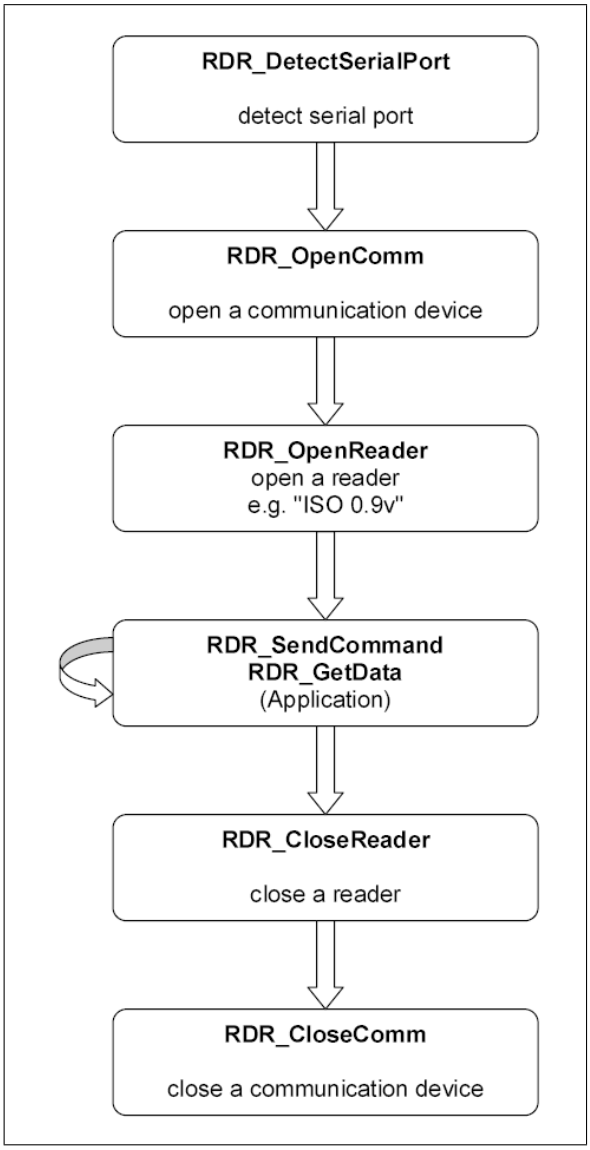


Abbildung 10.20: Flussdiagramm zur Verwendung der ACG RFID-CF-Karte [ACG 2005, S. 14].

Befehle für die Konfiguration der Protokolle sind aufgebaut aus dem Wort `use` und dem Protokoll-Bezeichner (`iso14443a`, `iso15693` oder `all`). Nun ist der Leser für Lesevorgänge vorbereitet.

Der Lesevorgang besteht aus mehreren Befehlen. Zunächst sollte der Empfangspuffer der Karte geleert werden, damit auch die zuletzt gelesenen RFID-Daten an die Anwendung weitergegeben werden können (Methode `RDR_EmptyCommRcvBuffer()`). Anschließend wird mit dem Befehl `select` als Parameter der Methode `SendCommandGetData()` ein Tag in Lesereichweite ausgewählt. Der Leser gibt daraufhin die Tag-ID an die Anwendung zurück. Im Fehlerfall können verschiedene Fehlercodes zurückgegeben werden [ACG 2005, S. 40]. Wird beispielsweise ein `N` von der Anwendung empfangen, dann befindet sich kein Tag in Reichweite. Der Leser kann auch mehrere Tags in einem Lesevorgang erfassen, wenn der Befehl `multiselect` an das Gerät gesendet wurde. Werden dann mehrere Tag-IDs in den Puffer geschrieben, liest die Anwendung diese IDs aus und kann dann entscheiden wie z. B. das mehrfache Lesen einer ID behandelt werden soll.

Wird die Anwendung geschlossen, so sollte die Verbindung zu dem Leser und die Kommunikation zu dem Gerät geschlossen werden (siehe Abbildung 10.20, Methoden `RDR_CloseReader()` und `RDR_CloseComm()`).

Für die Client-Anwendung werden weitere Methoden und Befehle nicht benötigt. Jedoch ist zu beachten, dass die Befehle `read register` und `read block` gänzlich verschiedene Speicherbereiche auslesen. Mit *Register* ist der Speicherbereich des Lesers gemeint, in dem auch die veränderbare Leser-ID abgelegt ist. *Block* ist der adressierbare Speicher auf dem Tag. Der Befehl `write block` hat n Byte als Parameter, wovon ein Byte die Adresse des Blocks ist und die restlichen n-1 Byte die zu schreibenden Daten. Dabei entscheidet die Datenstruktur des Tags, wie viele Bytes ein Block groß ist. In aller Regel sind dies vier oder acht Bytes. Bei speziellen Tags mit viel Speicherplatz gibt es entweder eine zusätzliche *Offset*-Adresse pro Block oder größere Blöcke zur Adressierung großer Datenmengen. Ein Leser kann leider nicht erkennen, welche Struktur der Tag hat. Dem Entwickler bleibt bei einer unbekannten Tag-Struktur nur das Ausprobieren des `write block` Befehls mit 2^n Daten-Bytes für verschiedene Werte von n.

GPS-Empfänger

Der GPS-Empfänger wird über Bluetooth eingebunden. Das Betriebssystem stellt eine serielle Schnittstelle zur Verfügung, welche von der Anwendung ausgelesen werden kann. Der Empfänger sendet, sofern er eingeschaltet ist, bestimmte Datensätze über die Bluetooth-Schnittstelle. Sind keine GPS-Satelliten in Reichweite, dann werden alle GPS-Werte der Datensätze mit Null belegt. Sollte eine zweite Anwendung[288] gestartet sein, die ebenfalls Daten dieser seriellen Schnittstelle einliest, dann kann es passieren, dass die Client-Anwendung keine oder deutlich weniger Informationen erhält, da die andere Anwendung diese bereits aus dem Puffer gelesen hat.

Vor dem Start der Anwendung muss die Bluetooth-Verbindung manuell hergestellt werden. Die Anwendung baut beim Programmstart keine automatische Verbindung auf. Diese Funktion ist eine mögliche Erweiterung der Anwendung, die den Komfort und die Robustheit erhöhen würde. Je nach Konfiguration der Komponenten kann es passieren, dass Geräte nach einer bestimmten Zeitspanne in den *Stand-By*-Modus gehen, weil dadurch Strom gespart werden kann.

Schließlich wird in der Anwendung nur der aktuellste GPRMC-Datensatz benötigt (Methode `GPS.leseGPRMC()`), in dem die geographische Länge und Breite enthalten sind. Diese Werte werden ausgelesen und in dem Datensatz der gelesenen ID gespeichert.

Kommunikation

Wie bereits erwähnt, muss der WLAN-Adapter nicht mehr gesondert installiert werden, da die Treiber bereits integriert sind. Mit Hilfe der entsprechenden Werkzeuge von Pocket PC kann das jeweilige Netz eingerichtet werden. Ebenso muss noch die IP-Konfiguration vorgenommen werden. Anschließend steht der Client-Anwendung diese Netzwerk-Verbindung zur Verfügung. Für die Nutzung dieser Verbindung werden keine weiteren Klassen oder Methoden benötigt, da die Kommunikation mit dem Web-Service über das Netzwerk von dem `WebService`-Objekt geführt wird. Die Netzwerk-Methoden werden für den Entwickler verborgen von diesem Objekt verwaltet. Der Entwickler kann somit jede aktive Netzwerk-Verbindung des Betriebssystems nutzen.

[288] Dies könnte im Fall des GPS-Empfängers eine Software zur Navigation sein, die die aktuellen Koordinaten benötigt.

Dieser Vorteil macht sich auch dann bemerkbar, wenn nicht der WLAN-Adapter, sondern eine Verbindung über ein öffentliches Mobilfunknetz, gebraucht wird. Wird auf dem PDA eine GPRS- oder UMTS-Verbindung hergestellt, so kann die Client-Anwendung auch diese Verbindung nutzen. Die Antwort- und Übertragungszeiten sind natürlich deutlich länger als Verbindungen im LAN.

10.3.7 Installation Client-Anwendung auf mobilen Gerät

Die programmierte Client-Anwendung kann direkt aus Visual Studio 2005 auf den PDA zum Starten kopiert werden[289]. Voraussetzung dafür ist, dass der PDA über seine Docking-Station an den Rechner angeschlossen ist und die Microsoft Anwendung ActiveSync gestartet und mit dem PDA verbunden ist.

Ist eine Version der Client-Anwendung bereit für einen Test auf dem PDA, dann kann durch die Auswahl von `Build Solution` (Kompilieren und Ausführen) oder `Start Debugging` (Kompilieren, Ausführen und Debugging ermöglichen) die kompilierte Anwendung direkt in das `Programme`-Verzeichnis kopiert und von dort gestartet werden. Dieser Vorgang dauert einige Sekunden, ermöglicht aber das Testen in der echten Umgebung. Möglich ist ebenfalls das Testen der Anwendung in einem Emulator, der in Visual Studio bereits enthalten ist, aber dann können bestimmte Geräte nicht verwendet werden, z. B. der RFID-Leser.

Die Anwendung auf dem PDA benötigt neben dem installierten .NET Compact Framework noch die API für die Nutzung des RFID-Lesers. Die API besteht aus der DLL-Datei und dem .NET C#-Wrapper. Da der Wrapper eine Referenz in der *Solution* ist, wird der Wrapper automatisch auf den PDA kopiert. Die DLL-Datei jedoch wird nicht automatisch kopiert, sondern muss manuell in das Verzeichnis der entstandenen EXE-Datei kopiert werden.

Nach der Entwicklung des Web-Service auf dem Backend und der Anwendung auf dem mobilen Client kann der Geschäftsprozess „Avisierung von leeren Containern“ mit Hilfe des RFID-Prototyp umgesetzt werden.

[289] Manchmal trifft man in der Literatur oder in Anleitungen den englischen Begriff *Deploy* für das Kopieren der Anwendung auf das Zielsystem an. In Beschreibungen wird dieses Substantiv auch in der eingedeutschten Verb-Form verwendet: *deployen*.

Kapitel 11

Fazit

Diese Arbeit beschäftigte sich mit der Entwicklung eines Systems zur Erfassung von mobilen RFID-Daten. Ausgehend von den technischen Grundlagen wurde die RFID-Technologie vorgestellt. Die Wahrung der Sicherheitsaspekte und die Einhaltung von Standards spielten während der gesamten Entwicklung eine große Rolle. Diese grundlegenden Kenntnisse über RFID bildeten die Grundlage für die weitere Vorgehensweise während der Planung und Umsetzung des Prototyps.

Das SCM bietet sich für den RFID-Einsatz an, weil durch die Integration verschiedener interorganisationaler Systeme die Effektivität und Transparenz in der Lieferkette gesteigert werden kann. Anhand eines ausgesuchten Geschäftsprozesses konnte gezeigt werden, wie die Entwicklung eines RFID-Systems geplant und realisiert werden kann.

Nach den technischen Grundlagen und den betriebswirtschaftlichen Aspekten konnte dann im dritten Teil die praktische Umsetzung des Prototyps beschrieben werden. Nach eingehender Planung und Modellierung konnten letztlich die Server- und Client-Anwendungen entwickelt und die verfügbare Hardware eingebunden werden. Der entstandene Prototyp besteht aus Standard-Komponenten (Hard- und Software) und verwendet bis auf die API des RFID-Lesers nur standardisierte Protokolle zur Kommunikation.

Wegen fehlender Daten konnten leider keine quantitativen Aussagen zur Wirtschaftlichkeit getroffen werden. Stattdessen wurden Kosten verursachende und Nutzen bringende Faktoren diskutiert. Jedoch wäre selbst bei gut kalkulierbaren Kosten der Nutzen ex ante schwer abzuschätzen gewesen.

11.1 Erreichte Ziele und Erkenntnisse

Im Folgenden werden kurz die Anforderungen, Ziele, Forschungsfragen und offenen Punkte der Arbeit und des Prototyps aufgelistet. Diese Zusammenfassung stellt somit eine Übersicht über die inhaltlichen Kernpunkte der Arbeit dar.

11.1.1 Erfüllte Anforderungen

Innerhalb des Geschäftsprozesses „Avisierung von leeren Containern“ wurden fünf Ziele verfolgt (siehe Kapitel 8.2), die einen Betrieb von RFID in der Lieferkette möglich machen können.

Die drei eher technischen Ziele der eindeutigen Identifikation, elektronischen Erfassung und Verknüpfung mit zusätzlichen Daten sind die Kernfunktionen des Prototyps. Die eindeutige ID ist in dem RFID-Tag enthalten, die elektronische Erfassung geschieht mit einem mobilen PDA und die verknüpften Daten liegen in einer Datenbank des Backends. Durch die höhere Datendichte und -genauigkeit wird die Transparenz in der Lieferkette gesteigert. Schließlich kann durch die eindeutige Erfassung und bessere Datenversorgung die Qualität des Produkts gesteigert werden, z. B. durch die Behandlung des Containers nach der Entleerung des Füllgutes.

Die Anforderungen an den Prototyp selbst wurden in Kapitel 8.3 genannt. In der folgenden Liste werden die Anforderungen erneut genannt und das realisierte Ergebnis bewertet:

- Entwicklung eines RFID-Systems für das Container-Management: Der Prototyp zur Erfassung von mobilen RFID-Daten behandelt einen exemplarischen Geschäftsprozess im Container-Management.

- Merkmal zur Identifizierung an jedem Container: Die ID des RFID-Tags ist das Merkmal zur Identifizierung des Containers und der dazugehörigen Daten in der Datenbank.

- Funktionsfähigkeit des Tags auch auf Metall und in der Nähe von Wasser: Durch die Verwendung eines *Mount-on-Metal*-Tags kann der RFID-Tag auf metallischen Oberflächen verwendet werden. Die Auswahl einer

Frequenz im HF-Bereich ermöglicht beim Einsatz in der Nähe von Flüssigkeiten eine Reduktion der Lesefehler gegenüber einer Verwendung von Tags im UHF-Frequenzband.

- Mobile und stationäre Erfassung: Aufgrund des modularen Aufbaus kann der Prototyp für beide Erfassungsarten verwendet werden. Lediglich die Einbindung der verschiedenen APIs der Hersteller stellt eine gewisse Herausforderung an den Entwickler dar.

- ID elektronisch lesbar: RFID-Tags werden durch elektromagnetische Felder ausgelesen. Die Daten können anschließend elektronisch weiterverarbeitet werden.

- Zusätzliche Daten auf Tag oder Backend: Die verknüpften Daten werden zentral auf dem Backend abgelegt, weil dadurch Fehlerquellen verringert, die Datensicherheit erhöht und die Verwaltung der Berechtigungen vereinfacht wurde.

- Mehrfachverwendung der Container und des Datenspeichers: Nach einem Umlauf in dem Kreislauf kann der Container erneut verwendet werden. Die verknüpfte ID kann wiederum als Bindeglied zwischen Container und Daten fungieren.

- Kommunikation mit dem IT-System (Backend): Die mobilen Geräte können mit verschiedenen Zugangsarten auf den Web-Service zugreifen. Die Beschränkung liegt bei dem verwendeten Betriebssystem, dessen Konfiguration genutzt wird.

- Zugriff zu jeder Zeit und jedem Ort: Der Web-Server ist stets erreichbar und wird von den mobilen Geräten über private oder öffentliche Netzwerke erreicht.

- Zugriffsbeschränkungen der Daten: Die Daten auf dem Backend werden durch verschiedene Berechtigungen geschützt. Die ID auf dem Tag kann von jedem Leser ausgelesen werden.

- Integration in bestehende Systemlandschaft: Die empfangenen Daten werden über eine standardisierte Schnittstelle (SQL) für die nachgelagerten Systeme bereit gestellt.

- Speicherung der Historie eines Containers: Empfangene Datensätze werden bei der nächsten Erfassung nicht überschrieben, sondern bleiben in den Tabellen der Datenbank erhalten, so dass eine lückenlose Historie ermöglicht wird.
- Test auf Originalität der Container: Beim Empfang der Daten werden nur IDs der eigenen Container zugelassen. Ist die ID nicht bekannt, wird der Empfang abgelehnt.
- Zugriff des Backends auf Stammdaten der BIS: Aufgrund der Integration des Backends in die bestehenden Systeme, kann das Backend auf Daten anderer Betrieblicher Informationssysteme zugreifen. In dem Fall des Prototyps wurde dies jedoch nicht umgesetzt. Da keine weiteren Systeme zur Verfügung standen, wurden die Stammdaten in den Tabellen der eigenen Datenbank abgelegt.
- Verknüpfung von ID zu Auftrag oder Kunde: Jede ID eines Containers kann einem Kundenauftrag zugeordnet werden. Damit ist gleichzeitig auch die Zuordnung zu einem Kunden vollzogen.

11.1.2 Beantwortung der Forschungsfragen

In Kapitel 1.4 wurden fünf Fragen gestellt, die dazu dienen, grundlegende Erkenntnisse zu gewinnen. Diese Erkenntnisse werden nun durch Beantwortung der Forschungsfragen zusammengefasst:

1. Wo liegt bei der mobilen Erfassung der Unterschied zur der stationären Erfassung? Welcher Mehrwert kann entstehen? Wo liegen die Gefahren?

   Technisch gibt es keinen großen Unterschied zwischen der mobilen und stationären Erfassung. Die Unterschiede liegen in den Anwendungen und den verwendeten Prozessen. Viele Nachteile bei der mobilen Erfassung (Reichweite, Netzwerkverbindung, weniger Rechenkapazität) werden durch Vorteile gegenüber der stationären Erfassung ausgeglichen (Flexibilität, Größe, Gewicht). Der entscheidende Aspekt ist die Formulierung der exakten Anforderungen an die Erfassung der Objekte. Ziele und Anforderungen müssen vorab geklärt werden. Anschließend können die getroffenen Maßnahmen zur Erreichung dieser Ziele in die Geschäftsprozesse integriert werden.

2. Welche Architektur verspricht eine sinnvolle und flexible Anordnung der Komponenten? An welcher Stelle der Architektur sind die funktionalen Komponenten angesiedelt? Von welcher Komponente wird welche Information geliefert/empfangen und weitere Prozesse angestoßen?

   Die gewählte Architektur basiert auf Standard-Komponenten, die sich in verschiedene Systemlandschaften integrieren lassen. Das Medium Internet spielt dabei eine große Rolle. Dabei ist die Zugangsart zum Internet unerheblich. Durch die Einsatzmöglichkeiten in lokalen Funk-Netzwerken (WLAN) oder in öffentlichen Netzen (GPRS) kann der mobile Client an fast jedem beliebigen Ort benutzt werden.[290] Durch die Nutzung von weit verbreiteten Internet-Standards können die mobilen Geräte auf verschiedene Arten mit dem Backend kommunizieren. Web-Services werden auf Web-Servern eingesetzt, die ebenfalls weit verbreitet sind und eine stabile Grundlage bieten. Die Verteilung der funktionalen Komponenten wurde – so weit möglich – auf das Backend verlagert, damit der mobile Client entlastet wird.

3. Kann auf dem mobilen Gerät eine Anwendung entwickelt werden, die unabhängig von den verwendeten Hardware-Komponenten einsetzbar ist? Wie lässt sich diese Anwendung in einer komponentenbasierten Architektur realisieren?

   Der Aufbau der Anwendung ist in verschiedene Schichten unterteilt, so dass eine flexible Erweiterung möglich ist. Die Anbindung von weiteren Geräten und die Wartbarkeit ist dadurch nicht zu komplex. Die Anbindung der RFID-Hardware ist bisher noch nicht standardisiert. Jeder Hersteller entwickelt eigene APIs für die Integration in selbst geschriebene Programme. Deswegen kann noch keine Anwendung entwickelt werden, die jegliche RFID-Hardware einbindet. Die Client-Anwendung benötigt für jede neue, zu verwendende CF-Karte eine neue C#-Klasse.

4. Welche Sicherheitsaspekte sind bei der Kommunikation und den mobilen Datenträgern zu beachten?

[290] Beide Zugangsarten wurden im Verlauf der Arbeit erfolgreich getestet. Aufgrund der niedrigen, übertragenen Datenmengen kann auch die schmalbandige GPRS-Verbindung ohne Probleme genutzt werden.

Die verwendeten Ansätze versprechen durch Authentifikation und Verschlüsselung einen hohen Grad an Sicherheit vor dem Abhören der übertragenen Daten vom Client zum Backend. Die Kommunikation zwischen Leser und Tag ist jedoch nicht verschlüsselt. Da die Tag-IDs selbst nicht geschützt sind, kann diese Einschränkung in Kauf genommen werden. Ein Angreifer kann somit nur die Tag-ID lesen. Andere Daten, die zu dem Backend übertragen oder auf dem Backend gespeichert werden, bleiben für einen Angreifer fast unerreichbar.

5. Welche Einsatzszenarien im *Supply Chain Management* sind unter Berücksichtigung von wirtschaftlichen Aspekten denkbar?

   Die Einsatzgebiete für RFID verteilen sich über die gesamte Lieferkette. In dieser Arbeit wurden Beispiele angeführt, die die interne und interorganisationale Verwendung (geschlossene und offene Kreisläufe) beschreiben. Dazu kommen örtlich begrenzte (lokale) und unbegrenzte (globale) Kreisläufe, die auch zu einem Netz aus vielen verschiedenen Prozessen ausgebaut werden können. In den Kapiteln 2.3, 7.4 und 8.5 wurden etliche Beispiel zu den genannten Varianten aufgeführt. Nicht zuletzt beschreibt der exemplarische Geschäftsprozess „Avisierung von leeren Containern“ eine an die Praxis angelehnte Anwendungsmöglichkeit.

11.1.3 Weitere Erkenntnisse

Neben den Antworten auf die Forschungsfragen wurden weitere Erkenntnisse herausgearbeitet, die in verschiedenen Kapiteln bereits angesprochen wurden. Diese Erkenntnisse werden nun kurz zusammengefasst:

- Die Anforderungen an die Anwendungen entscheiden über den geeigneten Einsatz von RFID. Die RFID-Technologie alleine ist nicht immer die beste Lösung zur Identifikation von Objekten. Deswegen ist die sorgfältige Beachtung einer geeigneten Reihenfolge bei der Einführung von großer Bedeutung: Identifikation der strategischen Ziele (Motivation), Auflistung der Anforderungen, Identifikation der kritischen Prozesse, Auswahl möglicher Lösungsalternativen und schließlich die Auswahl der günstigsten Alternative.

- Die Auswahl des geeignetsten Systems ist jedoch nicht nur auf die Frage, ob RFID die richtige Lösung ist, begrenzt. Nach einer Entscheidung für RFID muss aus den vielen Möglichkeiten innerhalb RFID eine annehmbare Kombination gefunden werden. Die technische Vielfalt verlangt nach einer besonderen Beachtung der vielen RFID-Ausprägungen. Zusammenfassend kann also festgestellt werden, dass es zwei Stufen bei der Auswahl eines RFID-Systems gibt.

- Man kann zwischen zwei verschiedenen Ansätzen bei der Planung unterscheiden: Bei der anwendungsgetriebenen Vorgehensweise (Unternehmen, Anwender von Hard- und Software) werden – wie in dieser Arbeit beschrieben – zunächst die Anforderungen identifiziert und dann die RFID-Technik ausgewählt. Bei der technikgetriebenen Vorgehensweise (Forschung und Entwicklung, Hersteller von Hard- und Software) werden für vorhandene Technologien Einsatzgebiete gesucht und die Technologie in diesen Gebieten etabliert.

- Beim RFID-Einsatz sind noch nicht alle Probleme gelöst. Herausforderungen für die Zukunft sind die Kosten der Tags und Leser (Wirtschaftlichkeit, Kosten/Nutzen-Verhältnis), der Einsatz im industriellen Umfeld (Metall- und Wasserverträglichkeit), die Etablierung von Standards und Datenschutz und -sicherheit.

- Die breite Akzeptanz wird RFID erst erlangen, wenn eine umfassende Regelung des Datenschutzes und der Wahrung der Privatsphäre gefunden wird. Dazu gehört u. a. die Aufklärung des Verbrauchers und ausreichende Information über gekennzeichnete Waren. Die Hoffnung auf die Durchsetzung von Richtlinien und Gesetzen alleine wäre jedoch zu naiv.

- Die Entwicklung von Standards hat in den letzten Jahren zugenommen, so dass noch gute Aussichten auf weltweit anerkannte und weit verbreitete Standards bestehen. In den nächsten Versionen sollten stabile und anerkannte Standards entwickelt werden. Ein gutes Beispiel dafür ist die Konvergenz von Gen 2 und ISO 18000-6.

11.2 Offene Punkte

Die offenen, nicht in dieser Arbeit umgesetzten Inhalte können in verschiedene Kategorien unterteilt werden. Im ersten Teil der Arbeit konnte die Entwicklung der RFID-Standards nicht eindeutig eingeordnet werden. Das Problem dabei ist, dass Standardisierungsorganisationen oder Hersteller nicht voraussagen können, welcher Standard den endgültigen Durchbruch schaffen kann. Zum Zeitpunkt der Erstellung dieser Arbeit hat Gen 2 das größte Potential für die Etablierung eines Standards im UHF-Bereich. Jedoch sind Prognosen sehr schwierig zu treffen. Aus diesem Grund ist eine weitere Beobachtung der Standardisierungsbemühungen notwendig.

Im Mittelteil der Arbeit wurde eine Untersuchung der Wirtschaftlichkeit unternommen, die aufgrund fehlender verlässlicher Zahlen (als Grundlage für eine quantitative Berechnung) nur qualitativ ausfallen konnte. Die Kosten und der Nutzen des exemplarischen Geschäftsprozesses konnten somit nicht berechnet werden.

Im praktischen, letzten Teil wurden zwar alle Anforderungen erfüllt, jedoch könnten zusätzlich die folgenden, optionalen Funktionen ergänzt werden:

- Funktionen:
  - Implementierung weiterer RFID-Leser,
  - Auslagerung der Schleife bei der Erfassung und das Versenden der Daten in einem zweiten Thread (Versendung im Hintergrund als Alternative zu der realisierten Lösung),
  - Fenster der Client-Anwendung als Thread innerhalb des Prozesses und nicht als eigener Prozess,
  - Dynamische Anpassung der Fenster-Inhalte bei der Einblendung der Tastatur der Client-Anwendung,
  - Bearbeitung von einzelnen Datensätzen bei der Form `Versendung`: z. B. Löschen oder Ändern von Datensätzen.
- Robustheit:
  - Verbesserung der allgemeine Reife und Robustheit des Prototyps,
  - Prüfung und ggf. Aufbau der Bluetooth-Verbindung aus dem Code der Client-Anwendung.

- Sicherheit:
  - Verschlüsselung der Luftschnittstelle,
  - Authentifikation zwischen Tag und Leser.

11.3 Anschlußarbeiten

Das letzte Kapitel dieser Arbeit listet mögliche, nachfolgende theoretische Untersuchungen oder praktische Weiterentwicklungen des Prototyps auf. Teilweise könnten diese Arbeiten mit den offenen Punkten aus dem vorherigen Kapitel kombiniert werden.

- Kompatibilitätstest der bereits erstellten Komponenten mit Java-Clients oder Tomcat-Servern, z. B. das Zusammenspiel von SOAP-Nachrichten oder der Aufruf von Web-Services.
- Durchführung einer Wirtschaftlichkeitsanalyse anhand eines echten Geschäftsprozesses und realen Zahlen eines Unternehmens.
- Integration des Prototyps in eine bestehende Systemlandschaft. Dies könnte z. B. die SAP Auto-ID Infrastructure sein.

Literaturverzeichnis

[ACG 2003] : *ACG 13.56 MHz RF PC Handheld Reader Module*. WWW. Dezember 2003. – URL http://www.acg.de/synformation/servlet/ContentServlet/fsXzmRPA/pdfs/acg_German_RfPc_flyer.pdf. – Zugriffsdatum: 2006-06-25

[ACG 2005] ACG Identification GmbH: *Reader.DLL*. 3.2.0. November 2005. – Manual ReaderDLL v3.2.0 Rev1.0.pdf

[Baset und Schulzrinne 2004] Baset, S. A. ; Schulzrinne, H.: *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol*. WWW. September 2004. – URL http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf. – Zugriffsdatum: 2006-08-29

[BSI 2004] *Risiken und Chancen des Einsatzes von RFID-Systemen*. WWW. November 2004. – URL http://www.bsi.de/fachthem/rfid/RIKCHA_barrierefrei.pdf. – Zugriffsdatum: 2006-08-29. – Bundesamt für Sicherheit in der Informationstechnik

[CDT 2006] : *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology*. WWW. Mai 2006. – URL http://www.cdt.org/privacy/20060501rfid-best-practices.php. – Zugriffsdatum: 2006-08-29

[Chang 2005] Chang, G.: A Feasible Security Mechanism for Low Cost RFID Tags. In: *International Conference on Mobile Business (ICMB'05)*. Washington, DC, USA : IEEE Computer Society, 2005, S. 675–677

[CSCMP 2005] CSCMP: *SUPPLY CHAIN and LOGISTICS – TERMS and GLOSSARY*. WWW. Februar 2005. – URL

http://www.cscmp.org/Downloads/Resources/glossary03.pdf. – Zugriffsdatum: 2006-08-29

[Dunlap u. a. 2003] Dunlap, J. ; Gilbert, G. ; Ginsburg, L. ; Schmidt, P. ; J.Smith: *If You Build It, They Will Come: EPC™ Forum Market Sizing Analysis*. WWW. Februar 2003. – URL http://www.autoidlabs.org/uploads/media/ACN-AUTOID-BC007.pdf. – Zugriffsdatum: 2006-08-29

[Eicar 2006] : *Leitfaden: RFID und Datenschutz*. WWW. April 2006. – URL http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf. – Zugriffsdatum: 2006-08-29

[Environmental Studies 2006] : *Gefahren – Bedenken – Nachteile – Probleme bei RFID Technologien: Beschreibung – Erklärung – Informationen*. WWW. 2006. – URL http://www.environmental-studies.de/Info/RFID/RF-11/rf-11.html. – Zugriffsdatum: 2006-08-29

[EPC 2004] : *Hardware Certification Program*. WWW. August 2004. – URL http://www.epcglobalus.org/SubscriberResources/Ceritification%20Paper%20Final%208.27.04.pdf. – Zugriffsdatum: 2006-07-05

[EPC 2005] EPCglobal Inc™: *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*. Version 1.0.9. Januar 2005. – URL http://www.epcglobalus.org/dnn_epcus/KnowledgeBase/Browse/tabid/277/DMXModule/706/Command/Core_Download/Default.aspx?EntryId=292. – Zugriffsdatum: 2006-08-29

[EPC 2006a] EPCglobal Inc™: *EPCglobal Tag Data Standards*. Version 1.3. Mätz 2006. – URL http://www.epcglobalus.org/dnn_epcus/KnowledgeBase/Browse/tabid/277/DMXModule/706/Command/Core_Download/Default.aspx?EntryId=297. – Zugriffsdatum: 2006-08-29

[EPC 2006b] : *Komponenten*. WWW. April 2006. – URL http://www.gs1-germany.de/internet/content/produkte/epcglobal/rfid_epc/epcglobal_netzwerk/komponenten/index_ger.html. – Zugriffsdatum: 2006-08-29

[Erickson 2005] Erickson, G.: *SQL Browser and Online book Questions*. WWW. Dezember 2005. – URL http://www.mcse.ms/message2031885.html. – Zugriffsdatum: 2006-08-29

[EU 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*. WWW. Januar 2002. – URL http://europa.eu/eur-lex/pri/de/oj/dat/2002/l_031/l_03120020201de00010024.pdf. – Zugriffsdatum: 2006-08-29. – Amtsblatt der Europäischen Gemeinschaften

[FDA 2004] : *COMBATING COUNTERFEIT DRUGS – A Report of the Food and Drug Administration*. WWW. Februar 2004. – URL http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency. – Zugriffsdatum: 2006-08-29

[Fielding 2000] Fielding, R. T.: *Architectural Styles and the Design of Network-based Software Architectures*, University of California, Irvine, California, Dissertation, 2000. – Prof. Dr. Richard N. Taylor

[Finkenzeller 2002] Finkenzeller, K.: *RFID Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*. 3., aktualisierte und erweiterte Auflage. München : Hanser, 2002

[Fishkin und Roy 2003] Fishkin, K.P. ; Roy, S.: Enhancing RFID privacy via antenna energy analysis. In: *RFID Privacy Workshop, MIT.* (2003). – URL http://www.rfidprivacy.us/2003/papers/fishkin.pdf. – Zugriffsdatum: 2006-08-29

[Fleisch 2001] Fleisch, E.: Betriebswirtschaftliche Perspektiven des Ubiquitous Computing. In: Buhl, H. U. (Hrsg.) ; Huther, A. (Hrsg.) ; Reitwiesner, B. (Hrsg.): *Information Age Economy*. Heidelberg : Physica-Verlag, 2001, S. 177–191

[Fleisch u. a. 2003] Fleisch, E. ; Dierkes, M. ; Kickuth, M.: Ubiquitous Computing: Auswirkungen auf die Industrie. In: *Industrie Management* 6 (2003), S. 29–31

[Fleisch u. a. 2002] Fleisch, E. ; Mattern, F. ; Österle, H.: *Betriebliche Anwendungen mobiler Technologien: Ubiquitous Commerce*. WWW. Februar 2002. – URL http://www.m-lab.ch/pubs/WP2.pdf. – Zugriffsdatum: 2006-08-29

[Fowler 2002] Fowler, M.: *Patterns of Enterprise Application Architecture*. Boston, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 2002. – ISBN 0321127420

[Gao u. a. 2005] Gao, X. ; Xiang, Z. ; Wang, H. ; Shen, J. ; Huang, J. ; Song, S.: An Approach to Security and Privacy of RFID System for Supply Chain. In: *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*. Beijing, China : IEEE Computer Society, September 2005, S. 164–168

[Garfinkel u. a. 2005] Garfinkel, S. ; Juels, A. ; Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. In: *IEEE Security and Privacy* 3 (2005), Mai/Juni, Nr. 3, S. 34–43

[Gilbert 2006] Gilbert, G.: *Debunking 10 More Myths of RFID*. WWW. März 2006. – URL http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=1490&page=2. – Zugriffsdatum: 2006-08-29

[GS1 Germany 2005] : *Strichcodes*. WWW. Februar 2005. – URL http://www.gs1-germany.de/internet/content/produkte/ean/auto_id_systeme/strichcodes/index_ger.html. – Zugriffsdatum: 2006-08-29

[Harmon 2005] Harmon, C. K.: *The Emperor's New Clothes*. WWW. 2005. – URL http://aidc100.org/fileadmin/OCT_2005_Meetings/

PowerPoint_Presentations/Harmon.ppt. – Zugriffsdatum: 2006-08-29. – AIDC 100 „Truth in Technologies: Supply Chain RFID“. Stony Brook University, Long Island, NY

[Havens 2006] Havens, J. C.: *The RFID Item-Level Tagging Debate: UHF, HF or Something New?* WWW. April 2006. – URL http://www.aimglobal.org/members/news/templates/rw.asp?articleid=1060&zoneid=42. – Zugriffsdatum: 2006-08-29

[Heinemann und Rau 2003] Heinemann, F. ; Rau, C. ; B. Hochlehnert, SAP A. (Hrsg.): *SAP Web Application Server - Entwicklung von Web-Anwendungen*. Bonn : SAP Press, Galileo Press GmbH, 2003

[Hilty u. a. 2003] Hilty, Lorenz ; Behrendt, Siegfried ; Binswanger, Mathias ; Bruinink, Arend ; Erdmann, Lorenz ; Fröhlich, Jürg ; Köhler, Andreas ; Kuster, Niels ; Som, Claudia ; Würtenberger, Felix: *Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt*. WWW. August 2003. – URL http://www.izt.de/pdfs/pervasive/Vorsorgeprinzip_Informationsgesellschaft_Pervasive_Computing_Langfassung.pdf. – Zugriffsdatum: 2006-08-29. – Studie des Zentrums für Technologiefolgen-Abschätzung, TA-Swiss, TA 46/2003

[Hülsenbeck 2006] Hülsenbeck, F.: *RFID 2005 – Logistiktrends in Industrie, Dienstleistung und Handel*. WWW. 2006. – URL http://www.iwi.uni-hannover.de/trim/huelsenbeck.pdf. – Zugriffsdatum: 2006-08-29

[Hopper und Blum 2001] Hopper, N. J. ; Blum, M.: Secure Human Identification Protocols. In: *Lecture Notes in Computer Science* 2248 (2001), S. 52–66. – URL http://www.aladdin.cs.cmu.edu/papers/pdfs/y2001/secure_human_identification_protocols.pdf. – Zugriffsdatum: 2006-08-29

[IBM 2006] : *RFID Solution for Asset Tracking*. WWW. 2006. – URL http://www-5.ibm.com/de/pressroom/cebit/pressreleases/060307_2en.html. – Zugriffsdatum: 2006-08-29

[Kaps 2006] Kaps, R.: *Hersteller gründen Entwickler-Plattform für mobiles Linux*. WWW. Juni 2006. – URL http://www.heise.de/newsticker/meldung/74315. – Zugriffsdatum: 2006-08-29

[Komma 2006] Komma, M.: *Hertzscher Dipol*. WWW. 2006. – URL http://www.mikomma.de/fh/eldy/hertz.html. – Zugriffsdatum: 2006-08-29

[v. Kortzfleisch 2005] Kortzfleisch, H. v.: *Informationsmanagement II*. SS 2005. – Vorlesung Universität Koblenz-Landau

[Krcmar 2004] Krcmar, H.: *Informationsmangement*. 4. Auflage. Berlin : Springer, 2004

[Kroll 2005] Kroll, U.: *RFID - in der Praxis – Integration in IT Infrastrukturen und Anwendungsszenarien*. RFID – Radio Frequency Identification: „Potenziale – Strategien – Praxisbeispiele“. Juni 2005. – Eine Tagung der TRIM-Reihe, Universität Hannover, Institut für Wirtschaftsinformatik

[Kuri 2005] Kuri, J.: *Weltweiter PDA-Markt wächst um 25 Prozent*. WWW. Mai 2005. – URL http://www.heise.de/newsticker/meldung/59305. – Zugriffsdatum: 2006-08-29

[Kuri 2006] Kuri, J.: *Metro zeigt RFID auf der CeBIT*. WWW. Januar 2006. – URL http://www.heise.de/newsticker/meldung/68313. – Zugriffsdatum: 2006-08-29

[Lange 2005] Lange, V.: RFID: Anspruch und Wirklichkeit. In: *ident Jahrbuch 2005* (2005), Februar, S. 64–67. – URL http://www.ident.de/fileadmin/user_upload/ident_2005_JB/ident_JB_05a_RFID_IML.pdf. – Zugriffsdatum: 2006-08-29

[Libbenga 2004] Libbenga, J.: *Vatican Library adopts RFID*. WWW. Juli 2004. – URL http://www.theregister.co.uk/2004/07/09/vatican_library_rfid/. – Zugriffsdatum: 2006-08-29

[MA-1 Datori 2005] : *kein Titel*. WWW. 2005. – URL http://www.ma-1.lv/ftp/images/Palmtop/HP/ipaq_hx4700_F.jpg. – Zugriffsdatum: 2006-08-29

[McCullagh 2003] McCullagh, D.: *Are spy chips set to go commercial?* WWW. Januar 2003. – URL http://news.zdnet.com/2100-9595_22-980345.html. – Zugriffsdatum: 2006-08-29

[McDonald's 2004] : *McDonald's Schweiz Umweltbericht 2004 – Logistik*. WWW. 2004. – URL http://www.environment.mcdonalds.ch/de/logistik.shtml#verpackung. – Zugriffsdatum: 2006-08-29

[Michael und McCathie 2005] Michael, K. ; McCathie, L.: The Pros and Cons of RFID in Supply Chain Management. In: *International Conference on Mobile Business (ICMB'05)*. Washington, DC, USA : IEEE Computer Society, 2005, S. 623–629

[Microsoft 2005a] : *„Aspnet_wp.exe could not be started" error message when you view an ASP.NET page*. WWW. Juli 2005. – URL http://support.microsoft.com/kb/811320/EN-US/. – Zugriffsdatum: 2006-08-29

[Microsoft 2005b] : *How to repair IIS mapping after you remove and reinstall IIS*. WWW. September 2005. – URL http://support.microsoft.com/kb/306005/EN-US/. – Zugriffsdatum: 2006-08-29

[Microsoft 2005c] : *Login failed for user ‚username'. The user is not associated with a trusted SQL Server connection. (Microsoft SQL Server, Error: 18452)*. WWW. Juni 2005. – URL http://support.microsoft.com/kb/555332/EN-US/. – Zugriffsdatum: 2006-08-29

[Microsoft 2006a] : *Microsoft SQL Server Management Studio Express*. WWW. April 2006. – URL http://www.microsoft.com/downloads/details.aspx?displaylang=

de&FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796. – Zugriffsdatum: 2006-08-29

[Microsoft 2006b] : *SQL Server 2005 Onlinedokumentation*. WWW. Juli 2006. – URL http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=be6a2c5d-00df-4220-b133-29c1e0b6585f. – Zugriffsdatum: 2006-08-29

[Mintert 2005] Mintert, S.: Implementierung von Webservices REST vs. SOAP. In: *Wirtschaftsinformatik* 47 (2005), S. 63–65

[Mullen 2006] Mullen, D. P.: *RFID Viruses: Your Cat is Safe*. WWW. Mai 2006. – URL http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=887&zoneid=43. – Zugriffsdatum: 2006-08-29

[MySQL 2006] : *MySQL 5.0 Reference Manual :: 23 Connectors :: 23.2 Connector/NET*. WWW. 2006. – URL http://dev.mysql.com/doc/refman/5.0/en/connector-net.html. – Zugriffsdatum: 2006-08-29

[Navilock 2005] : *Bluetooth GPS-Empfänger BT-308*. WWW. März 2005. – URL http://www.navilock.de/download/PDFs/61259_-_DatenblattSLASHDatasheet/157. – Zugriffsdatum: 2006-08-29

[Nedden 2005] Nedden, B.: *Was sagt Was sagt der Datenschutz zu RFID?* WWW. Juni 2005. – URL http://www.iwi.uni-hannover.de/trim/NeddenVortrag%20RFID.pdf. – Zugriffsdatum: 2006-08-29

[News 2005] News, Transponder: *Interview with Mike Marsh, Trolley Scan's managing director*. WWW. Mai 2005. – URL http://rapidttp.com/transponder/interv1.html. – Zugriffsdatum: 2006-08-29

[O'Connor 2006] O'Connor, M. C.: *Wal-Mart Seeks UHF for Item-Level*. WWW. März 2006. – URL http://www.rfidjournal.com/article/articleview/2228/1/1/. – Zugriffsdatum: 2006-08-29

[Ohkubo u. a. 2003] Ohkubo, M. ; Suzuki, K. ; Kinoshita, S.: Cryptographic approach to a privacy friendly tag. In: *RFID Privacy Workshop* (2003), November. – URL http://www.rfidprivacy.us/2003/papers/ohkubo.pdf. – Zugriffsdatum: 2006-08-29

[Ohkubo u. a. 2005] Ohkubo, M. ; Suzuki, K. ; Kinoshita, S.: RFID Privacy Issues and Technical Challenges. In: *Communications of the ACM* 48 (2005), September, Nr. 9, S. 66–71

[Philips 2006] : *World's First Commercial Roll Out of Near Field Communication (NFC) Technology Simplifies Travel for Consumers.* WWW. April 2006. – URL http://www.semiconductors.philips.com/news/content/file_1233.html. – Zugriffsdatum: 2006-08-29

[RFC 3261 2002] Rosenberg, J. ; Schulzrinne, H. ; U., Columbia ; Camarillo, G. ; Johnston, A. ; Peterson, J. ; Sparks, R. ; Handley, M. ; Schooler, E.: *SIP: Session Initiation Protocol.* WWW. Juni 2002. – URL http://www.ietf.org/rfc/rfc3261.txt. – Zugriffsdatum: 2006-08-29

[RFID Update 2006a] : *The Industry Reacts to RFID Virus Research.* WWW. März 2006. – URL http://www.rfidupdate.com/articles/index.php?id=1077. – Zugriffsdatum: 2006-08-29

[RFID Update 2006b] : *Report: HF Wins First Round of RFID Frequency Battle.* WWW. März 2006. – URL http://www.rfidupdate.com/articles/index.php?id=1083. – Zugriffsdatum: 2006-08-29

[Rieback u. a. 2006] Rieback, M. R. ; Crispo, B. ; Tanenbaum, A. S.: *Is Your Cat Infected with a Computer Virus?* WWW. Mai 2006. – URL http://www.rfidvirus.org/papers/percom.06.pdf. – Zugriffsdatum: 2006-08-29

[Rindle 2006] Rindle, K.: *RFID in der Praxis – Anwendungen und Beispiele für RFID Systeme*. Transponder Roadshow 2006, Köln. März 2006. – IBC EUROFORUM GmbH

[Römer u. a. 2004] Römer, K. ; Schoch, T. ; Mattern, F.: Smart Identification Frameworks for Ubiquitous Computing Applications. In: *Wireless Networks* 10 (2004), S. 689–700

[Sarma u. a. 2003] Sarma, S. E. ; Weis, S. A. ; Engels, D. W.: RFID Systems and Security and Privacy Implications. In: *CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*. London, UK : Springer-Verlag, 2003, S. 454–469. – ISBN 3-540-00409-2

[SATO FlagTag 2006] : *SATO: unterstützt RFID Generation 2*. WWW. 2006. – URL http://www.ident.de/typo3temp/b07221c12b.jpg. – Zugriffsdatum: 2006-08-29

[Schüler 2006] Schüler, Dr. Hans-Peter: *Firma markiert Mitarbeiter per RFID*. WWW. Februar 2006. – URL http://www.heise.de/newsticker/meldung/69438. – Zugriffsdatum: 2006-08-29

[Schmidt 2006] Schmidt, P.: *RFID-Grundlagen*. Transponder Roadshow 2006, Köln. März 2006. – IBC EUROFORUM GmbH

[Siemens 2006] : *Locating, Responding, Optimizing in Real Time: RFID System for the Locating*. WWW. 2006. – URL http://www.automation.siemens.com/simatic-sensors/html_76/rfid-systeme_ortung.htm. – Zugriffsdatum: 2006-08-29

[ST 2006] : *Using the 64-bit UID in Contactless RFID Applications*. Februar 2006. – URL http://www.st.com/stonline/products/literature/an/12122.pdf. – Zugriffsdatum: 2006-08-29

[Strassner 2005] Strassner, M.: *RFID im Supply Chain Management – Auswirkungen und Handlungsempfehlungen am Beispiel der Automobilindustrie*. Wiesbaden : DUV, Oktober 2005

[Strassner und Fleisch 2005] Strassner, M. ; Fleisch, E.: Innovationspotential von RFID für das Supply-Chain-Management. In: *Wirtschaftsinformatik* 47 (2005), S. 45–54

[T. L. Ashford 2005] : *T. L. Asford – Barcode Software*. WWW. – URL http://www.tlashford.com/Images/compliance_labels/ODETTE.jpg. – Zugriffsdatum: 2006-08-29

[TI HF 2006] : *Tag-it™ HF-I Standard Inlays: rectangle-large*. WWW. 2006. – URL http://www.ti.com/rfid/graphics/productImages/hf-i_lg-rectangle.jpg. – Zugriffsdatum: 2006-08-29

[TI UHF 2006] : *Texas Instruments Gen 2 Inlay*. WWW. 2006. – URL http://www.ti.com/rfid/docs/manuals/pdfSpecs/epc_inlay.pdf. – Zugriffsdatum: 2006-08-29

[TRS 2006] : *Podiumsdiskussion*. Transponder Roadshow 2006, Köln. März 2006

[US Congress 2000] : *TRANSPORTATION RECALL ENHANCEMENT, ACCOUNTABILITY, AND DOCUMENTATION (TREAD) ACT*. WWW. 2000. – URL http://www.nhtsa.dot.gov/nhtsa/Cfc_title49/publ414.106.pdf. – Zugriffsdatum: 2006-08-29

[VeriSign 2005] : *Securing RFID Data for the Supply Chain*. WWW. 2005. – URL http://www.verisign.com/static/028573.pdf. – Zugriffsdatum: 2006-08-29

[Völker u. a. 2003] Völker, J. ; Knobloch, H.-J. ; Schmidt, Dr. A.: *SSL-Studie – Referenzanwendungen, Analyse, Tests, Zertifizierungshierarchie, Konzeptentscheidungen*. WWW. Januar 2003. – URL http://www.bsi.bund.de/fachthem/verwpki/dokumente/BSI-SSL-Studie_34.pdf. – Zugriffsdatum: 2006-08-29

[Walk 2006] Walk, E.: RFID Standards 2006. In: *ident Jahrbuch 2006* (2006), Mai, S. 54–61. – URL http://ident.de/fileadmin/user_upload/ident_2006_JB/ident_JB_06a_Standards.pdf. – Zugriffsdatum: 2006-08-29

[Weinstein 2005] Weinstein, R.: RFID: A Technical Overview and Its Application to the Enterprise. In: *IT Professional* 7, Issue 3 (2005), Mai/Juni, S. 27–33

[Weis 2005] Weis, S. A.: Security Parallels between People and Pervasive Devices. In: *PERCOMW '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*. Washington, DC, USA : IEEE Computer Society, 2005, S. 105–109. – ISBN 0-7695-2300-5

[Weis u. a. 2004] Weis, S. A. ; Sarma, S. E. ; Rivest, R. L. ; Engels, D. W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: *Security in Pervasive Computing* Bd. 2802, 2004, S. 201–212

[Weiss und Müller 2005] Weiss, H. ; Müller, D.: *Übersehene Gefahr: RFID-Chips verseuchen das Trinkwasser*. WWW. Dezember 2005. – URL http://www.zdnet.de/itmanager/tech/0,39023442,39139086,00.htm. – Zugriffsdatum: 2006-08-29

[Yang und Jarvenpaa 2005] Yang, G. ; Jarvenpaa, S. L.: Trust and Radio Frequency Identification (RFID) Adoption within an Alliance. In: *HICSS '05: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 7*. Washington, DC, USA : IEEE Computer Society, 2005, S. 208.1. – ISBN 0-7695-2268-8-7

[Ziegler 2005] Ziegler, Peter-Michael: *Palm sattelt auf Windows um [Update]*. WWW. September 2005. – URL http://www.heise.de/newsticker/meldung/64277. – Zugriffsdatum: 2006-08-29