

Master Thesis

im Rahmen des
Universitätslehrganges „Geographical Information Science & Systems“
(UNIGIS MSc) am Zentrum für GeoInformatik (Z_GIS)
der Paris Lodron-Universität Salzburg

zum Thema

„Potentiale der Echtzeitortungssysteme für Energieversorgungsunternehmen

Beispiel einer Sicherheitslösung für
Kraftwerksbegehungen“

vorgelegt von

Dipl.-HTL-Ing. Manfred Farthofer, MAS(GIS)
U644, UNIGIS MSc Jahrgang 2007

Zur Erlangung des Grades
„Master of Science (Geographical Information Science & Systems) – MSc(GIS)“

Gutachter:
Ao. Univ. Prof. Dr. Josef Strobl

Henndorf, 28.12.2009

Danksagung

Als ich mich am Beginn der Arbeit mit dem Thema Echtzeitortungssysteme (Real Time Locating Systems, RTLS) erstmals auseinandergesetzt habe, war ich beeindruckt vom Einsatz dieser Technologie in anderen Branchen. Eine erste Internetrecherche ergab dann, dass es zwar eine Vielzahl von Dokumenten zu diesem Thema, allerdings nur einige wenige mit Bezug zu Energieversorgungsunternehmen (EVU) gab.

Ich nahm daraufhin Kontakt mit einem Unternehmen in der RTLS-Branche, der Firma Geodan in Salzburg auf. Herr Dipl. Ing. Dirk Schmidt, Geodan Salzburg, konnte meinen Eindruck, dass RTLS in EVU kaum eingesetzt werden, auch durch seine Berufserfahrung bestätigen. Ihm möchte ich in diesem Zusammenhang herzlich danken, dass er mich thematisch und inhaltlich mit Unterlagen, und auch durch einige persönliche Gesprächstermine, unterstützt hat.

Je mehr ich mich mit dem Thema auseinandergesetzt hatte, umso mehr reifte die Überzeugung, dass RTLS auch in EVU in zahlreichen Prozessen gewinnbringend angewendet werden könnten. Die Diskussion mit unseren internen fachlichen Verantwortlichen ergab, dass es einige Ansatzpunkte für den Einsatz der RTLS-Technologie im Kraftwerks- und im Servicebereich gibt. Mein besonderer Dank gilt dabei Herrn Dipl. Ing. Tscherne, Leiter des Bereiches Kraftwerke in der Salzburg AG, und Herrn Ing. Franz Zillner, mit dem ich das Sicherheitssystem diskutieren durfte.

Weiters danke ich Herrn Nicola Karl, Ubisense München, der mich mit praktischen Informationen zum Einsatz von Ultra Wideband, UWB, unterstützt hat und Herrn Dr. Walter Rieder fürs Korrekturlesen der Arbeit und für die Tipps zur Verbesserung.

Eigenständigkeitserklärung

Ich versichere, diese Master Thesis ohne fremde Hilfe und ohne Verwendung anderer als der angeführten Quellen angefertigt zu haben, und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat.

Alle Ausführungen der Arbeit, die wörtlich oder sinngemäß übernommen wurden sind entsprechend gekennzeichnet.

Henndorf, den 28. Dezember 2009

Zusammenfassung

Echtzeitortungssysteme (Real Time Locating Systems, RTLS) werden in unterschiedlichen Branchen mit Erfolg eingesetzt. Die Energieversorgungsunternehmen (EVU) gelten bislang nicht als Hauptzielgruppe für den Einsatz der RTLS-Technologie. Dies bestätigte auch die Umfrage über den Einsatz von RTLS in EVU in Österreich, die im Rahmen dieser Arbeit durchgeführt wurde.

Der Autor möchte in der vorliegenden Arbeit aufzeigen, dass RTLS-Lösungen auch in EVU mit Erfolg eingesetzt werden können. Dazu werden einführend die Grundlagen der RTLS-Technologie beleuchtet, und die Vor- und Nachteile der einzelnen Technologien herausgearbeitet. Auf Basis konkreter Lösungen wird untersucht, ob die Lösungsansätze auf die EVU-Branche übertragen werden können.

In allgemeinen Lösungsszenarien und im Besonderen am Beispiel einer Sicherheitslösung für Kraftwerksbegehungen wird gezeigt, dass die RTLS-Technologie auch für Prozesse in EVU wesentlichen Nutzen bringt. Dazu wurde für Begehungen im Rahmen des Betriebes eines Wasserkraftwerkes eine Lösung konzipiert, die durch die Kombination von Indoor- und Outdoor-Tracking die Arbeitssicherheit von Servicemitarbeitern in Kraftwerken deutlich erhöhen kann. Dabei liegt der Fokus auf der Konzeption der Lösung und nicht auf der praktischen Lösungseinführung.

Abschließend wird das Thema Privatsphäre (Privacy) in Zusammenhang mit RTLS diskutiert. Privacy ist ein entscheidendes Kriterium für die Akzeptanz der Lösungen im Berufseinsatz. Nur wenn es gelingt die Balance zwischen Aufgabe von Bereichen der Privatsphäre und erzielbarem Nutzen (auch persönlichem Nutzen wie z.B. mehr Sicherheit) zu finden, wird die Technologie in erfolgreichen Projekten Akzeptanz finden.

Abstract

Real Time Locating Systems (RTLS) are successfully deployed in different industries. Utility companies are currently not the main target group for RTLS. The survey in utility companies of Austria, performed within the scope of this paper, yield to the same result.

The author of this paper likes to show, that RTLS-solutions can be implemented with broad benefit in utility companies too. First this paper analyses, how RTLS-technology works, and discusses the pros and cons of various RTLS-technology. Based on implemented solutions the transferability to the processes in utility companies will be verified.

This paper shows some examples of use cases in utility companies in general, and one example of a safety solution in the maintenance of power plants in detail. Using a combination of indoor tracking and outdoor tracking it is possible, to substantially increase the safety of the service staff in the operation of water plants. The aim of this work is, to describe a concept of the safety solution and not the implementation of the system itself.

Finally this paper discusses the influences of RTLS in the field of privacy of the involved employees. Privacy is a critical point for the acceptance of RTLS. The systems will find acceptance only, if the balance between loss of privacy and rise of benefit (especially the benefit for the employees too) can be found.

Inhaltsverzeichnis

DANKSAGUNG	II
EIGENSTÄNDIGKEITSERKLÄRUNG	III
ZUSAMMENFASSUNG	IV
ABSTRACT	V
INHALTSVERZEICHNIS	VI
ABBILDUNGSVERZEICHNIS	IX
TABELLENVERZEICHNIS	X
ABKÜRZUNGSVERZEICHNIS	XI
1. EINFÜHRUNG	1
1.1. MOTIVATION, AUSGANGSLAGE	1
1.2. FRAGESTELLUNGEN	3
1.3. ZIELSETZUNGEN UND VORGEHEN	4
1.4. NICHTZIELE	5
1.5. BEGRIFFSERKLÄRUNGEN	5
2. GRUNDLAGEN	8
2.1. METHODEN ZUR POSITIONSBESTIMMUNG	8
2.1.1. <i>Angle of Arrival (AoA)</i>	8
2.1.2. <i>Line of Sight (LoS)</i>	9
2.1.3. <i>Time of Arrival (ToA) bzw. Time of Flight (ToF)</i>	9
2.1.4. <i>Time Difference of Arrival (TDoA)</i>	9
2.1.5. <i>Received Signal Strength Indication (RSSI)</i>	10
2.1.6. <i>Received Channel Power Indicator (RCPI)</i>	10
2.1.7. <i>Visuelle Verfahren</i>	10
2.1.8. <i>Cell of Origin (CoO)</i>	11
2.1.9. <i>Methoden für die Positionsbestimmung in Innenräumen</i>	12
2.2. KOMMUNIKATIONSNETZWERKE.....	13
2.2.1. <i>Mobiltelefonie</i>	14
2.2.2. <i>Wireless-LAN</i>	22
2.2.3. <i>Bluetooth</i>	25
2.2.4. <i>ZigBee</i>	27
2.2.5. <i>Infrarot IrDA</i>	29
2.3. RFID	30
2.3.1. <i>Allgemeines</i>	30
2.3.2. <i>Vorteile von RFID</i>	31
2.3.3. <i>Arten von RFID-Systemen</i>	32
2.3.4. <i>Datenfluss bei RFID-Tags</i>	33
2.3.5. <i>Pulkfähigkeit</i>	33
2.3.6. <i>Bauformen</i>	33
2.3.7. <i>Vergleich verschiedener RFID-Systeme</i>	34
2.3.8. <i>Standardisierung</i>	35
2.3.9. <i>EPC Global</i>	35
2.3.10. <i>Sicherheit in Zusammenhang mit RFID-Systemen:</i>	36
2.3.11. <i>Schlussfolgerung</i>	36
2.4. TECHNOLOGIEN ZUR POSITIONSBESTIMMUNG	36
2.4.1. <i>Arten von Positionsdaten</i>	36
2.4.2. <i>Raumbezugssystem, Koordinatensystem</i>	37
2.4.3. <i>Technologien zur Positionsbestimmung</i>	38

2.4.4.	Satellitennavigation	39
2.4.5.	Positionsbestimmung innerhalb von Gebäuden	43
2.4.6.	Netzwerkgestützte Verfahren	45
2.4.7.	Vergleich verschiedener Technologien	50
2.4.8.	Schlussfolgerung für die konzipierte Sicherheits-Lösung.....	51
2.5.	PRIVACY	53
2.5.1.	Was ist Privacy?.....	53
2.5.2.	Privacy als Menschenrecht oder Wirtschaftsgut?	54
2.5.3.	Was sind personenbezogene Daten?	55
2.5.4.	Datenschutz in Zusammenhang mit RFID und Ortsinformationen.....	56
2.5.5.	Datenschutzgesetze in Österreich und in Deutschland.....	56
2.5.6.	Beurteilungsschema für Geodaten	57
2.5.7.	Bedeutung der Geoinformation für die Privacy.....	58
2.5.8.	Wahrnehmung und Akzeptanz in der Öffentlichkeit	60
3.	LITERATURÜBERBLICK	63
3.1.	PRAKTISCHE PROJEKTE ZUR POSITIONSBESTIMMUNG IN GEBÄUDEN	63
3.1.1.	Active Badge.....	63
3.1.2.	WIPS	63
3.1.3.	Active Bat	64
3.1.4.	Cricket.....	64
3.1.5.	Radar	65
3.1.6.	Spot ON	66
3.1.7.	Magic Map und GRIPS.....	66
3.1.8.	IMAPS	67
3.1.9.	Weitere.....	67
3.2.	MARKTLÖSUNGEN	68
3.2.1.	Beispiel für ein UWB-System; System der Firma Ubisense	68
3.2.2.	Beispiel für ein Wi-Fi-System; System von Ekahau	69
3.2.3.	UWB-Ortung für Personensicherheit bei AREVA	70
3.2.4.	Verfolgung von Warenströmen mit RFID	70
3.2.5.	Hybrides RTLS in der Automobil-Branche	71
4.	ANWENDUNGSSZENARIEN IN EVU	73
4.1.	GRUNDSÄTZLICHE ANMERKUNGEN	73
4.2.	KRAFTWERKSBETRIEB	73
4.3.	LAGERWIRTSCHAFT	74
4.4.	ASSET-MANAGEMENT	75
4.5.	WORKFORCE-MANAGEMENT (WFM).....	78
4.6.	UMFRAGE RTLS UNTER EVU IN ÖSTERREICH	82
5.	KONKRETE LÖSUNG: SICHERHEITSLÖSUNG FÜR KRAFTWERKSBEGEHUNGEN	87
5.1.	INFORMATIONEN ZUM KRAFTWERK URSTEIN	87
5.2.	GRUNDLEGENDE ANFORDERUNGEN AN DIE LÖSUNG.....	89
5.3.	PROZESS-ANFORDERUNGEN AN DEN KONTROLLGANG	90
5.3.1.	Grundsätzlicher Prozessablauf.....	90
5.3.2.	Kontrollgang.....	91
5.4.	KONZIPIERTE LÖSUNG	93
5.4.1.	Grundsätzliche Gesichtspunkte	93
5.4.2.	Variante WLAN-Lokalisierung	93
5.4.3.	Variante UWB.....	95
5.4.4.	Gewählte Lösung.....	95
5.5.	KOSTENVERGLEICH UNTERSCHIEDLICHER LÖSUNGSVARIANTEN FÜR DIE KRAFTWERKSBEGEHUNG	111
5.6.	AUSWIRKUNGEN DER LÖSUNG AUF DIE PRIVACY, BETRIEBSVEREINBARUNG	113
6.	ERGEBNISSE UND SCHLUSSFOLGERUNGEN	117

6.1.	BEWERTUNG	117
6.2.	GRENZEN UND EINSCHRÄNKUNGEN.....	119
6.3.	AUSBLICK	120
ANHANG OPENLS		122
LITERATURVERZEICHNIS		125

Abbildungsverzeichnis

Abbildung 1: IT-Infrastruktur Salzburg AG	2
Abbildung 2: Struktur der Arbeit	4
Abbildung 3: Methoden der Positionsbestimmung.....	8
Abbildung 4: Verbesserung der Genauigkeit beim CoO-Verfahren durch Zellüberlappung	11
Abbildung 5: Chokepoints and Transit	12
Abbildung 6: Näherungsmethode	12
Abbildung 7: Coordinates	13
Abbildung 8: Hot-Spots	13
Abbildung 9: Klassifizierung drahtlose Kommunikationssysteme.....	14
Abbildung 10: Handybesitz bei Kindern und Jugendlichen in Deutschland; Angaben in %	15
Abbildung 11: Zellengrößen bei UMTS	21
Abbildung 12: WLAN-Netzwerkstruktur	24
Abbildung 13: Bluetooth-Piconet	26
Abbildung 14: ZigBee-Vernetzung.....	28
Abbildung 15: Prinzip der induktiven Kopplung.....	32
Abbildung 16: RFID-Frequenzen und maßgebliche Standards	35
Abbildung 17: Verfahren zur Positionsbestimmung.....	38
Abbildung 18: Ortungs- und Identifikationstechnologien	38
Abbildung 19: UWB-Charakteristik	49
Abbildung 20: Inhaltliche Dimensionen von Privacy	55
Abbildung 21: Beurteilungsschema "Sind Geodaten personenbezogene Daten?"	58
Abbildung 22: Feldstärkenverteilung; Beispiel Ekahau	69
Abbildung 23: Mit RFID ausgerüsteter Gabelstapler	71
Abbildung 24: Hybrides RTLS mit RFID und GPS	72
Abbildung 25: Nutzen RFID-gestütztes Asset Management.....	78
Abbildung 26: Wirtschaftlichkeitsberechnung, Darstellung ROI-Dauer.....	82
Abbildung 27: Umfrageergebnis Einsatz von RTLS-Lösungen in EVU in Österreich..	83
Abbildung 28: Kraftwerk Urstein	87
Abbildung 29: Lage KW Urstein	88
Abbildung 30: Prozess Kontrollgang KW Urstein	90
Abbildung 31: Grundsätzliche Lösung	96
Abbildung 32: Movida Software-Architektur.....	100
Abbildung 33: Sicherheitskonzept: VPN-Einbindung ins Firmennetzwerk	101
Abbildung 34: Alarmierung Flussdiagramm Teil 1	105
Abbildung 35: Alarmierung Flussdiagramm Teil 2	106
Abbildung 36: Alarmierung Flussdiagramm Teil 3	107
Abbildung 37: Flussdiagramm Auslöse Warnmeldung Außenbereich.....	108
Abbildung 38: Kostenvergleich Sicherheitssystem	112
Abbildung 39: Zusammenhang OpenLS mit weiteren Standards.....	122
Abbildung 40: Grundsätzlicher Ablauf OpenLS Request/Response	123
Abbildung 41: Verlauf einer OpenLS-Serviceanfrage.....	124

Tabellenverzeichnis

Tabelle 1: Klasseneinteilung der Bluetoothgeräte	25
Tabelle 2: Vergleich RFID-Systeme	34
Tabelle 3: Erreichbare Genauigkeiten bei GPS	41
Tabelle 4: Vergleich von RTLS-Technologien	50
Tabelle 5: Vergleich IrDA, RFID und Bluetooth für die Positionsbestimmung	51
Tabelle 6: Eignung unterschiedlicher Technologien für die konzipierte Lösung	52
Tabelle 7: Technische Daten KW Urstein	88

Abkürzungsverzeichnis

ACL	Asynchronous Connection Less
ADT	Abstract Data Types
A-GPS	Assisted-GPS
AoA	Angle of Arrival
AP	Access Point
API	Application Programming Interface
APOS	Austrian Positioning Service
BSC	Base Station Controller
BSS	Base Station Subsystem, Basic Service Set
BTS	Base Transceiver Station
CAD	Computer Aided Design
CDMA	Code-Division Multiple-Access
CoO	Cell of Origin
CRS	Coordinate Reference System
CS	Coordinate System
DGPS	Differential GPS
DMS	Dokumenten Managementsystem
DPS	DECT Positioning System
EAI	Enterprise Applikation Integration
ECG	Energie-Control-GmbH
EDGE	Enhanced Data Rates for GSM Evolution
EDV	Elektronische Datenverarbeitung
EGNOS	European Geostationary Navigation Overlay Service
E-OTD	Enhanced Observed Time Difference
EPC	Electronic Product Code
EPOF	European Privacy Officers Forum
EPSG	European Petroleum Survey Group Geodesy
ERP	Enterprise Ressource Planning
ESS	Extended Service Set
ETSI	European Télécommunication Standards Institute
EU	Europäische Union
EVU	Energieversorgungsunternehmen
FFD	Full Function Device
GIS	Geografisches Informations System
GLONASS	GLObal NAVigation Satellite System
GMS	GeoMobility Servers
GMSK	Gaussian Minimum Shift Key
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRIPS	Generic Radio-based Indoor Positioning System
GSM	Global System for Mobile Communications bzw. ursprünglich Group Special Mobile
GSN	GPRS Support Nodes
HF	High Frequency
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol

IEEE	Institute of Electrical and Electronics Engineers
IMT-2000	International Mobile Telecommunications at 2000MHz
IP	Internet Protocol
IrDA	Infrared Data Association
ISM	Industrial, Scientific, Medical
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Informationstechnologie
ITU	International Telecommunications Union
JIM	Jugend, Information (Multi)-Media
KW	Kraftwerk
LAC	Location Area Code
LAI	Location Area Identity
LAN	Local Area Network
LBS	Location Based Services
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LF	Low Frequency
LMU	Location Measurement Unit
LoS	Line of Sight
MAM/MAU	Mobile Asset Management / Mobile Asset Management for Utilities
MCC	Mobile Country Code
MGI	Militär-Geographisches Institut
MIT	Massachusetts Institute of Technology
MNC	Mobile Network Code
MPS	Mobile Positioning System
MSAS	Multi-Functional Satellite Augmentation System
MS	Mobile Station
MSC	Mobile Switching Center
OECD	Organisation for Economic Co-operation and Development
OGC	Open Geospatial Consortiums
OMC	Operation and Maintenance Center
OMSS	Operation and Maintenance Subsystem
OpenLS	OpenGIS Location Service
PDA	Personal Digital Assistant
PKW	Personenkraftwagen
RAN	Radio Access Network
RCPI	Received Channel Power Indicator
RFD	Reduced Function Device
RFID	Radio Frequency Identification
ROI	Return on Investment
RSSI	Received Signal Strength Indication
RTLS	Real Time Locating System
SA	Selective Availability
SAPOS	Satellitenpositionierungsdienst der deutschen Landesvermessung
SBAS	Satellite Based Augmentation System
SCO	Synchronous, Connection Oriented
SIG	Bluetooth Special Interest Group
SMLC	Serving Mobile Location Center
SMS	Short Messages Service
SMSS	Mobile Switching and Management Subsystem

SOA	Service Oriented Architecture
TA	Time Advance
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TDoA	Time Differenz of Arrival
ToA	Time of Arrival
ToF	Time of Flight
UHF	Ultra High Frequency
UMTS	Universal Mobile Telekommunication System
USA	United States of America
U-TDOA	Uplink-Time Difference of Arrival
UTC	Universal Time Coordinated
UTRAN	UMTS Terrestrial Radio Access Network
UWB	Ultra-Wideband
VPN	Virtual Private Network
WAN	Wide Area Network
WAAS	Wide Area Augmentation System
W-CDMA	Wideband Code Division Multiple Access
WFM	Workforce Management
WFMS	Workforce Management System
Wi-Fi	Wireless Fidelity
WIPS	Wireless Indoor Positioning System
WLAN	Wireless Local Area Network
WORM	Write Only, Read Many
WPAN	Wireless Personal Area Network
XML	Extensible Markup Language
16QAM	16 Quadratur Amplitude Modulation
8PSK	8 Phase Shift Key

1. Einführung

1.1. Motivation, Ausgangslage

In Energieversorgungsunternehmen (EVU) werden seit vielen Jahren umfangreiche unterschiedliche EDV-Lösungen für die Optimierung der Prozesse eingesetzt. Der Druck der Liberalisierung der Energiewirtschaft („Unbundling“)¹ durch entsprechende EU-Richtlinien² und in der Folge durch nationale Energiewirtschaftsgesetze brachte die weitere Intensivierung der Investitionen in die IT-Infrastruktur mit sich (vgl. WAGNER, R. et al (2005)).

EDV-Themen bei EVU sind vor allem ERP³-Lösungen (bei vielen EVU ist dies SAP⁴), sowie GIS⁵ und Prozessrechnersysteme für den technischen Bereich. Neben diesen Hauptsystemen gibt es noch weitere wichtige Lösungen wie Workforce Managementsysteme (WFMS) und Dokumenten Managementsysteme (DMS). Beispielshaft möchte ich hier die IT-Landschaft der Salzburg AG⁶ anführen (siehe Grafik weiter unten).

Neben der Zahl der Systeme, ist ein Hauptpunkt auch die Integration der verschiedenen IT-Lösungen. Die Integration soll dazu beitragen, dass die Prozesse durchgehend ohne Medienbrüche mit IT-Lösungen unterstützt werden können. Aktivitäten wurden vielfach unter dem Begriff Enterprise Applikation Integration (EAI) gebündelt. Wesentliche Vorteile der Integration sind (vgl. MARKO, T., SCHMIDLE, M. (2004)):

- Durchgehende Prozessunterstützung; Transparente Prozesse
- Vermeidung von Medienbrüchen
- Vermeidung von redundanter Datenführung bzw. kontrollierte Redundanz
- Verringerung der Datenerfassungsaufwendungen
- Verringerung der Fehlerkorrekturaufwendungen, weil weniger Fehler
- Weitere Automatisierung

¹ Unbundling ist die rechtliche, organisatorische und informelle Entflechtung der Energieversorgung in Erzeugung und Netzinfrastruktur

² Richtlinie 96/92/EG des Europäischen Parlaments und des Rates betreffend gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt vom 19. Dezember 1996

³ ERP = **E**nterprise **R**essource **P**lanning

⁴ SAP = Eine bekannte ERP-Software; in der Energieversorgungsbranche eindeutiger Marktführer (Eigenangabe SAP)

⁵ GIS = **G**eografisches **I**nformations **S**ystem

⁶ Die Salzburg AG für Energie, Verkehr und Telekommunikation, kurz Salzburg AG, ist der Energie- und Verkehrsdienstleister im Bundesland Salzburg in Österreich.

- Bessere Informationsbereitstellung

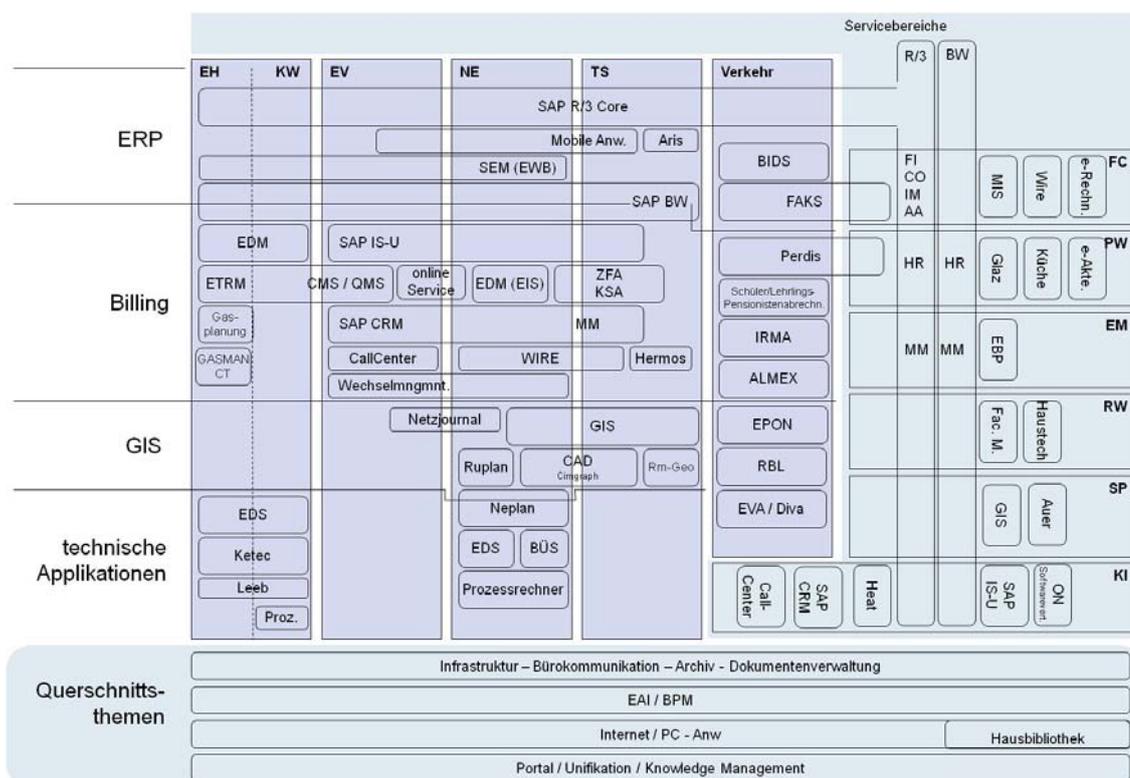


Abbildung 1: IT-Infrastruktur Salzburg AG

Quelle: Salzburg AG, BOCK, W. (2009)

Eine ganz wesentliche Komponente für die Verbesserung der Abläufe ist auch die zunehmende „Mobilisierung“ der Prozesse (vgl. DUTTA, S. (2008)). Dies ist auch ein Kernpunkt der Aktivitäten der letzten Jahre (seit 2006) in der Salzburg AG. Bei der Mobilisierung der Prozesse hat die geografische Information (die Position) eine besondere Bedeutung.

Die verschiedenen Betriebsmittel sind an bestimmten geografischen Positionen situiert, Arbeitsaufträge sind geografischen Positionen (z.B. Adressen) zugeordnet und auch die Kunden sind auf geografische Positionen abgebildet. Dementsprechend ist eine Reihe von Anwendungen in Betrieb, die mit der geografischen Position arbeiten. Dazu zählen insbesondere:

- Mobiles GIS in Verbindung mit GPS und Positionierung entsprechend der aktuellen GPS-Position.
- Mobile Datenerfassung auf MAM/MAU⁷-Basis in Verbindung mit der geografischen Position der Assets.

⁷ MAM/MAU = **M**obile **A**ssset **M**anagement / **M**obile **A**ssset Management for **U**tilities; Software-Lösung von SAP für mobile Prozesse

- Navigationslösung auf Basis von Standardnavigationssystemen (Tom Tom) mit Navigation zu den Standorten der Betriebsmittel. Hier sind die wichtigsten Betriebsmittel als „Points of Interest, POI“ direkt im Navigationssystem verfügbar.

In EVU noch kaum in Verwendung sind jedoch RTLS⁸-Lösungen, speziell Lösungen für die Positionsbestimmung in Innenbereichen. Hingegen wird diese Technologie in diversen anderen Branchen seit einigen Jahren sehr erfolgreich eingesetzt. Dies belegen zahlreiche Fallstudien, speziell für die Logistikbranche und Produktionsindustrie. Einige Beispiele dazu werden im Kapitel 3.2 dargestellt (vgl. z.B. Scholz-Reiter, B. (2007)).

Die vorliegende Arbeit hat zum Inhalt die technischen Grundlagen aufzuzeigen, ausgewählte Lösungen anderer Branchen zu untersuchen, und auf die Übertragbarkeit in das EVU-Umfeld zu beleuchten. Insbesondere spielen dabei die Gesichtspunkte der Einsetzbarkeit, Übereinstimmung mit und Nutzungsmöglichkeiten von bestehender Infrastruktur sowie wirtschaftliche Gesichtspunkte eine Rolle.

Die persönliche Motivation für die Wahl des Themas RTLS für die Arbeit liegt darin, dass der Autor der Arbeit seit mehreren Jahren bei Veranstaltungen im EVU-Umfeld von Themen wie RFID und auch RTLS gehört hat, ohne aber einen breiten Einsatz dieser Technologie bei den EVU erkennen zu können. Mit der detaillierten Beschäftigung mit diesen Technologien möchte der Autor konkrete Einsatzszenarien in EVU im Allgemeinen und für die Salzburg AG im Besonderen entwerfen.

1.2. Fragestellungen

In dieser Arbeit soll gezeigt werden, dass die RTLS-Technologie auch für Energieversorgungsunternehmen (EVU) entscheidende Vorteile für die Prozesse bringt. Dazu werden verschiedene Szenarien beleuchtet und für Anwendungsgebiete mögliche technische Lösungen skizziert.

Dazu sollen in der Arbeit folgende Fragen evaluiert werden:

- Welches sind Anwendungsszenarien in EVU, die mit RTLS unterstützt werden können? Welches sind die Kriterien hierfür, und welchen Nutzen bringt der Einsatz der RTLS-Technologie hierfür?

⁸ RTLS = Real Time Locating System

- Wie wirkt sich der Einsatz der RTLS-Technologie auf die Privatsphäre der Mitarbeiter aus?
- Werden bei anderen EVU in Österreich RTLS eingesetzt, und wie sind die Erfahrungen mit den Lösungen?
- Welche Verbesserungen bringt der Einsatz der RTLS-Technologie als Sicherheitssystem in Zusammenhang mit Kraftwerksbegehungen, und wie könnte eine solche Sicherheitslösung aussehen?

1.3. Zielsetzungen und Vorgehen

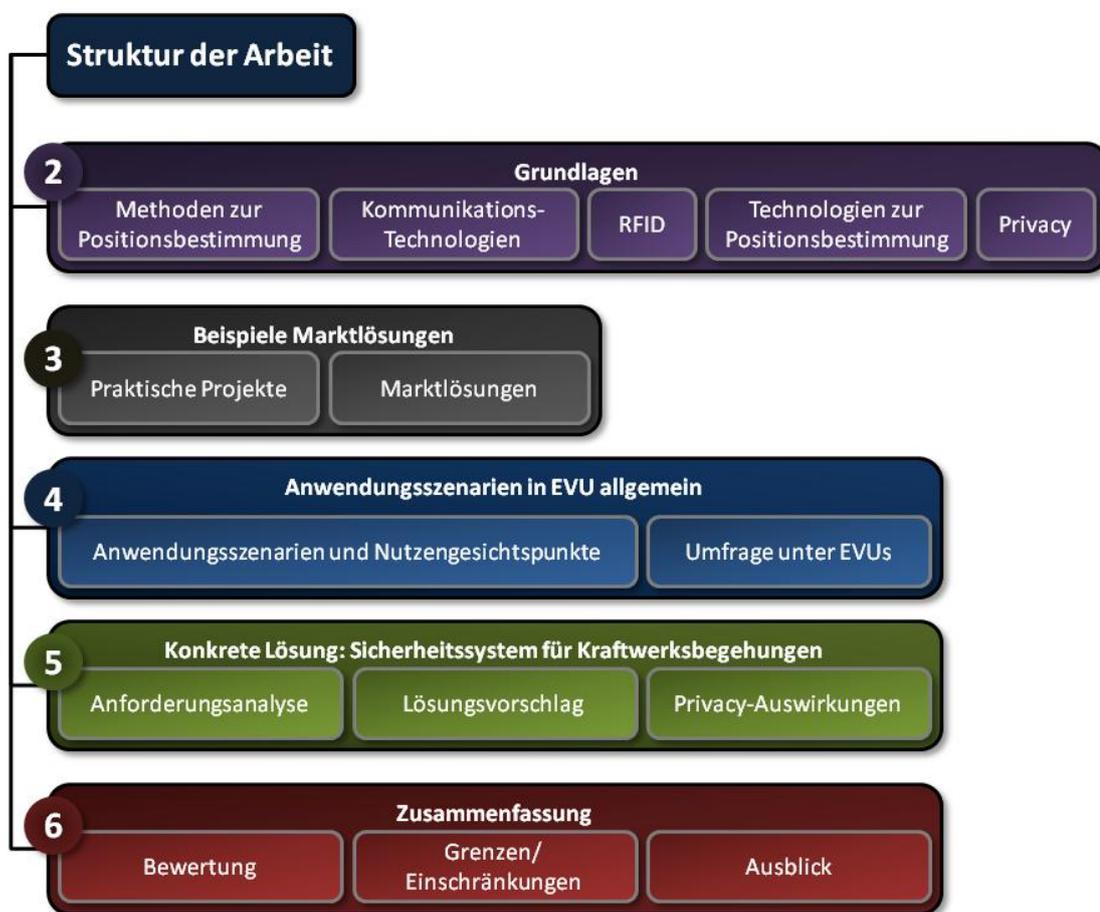


Abbildung 2: Struktur der Arbeit

Im **Kapitel 2** der Arbeit werden die in Zusammenhang mit RTLS eingesetzten Technologien beleuchtet. Daraus wird abgeleitet, welche Vor- und Nachteile die jeweiligen Technologien haben und wie sich die Technologien für die in der Arbeit angeführten Anwendungsszenarien eignen. Auch der Gesichtspunkt Privacy wird als kritischer Erfolgsfaktor beim Einsatz der RTLS-Technologie beleuchtet.

Im **Kapitel 3** der Arbeit werden einige Marktlösungen beschrieben und analysiert und daraus die Einsatzmöglichkeiten abgeleitet. Dies gilt im Besonderen für die in den konkreten Anwendungsfällen eingesetzte Technologie. Weiters wird die Übertragbarkeit der zugrundeliegenden Prozesse auf die konkreten Anwendungsbeispiele im EVU-Umfeld geprüft.

Im **Kapitel 4** werden allgemeine Anwendungsszenarien im EVU-Umfeld entworfen und Nutzungsgesichtspunkte herausgearbeitet. Im Rahmen einer Umfrage unter Energieversorgern wurde hinterfragt, inwieweit die RTLS-Technologie konkret eingesetzt wird. Die Ergebnisse der Umfrage schließen dieses Kapitel ab.

Im **Kapitel 5** wird ein Anwendungsszenario im EVU-Umfeld entwickelt. Aufbauend auf die einleitenden Kapitel wird eine geeignete Technologie ausgewählt und begründet. Der Anwendungsfall beinhaltet jeweils eine Indoorkomponente und eine Outdoorkomponente. Rahmenbedingung ist dabei, dass eine am Markt etablierte Standardlösung verwendet wird. Konkret wird auch beleuchtet, welche Auswirkungen diese Lösung unter dem Gesichtspunkt Privacy auf die Mitarbeiter hat. Auch arbeitsrechtliche Gesichtspunkte werden angesprochen.

Im **Kapitel 6** wird ein Fazit gezogen, und ein Ausblick auf die mögliche weitere Entwicklung im EVU-Umfeld gezeichnet.

1.4. Nichtziele

Nichtziele dieser Arbeit sind:

- Beschreibung aller möglichen RTLS-Technologien.
- Klärung aller technischen Details des entworfenen Einsatzszenarios.
- Konkrete Softwareentwicklung.
- Entwurf und Beschreibung von Softwarearchitekturen.
- Konkrete Hardwareauswahl

1.5. Begriffserklärungen

Nachfolgend werden einige wichtige Begriffe erklärt, deren Bedeutung für die Arbeit von wesentlichem Einfluss ist.

Real Time Locating Systems (RTLS)

Gemäß ISO/IEC 19762-5 ist ein RTLS (real-time locating system): *“combination of hardware and software that is used to continuously determine and provide the real time position of assets and resources equipped with devices designed to operate with the system”*.

Ein RTLS setzt sich normalerweise aus mobilen Geräten (PDAs, Tags, ...) einem Datennetzwerk, Serversoftware und einer Endbenutzeranwendung zusammen.

RTLS sind somit Systeme, welche den Standort (die Lokation) eines Objektes in Echtzeit bestimmen und in Applikationen einbeziehen. Dies geschieht mit Hilfe drahtloser Hardware und entsprechender Software.

Im Sinne dieser Arbeit werden unter einem RTLS speziell auch Systeme verstanden, die über weite Entfernungen die Position von Objekten in Echtzeit bestimmen, und an einen zentralen Server übermitteln.

Eine besondere Bedeutung für RTLS hat dabei der Gesichtspunkt *„Context Awareness“*, also der Einfluss der Umgebung (im allgemeinen Sinne) auf die RTLS-Anwendung, und als Untermenge speziell der Gesichtspunkt *„Location Awareness“*.

Context Awareness

Unter Context Awareness werden in allgemeiner Form Anwendungen, die in ihrem Ablauf Einflüsse der aktuellen Umgebung berücksichtigen verstanden (vgl. ROTH, J. (2005), S269).

DEY, A.K., ABOWD, G.D. (2000) definieren Context Awareness: *“context awareness is the ability of computing devices to detect and sense, interpret and respond to aspects of a user's local environment and the computing devices themselves”*.

Im speziellen Fall der *“Location Awareness”* ist es die räumliche Position (Lokation), auf die die Anwendung reagiert und entsprechende Ereignisse auslöst.

Ortung (engl. Tracking)

HIGHTOWER, J. et al (2000) definiert: *“Tracking systems, on the other hand, are those that monitor objects in their purview without involving the tracked objects in the computation“*.

Beim Tracking wird die Position eines Objektes durch ein Sensornetzwerk ermittelt, und nicht aktiv durch den Benutzer selbst (vgl. STEINBERG, T. (2007)).

Positionierung (engl. Positioning)

HIGHTOWER, J. et al (2000) definiert: „*Positioning systems are those that provide the means to determine location and leave it up to the user to compute his or her actual position.*”

Bei der Positionierung bestimmt der Benutzer selbst seine Position über technische Hilfsmittel (Empfänger) und entsprechende Software.

2. Grundlagen

2.1. Methoden zur Positionsbestimmung⁹

In der folgenden Abbildung sind die wesentlichen Methoden der Positionsbestimmung angeführt:

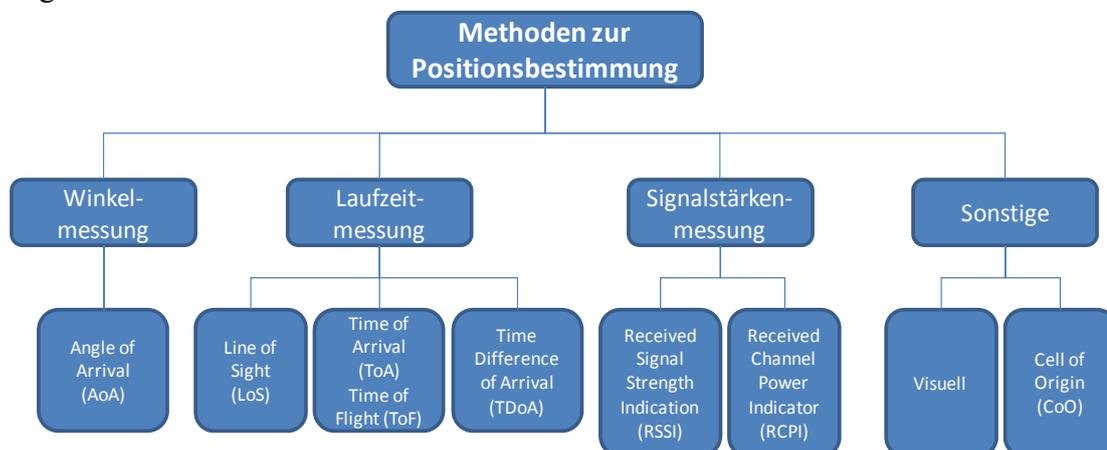


Abbildung 3: Methoden der Positionsbestimmung

2.1.1. Angle of Arrival (AoA)

Mit Antennen mit Richtwirkung, meist Antennenarrays¹⁰, kann bestimmt werden, aus welcher Richtung ein Signal eintrifft. Die Richtung kann auch durch rotierende Antennen bestimmt werden (siehe Radaranlagen zur Flugsicherung), was aber wesentlich teurere Antennenanlagen bedeutet. Die Winkelinformationen können entweder alleine dazu verwendet werden um die Position zu bestimmen, oder aber auch zur Verbesserung der Genauigkeit anderer Verfahren (z.B. von ToA¹¹) herangezogen werden. Für die Bestimmung der Position im 2D-Verfahren benötigt man zwei Winkel, für 3D-Bestimmungen zusätzlich den Azimut-Winkel. Die Positionsberechnung selbst erfolgt durch Triangulation¹². Die Winkelinformation wird an den Antennenarrays durch Messung der Differenz der Ankunftszeit (im Allgemeinen durch Bestimmung der Phasenlage) der Signale (Time Differenz of Arrival, TDoA) bei den einzelnen Sensorelementen des Antennenarrays errechnet.

Eine typische Anwendung für dieses Verfahren ist die Bestimmung der Geoposition von Mobiltelefonen oder die Ortung von „Piratensendern“.

⁹ Quellen sind wesentlich Wikipedia und Scheuring (2005)

¹⁰ Antennen-Arrays sind Sensoren, in einer zusammen geschalteten Einheit und in einer Matrix (auch z.B. V-Form) angeordnet

¹¹ ToA = Time of Arrival

¹² Triangulation ist die Bestimmung der Punktkoordinaten durch Dreiecksberechnung bei zwei gegebenen Winkeln und einer Basislinie [Vgl. Wikipedia <http://en.wikipedia.org/wiki/Triangulation>]

2.1.2. *Line of Sight (LoS)*

Dieses Verfahren berechnet die Entfernung vom Sender zum Empfänger, auf Basis der Ausbreitungszeit der Signale in der direkten Sichtverbindung (Line of Sight). Wird daher auf diese Art die Distanz zu zwei bekannten Senderstandorten bestimmt, kann durch Lateration die Position des Empfängers bestimmt werden. Oder die Position wird durch Nahe-Beziehung (Proximity) vom Sender übernommen.

2.1.3. *Time of Arrival (ToA) bzw. Time of Flight (ToF)*

Das Verfahren Time of Arrival (ToA) wird auch noch Time of Flight (ToF) genannt. Es beruht auf der Messung der Laufzeit eines Funksignals zwischen einem einzelnen Sender und einem einzelnen Empfänger. Aus der bekannten Ausbreitungsgeschwindigkeit der Radiowellen und der bekannten Frequenz kann direkt die Entfernung berechnet werden. Für die Berechnung der Entfernung wird dabei die absolute Zeit beim Eintreffen des Signales beim Empfänger herangezogen.

Die Berechnung der Position erfolgt durch Multilateration, wobei für die 3D-Lösung zumindest drei Entfernungen erforderlich sind.

Die notwendige hochpräzise Synchronisation der Uhren des Senders und Empfängers macht dieses Verfahren aufwändig. Das ToA-Verfahren wird bei vielen Positionierungssystemen eingesetzt, so z.B. bei GPS. Eine weitere Anwendungsmöglichkeit des ToA-Verfahrens ist die ToA-Messung von zwei Signalen mit unterschiedlicher Ausbreitungsgeschwindigkeit (z.B. Funk und Schall) die von einem Sender ausgesendet werden. Aus der Differenz der Ankunftszeit der beiden Signale kann direkt auf die Entfernung geschlossen werden.

2.1.4. *Time Difference of Arrival (TDoA)*

Beim TDoA-Verfahren wird die Zeitdifferenz beim Eintreffen der Signale von drei oder mehr synchronisierten Sendern gemessen. Geht man davon aus, dass die Positionen der Sender bekannt sind, kann aus der Zeitdifferenz auf die Entfernungen zu den Sendern geschlossen werden. Damit ist durch Multilateration die Berechnung der Punktkoordinaten des Empfängers möglich. Ebenso kann durch das umgekehrte Verfahren der TDoA-Messung eines von einem Sender ausgesandten Signals bei drei oder mehreren stationären Empfangstationen die Position des Senders berechnet werden. Je mehr Referenzstellen (Sender/Empfänger) vorhanden sind, umso genauer ist

die Positionsbestimmung möglich. Durch die erforderliche hochpräzise Synchronisation der Sender oder der Empfänger wird dieses Verfahren technisch aufwändig.

2.1.5. Received Signal Strength Indication (RSSI)

Diese Ortungstechnik basiert auf dem Ansatz, dass die empfangene Signalstärke (**R**eceived **S**ignal **S**trength **I**ndication) abhängig von der Entfernung der Mobilstation (MS) zu den Sendern ist. Aus der Signalstärke kann somit auf die Entfernung MS-Sender geschlossen werden. Über die Messung der Signalstärke mehrerer Sender kann mit einer Multilateration die Position der MS errechnet werden.

Die gemessene Signalstärke ist dabei im Wesentlichen eine Funktion der Entfernung (verringert sich quadratisch mit der Entfernung) und der Wellenlänge der Signale. Weiters ist zu berücksichtigen, dass die gemessene Signalstärke auch von der Umgebung und Witterungsverhältnissen deutlich beeinflusst wird (z.B. Hindernisse in Form von metallischen Gegenständen).

2.1.6. Received Channel Power Indicator (RCPI)

RCPI ist eine Variante von RSSI, die speziell in Wireless Systemen nach dem Standard 802.11 implementiert wurde. Dabei wird die Kanalleistung (Signal, Rauschen, Interferenzen) über das gesamte empfangene Frame in absoluten Werten und definierter Genauigkeit gemessen. Der RCPI ist daher das durchschnittliche Leistungsniveau über das gesamte Frame (vgl. ABUSUBAIH, M.; RATHKE, B. (2008)).

2.1.7. Visuelle Verfahren

Bei den visuellen Verfahren erfolgt die Positionsbestimmung durch Bilderkennung bzw. Konturerkennung bei der Auswertung von Videoaufnahmen. Dabei werden spezielle Softwareprodukte eingesetzt. Diese Verfahren sind sehr rechenintensiv. Durch Tragen spezieller Tags kann die Auswertung der Videobilder und die Positionsbestimmung wesentlich vereinfacht werden.

Aber auch die automatisierte Kontourauswertung (Silhouette) von Gebäuden, Personen, Geländeverlauf usw. kann bei bekanntem Standpunkt des Aufnahmegerätes (z.B. fest montierte Videokameras) zur Positionsbestimmung verwendet werden. Ein Beispiel dafür ist das Forschungsprojekt „Learning, Recognition, and Surveillance“ der Technischen Universität Graz, Institute for Computer Graphics and Vision, bei dem es

um das Tracking von Personen auf Basis automatisierter Personenerkennung durch Videobildauswertung geht. Ein weiteres Beispiel ist die automatische Objekterkennung durch Auswertung von Videobildern von fest montierten Kameras. Dieses Verfahren ist geeignet in Echtzeit Objekte (z.B. Fußgänger, Fahrzeuge) zu detektieren (vgl. STERNIG, S. et al (2009)).

Die visuellen Verfahren gewinnen mit steigender Leistungsfähigkeit der Hardware zunehmend an Bedeutung und sind geeignet in Echtzeit Objekte zu identifizieren und für RTLS-Anwendungen bereit zu stellen.

2.1.8. Cell of Origin (CoO)

Bei diesem Verfahren wird die Position dadurch ermittelt, dass sich das Empfangsgerät im von einem Sender „ausgeleuchteten“ Bereich (Zelle) befindet. Der Empfänger bekommt damit die bekannte Position des Senders. Die Genauigkeit des Verfahrens hängt maßgeblich von der Zellengröße ab. Je größer die Zellen, umso ungenauer die Positionsbestimmung. Beim Signal kann es sich dabei z.B. um ein Funksignal, Infrarot oder auch Ultraschall handeln.

Die einzelnen Zellen (CId) können durchaus auch eine unterschiedliche Form aufweisen, und werden häufig durch die topografischen Gegebenheiten bestimmt. Durch Überlappung von Zellen lässt sich die Ortungsgenauigkeit erhöhen. Befindet sich ein Empfänger R im Überschneidungsbereich von Zellen (Empfangsmöglichkeit des Empfängers zu zwei oder mehreren Sendestationen), so ist damit der geografische Bereich wesentlich genauer bestimmt.

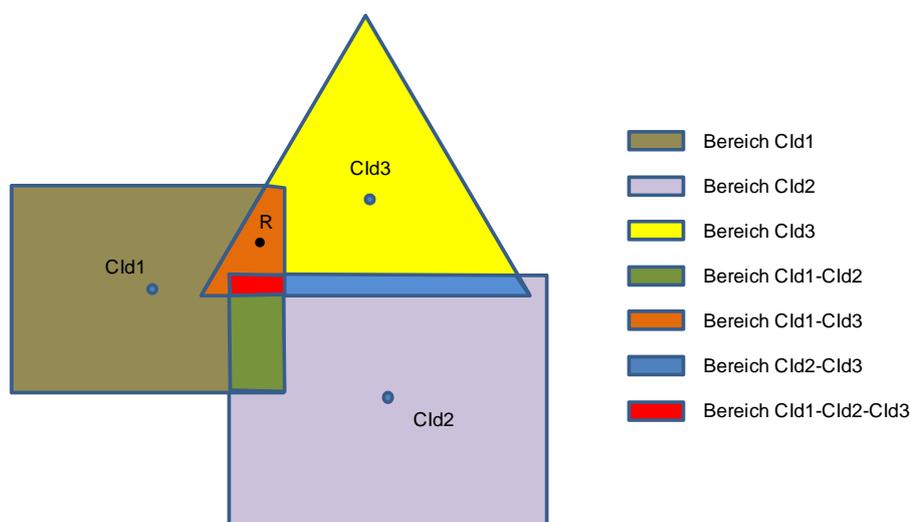


Abbildung 4: Verbesserung der Genauigkeit beim CoO-Verfahren durch Zellüberlappung

Weiters lässt sich die Genauigkeit der Positionsbestimmung steigern, wenn man das CoO-Verfahren mit dem AoA-Verfahren kombiniert.

2.1.9. Methoden für die Positionsbestimmung in Innenräumen¹³

2.1.9.1. Engstellen und Durchgang (Chokepoints and Transit)

Bei dieser Technologie wird die Position beim Durchgang an bekannten Punkten (Chokepoints) bestimmt. Die Genauigkeit der Methode hängt von der Anzahl und Anordnung der Sensoren ab. Der Bereich erstreckt sich von Einzelräumen bis zu gesamten Stockwerken eines Gebäudes. Bei Verwendung von „Dual Sensoren“ kann die Durchgangsrichtung bestimmt werden. Eingesetzte Technologien sind dabei z.B. IrDA, Active RFID, Wi-Fi, Bluetooth, ZigBee und Ultrawideband (UWB).



Abbildung 5: Chokepoints and Transit

Quelle: Geodan

2.1.9.2. Näherung (Proximity)

Diese Technologie verwendet die bekannte Position bestehender Objekte für die Positionsbestimmung. Das kann z.B. ein Computer sein, an dem ein Benutzer angemeldet ist, oder auch der Vorbeigang an Sensoren (z.B. Gates).

Eingesetzte Technologien sind dabei z.B. IrDA, Active RFID, Passive RFID, Bluetooth, ZigBee und UWB.



Abbildung 6: Näherungsmethode

Quelle: Geodan

¹³ Geodan Movida (2009): indoor location | Geodan. Online verfügbar unter <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-indoor-location/>, zuletzt geprüft am 25.08.2009.

2.1.9.3. Koordinaten (Coordinates)

Die Position wird über Triangulation oder Multiangulation berechnet. Die Genauigkeit hängt von der Anzahl der Sensoren und der eingesetzten Technologie ab und liegt im cm-Bereich bis m-Bereich. Eingesetzte Technologien sind dabei Wi-Fi und UWB.



Abbildung 7: Coordinates
Quelle: Geodan

2.1.9.4. Hot-Spots (Presence)

Bei dieser Technologie registriert der Sensor (Reader) die Tags innerhalb seiner Reichweite. Der „ausgeleuchtete“ Bereich kann dabei zwischen mehreren dm und mehr als 50 Meter liegen. Eingesetzte Technologien sind dabei IrDA, Active RFID, Wi-Fi, Bluetooth, ZigBee und Ultrawideband (UWB).

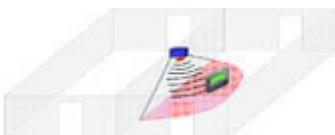


Abbildung 8: Hot-Spots
Quelle: Geodan

2.2. Kommunikationsnetzwerke

RTLS erfordern die Bestimmung der Position eines mobilen Clients in Echtzeit. Für diesen Zweck wird eine Kommunikationsverbindung zum Server vorausgesetzt. In der überwiegenden Zahl der Fälle erfolgt die Kommunikation zwischen mobilen Client und dem Server über eine mobile Kommunikationsverbindung. Bei den RTLS kommen vorwiegend folgende Verfahren zur Anwendung:

- Mobiltelefonie
- Wireless LAN
- Bluetooth
- Infrarot IrDa

Angelehnt an ROTH, J (2005) können die **mobilen Kommunikationssysteme** wie folgt klassifiziert werden:

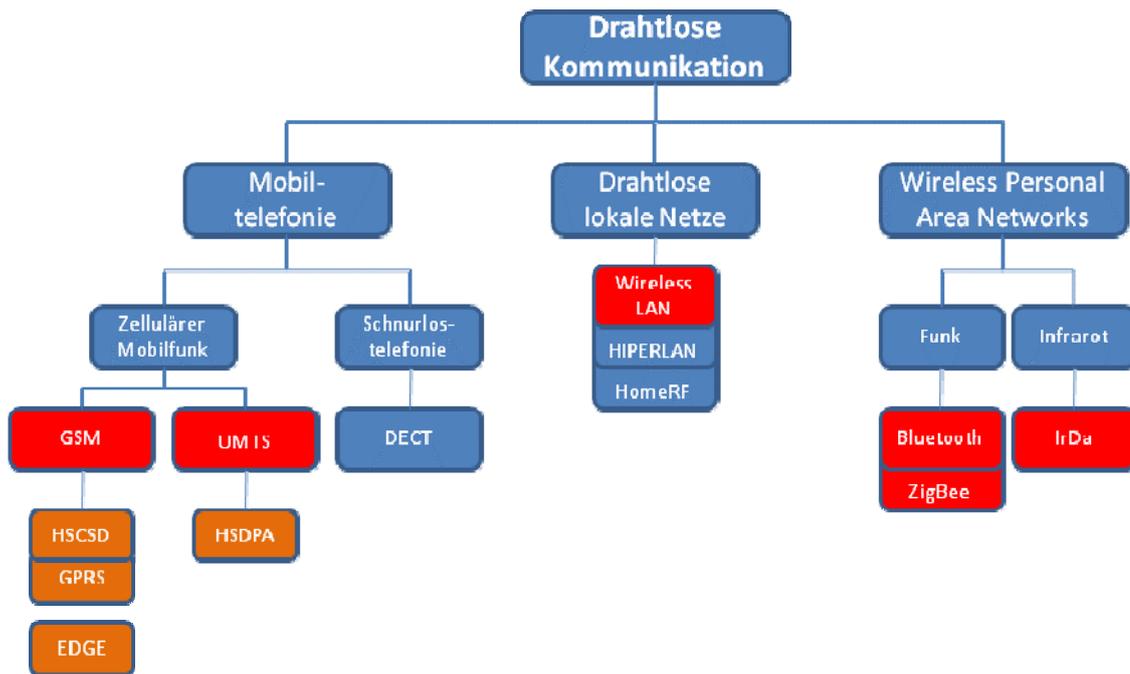


Abbildung 9: Klassifizierung drahtlose Kommunikationssysteme
 Quelle: angelehnt an ROTH, J. (2005)

In den folgenden Kapiteln soll auf den grundlegenden Aufbau und die Funktionsweise der für RTLS gängigsten Kommunikationsnetzwerke (in der obigen Grafik in rot und orange dargestellt) eingegangen werden. Eine umfassende Erörterung der eingesetzten Technologien würde den Rahmen dieser Arbeit sprengen.

2.2.1. Mobiltelefonie

Die Mobiltelefonie ist eine Technologie, die mittlerweile unser gesamtes Leben durchdrungen hat. Viele Menschen können sich ein Leben ohne Mobiltelefon (im deutschsprachigen Raum meist „Handy“ genannt) gar nicht mehr vorstellen. Dies gilt speziell für die jüngere Generation, bei der die Durchdringung mit Handys nahe 100% liegt.

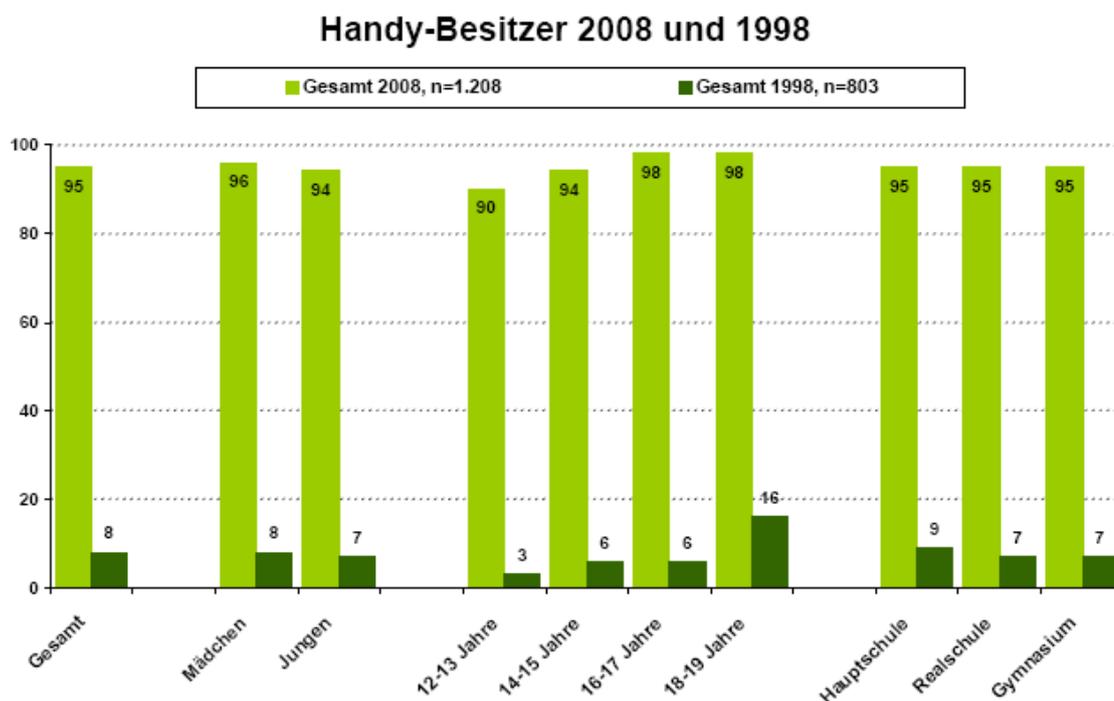


Abbildung 10: Handybesitz bei Kindern und Jugendlichen in Deutschland; Angaben in %
Quelle: JIM¹⁴ 2008 und JIM 1998

Waren die ersten Mobilfunknetze noch analoge Netze (Netze der ersten drei Generationen A-Netz, B-Netz und C-Netz) erfolgte im Jahr 1992 in Deutschland der Startschuss für die Markteinführung der digitalen Mobilfunknetze. In den nächsten Kapiteln sollen die wichtigsten digitalen Mobilfunknetze in der Übersicht behandelt werden.

2.2.1.1. *Mobilitätsmanagement*

Dem Mobilitätsmanagement kommt bei den Mobilfunknetzen entscheidende Bedeutung zu. Über das Mobilitätsmanagement wird sichergestellt, dass die Verbindung/Datenübertragung auch dann erhalten bleibt, wenn eine mobile Station, MS¹⁵ den Versorgungsbereich einer Basisstation verlässt. Dazu werden zwei Begriffe in diesem Zusammenhang angeführt. Definitionen nach (PISCHEL, E. (2002)):

Handover: „Die Übertragung der Verbindung des Nutzers von einem Funkkanal zum anderen. Dieser kann zur gleichen oder einer anderen Zelle gehören.“

¹⁴ JIM = Jugend, Information (Multi)-Media

Die Daten basieren auf der JIM-Studie 2008 des medienpädagogischen Forschungsverbundes Südwest; KUTTEROFF, A.; BEHRENS, P. (2008)

¹⁵ MS = Mobile Station

Roaming: „Roaming, d. h. das Nutzen von Mobilfunknetzen verschiedener Betreiber durch einen Teilnehmer mit demselben mobilen Endgerät“.

2.2.1.2. GSM-Technologie¹⁶

Im Jahr 1992 wurde in Deutschland mit dem D-Netz im 900 Mhz-Funkband (D steht hier nicht für digital sondern für die 4. (D) Generation) das digitale Mobilfunkzeitalter im kommerziellen Betrieb eröffnet. In Österreich wurde 1993 das erste digitale Mobilfunknetz unter der Bezeichnung E-Netz eingeführt. Diese Netze bauen auf dem GSM¹⁷-Standard auf. Schon im Jahr 1982 wurde die Basis für die digitale zelluläre Mobilfunktechnologie mit den ersten Arbeiten der Group Spéciale Mobile (GSM) gelegt. Ziel der Gruppe, die aus Mitgliedern von 26 Staaten bestand, war es einen gemeinsamen europäischen Standard für digitalen zellulären Mobilfunk zu erarbeiten. Die vorgesehene Frequenz dafür wurde mit 900 MHz festgelegt. 1987 wurden die Ergebnisse aus diesen Arbeiten in einen Memorandum of Understanding von 18 Staaten unterzeichnet. 1989 wurden die Arbeiten vom ETSI (European Télécommunication Standards Institute) übernommen und somit in die europäische Verantwortung überführt. 1990 wurde zusätzlich zur Frequenz von 900 MHz auch eine Spezifikation für 1.800 MHz erarbeitet. In den USA kam in der Folge der 1.900 MHz-Standard dazu. Mittlerweile gibt es mehrere Generationen von weiterentwickelten digitalen Mobilfunkstandards.

- 2G Digitaler Mobilfunk, z.B. GSM
- 2,5G Digitaler Mobilfunk mit Datenübertragung, z.B. GPRS, HSCSD
- 3G Breitbandiger digitaler Mobilfunk, z.B. UMTS, HSDPA
- 4G Vollständig IP-basierter digitaler Mobilfunk

Derzeit erreichen die GSM-Netze mehr als 80% der Weltbevölkerung. Sie werden in 219 Staaten von aktuell mehr als 3 Milliarden Menschen verwendet¹⁸.

Technische Grundlagen eines GSM-Netzes¹⁹:

Das GSM-Netz ist ein zelluläres Mobilfunknetz, d.h. das gesamte Gebiet ist in Versorgungszellen (Waben) eingeteilt. Eine drahtlose Kommunikationsverbindung

¹⁶ Quellen: HOGREFE, D. (2009); STEINBERG, T (2007);

http://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications, zuletzt geprüft am 24.10.2009

¹⁷ GSM = Global System for Mobile Communications bzw. ursprünglich Group Special Mobile

¹⁸ Quelle: www.gsmworld.com; zuletzt geprüft am 12.09.2009

¹⁹ Quelle: <http://www.umtslink.at/index.php?pageid=GSM-Start> zuletzt geprüft am 12.09.2009

sollte daher von jedem Punkt des Versorgungsgebietes aus möglich sein. Dies erfordert, dass eine Vielzahl von Sendestationen errichtet werden müssen. GSM überträgt Sprache und Daten bis zu einer Übertragungsgeschwindigkeit von max. 9,6 kbit/s) gemeinsam mit Textnachrichten, sogenannten SMS (Short Messages Service). Das GSM-Mobilfunknetz besteht aus drei Subsystemen:

- Dem Funk-Subsystem (Base Station Subsystem, BSS, oder auch Radio Access Network, RAN)
- Dem Vermittlungs-Subsystem (Mobile Switching and Management Subsystem, SMSS)
- Dem Betriebs-Subsystem (Operation and Maintenance Subsystem, OMSS)

Das **Funk-Subsystem** besteht aus den mobilen Endgeräten („Mobile Station MS), z.B. den Handys oder auch Datenübertragungskarten, sowie den Basisstationen, z.B. den Handymasten, (Base Transceiver Station, BTS) sowie den zugehörigen Controllern der Basisstationen (Base Station Controller, BSC). Eine BSC ist dabei für mehrere BTS zuständig. Die MS wird für den mobilen Zugang der Benutzer zum Funknetzwerk benötigt. Über die BTS wird die jeweilige Zelle mit Funksignalen abgedeckt. Die BTS bildet die Luftschnittstelle zur MS. In der BTS wird das Protokoll für die Übertragung der Informationen (Sprache, Daten) bereitgestellt. Die BTS sind an den BSC angeschlossen. Abhängig von der Ausprägung des Netzes ist eine unterschiedliche Anzahl von BTS an den BSC angeschlossen (zwischen 10 und 100). Der BSC überwacht die BTS und sorgt für die Frequenzallokation sowie die Weiterreichung (Handover) der MS beim Wechsel von einer BTS zur Nächsten.

Das **Vermittlungs-Subsystem** nimmt die Rolle einer „Schaltzentrale“ ein. Aufgabe der „Mobile Switching Center“ (MSC) ist es im klassischen Sinne eine Leitungsverbindung zwischen den beiden beteiligten Stationen herzustellen. Die MSC führen die Weiterreichung der Daten an das Netzwerk aus. Wiederum kann eine MSC für mehrere BSC zuständig sein.

Eine für den Netzbetreiber wichtige Aufgabe der MSC ist auch die Gebührenerfassung (im Sinne von Verbrauch von Netzwerkressourcen) für alle von der MS genutzten Dienste.

Das **Betriebs-Subsystem** kontrolliert, steuert und wartet das Netzwerk. Zentrales Element ist das „Operation and Maintenance Center“ (OMC), das einerseits für die Verwaltung der Kundeninformationen, wie Endgerätedaten, Abrechnungsdaten und andererseits für die Konfiguration und Wartung des Netzwerks sowie für die Netzwerksicherheit zuständig ist. Über die OMC werden z.B. Kunden neu eingerichtet oder auch Softwareupdates oder Fehlerbehebungen durchgeführt.

Location Area Identity (LAI):

Die Location Area Identity ist eine weltweit eindeutige Identifikation (2 Byte) für das Gebiet der Basisstation. Die LAI besteht aus dem Mobile Country Code (MCC), dem Mobile Network Code (MNC) und dem Location Area Code (LAC). Das BSS zeigt über die LAI der MS den Aufenthaltsbereich an.

2.2.1.3. Leitungsvermittelte Technologie versus paketvermittelte Technologien

Bei GSM handelt es sich um eine leitungsvermittelte Technologie. Das heißt, es wird eine für die Dauer der Session permanente logische Leitungsverbindung zwischen dem Sender und dem Empfänger hergestellt. Größter Vorteil dabei ist, dass eine zugesicherte Übertragungskapazität aufgrund des nur für diese Session blockierten Funkkanals besteht. Nachteile der leitungsvermittelten Technologie sind allerdings, dass der Funkkanal blockiert ist, unabhängig davon ob gerade Daten übertragen werden oder nicht. Dies führt einerseits zu Kosten für den Teilnehmer, auch wenn keine Daten übertragen werden, und andererseits dazu, dass die Übertragungskapazität nur unzureichend ausgenutzt wird.

Diese Nachteile beseitigt die paketvermittelte Technologie, weil bei Übertragungspausen eines Teilnehmers, diese Lücken von den anderen Teilnehmern genutzt werden können. Eine Verbindung wird nur während der Zustellung der Pakete aufgebaut. Das bedeutet, dass die Teilnehmer immer verbunden (d.h. always on) sein können, ohne das Kosten entstehen. Kosten entstehen nur, wenn Daten übertragen werden.

2.2.1.4. Technologien für höhere Datenraten in GSM-Netzen

GSM hat für die Datenübertragung nur eingeschränkte Möglichkeiten. Die Geschwindigkeit ist mit 9.600 kbit/s begrenzt. Diese Geschwindigkeit ist für viele Anwendungen nicht ausreichend. Aus diesem Grund wurden schon bald Verfahren

gesucht, die deutlich höhere Übertragungsraten ermöglichen. Eine Erweiterung der GSM-Technologie für höhere Datenraten ist die HSCSD²⁰-Technologie. Dabei werden bis zu 8 Kanäle zu einer Übertragungsleitung gebündelt. Weiters wird ein gegenüber GSM neues Kanalcodierungsverfahren eingesetzt, das eine Nettodatenrate je Kanal von 14,4 kbit/s erlaubt. Mit diesen beiden Maßnahmen lassen sich theoretisch 76,8 kbit/s (115,2 kbit/s) erreichen. HSCSD ist weiterhin eine leitungsvermittelte Technologie. Einen anderen Weg beschreitet *GPRS*²¹.

Im Unterschied zu GSM ist GPRS eine paketvermittelte Technologie, d.h. es wird zwischen Sender und Empfänger kein permanenter Datenkanal mehr aufgebaut. Mit GPRS lässt sich die Übertragungsrate bei Bündelung der 8 Zeitslots und noch einigermaßen sicherer Fehlerschutzverfahren auf 8x14,4 kbit/s, das sind 115,2 kbit/s steigern (maximal wären 171,2 kbit/s möglich). Die Paketvermittlung wird durch eine Änderung der Architektur durch Einführung der GPRS Support Nodes (GSN) verwirklicht. Diese sind für die Paketvermittlung zuständig, funktionieren als Gateways zu den paketorientierten Datennetzen und übernehmen das Roaming der MS. Der MS wird temporär eine dynamische IP-Adresse zugeordnet. Die MS kann daher wie in einem „normalen“ IP-Netzwerk über die IP-Adresse angesprochen werden. GSM und GPRS können parallel in den Zeitslots eines Kanals betrieben werden, wobei die GSM-Verbindungen Vorrang gegenüber den GPRS-Datenverbindungen haben.

EDGE²² ist eine Erweiterung für die bestehenden GSM-Verfahren. Dabei wird eine andere Modulationstechnik an der Funkschnittstelle verwendet (8PSK²³ anstatt den im GSM üblichen GMSK²⁴-Verfahren). Diese Änderung erlaubt es, in einem Takt gleichzeitig 3 Bit zu codieren. Dadurch kann eine wesentliche Steigerung der Übertragungsraten auf bis zu 384 kbit/s (vgl. PISCHEL, E. (2002)) möglich; bei Bündelung von 8 Kanälen bis zu 473,6 kbit/s (vgl. STEINBERG, T. (2007)). Edge kann sowohl in Kombination mit leitungsvermittelten Technologien als auch mit paketvermittelten Technologien eingesetzt werden (z.B. ECSD, EGPRS)

²⁰ HSCSD = **H**igh **S**peed **C**ircuit **S**witched **D**ata

²¹ http://www.umtslink.at/index.php?pageid=GPRS_GPRS_einfuehrung, zuletzt geprüft am 14.10.2009

²² EDGE = **E**nhanced **D**ata **R**ates for **G**SM **E**volution

²³ 8PSK = **8** **P**hase **S**hift **K**ey

²⁴ GMSK = **G**aussian **M**inimum **S**hift **K**ey

2.2.1.5. UMTS-Technologie²⁵

Die UMTS²⁶-Technologie ist ein Mobilfunkstandard der 3. Generation (3G). Großer Vorteil gegenüber der GSM-Technologie ist, dass mit UMTS wesentlich höhere Datenraten (theoretisch bis zu 2 Mbit/s) möglich sind, und die Sicherheitsstandards deutlich besser sind. Dementsprechend interessant ist UMTS für die Mobilfunkanbieter. Infolge der Marktöffnung wurden die UMTS-Frequenzen in Versteigerungsverfahren an die Marktteilnehmer weitergeben, was den Staaten Einnahmen in enormer Höhe bescherte (50 Mrd. Euro in Deutschland, 7 Mrd. Euro in Österreich)²⁷.

Seinen Anfang nahm UMTS im Jahr 1992 mit der Gründung des IMT-2000²⁸ Spezifikationspools durch die ITU²⁹. In dieser Initiative sollten die Standards für die Mobilfunktechnologie der dritten Generation (3G) erarbeitet werden. Ziel dabei war es auch, einen weltweit einheitlichen Standard für den Mobilfunk der dritten Generation einzuführen, was in der Folge aber nicht gelang, da parallel zur IMT-2000 weitere Gruppen an einer Standardisierung arbeiteten.

Technologisch unterscheidet sich UMTS deutlich von GSM. Das ist auch der Grund, warum für UMTS neue Standorte aufgebaut werden mussten. UMTS basiert auf dem neuen Funknetzteil UTRAN³⁰. Dieses arbeitet paketvermittelt und verwendet das W-CDMA³¹ Multiplex-Verfahren (im Unterschied zum TDMA-Verfahren bei GSM). Damit lässt sich das Frequenzband wesentlich besser ausnützen, weil mehrere Teilnehmer gleichzeitig auf dem gleichen Frequenzkanal kommunizieren können, ohne sich gegenseitig zu stören. UMTS ist im Frequenzband von 2.000 MHz angesiedelt. Ein Frequenzband in UMTS ist mit 5 MHz um ein vielfaches breiter als ein GSM-Frequenzband (hier 200 kHz).

Ein weiteres Merkmal von UMTS ist, dass das Versorgungsgebiet in Zellen unterschiedlicher Größe eingeteilt werden kann. Es gibt:

- Femtozellen; das sind kleinste UMTS-Zellen in Bürogebäuden, welche die Breitbandübertragung in geschlossenen Räumen verbessern sollen.
- Picozellen; das sind kleine Zellen bis zu 50 m in Ballungsräumen.

²⁵ <http://www.umtslink.at>, zuletzt geprüft am 24.10.2009

²⁶ UMTS = **U**niversal **M**obile **T**elekommunication **S**ystem

²⁷ Quelle: http://de.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System, zuletzt geprüft am 12.09.2009

²⁸ IMT-2000 = **I**nternational **M**obile **T**elecommunications at **2000**MHz

²⁹ ITU = **I**nternational **T**elecommunications **U**nion

³⁰ UTRAN = **U**MTS **T**errestrial **R**adio **A**ccess **N**etwork

³¹ W-CDMA = **W**ideband **C**ode **D**ivision **M**ultiple **A**ccess

- Mikrozellen; das sind Zellen mit einer Größe bis zu einigen Kilometern, in urbanen Bereichen anzutreffen.
- Makrozellen; das sind Zellen bis zu einigen 10 Kilometern in den Überlandbereichen.

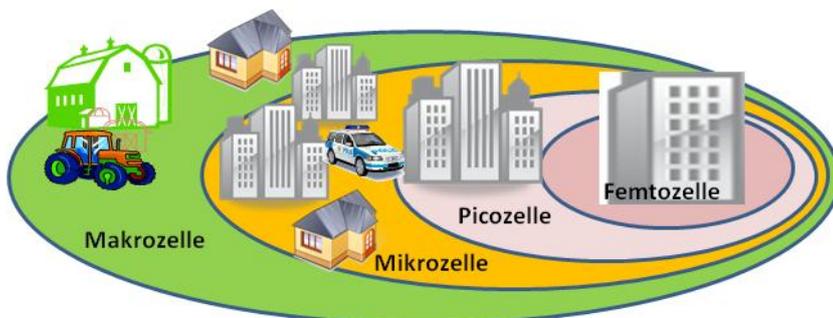


Abbildung 11: Zellengrößen bei UMTS

Quelle: angelehnt an STEINBERG, T. (2007)

Die Technik von UMTS erfordert für die Abdeckung eines Gebietes mit hohen Übertragungsraten den Aufbau einer großen Zahl von Basisstationen mit dementsprechend hohen Kosten. Dies ist auch der Grund dafür, warum UMTS zumindest in mittelfristiger Zeit nicht flächendeckend angeboten werden wird.

2.2.1.6. HSDPA³²

HSDPA³³ ist die nächste Entwicklungsstufe in der Mobilfunktechnologie. In Analogie zu GPRS wird HSDPA auch als Standard der 3,5-ten Generation (3,5G) bezeichnet. HSDPA ist eine Weiterentwicklung von UMTS. HSDPA bietet Datenraten bis zu 14,4 Mbit/s im Downlink. Erreicht wird dies durch eine deutliche Verkürzung der Latenzzeit (wirksam bei kurzen Unterbrechungen in der Datenübertragung) und durch bessere Ausnutzung der Frequenzbänder durch „intelligenteres“ Kapazitätsmanagement, sowie ein wirkungsvolleres Modulationsverfahren (16QAM), das die Datenrate gegenüber dem alten Modulationsverfahren verdoppelt (mit jedem Übertragungsimpuls können nun 4 Bit übertragen werden).

2.2.1.7. Zusammenfassung

Die Mobilfunktechnologie ist besonders für die Übermittlung der Clientdaten an einen zentralen Server sehr gut geeignet. Da keine eigene technische Infrastruktur aufgebaut werden muss, lässt sich ein RTLS mit Mobilfunkverbindung sehr kostengünstig

³² Quelle: http://www.umtslink.at/index.php?pageid=hsdpa_grundlagen2 zuletzt geprüft am 18.09.2009

³³ HSDPA = High Speed Downlink Packet Access

aufbauen. Als Technologie für die Positionsbestimmung ist Mobilfunk für den gegenständlichen Fall allerdings nicht geeignet. Auf Basis der verfügbaren Verfahren für die Positionsbestimmung in Mobilfunknetzen ist die Ortungsgenauigkeit für die gegenständliche Sicherheitslösung zu gering. BEINAT et al (2007) führt dazu an, dass die Mobilfunktechnologie von allen Positionsbestimmungstechnologien die geringste Genauigkeit aufweist.

Hinsichtlich Datensicherheit weist Mobilfunk zahlreiche technische Vorkehrungen auf. Da die Daten allerdings über eine weitreichende Luftschnittstelle übertragen werden, bietet Mobilfunk potentiellen Angreifern die meisten Möglichkeiten.

Im gegenständlichen Projekt sind vor allem die kostengünstigen Übertragungsmöglichkeiten von Interesse.

2.2.2. *Wireless-LAN*³⁴

Die WLAN³⁵-Technologie ist neben der Mobilfunktechnologie die im Privatbereich wohl am meist verbreitete mobile Funkübertragungstechnologie, nützen doch viele Computeranwender zu Hause WLAN für die Anbindung mobiler Computer (z.B. Laptops) an das Internet. Auch im Bereich der RTLS stellt WLAN (hier häufig auch Wi-Fi³⁶ genannt) eine häufig verwendete Technologie dar. Dabei wird WLAN einerseits für die Datenübertragung und andererseits für die Positionsbestimmung eingesetzt. WLAN ist ein Sammelbegriff für alle drahtlosen Netzwerke (vgl. STEINBERG, T. (2007)). Hauptsächlich gemeint sind mit WLAN die Standards der IEEE 802.11-Familie. Diese Funknetzwerk-Standards haben ihren Ursprung im Jahr 1997, wobei der erste IEEE 802.11-Standard Datenübertragungsraten von bis zu 2 Mbit/s erlaubte. In den Folgejahren wurden immer leistungsfähigere Erweiterungen in den Standard implementiert, die der rasant fortschreitenden technologischen Entwicklung Rechnung trugen. Der nunmehr aktuelle Standard 802.11n ermöglicht bereits Übertragungsraten von bis zu 600 Mbit/s. Es gibt zwei Hauptlinien der 802.11 Standards, nämlich jene im ISM-Frequenzband von 2,4 GHz und jene im 5 GHz-Band. Die Standards im 5 GHz-Band ermöglichen deutlich höhere Übertragungsraten, haben aber strengere Auflagen seitens der Behörden. Jeder WLAN-Adapter unterstützt die Betriebsmodi „AD-Hoc-Modus“ und „Infrastrukturmodus“.

³⁴ http://www.umtslink.at/index.php?pageid=WLAN_WLAN-Start zuletzt geprüft am 20.09.2009

³⁵ WLAN = **W**ireless **L**ocal **A**rea **N**etwork

³⁶ Wi-Fi = **W**ireless-**F**idelity

2.2.2.1. Ad-Hoc Modus

Im Ad-Hoc Modus verbinden sich zwei oder mehrere Geräte mit WLAN direkt ohne Zwischenschaltung einer Steuereinheit (entspricht einem Peer-to-Peer Netzwerk). Jeder WLAN-Adapter ist gleichwertig. Es gibt keine zentrale WLAN-Funkstation für die Regelung des Funkverkehrs zwischen den Stationen. Die Reichweite liegt in dieser Betriebsart im Inneren von Gebäuden bei ca. 30 Meter und im Freien bei ca. 300 Meter (vgl. ROTH, J. (2005)).

2.2.2.2. Infrastrukturmodus

Im Infrastrukturmodus übernimmt ein WLAN-Adapter die Rolle der zentralen Netzwerksteuereinheit, Basisstation oder auch Accesspoint, AP, genannt. Die Geräte kommunizieren nicht mehr direkt miteinander sondern über diesen zentralen AP. Damit lassen sich deutlich mehr Geräte vernetzen, weil der Funkverkehr in „geordneten“ Bahnen abläuft. Die Basisstation arbeitet analog einem Switch in einem fest verdrahteten Netzwerk. Die Ausdehnung des Netzwerkes kann im Infrastrukturmodus in Innenräumen ca. 60 m betragen. Es ist aber auch möglich ein drahtloses Netzwerk mit mehr als einem AP zu betreiben. Der Infrastrukturmodus kann in die Untergruppen „**Basic Service Set**“, BSS und „**Extended Service Set**“, ESS, eingeteilt werden.

Ein BSS liegt vor, wenn das drahtlose Netzwerk nur aus einem AP und mobilen Geräten mit WLAN-Funkmodulen besteht. Ein ESS liegt vor, wenn mehrere BSS vernetzt werden. Die Vernetzung kann entweder über eine „normale“ LAN-Verkabelung oder auch über Funk (Bridges) erfolgen. Die Infrastruktur, die für die Vernetzung der APs erforderlich ist, nennt man auch „Distributionssystem“.

Da alle WLAN-Geräte eines BSS sich die Übertragungskapazität des AP teilen müssen, ist die Anzahl der Geräte je AP praktisch auf ca. 5 begrenzt, um noch brauchbare Datenraten zu erreichen. Es können für die Erhöhung der Übertragungskapazität einfach zusätzliche BSS (bei geeigneter räumlicher Anordnung) zu einem ESS hinzugefügt werden.

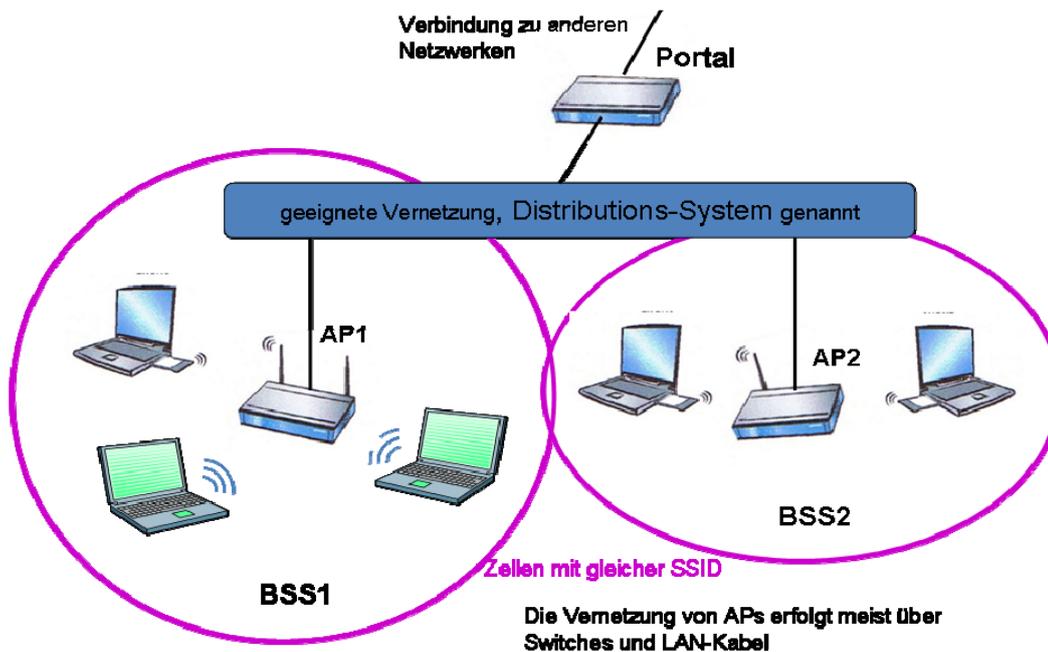


Abbildung 12: WLAN-Netzwerkstruktur
Quelle: nach STEINBERG, T. (2007)

2.2.2.3. Zusammenfassung

WLAN ist sowohl als Datenübertragungstechnologie zwischen Client und Server, bei RTLS zwischen mobilem Client und Empfänger, als auch als Positionsbestimmungstechnologie für RTLS gut geeignet. Positiv ist vor allem, dass WLAN als Standardtechnologie in vielen mobilen Geräten kostengünstig, meist ohne Aufpreis, verfügbar ist.

Hinsichtlich Datensicherheit lässt WLAN in den aktuellen Standards kaum Wünsche offen. Sowohl die Einbindung in die bestehende Netzwerksicherheitsarchitektur als auch die Verschlüsselung der Datenübertragung sind im Standard gegeben.

2.2.3. Bluetooth

Bluetooth ist eine WPAN³⁷- Technologie. WPAN ist eine Netzwerktechnologie, die für den Nahbereich ausgelegt ist. WPAN weist gegenüber WLAN folgende Eigenschaften auf (nach ECKERT, C. (2009)):

- WPAN unterstützen vorwiegend die Ad-Hoc-Vernetzung
- Geringere Datenübertragungsraten (≈ 1 Mb/s)
- Deutlich geringere Reichweiten (≈ 10 m)
- Relativ niedriger Stromverbrauch (≈ 1 mW)

Der niedrigere Energieverbrauch ist für diese Technologie wesentlich, weil die Einsatzzeiten der mobilen Geräte ohne Akkunachladung deutlich verlängert werden sollen. WPANs werden über die 802.15-Standardfamilie spezifiziert. Für Bluetooth ist der entsprechende Ursprungsstandard 802.15.1. Seinen Ursprung hat Bluetooth bereits im Jahr 1994, in dem Ericson den Standard für die Verbindung von mobilen Geräten wie Druckern, Handys, Notebooks konzipierte. Über Bluetooth können unterschiedlichste Arten von Daten übertragen werden (z.B. Sprache, Musik, Bild, Video).

Bluetooth arbeitet im ISM³⁸-Frequenzband von 2,4 GHz (2,402 bis 2,480 GHz) und kann somit lizenzfrei betrieben werden. Um die Verbindung möglichst störungsfrei zu gestalten, wird bei Bluetooth ein spezielles Verfahren, das sogenannte Frequenzwechselverfahren („frequency hopping“) eingesetzt. Nach einem Muster, das ein Pseudozufallsgenerator steuert, wird bei der Datenübertragung 1.600-mal in der Sekunde zwischen den Kanälen gewechselt. Geräte, die miteinander kommunizieren, setzen dabei die gleiche Wechselabfolge ein.

BTs werden in drei Klassen eingeteilt:

Klasse	Sendeleistung	Reichweite im Freien (Outdoor)	Reichweite in Gebäuden (Indoor)
1	1mW - 100 mW (20 dBm)	100-130 Meter	50-80 Meter
2	0,25 mW – 2,5 mW (4 dBm)	25-35 Meter	20-30 Meter
3	1 mW (0 dBm)	10-18 Meter	8-12 Meter

Tabelle 1: Klasseneinteilung der Bluetoothgeräte

Quelle: http://www.tomshardware.com/de/bluetooth-grundlagen_testberichte-956.html, zuletzt geprüft am 22.09.2009

³⁷ WPAN = **W**ireless **P**ersonal **A**rea **N**etwork

³⁸ ISM = **I**ndustrial, **S**cientific, **M**edical

2.2.3.1. Bluetooth-Vernetzung

Bis zu acht Bluetooth-vernetzte Geräte (BTs) kommunizieren dabei in einem sogenannten Piconet aktiv. In diesem Piconet können bis zu 248 weitere Geräte zwar angemeldet sein, müssen aber passiv bleiben (Standby). Von den acht aktiven Teilnehmern ist ein Gerät der Master, die sieben anderen arbeiten im Slave-Modus. Jedes BT hat dabei seine eigene, 48 Bit lange, weltweit eindeutige Adresse (Bluetooth Device Adress). Die Verbindung mehrerer Piconets nennt man Scatternet.

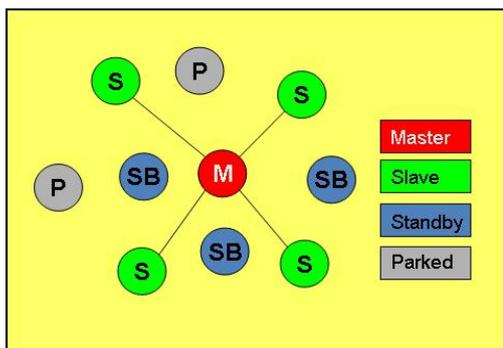


Abbildung 13: Bluetooth-Piconet

Quelle: angelehnt an ECKERT, C. (2009)

2.2.3.2. Profile

Es gibt zahlreiche Bluetooth-Profile, die von der SIG³⁹ standardisiert werden. In einem Profil sind die Regeln und Protokolle (komplette Parametersätze) für ein bestimmtes Einsatzgebiet definiert. Damit ist sichergestellt, dass sich unterschiedliche Geräte „verständigen“ können, wenn sie das gleiche Profil beherrschen, ohne dass der Benutzer die Parameter am Gerät manuell einstellen muss. Einige Profile werden von fast allen BTs unterstützt.

Bluetooth unterstützt sowohl synchrone, SCO⁴⁰, (Sprachübertragung) als auch asynchrone, ACL⁴¹ (das sind vorwiegend Datenverbindungen), Verbindungen.

2.2.3.3. Positionsbestimmung mit Bluetooth

Da die Reichweite von Bluetooth-Geräten beschränkt ist, bieten sich für die Positionsbestimmung die Proximity- und Presence-Methoden an. Wenn sich ein BT mit einem anderen BT (z.B. einer Bluetooth-Bake) verbindet, dessen Position bekannt ist, kann die Position der BT mit einer Genauigkeit bestimmt werden, die der Reichweite des BTs entspricht. Für BTs der Klasse 3 sind dies ca. 10 Meter.

³⁹ SIG = Bluetooth Special Interest Group

⁴⁰ SCO = Synchronous, Connection Oriented

⁴¹ ACL = Asynchronous Connection Less

HALLBERG, J., NILSSON, M. (2002) führen ein System an, bei dem die BTs ihre Position an andere BTs übermitteln, bzw. die Positionsdaten von BTs über eine Internetverbindung von einem zentralen Server abfragen können. Bei bekannten Positionen mehrerer BTs in Reichweite kann daraus durch Multilateration die Position noch wesentlich genauer bestimmt werden.

Eine weitere Möglichkeit besteht darin, über synchronisierte Bluetooth-Basisstationen und TDoA-Messung beim mobilen BTs die Entfernungen zu den Basisstationen zu berechnen, und daraus durch Multilateration die Position zu bestimmen. Damit sind Genauigkeiten im Bereich von 1 Meter erzielbar (vgl. FISCHER, G. et al (2004)).

2.2.3.4. Zusammenfassung:

Bluetooth ist sowohl als Datenübertragungstechnologie als auch als Positionsbestimmungstechnologie für das gegenständliche Projekt gut geeignet. Da die Reichweite in Innenbereichen meist auf einen Raum begrenzt ist (ca. 10m), ließe sich mit Bluetooth mit relativ einfachen Mitteln ein Proximity- bzw. Presence-Verfahren für die Positionsbestimmung umsetzen. Aufgrund des Frequency-Hoppings und der verfügbaren Verschlüsselungsmechanismen ist auch eine gute Datensicherheit gegeben. Dies auch wegen der geringen Reichweite von Bluetooth, was ein Abhören aufgrund der notwendigen örtlichen Nähe wesentlich erschwert.

Nachteilig ist, dass bei Bluetooth der Verbindungsaufbau einige Sekunden in Anspruch nehmen kann. Die Datenübertragung zu einem zentralen Server ist allerdings mit Bluetooth alleine nicht umsetzbar.

2.2.4. ZigBee⁴²

ZigBee gehört zur Familie der WPANs, setzt auf dem Standard IEEE 802.15.4 auf, und ist für kostengünstige, energiesparende ad hoc Netzwerke im Nahbereich (bis zu ca. 100m) konzipiert. ZigBee ist speziell für die Vernetzung von z.B. „smarten“ Haushaltsgeräten und auch technischen Industriegeräten (Kleingeräten) auf kurzer Distanz ausgelegt. Die Datenübertragungsraten sind relativ gering (20-250 kBit/s; Quelle: ZigBee Alliance).

⁴² Informationen stammen von ASHTON, S. (2009) und <http://de.wikipedia.org/wiki/ZigBee>, zuletzt geprüft am 24.10.2009

2.2.4.1. ZigBee-Vernetzung

ZigBee unterstützt verschiedene Vernetzungsformen (vermaschte Netze, Baumstrukturen) und enthält auch zeitgemäße Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung auf Netzwerkebene und Anwendungsebene.

ZigBee ist sowohl für das UHF-Band als auch für das Mikrowellenband definiert. Die Hardwareanbieter konzentrieren sich aber zum überwiegenden Teil auf das Mikrowellenband im 2,4 Ghz-Bereich (vgl. <http://wiki.informatik.hu-berlin.de/nomads/index.php/Rfid#ZigBee>).

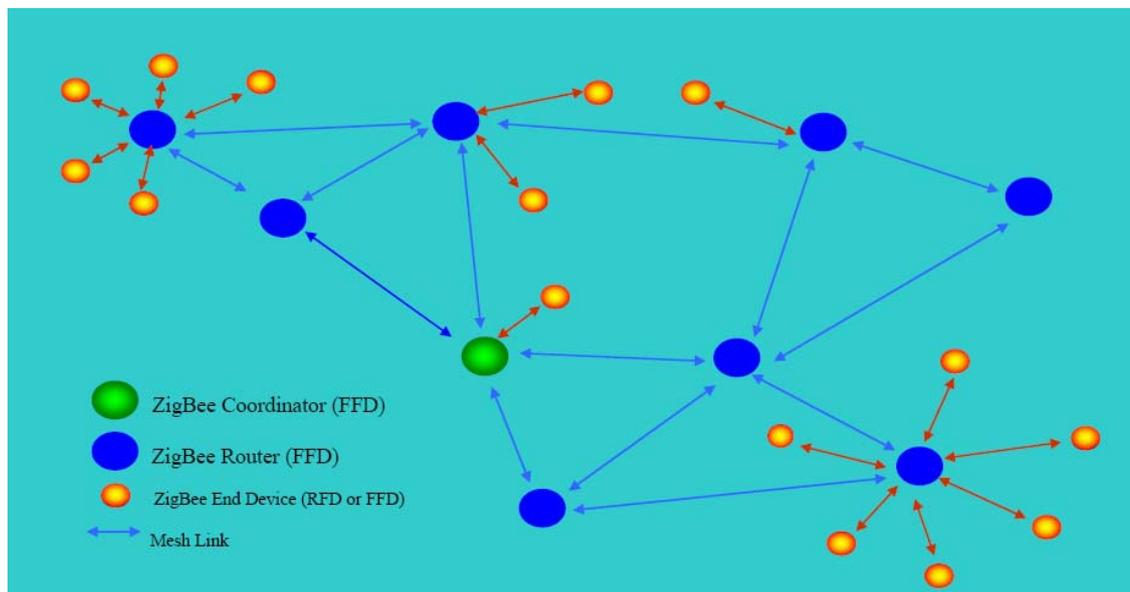


Abbildung 14: ZigBee-Vernetzung

Quelle: ASHTON, S. (2009)

ZigBee bildet selbstorganisierende Sensornetzwerke, da jedes ZigBee-Gerät auch eine Routingfunktionalität beinhaltet. Im Netzwerk gibt es ZigBee-Geräte in drei verschiedenen Rollen:

- Koordinator (FFD⁴³): Genau ein Gerät übernimmt die Rolle des Koordinators. Dieser steuert und überwacht das Netzwerk.
- Router (FFD): Diese übernehmen Routingaufgaben im Netzwerk und bilden die Netzwerktopologie aus.
- Endgerät: sind entweder Geräte mit reduziertem Funktionsumfang (RFD⁴⁴) oder mit vollem Funktionsumfang (FFD)

⁴³ FFD = Full Function Device

⁴⁴ RFD = Reduced Function Device

2.2.4.2. Anwendungsprofile

Für den Einsatz in verschiedenen Einsatzgebieten gibt es eine Reihe von Anwendungsprofilen (Application Profiles). Die Anwendungsprofile wurden von Anwendern, Geräteherstellern bzw. Service-Providern erstellt, und sollen den Einsatz für bestimmte Einsatzszenarien vereinfachen. In den Profilen sind z.B. geregelt:

- Netzwerk und Sicherheitseinstellungen
- Gerätetypen für das jeweilige Anwendungsprofil
- Meldungen und Attribute für die Geräte

Profile gibt es z.B. für das Gesundheitswesen, Telekommunikationsservices, Gebäudeautomatisierung, Haushaltsautomatisierung und weitere.

2.2.4.3. Schlussfolgerung

ZigBee ist als aufstrebender Standard in Sensornetzwerken und hier speziell in aktiven RFID-Tags für RTLS in Gebäuden sehr gut geeignet. Da ZigBee-Netzwerke „selbstorganisierend“ sind, und vermaschte Strukturen bilden, sind sie schnell und kostengünstig aufgebaut. Auch für die konzipierte Sicherheitslösung wären aktive RFID-Tags auf ZigBee-Basis sehr gut geeignet. Über WLAN oder LAN erfolgt die Einbindung in die Kommunikationsinfrastruktur (vgl. HEGLI, R. (2008)). Ein weiterer Vorteil ist, dass der Energieverbrauch der Tags sehr niedrig und daher eine lange Einsatzdauer ohne Batteriewechsel gegeben ist, was ein wichtiges Kostenargument ist.

2.2.5. Infrarot IrDA⁴⁵

IrDA ist ebenfalls eine WPAN-Übertragungstechnologie. Als Übertragungsmedium wird Infrarot-Licht eingesetzt. Infrarot-Licht ist eine elektromagnetische Welle mit einer Wellenlänge zwischen 780 und 1.000 nm, wobei IrDA den Bereich von 850 bis 900 nm verwendet. Im Unterschied zu Bluetooth ist bei IrDA eine Sichtverbindung erforderlich, weil Infrarot-Licht keine massiven Gegenstände durchdringen kann. Nachteilig wirkt sich auch aus, dass bei dieser Technologie die Übertragung durch Sonnenlicht erheblich gestört wird, daher ist diese Übertragungstechnologie nur für Innenräume geeignet. Ein weiterer Unterschied zur Bluetooth ist, dass Infrarot-Verbindungen eine relativ starke Richtwirkung haben.

⁴⁵ IrDA = **I**nfrared **D**ata **A**ssociation
Manfred Farthofer

Die IrDA-Technologie hat ihren Ursprung im Jahr 1993 und in der Firma HP. Diese schloss sich in der Folge bei der Entwicklung des Standards mit zahlreichen weiteren Unternehmen zur IrDA-Gruppe zusammen. IrDA 1.0 war ursprünglich auf 115,2 kBit/s ausgelegt, wurde in der Folge aber schnell auf 4 Mbit/s erweitert (Fast IR; IrDA 1.1). 1999 wurde der Standard nochmals auf 16 Mbit/s erweitert (Very Fast IR; IrDA 1.3).

Die Spezifikation des IrDA-Standards umfasst zwei Teilstandards, nämlich IrDA-Control und IrDA-Data (vgl. ROTH, J. (2005)). IrDA Control ist für die Verbindung von einfachen Peripheriegeräten gedacht (z.B. Mäusen, Tastaturen). Die Datenraten von IrDA-Control sind relativ gering (bis zu 75 kbit/s); die Entfernung darf dabei bis zu 5 m betragen. IrDA-Data ist für höhere Datenübertragungsraten ausgelegt und dementsprechend für die Kommunikation zwischen Geräten wie digitalen Kameras, Drucker, usw. geeignet.

2.2.5.1. Zusammenfassung:

Die Begrenzung von IrDA-Datenübertragung auf einen Raum lässt ein einfaches Proximity bzw. Presence-Verfahren für die Positionsbestimmung mit Raumgenauigkeit zu. Die Infrarotdatenübertragung ist für das gegenständliche Projekt aber wegen der notwendigen Sichtverbindung und der damit zusammenhängenden notwendigen aktiven Ausrichtung des Empfangsgerätes zum Sender wenig geeignet. Weiters wären wegen Tageslicht in zahlreichen Räumen teilweise erhebliche Störungen zu erwarten.

Vorteil wäre, dass es sich um eine kostengünstige Technologie handelt, die in vielen Geräten im Standard verfügbar ist.

Die IrDA-Technologie weist auch eine hohe Sicherheit gegen Abhören auf, weil dafür aufgrund der geringen Reichweite die örtliche Nähe (sowohl in Entfernung als auch in Richtung) erforderlich ist.

Da die Nachteile überwiegen, wird der IrDA-Ansatz nicht mehr weiter verfolgt.

2.3. RFID

2.3.1. Allgemeines

Jonathan COLLINS⁴⁶ definiert RFID in seiner umfassendsten Form als: “*RFID encompasses any system that uses radio frequency to identify an object*”.

⁴⁶ <http://www.rfidjournal.com/article/view/4819>, zuletzt geprüft am 24.10.2009

FASTH, Å. et al (2005) verstehen in ihrer Arbeit unter RFID eine Technologie für die automatische Datenerfassung, die Funkwellen verwendet, um Daten zwischen einem Lesegerät und einer mobilen Einheit zu übertragen um diese zu identifizieren, zu kategorisieren und zu verfolgen. RFID (Radio Frequency Identification) ermöglicht somit das berührungslose Identifizieren von Objekten, die mit einem Gerät, sogenannten Tags (Transponder), gekennzeichnet sind.

Die RFID-Technologie hat ihren Ursprung in den 1940-er Jahren (vgl. OECD (Hg.) (2004)). In dieser Zeit wurden aufbauend auf den Erkenntnissen aus der Funktechnik und der Radartechnik erste Konzepte auf Basis der Modulation von reflektierten elektromagnetischen Wellen erarbeitet. Weitere Verbreitung fand die RFID-Technologie in den 1990-er Jahren. Hier waren das aber vor allem proprietäre RFID-Systeme. Die unterschiedlichen Systeme waren dabei meist inkompatibel, was einen breiteren Einsatz erschwerte. Erst in den späten 1990-er Jahren schritt die Standardisierung der RFID-Systeme voran (ISO 18.000-Serie und „Auto-ID Centre Specifications“). Dies förderte die breitere Verwendung der RFID-Technologie und senkte die Kosten der Systeme deutlich.

2.3.2. Vorteile von RFID

RFID hat gegenüber anderen Kennzeichnungssystemen, wie z.B. Barcode, wesentliche Vorzüge. Diese sind (vgl. OECD (Hg.) (2004)):

- Es ist keine Sichtverbindung zwischen Lesegerät und Tag erforderlich.
- Die Tags können automatisch ausgelesen werden.
- Die Information kann unabhängig vom Zeitpunkt der Tagproduktion auf die Tags geschrieben werden.
- Die Tags sind je nach Bauweise auch wiederbeschreibbar.
- Es können viele Tags innerhalb kürzester Zeit ausgelesen werden (Pulkfähigkeit).
- Zum Teil hohe Datenübertragungsgeschwindigkeit.
- Einsatzmöglichkeit von Authentifizierung und Verschlüsselung.
- RFID-Tags sind unempfindlich gegenüber Umwelteinflüssen.

2.3.3. Arten von RFID-Systemen

Die Daten bei RFID-Systemen werden auf sogenannten Transpondern⁴⁷ (auch „Tags“ genannt) gespeichert und über geeignete Lesegeräte ausgelesen. Transponder bestehen aus einem Mikrochip und einer Antenne. Es gibt unterschiedlichste Tags in verschiedensten Formen. Häufige Formen sind z.B. das Kreditkartenformat oder die Etikettenform, Ohrmarken, Scheibenform oder auch Glasröhrchen (vgl. Andres, M. (2007)). Generell unterscheidet man zwischen aktiven Tags und passiven Tags. Aktive Tags besitzen eine eigene Energieversorgung über eine eingebaute Batterie, passive Tags werden ausschließlich über die elektromagnetischen Wellen des Lesegerätes mit Energie versorgt (z.B. induktive Kopplung).

Aufgrund der Übertragungreichweiten werden bei passiven Tags induktiv gekoppelte Systeme eingesetzt und bei aktiven Tags vorwiegend Backscatter-Systeme.

Es gibt auch noch Zwischentypen von Transpondern, wie die Semi-passiven Tags. Diese erweitern die Funktionalität passiver Tags, in dem sie auch Informationen speichern können, ohne dafür einen Reader zu benötigen. Dazu haben sie eine Batterie eingebaut. Semi-passive Tags werden häufig eingesetzt um Umweltdaten zu sammeln.

2.3.3.1. Induktive Kopplung

Induktiv gekoppelte Systeme nutzen das magnetische Feld für die Energieversorgung und Datenübertragung zwischen Schreib/Lesegerät (Reader) und Transponder.

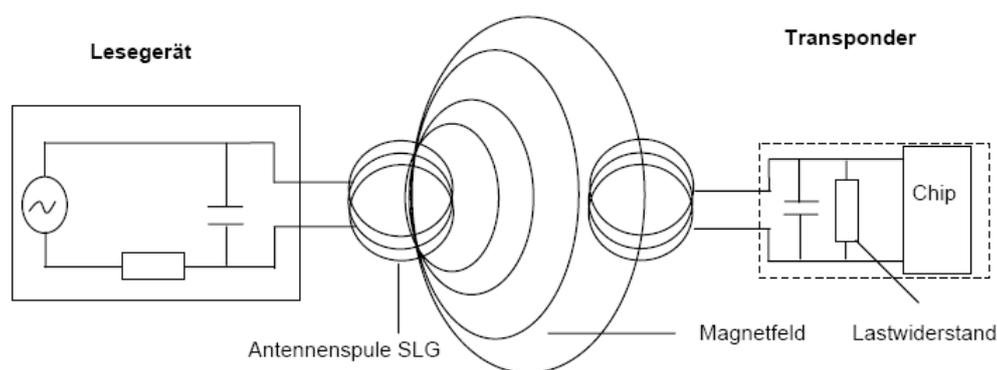


Abbildung 15: Prinzip der induktiven Kopplung

Quelle: Jansen, R. (2004)

⁴⁷ Transponder ist die Mischform aus Transmitter und Responder

2.3.3.2. Backscatter-Systeme

Backscatter-Systeme sind Systeme mit aktiven RFID-Tags und basieren auf Prinzipien der Radartechnik. Diese Tags besitzen eine eingebaute Batterie als Spannungsversorgung für den Chip. Ist der aktive Tag nicht in Reichweite eines Lesegerätes, so befindet sich der Tag im „Ruhemodus“, Standby oder auch Power-down-Modus. Die Energieaufnahme ist dabei stark reduziert. Erst durch die Energieeinwirkung der elektromagnetischen Wellen vom Lesegerät wird der Tag aktiviert. Die eingebaute Batterie dient dabei nicht der Datenübertragung. Die Übertragung der Informationen erfolgt ausschließlich über Modulation des von der Antenne des aktiven Tags rückgestrahlten Signals des Lesegerätes (daher der Name Backscatter). Sowohl Lesegerät als auch Tag haben bei Backscatter-Systemen Dipolantennen (zwecks Ausnutzung des Resonanzeffektes).

2.3.4. Datenfluss bei RFID-Tags

Im Wesentlichen gibt es drei Arten von Tags:

- Tags, die fest programmiert sind (nur Lesen; read only)
- Tags, die einmal beschrieben werden können (**Write Only**, **Read Many**; **WORM**)
- Tags, die mehrfach gelesen und beschrieben werden können (Read-Write)

2.3.5. Pulkfähigkeit

Eine weitere zentrale Eigenschaft der unterschiedlichen RFID-Systeme ist die „Pulkfähigkeit“, d.h. die Kommunikationsfähigkeit bei vielen Transpondern an einer Stelle. Würden alle Transponder gleichzeitig auf ein RFID-Lesegerät ansprechen, so würde keine geordnete Datenübertragung zwischen Transponder und Lesegerät zustande kommen. Deshalb müssen die Transponder und/oder die Lesegeräte besondere Funktionen (Antikollision) implementiert haben. Moderne RFID-Systeme können dutzende bis einige hundert Tags innerhalb einer Sekunde auslesen (vgl. OECD (Hg.) (2004)).

2.3.6. Bauformen

RFID-Tags gibt es in vielen Bauformen. LOSSAU, V. (2007) führt dazu an: Scheibenbauform von wenigen mm Größe bis zu 10 cm Durchmesser, Glasröhrchen-

Bauweise (z.B. zur Tierkennzeichnung), Chipkarten-Transponder (am Verbreitesten sind Transponder in Kreditkartengröße), eingebaut in Schlüssel (z.B. bei PKW-Zündschlüssel) sowie in zahlreiche andere Gehäuse und Geräte. Für HF und UHF-Tags gibt es sogenannte Smart-Label-Bauformen. Das sind auf Rollen erhältliche RFID-Aufkleber in Etikettenform mit nur 0,3 mm Dicke.

Neben den Transpondern (Tags) in unterschiedlichsten Bauformen gibt es auch Lesegeräte in unterschiedlichsten Bauformen. Diese reichen von der in Kaufhäusern üblichen „Schleusenbauweise“ der Gate-Reader, die aus zwei gegenüberliegenden Einzelantennen bestehen, über Tunnelreader z.B. in der Warenlogistik, RFID-Druckern mit eingebautem RFID-Lesegerät bis zu handlichen PDAs mit integrierter RFID-Lesefunktion. Allgemein gilt, je niedriger die Frequenz des RFID-Systems, umso größer muss die Antenne und damit die Bauform des Lesegerätes sein.

2.3.7. Vergleich verschiedener RFID-Systeme

Im Vergleich dazu gibt JANSEN, R. (2004) folgende Tabelle der RFID-Systeme:

RFID-System	LF (125/134 kHz) passiv	HF (13,56 MHz) passiv	UHF (868/915 MHz) passiv	SHF (2,45 GHz) aktiv
Leseabstand ²⁷	bis 1000mm	bis 1700mm	bis 8000mm	bis 6000mm
Leseabstand bei Transponderapplikation auf Metall	bis 100mm (teilw. Ferritkerne notwendig)	bis 100mm (mit Ferritschicht)	nicht lesbar bei direkter Applikation auf Metall	bis 6000mm
Pulzfähigkeit	technisch noch nicht realisiert	bis zu 70 Transponder	bis zu 200 Transponder	bis zu 10 Transponder
Funktionsprinzipien	induktive Kopplung mit magnetischen Feldern		elektromagnetische Kopplung mit Radiowellen	
Datenspeicherung	Read Only und Read/Write	fast ausschließlich Read/Write	Read Only und Read/Write	fast ausschließlich Read/Write
Einfluss von Metall	niedrig (bei Ferromagnetika)	hoch (bei Ferromagnetika)	Reflexion an Metallen	Reflexion an Metallen
Einfluss von Flüssigkeiten	sehr niedrig	sehr niedrig	hoch	sehr hoch
Lebensdauer	EEPROM-Speicher bei Read/Write Systemen ist auf ca. 50.000 Schreibzyklen begrenzt		bis 10 Millionen Leseoperationen	8 Jahren oder 30 Millionen Leseoperationen
Datenübertragungsraten	niedrig	hoch	sehr hoch	sehr hoch
Preis je Transponder	0,3-0,6 €	0,3-1,0 €	0,2-0,5 €	30-50 €

Tabelle 2: Vergleich RFID-Systeme

Quelle: JANSEN, R. (2004)

Systeme bei denen die Entfernung zwischen Transponder und Lesegerät deutlich mehr als 1 Meter beträgt werden auch als „**Long Range- Systeme**“ bezeichnet.

Passive LF- und HF-Tags setzen als Übertragungsart die induktive Kopplung ein. UHF und Mikrowelle setzen vorwiegend Backscatter für die Kommunikation ein (vgl. BIZER, J. et al (2006)). Auch TCP/IP als Protokoll ist erst mit aktiven Tags möglich. Passive Tags scheitern wegen des hohen Protokoll-Overheads bei TCP/IP und des damit

zusammenhängenden größeren Energieaufwands für die Datenübertragung (es müssen einfach mehr Daten bei TCT/IP übertragen werden).

2.3.8. Standardisierung

Die Standardisierung der RFID-Technologie wird als wichtigster Treiber für die weitere Verbreitung dieser Technologie angesehen (vgl. VAN LIESHOUT, M. et al (2007)). Besondere Herausforderung dabei ist, dass die weltweiten Warenströme eine Standardisierung auf globalem Niveau erfordern. Eine wichtige Rolle dabei spielt EPC Global.



Abbildung 16: RFID-Frequenzen und maßgebliche Standards

Quelle: VAN LIESHOUT, M. et al (2007)

2.3.9. EPC Global

Eine besondere Bedeutung in Zusammenhang mit dem Einsatz von RFID, speziell auch in Richtung Standardisierung hat EPC⁴⁸ Global. EPC Global ist eine Organisation von Firmen und Industrien mit dem Ziel globale Standards für den EPC zu entwickeln, um damit die Verwendung der RFID-Technologie voran zu treiben. Beim EPC handelt es sich um einen standardisierten elektronischen Produktcode. Der EPC ist ein weltweit eindeutiger Code, mit standardisiertem Aufbau. Die Vision von EPC Global ist, dass quer über die Industrien durch Verwendung eines einheitlichen Standards die Effizienz entlang der gesamten Versorgungskette verbessert wird, und dass es für die Firmen möglich wird, in Echtzeit ihr Produkt von überall auf der Welt zu verfolgen (vgl. VAN LIESHOUT, M. et al (2007)). Der EPC wird in RFID-Tags gespeichert und identifiziert

⁴⁸ EPC = Electronic Product Code

einen Artikel eindeutig. EPC Global geht jedoch wesentlich weiter als „nur“ elektronische Produktcodes bereit zu stellen. Ziel ist es, die Warenströme vollständig zu automatisieren und mittels dem EPC Global Architecture Framework (EPC Global (2009)) entsprechende Web-Services bereitzustellen.

2.3.10. Sicherheit in Zusammenhang mit RFID-Systemen:

Da die Datenübertragung in der RFID-Technologie über eine Luftschnittstelle erfolgt, gibt es die in Funksystemen bestehenden Sicherheitsprobleme. Es kann einerseits die Datenübertragung von Dritten, die in Reichweite sind, abgehört werden, und es kann andererseits von Dritten eine nicht autorisierte Datenübertragung zu den Tags stattfinden. Die Datenübertragung zwischen Transponder und Lesegerät sollte bei sensiblen Informationen in verschlüsselter Form erfolgen. Die Verschlüsselungsmöglichkeit erhöht aber deutlich die Kosten für die Tags und die Lesegeräte und vermindert die Performance (vgl. OECD (Hg.) (2004)).

2.3.11. Schlussfolgerung

Die RFID-Technologie ist für die Ortung von Ressourcen nach den Proximity- und Presence-Methoden bestens geeignet. Durch die geringe Entfernung bei der Kommunikation zwischen Lesegerät und Transpondern ist eine Bestimmung zumindest auf Raumgenauigkeit auf Basis von mit Tags markierten Lokationen sehr gut möglich. So können z.B. ortsfeste Betriebsmittel (wie Maschinen) mit Tags gekennzeichnet werden. Das Auslesen der Tag-ID durch das mobile Lesegerät gibt bei bekannter Position des Betriebsmittels somit den Standort des Lesegerätes und damit des „Auslesers“ wieder. Beim Durchgang von einem Raum in den nächsten kann ebenfalls über entsprechende Anbringung der RFID-Tags der Standort raumgenau bestimmt werden, was für das gegenständliche Projekt ausreichend ist.

Da die Tags relativ preiswert sind, ist eine Kennzeichnung fester Punkte mit Tags für die Positionsbestimmung zu relativ niedrigen Kosten möglich.

2.4. Technologien zur Positionsbestimmung

2.4.1. Arten von Positionsdaten

Die Positionsbestimmung ist eine wichtige Aufgabe in Real Time Locating Systemen. Dabei kann die Angabe der Position auf unterschiedliche Arten erfolgen, je nachdem in

welchem Zusammenhang die Positionsangabe zu sehen ist, und welche Technologie eingesetzt wird. Vgl. ROTH, J. (2005) und SCHEURING, L. (2005).

Abhängig vom jeweiligen Kontext sind folgende Positionsangaben von Bedeutung:

- Absolute Position: Die Angabe der Position erfolgt durch die Angabe der 2D bzw. 3D-Position im Raum. Über die absolute Position kann jeder Punkt der Erdoberfläche eindeutig bestimmt werden.
- Relative Position: Bei der relativen Position erfolgt die Angabe bezogen auf einen bestimmten Punkt.
- Orientierung (Winkel) im Raum
- Semantische Position: Bei der semantischen Position wird die Position durch eine textliche Beschreibung angegeben. Eine semantische Position kann z.B. eine Adresse, eine Raumbezeichnung, eine Raumnummer, eine bestimmte Regalnummer, usw. sein.

2.4.2. Raumbezugssystem, Koordinatensystem

Wird die Raumposition über Koordinaten bestimmt, ist es wichtig zu wissen, wie sich die Koordinaten errechnen. Die Grundlagen zum Raumbezug sind in der ISO-Norm ISO 19111 enthalten. Diese Norm definiert das konzeptionelle Schema für Koordinatenreferenzsysteme (CRS⁴⁹). Dabei wird der Zusammenhang zwischen Koordinatenreferenzsystem, geodätischem Datum und Koordinatensystem (CS)⁵⁰ dargestellt. Eine weit verbreitete Referenz für Raumbezugssysteme ist das Verzeichnis der EPSG⁵¹.

Als Beispiele werden hier die in Österreich gültigen Gauß-Krüger-Systeme MGI (Ferro) / M28, M31 bzw. M34, auch „Bundesmeldenetz“ genannt, angeführt. Eine Liste der weltweit verfügbaren Koordinatenreferenzsysteme ist wiederum in der EPSG-Datenbank⁵² enthalten.

Bei gemeinsamer Betrachtung (Prozessierung) von unterschiedlichen Positionsdaten (z.B. mit semantischen Positionsinformationen und Koordinateninformationen) ist es erforderlich, ein gemeinsames Bezugssystem herzustellen, z.B. indem jeder semantischen Positionsinformation eine Koordinate (2D oder 3D) im entsprechenden Raumbezugssystem zugewiesen wird.

⁴⁹ CRS = Coordinate Reference System

⁵⁰ CS = Coordinate System

⁵¹ EPSG= European Petroleum Survey Group Geodesy; siehe www.epsg.org

⁵² http://www.epsg.org/databases/Discv6_18.html; zuletzt geprüft am 15.03.2009

2.4.3. Technologien zur Positionsbestimmung

Bei der Positionsbestimmung kann grundsätzlich eine Einteilung in drei Gruppen erfolgen. (vgl. ROTH, J.. (2005)). ROTH unterscheidet in „Satellitennavigation“, „Navigation innerhalb von Gebäuden“ und Netzwerkgestützte Navigation.

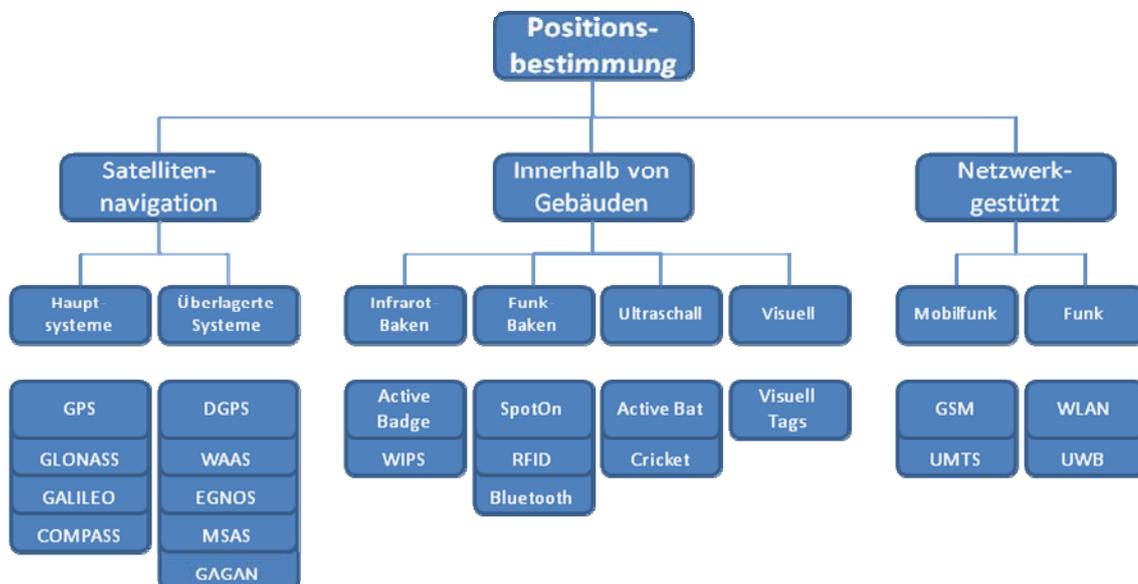


Abbildung 17: Verfahren zur Positionsbestimmung

Quelle: Vgl. ROTH, J (2005), Mobile Computing, S278; mit eigenen Ergänzungen

BEINAT et al (2007) führt hinsichtlich Einsatzbereich und Genauigkeit der Positionsbestimmung dazu an:

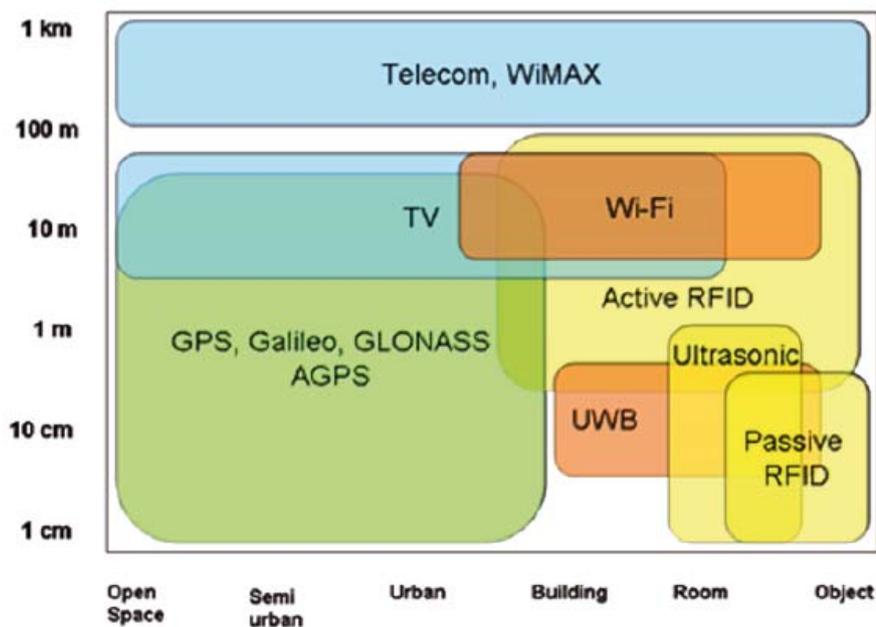


Abbildung 18: Ortungs- und Identifikationstechnologien

Quelle: BEINAT et al (2007)

2.4.4. Satellitennavigation

Da die Satellitennavigation für die beschriebenen Anwendungsszenarien in EVU eine zentrale Rolle für die Positionsbestimmung einnimmt, wird hier auf die Technik näher eingegangen.

In Wikipedia⁵³ ist folgende Definition für ein Globales Satellitennavigationssystem angeführt: „*Global Navigation Satellite System (GNSS) is the standard generic term for satellite navigation systems that provide autonomous geo-spatial positioning with global coverage.*”

Unter Satellitennavigation wird also die Positionsbestimmung einer Mobilstation (MS) auf der Erde durch Empfang und Auswertung der Signale von Satelliten verstanden. Dabei werden von der MS gleichzeitig die Signale von mehreren Satelliten empfangen und ausgewertet. Aus den Signalen lässt sich die genaue Entfernung der MS zu den Satelliten berechnen. Als Verfahren kommt hier das ToA-Verfahren⁵⁴ kombiniert mit Multilateration zum Einsatz. Um die Position im Raum bestimmen zu können, benötigt man zumindest den Empfang der Signale von drei Satelliten. Durch den Schnitt dreier Kugeln kann daraus die Position berechnet werden. Um auch den Zeitfehler eliminieren zu können, ist der Empfang des Signales von zumindest noch einem vierten Satelliten erforderlich, daher sind für die genaue Positionsbestimmung in einem dreidimensionalen Raum, mindestens vier Satelliten erforderlich.

Vorteile der Positionsbestimmung über Satellitennavigation sind (Vgl. ROTH, J. (2005)):

- Anwendung ist weltweit mit großer Genauigkeit möglich.
- Es sind unterschiedlichste bereits sehr kostengünstige Standardempfänger am Markt verfügbar.
- Die Nutzung des zivilen Dienstes ist kostenfrei.
- Umwelteinflüsse haben nur einen geringen Einfluss auf die Genauigkeit.

Nachteile sind:

- Es ist eine Sichtverbindung zwischen Satelliten und MS erforderlich. Im inneren von Gebäuden ist keine Positionsbestimmung möglich; Abschattungen in dicht bewaldeten Gebieten und in Straßenschluchten.
- Der Erhalt und der Betrieb der Systeme ist kostenaufwändig.

⁵³ http://en.wikipedia.org/wiki/Global_navigation_satellite_system, geprüft am 12.03.2009

⁵⁴ TOA = Time of Arrival

- GPS ist militärisch orientiert, daher keine Garantie für die Verfügbarkeit des zivilen Signals.
- Keine Integritätsinformationen für zivile Nutzer.

2.4.4.1. GPS

Das bei uns (in Europa) meist verwendete Satellitennavigationssystem ist das **Global Positioning System (GPS)**⁵⁵ der vereinigten Staaten von Amerika. Das GPS hat seinen Ursprung im militärischen Bereich, und hat über die Jahre eine hohe zivile Bedeutung erlangt. GPS ist ein global verfügbares System. Ihm liegt die Idee zugrunde, dass an jedem Punkt der Erde die Position (Koordinaten in Form von Längen und Breitengraden sowie der Höhe) sehr genau bestimmt werden kann. Zu den Koordinaten kann auch noch die Zeit⁵⁶ sehr genau bestimmt werden. Beim GPS senden alle Satelliten die Signale auf einer Frequenz von 1575,42 MHz. Damit sich die Signale der einzelnen Satelliten nicht gegenseitig stören, werden diese über ein spezielles Verfahren⁵⁷ „zerstückelt“. Jeder Satellit kann dann über sein spezielles Muster identifiziert werden. Die Informationsinhalte der GPS-Signale sind im Detail (vgl. ZOGG, J.M. (2006), S23):

- Satellitenzeit und Synchronisationssignale
- Präzise Bahndaten des Satelliten (Ephemeriden)
- Zeitkorrekturinformationen zur Bestimmung der exakten Satellitenzeit
- Ungenauere Bahndaten aller Satelliten (Almanach)
- Korrektursignale zur Berechnung der Laufzeit
- Daten über die Ionosphäre
- Informationen über den technischen Zustand (Status) der Satelliten

Das GPS besteht aus dem „**Raumsegment**“, dem „**Kontrollsegment**“ und dem „**Benutzersegment**“. Das Benutzersegment ist das für die Nutzung der GPS-Anwendungen maßgebliche Segment. Über das Kontrollsegment wird das GPS gesteuert, und im Raumsegment befinden sich die Satelliten.

⁵⁵ die vollständige Bezeichnung lautet: **NAV**igation System with **T**iming **A**nd **R**anging **G**lobal **P**ositioning System, NAVSTAR-GPS

⁵⁶ Weltzeit: Universal Time Coordinated, UTC

⁵⁷ CDMA-Multiplex-Verfahren (**C**ode-**D**ivision **M**ultiple-Access **V**erfahren)

Beim GPS umkreisen die Satelliten die Erde in 6 Bahnen. Die Bahnen sind zum Äquator um 55° geneigt. Mit Stand November 2009⁵⁸ besaß das GPS 32 aktive Satelliten. Jeder Satellit ist mit vier hochpräzisen Atomuhren ausgestattet.

Derzeit gibt es auf den Frequenzen L1 und L2 jeweils unterschiedliche Signalqualitäten für den zivilen und den militärischen Bereich. Für den zivilen Bereich ist der SPS (Standard Positioning Service) frei verfügbar. Das hochpräzise militärische Signal PPS (Precise Positioning Service) kann nur von autorisierten Stellen genutzt werden.

Für die Genauigkeit des Systems ist eine Vielzahl von Einflussfaktoren maßgeblich. Besonders anzuführen sind Einflüsse der Ionosphäre⁵⁹ und der Troposphäre⁶⁰ für die Signalübertragung Satellit – MS, die Genauigkeit der Atomuhren an Board der Satelliten, sowie Hintergrundrauschen und Multipath-Effekte⁶¹ (vgl. OOSTERLINCK (2004), S79). Durch Anwendung abgestimmter Modelle (z.B. eines entsprechenden Ionosphären-Modells) kann die Genauigkeit deutlich verbessert werden.

Erzielbare Genauigkeit mit handelsüblichen GPS-Empfängern:

Genauigkeit des ursprünglichen GPS-Systems mit aktivierter SA ⁶²	±100 Meter
Typische Positionsgenauigkeit ohne SA	±15 Meter
Typische Differential-GPS (DGPS)-Genauigkeit	±3-5 Meter
Typische Genauigkeit mit aktiviertem WAAS/EGNOS	±1-3 Meter

Tabelle 3: Erreichbare Genauigkeiten bei GPS

Quelle: <http://www.kowoma.de/gps/Genauigkeit.htm>, geprüft am 24.10.2009

2.4.4.2. GLONASS

Neben dem GPS der US-Amerikaner betreibt auch die Russische Föderation ein globales Satellitennavigationssystem mit dem Namen GLONASS⁶³. Nach vorübergehenden Problemen um die Jahrtausendwende verfügt GLONASS nun wieder über einen stabilen Betrieb. Derzeit⁶⁴ sind 17 Satelliten aktiv, zwei sind in Wartung.

⁵⁸ Quelle <http://www.kowoma.de/gps/gpsstatus/>; zuletzt geprüft am 21.11.2009

⁵⁹ Die Ionosphäre ist jener Teil der Erdatmosphäre, der oberhalb ca. 80 km Höhe beginnt und bis ins Weltall reicht. Dieser Teil enthält signifikante Anteile geladener Teilchen (Ionen und Elektronen), daher auch der Name Ionosphäre

⁶⁰ Die Troposphäre ist die unterste Schicht der Atmosphäre und reicht je nach Ort von zwischen 8 und 18 km hoch.

⁶¹ Multipath-Effekte entstehen durch Reflexion der Signale an Objekten. Die Empfänger fangen dann nicht nur die Signale auf direktem Weg, sondern auch die reflektierten, zeitlich versetzten Signale auf. Dadurch kommt es zur Überlagerung von Signalen und entsprechenden Fehlern.

⁶² SA = Selective Availability; künstliche Verfälschung der GPS-Signale durch den Betreiber (Militär)

⁶³ GLONASS = GLObal NAVigation Satellite System

⁶⁴ Lt. Info auf der Webseite der Russian Space Agency vom 24.10.2009; online unter <http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:20:1200169092638667370::NO:::>, zuletzt geprüft am 24.10.2009

2.4.4.3. GALILEO

Europa entwickelt zurzeit ein eigenes Satellitennavigationssystem mit dem Namen Galileo. Die Einsatzfähigkeit dieses Systems soll etwa 2013⁶⁵ gegeben sein. Das Ziel von GALILEO ist es, ein eigenständiges europäisches globales Satellitennavigationssystem auf ziviler Basis zu errichten, das eine sehr genaue Positionsbestimmung ermöglicht und interoperabel mit anderen existierenden GNNS (z.B. GPS und GLONASS) ist (Vgl. OOSTERLINCK (2004), S80). Das vollständige System Galileo⁶⁶ wird aus 30 Satelliten und der zugehörigen Bodeninfrastruktur bestehen.

2.4.4.4. DGPS⁶⁷

Dabei handelt es sich um ein System bei dem die GPS-Empfänger zusätzlich Korrekturdaten verwenden, um die Genauigkeit der Positionsbestimmung zu verbessern. Die Korrekturdaten werden an sogenannten Referenzstationen ermittelt, deren Position sehr genau bekannt ist. Aus der bekannten Position und über die aus den GPS-Signalen errechnete Position kann ein Korrekturvektor berechnet werden, der die Fehlereinflüsse (insbesondere jene der Ionosphäre) ausgleicht. Die Korrekturdaten werden über eine Kommunikationsverbindung (z.B. GSM) zu den Empfängern übermittelt und auf die im GPS-Empfänger ermittelte Position angewendet. Damit ist eine sehr genaue Positionsbestimmung (je nach Empfänger bis in den cm-Bereich) möglich. Die Korrekturdaten sind nur in einem begrenzten Bereich um die Referenzstation (ca. 70-200 km) gültig. Im Realbetrieb werden deswegen Netze mit Referenzstationen gebildet, um ganze Länder mit Korrekturdaten versorgen zu können (siehe z.B. SAPOS in Deutschland bzw. APOS, NetFOCUS in Österreich). Die Nutzung der Korrekturdaten ist meist kostenpflichtig.

2.4.4.5. WAAS, EGNOS, MSAS, GAGAN

Dies sind im Prinzip satellitenbasierte DGPS. Man nennt diese Systeme auch SBAS (Satellite Based Augmentation System). WAAS⁶⁸ ist das System der Amerikaner, EGNOS⁶⁹ das System der Europäer, MSAS⁷⁰ das System der Japaner bzw. weiterer

⁶⁵ Quelle: http://ec.europa.eu/transport/galileo/programme/programme_en.htm; zuletzt geprüft am 12.03.2009

⁶⁶ Vgl. http://ec.europa.eu/transport/galileo/index_en.htm; zuletzt geprüft am 12.03.2009

⁶⁷ DGPS = **D**ifferential **G**PS

⁶⁸ WAAS = **W**ide **A**rea **A**ugmentation **S**ystem

⁶⁹ EGNOS = **E**uropean **G**eostationary **N**avigation **O**verlay **S**ervice

⁷⁰ MSAS = **M**ulti-**F**unctional **S**atellite **A**ugmentation **S**ystem

asiatischer Staaten und GAGAN das in Aufbau befindliche System der Inder. Die Systeme decken immer nur einen begrenzten geografischen Bereich ab. Entwickelt wurden die Systeme für die Luftfahrt, um die Zuverlässigkeit und Genauigkeit von GPS zu erhöhen, und damit für die Luftfahrt nutzbar zu machen. Bei allen diesen Systemen werden jeweils in einem zentralen Rechenzentrum, die über ein Netz von genau eingemessenen Referenzstationen am Boden empfangenen GPS-Signale miteinander verrechnet.

2.4.5. Positionsbestimmung innerhalb von Gebäuden

2.4.5.1. Infrarot-Baken

Die Positionsbestimmung auf Infrarotbasis wendet das Proximity- bzw. Presence-Verfahren ein. Da Infrarot nur auf relativ kurze Distanzen funktioniert, vom Tageslicht gestört wird und Wände nicht durchdringen kann, wird es nur in Innenräumen eingesetzt. Es gibt Lösungen mit stationären Infrarot-Badges als Empfangsgeräten, welche die Infrarot-Impulse von mobilen Sendern empfangen (siehe System Active Badge) aber auch Systeme mit mobilen Infrarot-Empfangsgeräten, welche die Infrarotsignale von stationären Infrarot-Baken auffangen (siehe System WIPS).

Gemeinsam ist den Infrarotsystemen, dass sie kostengünstig aufgebaut werden können, die benötigte Hardware kostengünstig ist und einen geringen Energieverbrauch aufweisen. Für die Funktionsfähigkeit ist eine direkte Sichtverbindung erforderlich.

Nähere Erläuterungen sind in den Beschreibungen der jeweiligen Lösungen zu finden.

2.4.5.2. Funk-Baken

Bei Funk-Baken handelt es sich um Systeme mit meist fest angebrachten Funksendern und mobilen Empfangsgeräten. Die mobilen Empfangsgeräte empfangen die Signale der stationären Funkbaken und werten die Signale aus. Aber auch Systeme mit umgekehrtem Weg, nämlich mobile Sendegeräte (Funkbaken) und stationäre Empfangsgeräte werden eingesetzt (siehe z.B. Lösung Spot On). Häufig anzutreffen ist auch die Variante, dass sowohl Funkbake (z.B. in Form eines Transponders oder einer Funkwanze) als auch Empfangsgerät mobil sind. Als typisches Beispiel kann hier die RFID-Lösung mit aktiven Tags angeführt werden. Es kommen unterschiedliche Verfahren für die Positionsbestimmung in Frage:

- Proximity

- Presence
- CoO
- Multilateration
- Triangulation
- TDoA
- RSSI

Es werden unterschiedliche Funktechniken eingesetzt wie z.B. RFID, Bluetooth, UWB und ZigBee. Mehr dazu in den jeweiligen Kapiteln.

Gemeinsam ist den funkbasierten Systemen, dass keine Sichtverbindung (Line of Sight) erforderlich ist, und dass die Systeme zumeist kostengünstig und schnell aufgebaut werden können. Schwieriger gestaltet sich allerdings die Abgrenzung der Zellen, da Funksignale feste Gegenstände (wie z.B. Wände durchdringen können). Zur Feststellung der Nahebeziehung ist im Empfangsbereich mehrerer Baken zusätzlich z.B. eine Signalstärkenmessung erforderlich. Empfindlich sind funkbasierte Systeme gegenüber Multipath-Effekten.

2.4.5.3. Ultraschall

Ultraschallbasierte Lösungen haben aufgrund der Langwelligkeit der Schallwellen gegenüber Funkwellen eine wesentlich bessere räumliche Auflösung. Ultraschall wird dabei zur Messung der Abstände zwischen Sender und Empfänger eingesetzt. Es gibt wiederum Lösungen mit mobilen Sendern und festen Empfängern (siehe System Active Bat) als auch umgekehrt mit mobilen Empfängern und festen Sendern (siehe System Cricket). Gemeinsam ist den beiden Systemen ihre hohe Genauigkeit (im cm-Bereich), aber auch ihr aufwändiger, kostenintensiver Aufbau. Weiters ist Ihnen gemeinsam, dass sie für sich alleine nicht funktionieren, sondern zusätzlich Funk zur Zeitsynchronisation und Kommunikation benutzen, da Ultraschall ausschließlich für die Entfernungsbestimmung verwendet wird. Für die genaue Positionsbestimmung ist eine Sichtverbindung erforderlich. Multipath-Effekte können die Genauigkeit der Messungen empfindlich stören. Eingesetzte Verfahren für die Positionsbestimmung sind Presence, Multilateration und TDoA.

2.4.6. Netzwerkgestützte Verfahren

2.4.6.1. Positionsbestimmung über Mobilfunk

In Verbindung mit Mobilfunk gibt es zahlreiche Verfahren die Position einer MS zu bestimmen.

2.4.6.1.1. AoA⁷¹:

Bei diesem Verfahren werden bei der BTS Antennen mit Richtungscharakteristik verwendet. Aus den gemessenen Winkeln unter dem die Signale der MS bei der Antenne der BTS einlangen und den bekannten Standorten der BTS kann durch Angulation die Position der BTS berechnet werden. Die Genauigkeit liegt zwischen 50 und 150 Meter.

2.4.6.1.2. Cell-Identification (Cell-Id)

Eine weitere Methode zur Positionsbestimmung in Mobilfunknetzen ist die Cell-Id. Dabei erhält das mobile Gerät die Koordinate der jeweiligen BTS, bei der die MS angemeldet ist. Die Cell-Id ist auch der MS bekannt. Die Genauigkeit dieser Methode hängt von der Zellgröße ab und schwankt zwischen 50m und mehreren 10 km (Femtozellen bis Makrozellen).

2.4.6.1.3. RX-Methode in Verbindung mit CI

Bei diesem Verfahren wird bei der MS zusätzlich die Signalstärke der BTS-Signale gemessen. Die Signalstärke ist ein Maß für die Entfernung MS-BTS. Die Methode ist allerdings relativ ungenau, weil die Signaldämpfung verschiedenen Umgebungseinflüssen und Witterungseinflüssen unterliegt. Die Genauigkeit liegt zwischen 100 Meter und bis zu 20 km (je nach Zellgröße).

2.4.6.1.4. U-TDOA⁷²

Bei diesem Verfahren werden im Mobilfunknetz die Laufzeitunterschiede der Signale vom Aussenden eines Signals bei der BTS und dem Empfangen der Antwort von der MS bestimmt, und daraus die Entfernungen MS-BTS berechnet. Das Mobilfunknetz

⁷¹ AoA = **A**ngle of **A**rriVal

⁷² U-TDOA = **U**plink-**T**ime **D**ifference of **A**rriVal

muss dabei erweitert werden, und zwar die BTS mit einer LMU⁷³, und das gesamte Netzwerk mit einer zentralen SMLC⁷⁴. Die Positionsbestimmung erfolgt über Multilateration durch die SMLC. Die Genauigkeit dieses Verfahrens liegt bei ca. 50 bis 200 Meter.

2.4.6.1.5. E-OTD⁷⁵

E-OTD entwickelt sich derzeit zum De-Facto-Standard für die Positionsbestimmung in Mobilfunknetzen. Das Verfahren basiert auf dem Umstand, dass die Funksignale verschiedener BTS entsprechend der Laufzeiten der Signale zu unterschiedlichen Zeiten bei einer MS ankommen. Die MS sendet eine Aufforderung an alle BTS in der Nähe. Diese senden eine Antwort. Die Laufzeitdifferenzen zwischen Aussenden der Aufforderung und Eintreffen der Antworten der verschiedenen BTS werden von der MS mit gewissen Toleranzen gemessen, und an die SMLC übertragen, die daraus den Abstand der MS zu den jeweiligen BTS errechnet. Die Position wird durch Multilateration (zumindest 3 Entfernungen) bestimmt (vgl. WILDE, G. et al (2002)).

Die Genauigkeit der Methode liegt zwischen 50 (20) bis 200 Meter im GSM-Netz, und ist abhängig von der Anzahl der LMUs im Netzwerk.

2.4.6.1.6. TA⁷⁶-Verfahren

Verbessert werden kann die Positionsbestimmung mittels Cell-ID durch Verwendung des TA-Wertes. Dabei misst die BTS zu welcher Zeit, die von der MS ausgesendeten Bursts eintreffen, und fordert die MS ggf. auf, die Burst etwas früher oder später zu senden, damit der vorgesehene Zeitschlitz genau getroffen wird. Die Messung ist allerdings nur möglich, wenn eine aktive Gesprächsverbindung besteht. Die Genauigkeit dieser Methode liegt bei etwa 500 Meter auch in großen Zellen (vgl. KREMPL, S. (2003)).

2.4.6.1.7. GPS

Das Mobilfunkgerät hat einen eingebauten GPS-Empfänger. Methode siehe dazu im Kapitel 2.4.4. Genauigkeit ca. 10 bis 30 Meter.

⁷³ LMU = Location Measurement Unit

⁷⁴ SMLC = Serving Mobile Location Center

⁷⁵ E-OTD = Enhanced Observed Time Difference

⁷⁶ TA = Time Advance-Wert

2.4.6.1.8. A-GPS⁷⁷

Bei dieser Methode werden die GPS-Messungen durch Referenzdaten für die jeweilige Position aus zentralen Servern verbessert. Damit lässt sich die Genauigkeit deutlich verbessern, weil vom Server zusätzliche Bahndaten von Satelliten abgerufen, und auch die atmosphärischen Bedingungen besser berücksichtigt werden können. Weiterer Vorteil ist, dass dadurch die Zeit bis zu einer ersten Positionsbestimmung (Time to fix) deutlich verkürzt werden kann (vgl. SHU, W. et al (2008)). Genauigkeit ca. 5-10 Meter.

2.4.6.1.9. Korrelations-Verfahren:

Ein weiteres Verfahren ist es, eine „Landkarte“ der Funkdaten (z.B. Signalstärke, TDoA, ...) zu erstellen. Dabei wird in einem Raster berechnet bzw. gemessen, wie hoch die unterschiedlichen Funkdaten, in Bezug auf die BTS in Reichweite, in dieser Rasterzelle sind, und die Werte in einer Datenbank gespeichert.

Für die Positionsbestimmung werden nun die gemessenen Werte einer MS mit den gespeicherten Werten verglichen, und daraus jene Rasterzelle ermittelt, deren gespeicherte Messwerte am Besten mit den tatsächlich gemessenen Werten korrelieren. Dieses Verfahren ist jedoch sehr aufwändig, weil sich die Umgebung und damit die Funkdatenlandkarte ständig ändern. Die Genauigkeit der Positionsbestimmung hängt letztlich von der Rasterzellengröße ab.

2.4.6.2. Wi-Fi⁷⁸ - WLAN⁷⁹

Die WLAN-Lokalisierungstechnik ist jene, die derzeit in vielen Projekten erforscht und auch produktiv eingesetzt wird. Wi-Fi ist ein Kunstbegriff der 1999 von der Wi-Fi-Alliance in Anlehnung an den bekannten Begriff Hi-Fi (High-Fidelity), für drahtlose Produkte nach der IEEE⁸⁰-Spezifikation 802.11 geprägt wurde. Mittlerweile sind in der Wi-Fi-Alliance mehr als 300 Unternehmen vertreten (siehe <http://www.wi-fi.org/organization.php>, zuletzt geprüft am 17.10.2009).

Die Positionsbestimmung mit WLAN verwendet die Methode RSSI. Die gemessene Signalstärke der Accesspoints beim mobilen Empfänger ist dabei eine Funktion der Entfernung Sender – Empfänger und der Frequenz. Es kann somit aus der Signalstärke die Entfernung zum Sender berechnet werden.

⁷⁷ A-GPS = Assisted-GPS

⁷⁸ Wi-Fi = Wireless Fidelity

⁷⁹ WLAN = Wireless Local Area Network

⁸⁰ IEEE = Institute of Electric and Electronic Engineers

$$dB = 92,4 + 20 \cdot \log_{10}(r) + 20 \cdot \log_{10}(f)$$

Quelle: DORNBUSCH, P., ZÜNDT, M. (2002)

wobei r der Abstand Sender – Empfänger, f die Funkfrequenz ist und db die Signalstärke in Dezibel ist.

Die eigentliche Positionsbestimmung kann über mehrere Verfahren erfolgen:

- durch Multilateration aufgrund der bekannten Positionen der Accesspoints und den ermittelten Entfernungen Mobiles Gerät – Access-Points.
- durch die Fingerprintmethode (auch Korrelationsmethode), bei der die gemessenen Signalstärken der Accesspoints an einer bestimmten Stelle mit den Werten in einer Datenbank verglichen werden.
- Durch Kombination von Multilateration mit dem Fingerprint-Verfahren.
- Presence-Methode zur Bestimmung der Position auf Zellengenauigkeit (z.B. Raumgenauigkeit). Dabei bekommt das Mobile Gerät die Position des Accesspoints, über den die Verbindung hergestellt wurde (entspricht CoO).

Vorteil der Positionsbestimmung mittels WLAN ist, dass dazu keine eigene Infrastruktur aufgebaut werden muss. Es können, soweit ausreichend in Anzahl und Position, die bestehenden Accesspoints verwendet, und rein softwarebasierte Lösungen eingesetzt werden. Die Accesspoints sind außerdem kostengünstig.

Nachteilig ist, dass die Umgebungseinflüsse relativ groß sind, und dass speziell bewegte metallische Objekte (z.B. Fahrzeuge) die Empfangsverhältnisse beeinflussen. WLAN ist empfindlich gegenüber Multipath-Effekten und daher als Technologie in Umgebungen mit metallischen Einbauten (z.B. Rohrleitungen, Gitterrosten) nur bedingt geeignet.

WLAN arbeitet im freien 2,4 GHz-Band. Die Genauigkeit WLAN-basierter Systeme liegt im Innenbereich bei ca. 2-5 Meter. Im Außenbereich bei ca. 5 bis 100 m. Die erreichbare Genauigkeit verschiedener WLAN-basierter Lösungen hängt maßgeblich auch vom verwendeten Algorithmus für die Positionsberechnung ab.

2.4.6.3. Ultrabreitband (engl. Ultra Wideband, UWB)

Die Ultrabreitbandtechnologie ist eine netzwerkgestützte Funk-Technologie für RTLS. Bei Ultrawideband handelt es sich um sehr kurze Funkimpulse (typischerweise < 1 ns) mit großer Bandbreite (mindestens 500 MHz).

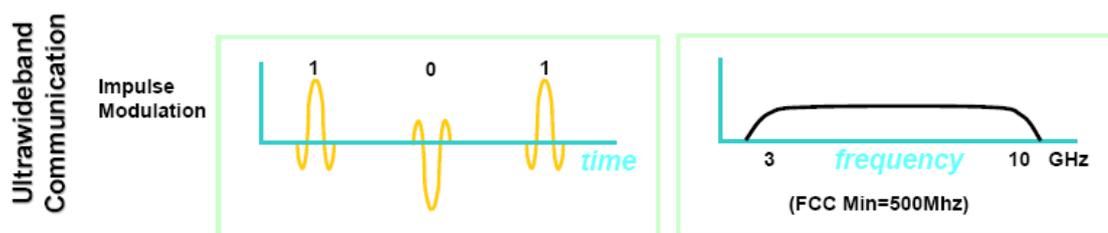


Abbildung 19: UWB-Charakteristik

Quelle: BEINAT, E. [2] (2008)

Der genehmigte Frequenzbereich für die höchsten UWB-Sendeleistungen liegt im EU-Raum (Entscheidung der Europäischen Kommission 2007/131/EC) bei 6 bis 8,5 GHz und in den USA bei 3 bis 10 GHz.

Dabei senden UWB-Tags diese kurzen Impulse aus, die von Empfängern (Sensoren oder auch Reader genannt) gelesen werden. Die Sendeleistung ist dabei sehr gering, und der Pegel liegt im Bereich des natürlichen Grundrauschens. Dadurch ist auch der Energiebedarf der Tags sehr gering, was lange Einsatzzeiten der Tags ohne Batteriewechsel ermöglicht.

Die Sensoren werden meist an höheren Punkten (z.B. Masten) positioniert, ausgerichtet vermessen und kalibriert. Die Positionsbestimmung mit UWB verwendet die Methode TDoA, teilweise in Verbindung mit AoA (z.B. bei Ubisense-Produkten). Die Reader sind über eine übliche Netzwerkinfrastruktur (LAN bzw. WAN oder Wireless; hier allerdings ohne TDoA-Funktionalität) mit einem zentralen Server verbunden. Dort erfolgt auch die Positionsbestimmung durch Multilateration zum Teil in Verbindung mit Angulation.

Ein großer Vorteil der UWB-Technologie ist, dass das Verfahren wesentlich unempfindlicher gegenüber Multipath-Effekten ist, was bei herkömmlicher Funktechnologie eine erhebliche Fehlerquelle ist. Dies vor allem bei Umgebungsbedingungen mit bewegten metallischen Objekten (z.B. großen Fahrzeugen).

Nachteilig von UWB ist, dass der Aufbau der Infrastruktur relativ teuer ist, und dass die Tags ebenfalls relativ teuer sind. Durch entsprechende Zulassungsbestimmungen im EU-Raum für UWB muss die Sendeleistung soweit gedrosselt werden, dass die UWB-Strahlung den menschlichen Körper nicht durchdringen kann. Dies erfordert die Installation von deutlich mehr Sensoren aufgrund der Abschattung, wenn der UWB-Tag vor der Brust getragen wird. Um die Anzahl der Sensoren zu minimieren, wird daher

getrachtet, den Tag möglichst hoch (z.B. am Schutzhelm) zu befestigen. Ein weiterer Punkt, der die technische Installation aufwändig macht ist, dass die Sensoren hochpräzise synchronisiert werden müssen, was eine leitungsgebundene Vernetzung der Sensoren bedingt, um die volle Genauigkeit zu erreichen.

2.4.7. Vergleich verschiedener Technologien

In den nachfolgend angeführten Vergleichen sollen einige Beispiele aus der Literatur über die Stärken und Schwächen der unterschiedlichen Technologien angeführt, und daraus ein Schluss auf das in der Arbeit konzipierte Sicherheitssystem gezogen werden.

MUTHUKRISHNAN, K. et al (2005) führt folgenden Vergleich der unterschiedlichen RTLS-Technologien an:

Technologie	Genauigkeit	Verfahren zur Positionsbestimmung	Beispiel
Infrarot basierend	5-10m	Näherung	Active Badge
Ultraschall basierend	1-10 cm	ToF-Lateration	Active Bat
Visuell basierend	1cm-1m	Szene Analyse	Easy Living
UWB basierend	6-10 cm	ToF-Triangulation	Ubisense
Bluetooth basierend	2-10m	Näherung, Triangulation	
WLAN basierend	2-100m	Triangulation, Näherung und Scene Analyse	Radar
Satelliten basierend	5-10m	Triangulation	GPS
Zell basierend	50-100m	Triangulation und Näherung	GSM-Lokalisierung
RFID basierend	5cm-5m	Näherung	Landmarc

Tabelle 4: Vergleich von RTLS-Technologien

Quelle: nach MUTHUKRISHNAN, K. et al (2005)

HALLBERG, J., NILSSON, M. (2002) geben den u.a. Vergleich von IrDA, RFID und Bluetooth für die Positionsbestimmung an. Der Vergleich zeigt, dass alle drei Technologien gut für die Positionsbestimmung geeignet sind, IrDA aber aufgrund der geringen Reichweite und notwendigen Sichtverbindung Nachteile gegenüber RFID und Bluetooth hat.

	IrDA	RFID	Bluetooth
Positioning task	Yes	Yes	Yes
Network	4 Mbps	N/A	1 Mbps
Exchange of position	Yes, limited	No	Yes
Security	Good	Good	Very Good
Range	Typically 1m	0 - 20m	100m/20m/10m
Power consumption	Low	Low	Low
Angle dependency	Yes, Line of sight	No	No
Accuracy	Range	Range/ (Triangulation)	Range/ (Triangulation)
Automatization	Yes	Some	Yes
Reliability	Very Good	Good	Very Good

Tabelle 5: Vergleich IrDA, RFID und Bluetooth für die Positionsbestimmung

Quelle: HALLBERG, J., NILSSON, M. (2002)

2.4.8. Schlussfolgerung für die konzipierte Sicherheits-Lösung

Unter Berücksichtigung der technischen Merkmale der unterschiedlichen Lösungen wird für die konzipierte Sicherheitslösung folgende Schlussfolgerung gezogen.

System	Vorteile	Nachteile	Eignung für die konzipierte Lösung
Infrarot	<ul style="list-style-type: none"> • Kostengünstig einfache Lösung • Gut Geeignet als Proximity- bzw. Presence-Lösung 	<ul style="list-style-type: none"> • Tageslichtempfindlich • Direkte Sichtverbindung notwendig • In Außenbereichen nicht einsetzbar 	Wegen Tageslicht-Empfindlichkeit nicht geeignet
Ultraschall	<ul style="list-style-type: none"> • Bewährte Technologie • Hohe Genauigkeit 	<ul style="list-style-type: none"> • Beeinflussung durch Multipath-Effekte aufgrund der industriellen Umgebung • In Außenbereichen nicht geeignet • Teure Installationskosten 	Für konkreten Einsatz nicht geeignet
WLAN, Wi-Fi,	<ul style="list-style-type: none"> • Standardhardware • Für CoO-Anwendung kostengünstige Lösung • Im Freien gute Ortungsergebnisse • Viele unterschiedliche 	<ul style="list-style-type: none"> • Beeinflussung durch Multipath-Effekte • Viele Accesspunkte erforderlich, weil Betonwände stark abschirmen, • Stromversorgung und Netzwerkanbindung für Accesspoints notwendig 	<ul style="list-style-type: none"> • System ist sowohl für Innen- als auch für Freibereiche sehr gut geeignet • Es gibt aber kostengünstigere Lösungen

	Lösungen verfügbar	<ul style="list-style-type: none"> • Wenn Einsatz im Fingerprintverfahren, notwendige Trainingsphase 	
Bluetooth, ZigBee	<ul style="list-style-type: none"> • In Innenräumen als Nahelösung • Kostengünstig • Sehr geringer Energieverbrauch, dadurch lange Batteriestandzeit • Infos können auf Tags geschrieben werden 	<ul style="list-style-type: none"> • Keine Eignung für Außenbereiche • Bei Bluetooth rel. Lange Zeit für Verbindungsaufbau 	<ul style="list-style-type: none"> • Als alleinige Lösung nicht geeignet, wohl aber in Kombination mit anderen Technologien sehr gut geeignet.
UWB	<ul style="list-style-type: none"> • Hohe Ortungs-genauigkeit • Robust gegenüber Multipath-Effekten 	<ul style="list-style-type: none"> • Teuer in der Installation • Betonwände schirmen UWB ab • UWB als Presence-Lösung zu teuer 	<ul style="list-style-type: none"> • Technisch sehr gut geeignet, aber sehr teure Lösung
RFID	<ul style="list-style-type: none"> • Kostengünstig • Für Proximity- und Presence-Lösung gut geeignet • Daten können auf Tags geschrieben werden 	<ul style="list-style-type: none"> • Batterien der aktiven Tags • Lesegerät muss permanent aktiv sein → permanente elektrom. Strahlung • In Außenbereichen nicht geeignet • Meist proprietäre Systeme mit unterschiedlichen Tagtypen(Passiv/ Aktiv) 	<ul style="list-style-type: none"> • Als alleinige Lösung nicht geeignet • Sehr gut geeignet für kombinierten Einsatz
GPS	<ul style="list-style-type: none"> • Standard-technologie • Viele Geräte am Markt • In Außenbereichen sehr gut einsetzbar • Ausreichende Genauigkeit 	<ul style="list-style-type: none"> • Kein Innenraumeinsatz möglich 	<ul style="list-style-type: none"> • für kombinierten Einsatz hervorragend geeignet
Mobilfunk-basierte Systeme	<ul style="list-style-type: none"> • Keine eigene Infrastruktur erforderlich 	<ul style="list-style-type: none"> • Geringe Genauigkeit 	<ul style="list-style-type: none"> • Für Positionsbestimmung auf Raumgenauigkeit zu ungenau • Sehr gut geeignet für mobile Datenübertragung

Tabelle 6: Eignung unterschiedlicher Technologien für die konzipierte Lösung

2.5. Privacy

Die allgegenwärtige Computerisierung und darunter die RTLS-Technologie hat umfassende Auswirkungen auf die Privatsphäre (in der Folge mit dem Fachbegriff „Privacy“ bezeichnet). Neben den Informationen, die bei Einsatz der RTL-Technologie begleitend erfasst werden, ist insbesondere die Ortsinformation geeignet in die Privatsphäre einzugreifen. Zu wissen wo sich Personen, Mitarbeiter, Geräte usw. zu einem bestimmten Zeitpunkt aufhalten, schafft zahlreiche Eingriffsmöglichkeiten für einen Dritten, Handlungen zu steuern und zu beeinflussen.

Privacy ist für die Umsetzung von RTLS-Projekten ein erfolgskritischer Faktor. Ist es doch möglich in Echtzeit die Position der Mitarbeiter zu bestimmen. Sind solche Daten in einer Datenbank gespeichert, könnten daraus Bewegungsprofile erstellt werden, und über diese eine genaue Beurteilung der Arbeitsleistung auf Mitarbeitererebene erfolgen. Die Regelungen darüber, wer welche Informationen einsehen darf und wie sie ausgewertet werden dürfen, haben maßgeblichen Einfluss auf die Akzeptanz, und damit den Erfolg der Lösungen. Daher soll in den folgenden Kapiteln das Thema Privacy näher beleuchtet werden. Das Ziel ist dabei von den allgemeinen Überlegungen zur Privacy ausgehend, die Besonderheiten der RTLS-Technologie hinsichtlich Privacy herauszuarbeiten. Die konkreten Maßnahmen betreffend Privacy in Bezug auf die Sicherheitslösung werden im Kapitel 5 behandelt.

2.5.1. Was ist Privacy?

Betrachtet man den Begriff Privacy, so ist zunächst zu klären, was wir unter Privacy verstehen. Dies auch deshalb, weil in unterschiedlichen Kulturkreisen auch ein unterschiedliches Verständnis hinsichtlich Privacy besteht. Daneben ist Privacy in unterschiedlichen Betrachtungsweisen zu sehen. Nach CLARKE, R. (2006) gehören dazu:

- Privacy im philosophischen Sinne
- Privacy im psychologischen Sinne
- Privacy im soziologischen Sinne
- Privacy im wirtschaftlichen Sinne
- Privacy im politischen Sinne

Im weitesten Sinn sieht CLARKE, R. (2006) Privacy als den Erhalt der „*Integrität des Individuums*“ welche den Schutz der Person, des persönlichen Verhaltens, der persönlichen Kommunikation und der persönlichen Daten umfasst und definiert daraus:

“Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations”.

Privacy geht also weit über den Zusammenhang mit Informationsverarbeitung hinaus und hat mehrere Dimensionen. So kann z.B. die Beantwortung der Frage „Wer hat sich mit wem, wo und wann getroffen?“ schon eine schwerwiegende Auswirkung auf die „politische Privacy“ haben. Allen Dimensionen gemeinsam ist, dass es einen persönlichen Freiraum, einen Rückzugsraum, geben muss, der vom Einfluss anderer verschont bleibt. Aus diesem Privacy-Begriff abgeleitet ist nach CLARKE, R. (2006) der Schutz der Privatsphäre:

Privacy Protection is a process of finding appropriate balances between privacy and multiple competing interests.

Es gilt also die Balance zwischen individuellen persönlichen Interessen und anderen von außen einwirkenden Interessen zu finden. Der Schutz der Privatsphäre ist dabei keine Angelegenheit mit klaren sich sachlich ergebenden fixen Regeln, sondern ein fortwährender Prozess, der das allgemeine Interesse, im Falle der RTLS-Lösungen im Berufsumfeld die Interessen des Arbeitgebers, gegen das persönliche Schutzbedürfnis abwägt („appropriate balances“). Damit ist auch klar, warum in unterschiedlichen Kulturkreisen ein unterschiedlicher Zugang zu Privacy besteht, und warum die Interpretation der Privacy einem generellen Wandel unterliegt.

2.5.2. Privacy als Menschenrecht oder Wirtschaftsgut?

Ist nun Privacy ein grundlegendes Menschenrecht oder gar ein wirtschaftliches Gut. Diese Frage zu beantworten ist wiederum vom Kulturkreis abhängig. Betrachten wir z.B. die Adresse einer Person. Fällt diese unter dem Schutz der Privatsphäre? Oder ist diese auf der anderen Seite eine Handelsware? Beide Sichten sind in diesem Fall anzutreffen. Wir sehen, dass gerade bei Informationen das Thema Privacy schwierig zu fassen ist.

WESTIN, A. (1967) definiert dazu:

“Privacy is the claim of individuals, groups or institutions to determine when, how, and to what extent information about them is communicated to others”.

Oder wiederum nach CLARKE, R. (2006):

***Information Privacy** is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.*

Es geht somit um die Selbstbestimmung, also selbst zu entscheiden, welche Informationen über meine Person (=personenbezogene Daten) an andere kommuniziert werden. Diese informatorische Selbstbestimmung ist sowohl im privaten Bereich als auch im Arbeitsleben zu sehen. Im Speziellen erfordern es die neuen Technologien, dass die informatorische Selbstbestimmung auch in dem Begriff „Privacy“ eingeschlossen wird.

BEINAT, E. [1] (2008) definiert die inhaltlichen Felder von Privacy dazu als die Schnittmenge aus Verhalten, Demographie und persönlichen Merkmalen:

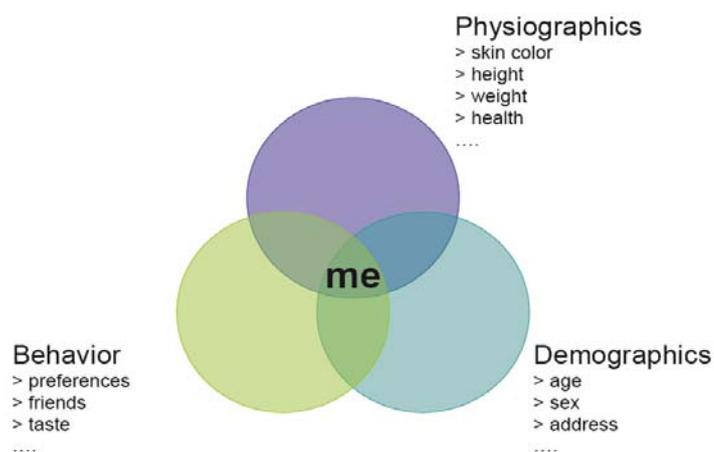


Abbildung 20: Inhaltliche Dimensionen von Privacy

Quelle: Beinat, Euro (2008)

2.5.3. Was sind personenbezogene Daten?

Das österreichische Datenschutzgesetz DSG 2000 definiert personenbezogene Daten als „Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist“. Gemäß deutschem Bundesdatenschutzgesetz (BDSG): § (1) „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Z.B. werden Gesundheitsdaten erst dann zu personenbezogenen Daten, wenn diese den Rückschluss auf eine Person erlauben.

2.5.4. *Datenschutz in Zusammenhang mit RFID und Ortsinformationen*

In Zusammenhang mit RFID-Anwendungen hat sich die Artikel-29-Datenschutzgruppe der EU klar geäußert, was unter personenbezogenen Daten zu verstehen ist:

„Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird.[...] alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“.

Die Artikel-29-Datenschutzgruppe führt als Beispiel für personenbezogene Daten die Standortüberwachung von Taxis in Echtzeit über ein Satellitenortungssystem an. Es ist davon auszugehen, dass RTLS-Anwendungen allgemein den Datenschutzbestimmungen unterliegen, es sei denn, es werden die Standortdaten so anonymisiert, dass keine Rückschlüsse auf bestimmte Personen mehr möglich sind (unter Annahme der Mittel, die „vernünftigerweise“ eingesetzt werden).

Auch Bewegungsdaten in Zusammenhang mit der Verwendung von RFID fallen unter den Datenschutz. ANDRES führt dazu an: *„In Bezug auf RFID lässt sich jedoch kein berechtigtes Interesse des Unternehmens an Aufenthaltsdaten oder Bewegungsdaten von Kunden in Geschäften erkennen, das dem Schutz der Privatsphäre des Kunden überwiegt“.*

2.5.5. *Datenschutzgesetze in Österreich und in Deutschland*

Den Zugriff auf private Datenbanken regeln nationale Datenschutzgesetze (in Österreich das "Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999", in Deutschland das Bundesdatenschutzgesetz BDSG 1990 i.d.g.F.), welche die Inhalte der Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 in nationales Recht umsetzen. Für Österreich und auch Deutschland sind dabei dem Artikel 8 entsprechende Bestimmungen übernommen. Die Datenschutzrichtlinie bezieht sich auf *„jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“*. Sie verpflichtet *„Daten nach Treu und Glauben und auf sichere Art zu verarbeiten und personenbezogene Daten ausschließlich für eindeutig festgelegte und rechtmäßige Zwecke zu verwenden“* (Europäische Union GD Binnenmarkt (2004)). Hinsichtlich der Datenverarbeitung besteht ein „Transparenz-

Gebot“. Die Transparenz der Erhebungs- und Verarbeitungszusammenhänge ist die Voraussetzung dafür, dass die Person ihr Recht auf informelle Selbstbestimmung umsetzen kann (Vgl. ANDRES, M. (2007)).

ANDRES, M. (2007) führt an: *„Verbraucher bzw. Personen, die mit automatisierter Datenverarbeitung in Kontakt kommen, haben grundsätzlich das Recht, selbst darüber zu bestimmen, an wen und zu welchem Zweck sie persönliche Daten weitergeben möchten.“*

2.5.6. Beurteilungsschema für Geodaten

FORGÒ, N. (2008) hat für Geodaten ein Beurteilungsschema entworfen, wobei er anführt, dass es eine generelle Erlaubnis, für die Verarbeitung von Geodaten nicht gibt, und auf allgemeine Erlaubnissätze zurück zu greifen ist. Weiters sind lt. FORGÒ Geodaten zunächst nicht personenbezogen sondern sachbezogen.

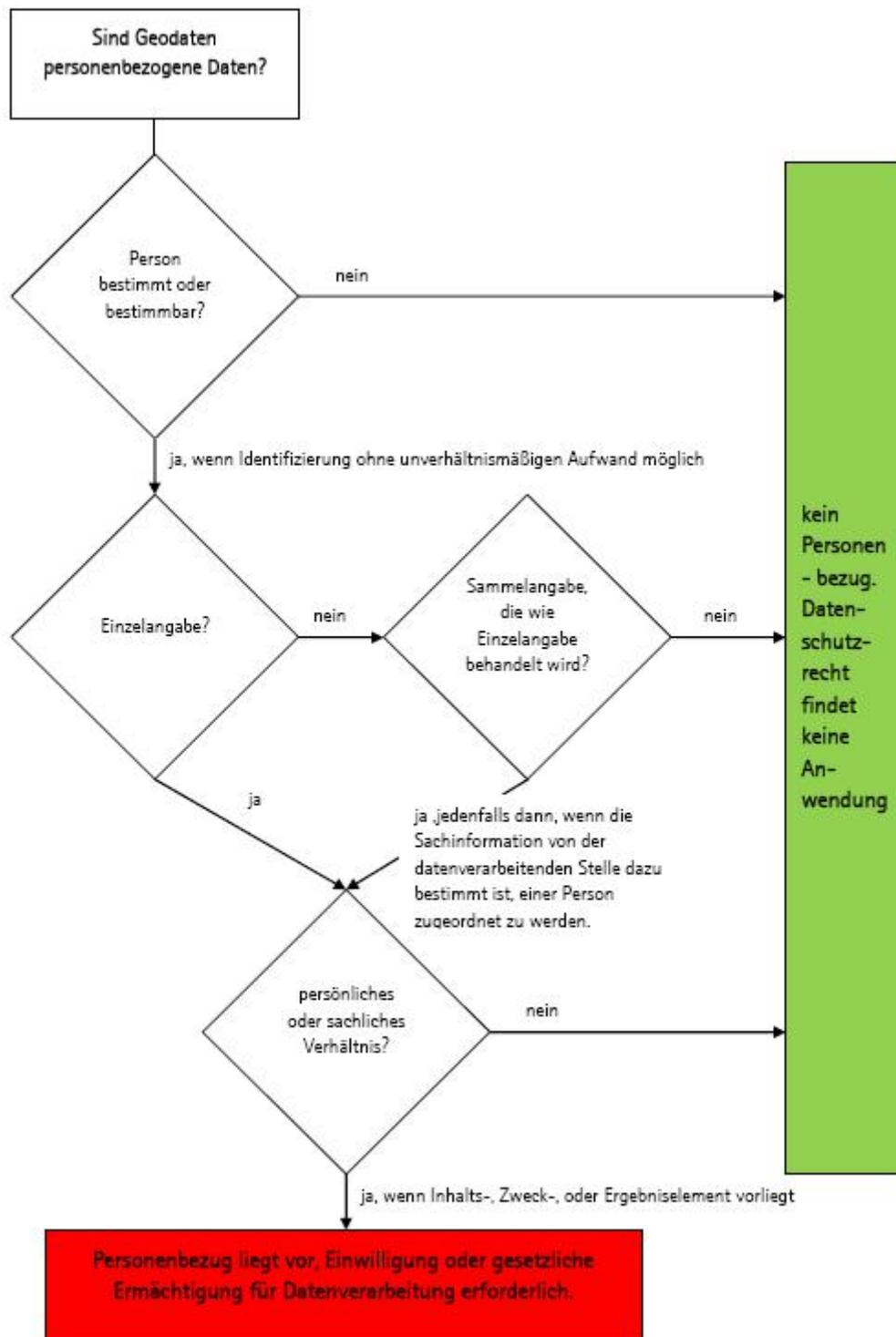


Abbildung 21: Beurteilungsschema "Sind Geodaten personenbezogene Daten?"
 Quelle: FORGÒ, N. (2008)

2.5.7. Bedeutung der Geoinformation für die Privacy

Besonders die Technologie von RTLS besitzt hohes Potential durch Preisgabe der Ortsinformation (Geoinformation) in die Privatsphäre von Menschen einzugreifen, sowohl im privaten Bereich als auch im Berufseinsatz. Dies zeigen auch eine Reihe von konkreten RTLS-Anwendungen, wie z.B. im Strafvollzug oder die Überwachung von

verwirrten alten Menschen, oder auch Anwendungen aus dem Sicherheitsbereich. Die Kenntnis der genauen örtlichen Position in Echtzeit ist geeignet, die Freiheit eines Menschen erheblich einzuschränken. Dadurch besteht die Möglichkeit auf die Handlungen der Personen abhängig vom räumlichen Umfeld unmittelbar zu reagieren und diese zu steuern, also die Personen „abhängig“ zu machen.

Interessante Gesichtspunkte dazu beschreiben DOBSON und FISHER (2003) in ihrem Beitrag „Geoslavery“ *„Society must contemplate a new form of slavery, characterized by location control“*.

Geoslavery ist die Überwachung (offen oder heimlich) der physischen Position einer Person durch eine andere. DOBSON und FISCHER (2003) führen aus, dass durch die Kombination von drei Technologien – kleine GPS-Empfänger, kleine Sender für die Datenübertragung und einem GIS für die Darstellung und Analyse – die Handlungen einzelner Personen oder ganzer Gruppen effektiv und umfassend überwacht und gesteuert werden können. Personen-Tracking-Systeme kombinieren diese drei Technologien. Neben diesen Systemen bieten sich zunehmend Mobiltelefone für die Positionsbestimmung (respektive Überwachung) an. Vor allem die neueren Geräte bieten schon beachtliche Genauigkeiten in der Positionsbestimmung. Hauptargument für die Nutzung der Positionsbestimmungsfunktionalitäten bei Mobilfunk ist allerdings das Sicherheitsargument in Zusammenhang mit Notrufen (siehe Artikel 26 der Direktive 2002/22/EC vom 7. März 2002). Eine analoge Vorschrift gibt es auch in den USA FCC E911.

Der Grat zwischen positiver Anwendung dieser Technologie und der missbräuchlichen Verwendung ist sehr schmal. Wo endet das berechtigte Interesse einer Behörde, der Polizei, einer privaten Person oder eines Arbeitgebers, und wo beginnt bereits die unfreiwillige Überwachung?⁸¹ Oder wo endet eine bei Flottenmanagementsystemen beabsichtigte Kostenreduktion durch bessere Steuerung der Fahrzeuge und wo beginnt die übertriebene Überwachung der Mitarbeiter?

MATTERN, F. (2008), führt aus: *„Die weiter anhaltenden Technologietrends zeigen eindeutig in Richtung einer umfassenden Informatisierung der Welt“*. Es ist damit zu rechnen, dass durch den Trend in Richtung *„Ubiquitous Computing“* weitere Geräte und Anwendungen entstehen, welche die Informationen vernetzen und speziell auf Basis der Ortsinformation („Location aware“) Auswahlen und Entscheidungen treffen. Weiters hält MATTERN, F. (2008) fest:

⁸¹ Beispiel Handyortung: www.Trackyourkid.de

„Besondere Beachtung hinsichtlich des Privatsphärenschutzes dürfte in Zukunft vor allem der „location privacy“ zukommen.“ und weiter [...] „Lokalisierungstechnologien bergen also einiges an sozialem Sprengstoff: nicht nur, weil man damit Leuten hinterher spionieren kann, sondern weil dies auch ein bewusst eingesetztes Kontrollinstrument werden kann“.

In diesem Zusammenhang wird auch von „Data Surveillance“ oder „Dataveillance“ gesprochen. CLARKE (2008) führt unter Anderem folgende besondere Gefahren an, die von den Locating- und Tracking-Technologien ausgehen:

- Psychologische Schädigung durch Beschämung, aufgrund der Überwachung
- Soziale, kulturelle, wissenschaftliche und wirtschaftliche Schädigung aufgrund des beobachteten Verhaltens bei der Überwachung
- Bewegungsprofilerstellung und Verdächtigungen aufgrund der Bewegungsmuster
- Transparenz des Verhaltens
- Unterdrückung der überwachten Personen

2.5.8. Wahrnehmung und Akzeptanz in der Öffentlichkeit

Aber nicht allgemein wird von den Anwendern die Verringerung der Privatsphäre als deutlich negativ erlebt. Vielmehr scheint es so, dass bei Vorhandensein eines entsprechend großen Nutzens der Einfluss auf die Privacy als Begleiterscheinung in Kauf genommen wird. MATTERN, F. (2008) führt dazu schlussfolgernd auf Untersuchungen anderer Wissenschaftler an, dass *„in diesem Zusammenhang ein gewisser Trend zur bewussten Aufgabe von Privatheit ...“* beobachtet werden kann. Und weiters:

„Offenbar wird von vielen, vielleicht sogar einer Mehrheit der Bevölkerung, eine Einschränkung der Privatheit nicht als gravierend empfunden.“

Denken wir nur an das Mobiltelefon, so wird von vielen die Ortungsmöglichkeit sogar als positives „Feature“ gesehen. Besonders auch als Sicherheit bei privaten Notfallsituationen.

Dennoch benötigt man ein klares gesetzliches Rahmenwerk, wie mit der Ortsinformationen umgegangen werden darf. In Zusammenhang mit der Telekommunikation ist dies bereits geregelt. In der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung

personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (in Österreich mit dem Telekommunikationsgesetz 2003 umgesetzt) ist in (35) eine Bestimmung mit dem Umgang von geografischen Standortdaten aus Mobilfunknetzen angeführt:

„Die Verarbeitung solcher Daten für die Bereitstellung von Diensten mit Zusatznutzen soll nur dann gestattet werden, wenn die Teilnehmer darin eingewilligt haben. Selbst dann sollten sie die Möglichkeit haben, die Verarbeitung von Standortdaten auf einfache Weise und gebührenfrei zeitweise zu untersagen“.

Damit kommt klar zum Ausdruck, dass es sich bei den Standortdaten um schützenswerte personenbezogene Verkehrsdaten handelt.

Handlungsbedarf besteht vorwiegend in der Privatwirtschaft. Hier fehlen in vielen Unternehmen entsprechende Regelungen. Dies ist jedoch eine Voraussetzung dafür, dem Nutzer das Vertrauen in die Technologie zu geben, und somit das positive Wachsen dieses Wirtschaftszweiges zu ermöglichen (vgl. VAN RIPER, D., WHITFIELD, T. (2004)).

Ganz Allgemein kann festgehalten werden, dass betreffend Datenschutz zahlreiche gesetzliche Regelungen sowohl auf EU-Ebene als auch auf nationaler Ebene bestehen. Dies sowohl für den Privatbereich als auch für das berufliche Umfeld. Das „European Privacy Officers Forum (EPOF)⁸² meint dazu: *„In sum, EPOF joins the many stakeholders who believe that there is no compelling need for additional legislation on employee privacy and data protection. The existing European and national legislative framework sufficiently protects the rights of the employees.“* (EPOF, (2003))

Die Datenschutzgesetze legen fest, was personenbezogene Daten sind, und wie mit diesen umgegangen werden darf. Was bleibt ist eine negative Wahrnehmung der Öffentlichkeit betreffend Umgang der Firmen mit den Daten der Kunden und speziell auch mit den Daten der Mitarbeiter. Zahlreiche Skandale⁸³ namhafter Unternehmen in

⁸² EPOF setzt sich aus Datenschutzbeauftragten von Unternehmen und Rechtsberatern zusammen, und hat das Ziel den Datenschutz in Europa zu überwachen.

Homepage: <http://www.hunton.com/Resources/Sites/general.aspx?id=441>, zuletzt geprüft am 04.05.2009

⁸³ Z.B. siehe „Abhörskandal bei der deutschen Telekom“ vom 27. Mai 2008 unter

<http://www.sueddeutsche.de/wirtschaft/565/443304/text/> oder

der letzten Zeit bestätigen diese Befürchtungen, und verstärken den Ruf nach neuen gesetzlichen Regelungen. Notwendig ist es, die unterschiedlichen Auslegungen der Datenschutzrichtlinie in den nationalen Datenschutzgesetzen zu harmonisieren, um vor allem bei international tätigen Unternehmen eine Rechtssicherheit zu erreichen (vgl. EPOF (2002)).

Speziell im Arbeitsumfeld sind nicht nur die datenschutzrechtlichen Bestimmungen von Bedeutung, sondern auch kollektivvertragliche Regelungen oder auch Regelungen über den Schutz der Arbeitsumgebung/Arbeitsumwelt. Wenn es in Zusammenhang mit RTLS auch individuelle Kontrollmöglichkeiten der Arbeitsleistung einzelner Mitarbeiter gibt, sind Mitbestimmungsrechte des Betriebsrates zu beachten. Eine Risikominimierung ist möglich, wenn den Mitarbeitern die Datenverarbeitungsprozesse betreffend ihrer personenbezogenen Daten bekannt sind (vgl. BIZER, J. et al (2006)). Dies trägt auch zu mehr Transparenz in Umgang mit den Daten und zu mehr Vertrauen bei.

Neben den belastenden Seiten und den möglichen negativen Einflüssen auf die Privacy, die in den o.a. Beiträgen genannt werden, dürfen die positiven Aspekte der Technologie nicht übersehen werden. Der verantwortungsvolle Umgang mit der RTLS-Technologie ermöglicht es, wie in den folgenden Kapiteln gezeigt wird, die Prozesse zu optimieren, mehr Transparenz in die Abläufe zu bringen, die Sicherheit der beteiligten Mitarbeiter zu erhöhen und durch gesteigerte Wirtschaftlichkeit somit zum Erhalt der Arbeitsplätze beizutragen. Gerade in wirtschaftlich schwierigen Zeiten ein wichtiger Punkt.

„Abhörskandal bei der Bahn“ vom 21.1.2009 unter http://www.volkerbeck.de/cms/index.php?option=com_content&task=view&id=1587&Itemid=167, Zitat: „Neben einem Datenschutzgesetz mit Biss brauchen wir dringend mehr Kontrolle des Datenschutzes in der Wirtschaft durch die unabhängigen, staatlichen Datenschutzbeauftragten.“
Datenskandal beschert ÖBB-Chef Krise vom 22.09.2009 unter <http://www.handelsblatt.com/unternehmen/koepfe/datenskandal-beschert-oebb-chef-krise;2459312>

3. Literaturüberblick

3.1. Praktische Projekte zur Positionsbestimmung in Gebäuden

In diesem Kapitel soll ein Überblick über bestehende Lösungen für die Positionsbestimmung in Gebäuden und kleinräumigen Außenbereichen gegeben werden. Mittlerweile gibt es zahlreiche unterschiedliche Lösungen. Auf alle einzugehen würde den Rahmen dieser Arbeit sprengen. Daher wird der Fokus auf Lösungen gelegt, die in den in den Kapiteln 4 und 5 behandelten Anwendungsszenarien zur Anwendung kommen.

3.1.1. Active Badge

Die Informationen zu diesem System stammen aus dem Fachartikel WANT, R. et al (1992). Dabei geht es um eine Anwendung, die mit Hilfe von Infrarot die Positionen von Personen in Innenräumen bestimmt. Das System wurde 1992 von den Olivetti Research Ltd. (ORL) in Cambridge, England, entwickelt.

Angestellte wurden mit Sendern (Badges) auf Infrarotbasis ausgestattet. Die vom Infrarotsender periodisch ausgesendeten Signale (alle 15 Sekunden wird für eine Zehntelsekunde ein eindeutiger Code ausgesendet; die Id des Senders) werden von einem Infrarotempfänger im Raum registriert und an ein zentrales Rechnersystem übermittelt. Die Positionsinformation wird über eine zentrale Anwendung visualisiert und berechtigten Dritten zur Verfügung gestellt. Das bei Active Badge eingesetzte Ortungsverfahren entspricht einem Presence-Verfahren. Active Badge hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung.

3.1.2. WIPS

Die „Umkehrung“ zum System Active Badge ist das System WIPS⁸⁴, das 2000 in Schweden entwickelt wurde. Dabei werden die Infrarotsignale von stationären Baken ausgesendet und von einem mobilen Empfangsgerät (mobiler Computer, PDA) gelesen. Da Infrarot keine Wände durchdringen kann, ist die Id der Baken gleich der Identifikation des Raums. Vorteil dabei ist, dass die Position nur dem Benutzer bekannt ist. Es bestehen somit keine Privacy-Probleme (vgl. WIPS (2000)). WIPS hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung.

⁸⁴ WIPS = **W**ireless **I**ndoor **P**ositioning **S**ystem

3.1.3. Active Bat

Diese Lösung verwendet Ultraschall zur Ortung und wurde 1997 von den AT&T Laboratories in Cambridge als Nachfolgelösung zu Active Badge entwickelt. Die Person trägt einen Ultraschallsender (Active Bat) mit eingebauter Funkeinheit.

An der Decke des Raumes sind in einem regelmäßigen Raster (Rasterweite 1,2 Meter) Ultraschallempfänger angebracht, die mit einer zentralen Rechneinheit vernetzt sind (vergl. WARD, A. et al (1997)). Jede Bat wird über einen eindeutigen 48 Bit-Code identifiziert, und ist über einen 433 MHz-Funkkanal über einen ACCESS-Point mit dem zentralen Server verbunden (vgl. AT&T Laboratories Cambridge (Hg.) (2002)). Der Access-Point sendet (gesteuert vom zentralen Server) periodisch die Kennungen aller Bats aus, die bei ihm registriert sind. Empfängt nun eine Bat ihre Kennung, so sendet sie einen Ultraschallpuls aus, der von den Deckensensoren registriert wird. Aus der Laufzeit der Ultraschallsignale kann auf die Entfernung des Senders zum jeweiligen Empfänger geschlossen werden.

Durch Multilateration, über die bekannten Positionen der Deckensensoren, kann daraus die Position des Senders (der Person) sehr genau dreidimensional errechnet werden (95% besser 3 cm, 99% besser 10 cm) (vgl. HOPPER, A. (2003)). Die Lösung Active Bat verwendet das Positionsbestimmungsverfahren ToA bzw. ToF. Active Bat hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung.

3.1.4. Cricket⁸⁵

Das System Cricket wurde 1997 am MIT⁸⁶ entwickelt und basiert auf Ultraschall in Kombination mit Funk. In der aktuellen Version liefert Cricket detaillierte Positionsinformationen, semantische Raum-Informationen und genaue Koordinaten und die Orientierung im Raum. Cricket ist eine Technologie für Innenräume und Außenbereiche mit geringer Ausdehnung. An den Wänden und Decken sind in einem Raster verteilt über das Gebäude Sender (Beacons) montiert. Die Beacons senden periodisch einerseits Funksignale, und mit diesen gleichzeitig Ultraschallimpulse aus. Die Person oder das Objekt trägt ein Empfangsgerät (einen sogenannten Listener). Empfängt nun der Listener ein Funksignal, so wird nach den ersten Bits auch Ultraschallempfang aktiviert, da vom Beacon gleichzeitig mit dem Funksignal ein

⁸⁵ <http://cricket.csail.mit.edu/>

⁸⁶ MIT = Massachusetts Institute of Technology

Ultraschallimpuls ausgesendet wird. Die Differenz der Laufzeit zwischen Funksignal und Ultraschallsignal ist ein Maß für die Entfernung Sender – Empfänger.

Das Cricket-System kann sowohl als Näherungsverfahren (Proximity, Presence) eingesetzt werden, als auch über die Koordinaten der Beacons wiederum über Multilateration die exakte Position des Empfangsgerätes errechnen. Das System erreicht eine Genauigkeit von 4-5 cm in der Entfernungsmessung (vgl. PRIYANTHA, N. B. (2005)).

Die Berechnung der Position erfolgt durch den Listener. Die Positionsinformation ist daher nur dem Träger des Empfangsgerätes bekannt (Vorteil keine Privacy-Implicationen). Über eine WLAN-Verbindung kann die Positionsinformation alternativ zu einem zentralen Server übertragen werden; ggf. nach Freigabe durch den Benutzer. Das System verwendet zur Positionsbestimmung die TDoA-Methode bzw. das Proximity- und Presence-Verfahren. Cricket hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung.

3.1.5. Radar⁸⁷

Das System Radar wurde im Jahr 2000 von Microsoft entwickelt. Das System basiert auf der Positionsbestimmung aufgrund der Signale von WLAN-Access-Points (IEEE 802.11-Infrastruktur). Radar ist sowohl für die Positionsbestimmung in Gebäuden als auch im Freien einsetzbar. Die Genauigkeit beträgt ca. 2-3 Meter.

Von den Accesspoints werden in regelmäßigen Abständen Funksignale (Funk-Beacons) ausgesendet, welche auch die eindeutige Id des Accesspoints beinhalten. Das mobile Gerät empfängt diese Beacons, und misst dabei auch die Signalstärke.

Das System erfordert eine Trainingsphase (off-line-Phase), das heißt mit einem mobilen Empfangsgerät (z.B. Laptop mit WLAN) wird auf Basis eines Gebäudeplans oder Geländeplans die gemessene Signalstärke verschiedener Accesspoints an unterschiedlichen Stellen registriert und in einer Datenbank gespeichert. Dadurch entsteht eine Landkarte der Signalstärken („Fingerprinting“-Verfahren). Im Einsatz für die Positionsbestimmung (on-line-Phase) werden dann die gemessenen Signalstärken mit den Signalstärken in der Datenbank verglichen, und daraus die Position berechnet, die am Besten mit den gemessenen Werten korreliert. Das System verwendet die RSSI-Methode in Verbindung mit Korrelationsalgorithmen zur Positionsbestimmung. Radar könnte für die angeführte Sicherheitslösung sehr gut eingesetzt werden.

⁸⁷ STEINBERG, T. (2007)

3.1.6. *Spot ON*

Spot On wurde 2000 an der Universität Washington entwickelt. Ein mobiles Gerät (Badge) sendet Funksignale (916,5 MHz) aus, die von fest installierten Empfängern, die mit einem zentralen Server vernetzt sind, empfangen werden. An den Empfängern wird die Signalstärke gemessen, über die auf die Entfernung zurückgeschlossen werden kann. Die Positionsbestimmung erfolgt dann durch Multilateration. Die Genauigkeit der Positionsbestimmung liegt bei ca. 1 Meter (vgl. HIGHTOWER, J. et al (2000)). SpotON hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung, könnte aber bei der Sicherheitslösung für die Innenbereiche eingesetzt werden.

3.1.7. *Magic Map*⁸⁸ und *GRIPS*

Magic Map wurde 2004 an der Humboldt Universität zu Berlin entwickelt. Unabhängig von Magic Map entstand zur gleichen Zeit am Fraunhofer FOKUS in Berlin die Lösung GRIPS⁸⁹. Beide Systeme verfolgen vergleichbare Ansätze. Jeder beteiligte Peerknoten misst von allen Knoten (Access-Points, andere Peers), die empfangen werden können, die Signalstärken. Die Signalstärke wird dabei über mehrere Messungen gemittelt, und über verschiedene Funktechnologien normalisiert. In einer Näherung kann daraus die Entfernung Sender – Peerknoten geschätzt werden. Es entsteht ein Graph mit gerichteten Kanten zwischen sendenden und empfangenden Knoten. Knoten, deren Position bereits bestimmt wurde, werden in einer Karte fixiert. Noch nicht bestimmte Knoten wandern durch fortlaufende Messungen in Richtung ihrer wahrscheinlichsten Position. Nach kurzer Zeit können so die tatsächlichen Positionen der Knoten bestimmt werden. (vgl. IBACH, P. et al (2005)). Die Genauigkeit der Lösung liegt im Bereich mehrerer Meter (vgl. HERGLOTZ, A. (2006)), teilweise aber auch wesentlich darunter (1 Meter) (vgl. TANNÒ, N.; TOMASONE, N. (2007)). Die Berechnung der Position erfolgt durch ein hybrides Verfahren von Multilateration, Radio Map und probabilistischem Graph Mapping. Magic Map und GRIPS sind reine Softwarelösungen. Außer WLAN ist keine weitere Hardware für die Positionsbestimmung erforderlich. Aber nicht nur WLAN kann zur Positionsbestimmung herangezogen werden, sondern auch andere Technologien wie Bluetooth, RFID, ZigBee, GSM und weitere.

⁸⁸ <http://wiki.informatik.hu-berlin.de/nomads/index.php/MagicMap>, zuletzt geprüft am 24.10.2009

⁸⁹ GRIPS = Generic Radio-based Indoor Positioning System

Die Koordinaten der Knoten (Accesspoints) werden in der zentralen Magic Map-Datenbank gespeichert. Ein Beispiel für den Einsatz von Magic Map ist der Busbahnhof Potsdam. Hier wird die Lösung für die Parkraumplanung und Koordination der über Nacht parkenden Busse verwendet. Magic Map ist als Lösung für einzelne EVU-Szenarien eine geeignete Lösung.

3.1.8. *IMAPS*⁹⁰

IMAPS wurde im Jahr 2006 an der Hochschule für angewandte Wissenschaften Hamburg entwickelt und hat Cricket als Vorbild. Das System ist ein Indoor-Ortungssystem, das für Anwendungen im Kontext von Ambient Intelligence entwickelt wurde. Es besteht aus Sendern (Beacons, die einen Funktransceiver und einen Ultraschallsender enthalten), die im Abstand von 1,2 Meter an der Decke montiert sind. Die von den Beacons ausgesendeten Signale (in zufälligen Zeitabständen werden Funk- und Ultraschallsignale ausgesendet) werden von mobilen Empfängern (Listener) registriert und verarbeitet. Die Beacons senden dabei ihre Id und die eigenen Positionsdaten. Am Empfänger wird die Laufzeitdifferenz zwischen den Funksignalen und den Ultraschallsignalen gemessen und daraus die Entfernung Sender – Empfänger berechnet (Methode TDoA). Die Positionsbestimmung erfolgt über Multilateration am Empfänger, was Privacy-Implicationen vermeidet. Der Benutzer kann jedoch seine Positionsdaten über eine Kommunikationsverbindung an einen zentralen Server übermitteln, wenn er dies möchte. Die Genauigkeit von IMAPS liegt bei 1 cm und ist somit sehr genau. IMAPS hat für die angeführten Anwendungsszenarien in EVU keine weitere Bedeutung.

3.1.9. *Weitere*

Es gibt noch zahlreiche weitere Lösungen auf die jedoch in dieser Arbeit nicht weiter eingegangen wird. Dazu zählen:

- Hipath DPS⁹¹ ein System von Siemens, das auf der DECT-Technologie beruht. Die Genauigkeit liegt bei 8-15 Meter.
- Das System MPS⁹² der Firma Ericsson, das die Positionsbestimmung mittels GSM in Verbindung mit GPS durchführt. Die Genauigkeit liegt bei ca. 50 Meter.

⁹⁰ GREGOR, S. (2006)

⁹¹ DPS = **D**ECT **P**ositioning **S**ystem; siehe dazu

http://www.telenova.org/cms/upload/pdf/HiPath_Cordless_DPS.pdf, zuletzt geprüft am 14.10.2009

- PinPoint 3D von der Firma RF Technologies, das mittels Funk-Tags und Basisstationen arbeitet. Die Genauigkeit liegt bei ca. 3 Meter. Vgl. GREGOR, S. (2006).
- HiBall Tracker ein System der University of North Carolina, das mit Infrarotsensoren, Kameras und LEDs arbeitet, wobei eine sehr hohe Genauigkeit von 0,5 mm erreicht wird. Vgl. GREGOR, S. (2006).
- TV-Positionierung von der Firma Rosum Corporation. Dabei werden über ein lokales Referenzgerät (z.B. für die Abdeckung von Stadtbereichen) die TV-Signale gemessen und ergänzende Daten generiert, die an den Location/Timing-Server von Rosum übertragen werden (vgl. ROSUM (2009)). Die Genauigkeit liegt zwischen 5 und 50 Meter.

3.2. Marktlösungen

3.2.1. *Beispiel für ein UWB-System; System der Firma Ubisense*⁹³

Das Ubisense-System arbeitet mit einer Funkverbindung (proprietäres Protokoll) im freien 2,4 GHz-Band für die Kommunikation mit den Tags. Über diesen Funkkanal werden Infos vom Tag ausgelesen (z.B. Batteriezustand), bzw. wird der Tag parametrisiert und angesteuert.

Beim Ubisense-System genügen für eine 3D-Bestimmung zwei Sensoren (weil AoA mitverwendet wird), bei anderen Herstellern sind zumindest 3 Sensoren erforderlich.

Der abzudeckende Bereich wird dabei in Zellen eingeteilt, wobei eine Zelle im Regelfall aus vier Sensoren gebildet wird, und ein Sensor die Rolle des Masters übernimmt. Dieser kommuniziert mit dem Server, steuert die anderen Sensoren und die Tags im Bereich der Zelle. Der Master weist den Tags jeweils einen Zeitschlitz zu, in dem der Tag den UWB-Puls senden darf. Die Sensoren registrieren dann diesen Puls und messen einerseits den Winkel (AoA) und andererseits die Zeitdifferenz des ankommenden Signals (TDoA). Voraussetzung dabei ist, dass die Sensoren einer Zelle sehr genau synchronisiert sind. Die Positionsberechnung erfolgt durch den Master, der die Position dann an den zentralen Server übermittelt.

⁹² MPS = **M**obile **P**ositioning **S**ystem; siehe dazu

http://www.ericsson.com/ericsson/corpinfo/publications/review/1999_04/files/19990406.pdf, , zuletzt geprüft am 14.10.2009

⁹³ Infos zum Thema UWB stammen, soweit nicht anders zitiert, von Nicolai Karl, Techniker bei Ubisense Deutschland

In üblichen Umgebungsbedingungen kann mit 4 Sensoren ein Gebiet von 50 x 50 m lückenlos abgedeckt werden; bei sehr günstigen Verhältnissen 75 x 75 m. Die Sensoren werden dabei an den Außenseiten (Ecken) des abzudeckenden Gebietes angeordnet. Zur Abstützung in kritischen Bereichen (z.B. Metallgitterböden) können innerhalb des Bereiches zusätzliche Sensoren angeordnet werden. Tags, die nicht im Empfangsbereich der Sensoren liegen, werden in den Ruhezustand versetzt um Energie zu sparen.

Die Genauigkeit der UWB-Systeme liegt bei 10-30 cm, z.B. beim Ubisense-System bei ca. 15 cm und daher im genaueren Segment der RTLS. Neben der genauen Positionsbestimmung können UWB-Sensoren auch im Presence-Modus betrieben werden. Dabei registriert ein Sensor, die Tags, die in seinem Empfangsbereich liegen.

3.2.2. *Beispiel für ein Wi-Fi-System; System von Ekahau*

Als Beispiel für eine WLAN-basierte Lösung wird die Lösung der Firma Ekahau angeführt, die eine rein softwarebasierte Lösung ist, und mit bestehender 802.11-Infrastruktur arbeitet, sowie zur Ergänzung Wi-Fi-Beacons verwendet. Für den mobilen Bereich können entweder eigene Wi-Fi-Tags oder Standard Wi-Fi-Geräte wie z.B. Laptops, Handhelds, usw. eingesetzt werden. Wi-Fi-Tags besitzen ein besonderes Energiemanagement, wie z.B. Bewegungssensoren, die den Tag in den Ruhezustand versetzen, wenn keine Ortsveränderung erfolgt, sodass die Lebensdauer der Batterie bis zu 5 Jahre beträgt (vgl. EKAHAU [2] (2009)). Über eine mitgelieferte API kann das System (Positioning Engine) in bestehende Applikationen integriert werden, und somit bestehende Lösungen um die „Location“-Funktionalität ergänzen.

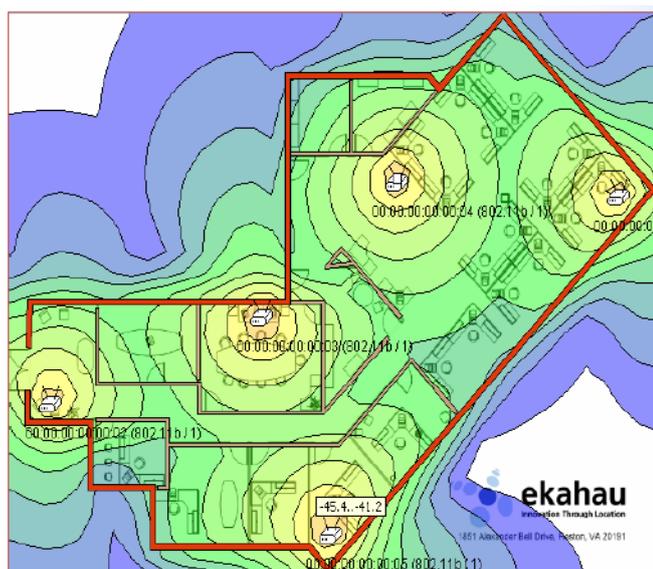


Abbildung 22: Feldstärkenverteilung; Beispiel Ekahau
Quelle: Ekahau [1] (2009)

Für die Positionsbestimmung wird ein patentiertes Verfahren eingesetzt, das auf der Fingerprinting-Methode beruht. Es wird in einer Kalibrierungsphase eine Feldstärkenlandkarte des abzudeckenden Bereiches erstellt. Eka hat für sein System eine Genauigkeit bis in den Submeter-Bereich an (mit zusätzlichen Location Beacons).

3.2.3. UWB-Ortung für Personensicherheit bei AREVA⁹⁴

Im Zentralarchiv der AREVA NP GmbH (dem weltweit führenden Kerntechnikunternehmen) in Erlangen wurde im Februar 2009 ein Personensicherheitssystem auf Basis der Echtzeitortung von Ubisense in Betrieb genommen. Hintergrund ist, dass zur Vermeidung von Löschschäden der Gebäudekomplex mit einem Stickstofflöschsystem ausgestattet wurde. Im Falle eines Brandes wird das Gebäude mit Stickstoff geflutet, der den Flammen den Sauerstoff entzieht, indem es rasch die vorhandene Luft verdrängt. Die Stickstofflöschung setzt erst nach einer Vorwarnzeit für die Evakuierung von Personen ein. Das bedeutet aber auch, dass danach für alle noch im Gebäude befindlichen Personen Lebensgefahr besteht. Stickstoff ist zu 71% in der Luft enthalten und an und für sich ungiftig. Die Gefahr geht durch Erstickung aufgrund von Sauerstoffmangel aus.

Um einen Überblick über die im Gebäude befindlichen Personen zu haben, müssen alle Mitarbeiter und Besucher des Archivs UWB-Tags tragen. Die vernetzten Sensoren registrieren die Signale der Tags und berechnen die Positionen der Personen sehr genau (15-30 cm; Technik siehe Kapitel 3.2.1). Über eine in die Gesamtlösung integrierte 3D-Visualisierung besteht jederzeit die Übersicht darüber, wo sich wie viele Personen aufhalten. Die Rettungskräfte können daher gezielt eingreifen.

Dieses System wäre auch als Sicherheitssystem im Kraftwerksbereich sehr gut geeignet. Terry Phebey, Vorstand der Ubisense AG, stellt in der Aussendung fest, dass die Ubisense-Systeme zunehmend für Personensicherheitslösungen eingesetzt werden.

3.2.4. Verfolgung von Warenströmen mit RFID⁹⁵

Die Fa. Gerolsteiner Brunnen GmbH & Co. KG setzt eine Lösung ein, bei der über 2.500 in den Boden der Lagerhalle eingelassene RFID-Transponder jederzeit die Warenströme verfolgt werden können, und damit eine lückenlose Dokumentation der Chargen ermöglicht. Diese lückenlose Dokumentation ist aufgrund einer EU-

⁹⁴ Informationen stammen von der Presse-Aussendung der Fa. Ubisense vom 10.2.2009

⁹⁵ Electronic Commerce Centrum (2007)

Verordnung im Lebensmittelbereich erforderlich. Dabei sind die Stapler mit entsprechenden Antennen ausgestattet, welche die in den Boden eingelassenen Transpondersignale inkl. Id empfangen, und über WLAN an einen Server weiterleiten. Jedem Transponder ist dabei eine Position zugeordnet, und damit kann die genaue Position des Staplers bestimmt werden. Über einen am Stapler angebrachten Scanner und eine Touchscreen-Anwendung im Cockpit des Staplers werden die Paletten identifiziert. Damit lassen sich die Transportabläufe vom Lagerplatz zum LKW lückenlos verfolgen und dokumentieren.

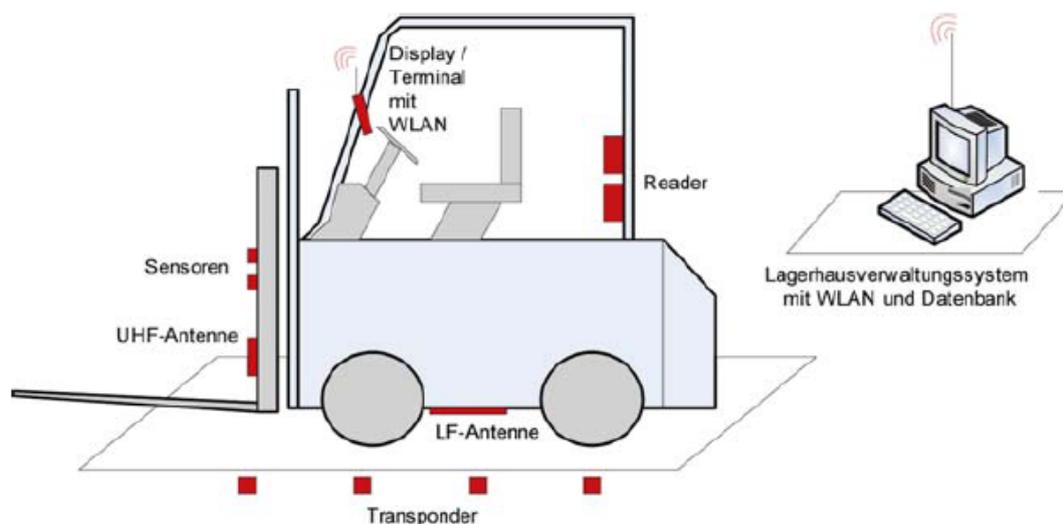


Abbildung 23: Mit RFID ausgerüsteter Gabelstapler

Quelle: Scholz-Reiter, B. (2007)

Da die RFID-Tags in den Boden eingelassen sind, ist dieses Verfahren sehr aufwändig, und nur bei Errichtung von neuen Lagern sinnvoll. Das Verfahren ist aber sehr gut geeignet Lagerabläufe (auch in EVU) zu automatisieren, da auf diese Art und Weise natürlich auch die Einlagervorgänge (Bodenlager) lückenlos verfolgt werden können. Die räumliche Auflösung wird durch die Maschenweite der Tags im Boden bestimmt.

3.2.5. *Hybrides RTLS in der Automobil-Branche*

Scholz-Reiter, B. (2007) beschreibt den Einsatz eines hybriden RTLS in der Automobilbranche. Dabei wird jedes Fahrzeug hinter der Windschutzscheibe mit einem passiven RFID-Tag ausgestattet. Die Informationen des Tags werden mit einem mobilen RFID-Lesegerät, Mobile Datenerfassung (MDE), ausgelesen bzw. beschrieben. Das MDE-Gerät hat ein GPS eingebaut. Bei jedem Lese- bzw. -Schreibvorgang wird dabei die GPS-Position mitgespeichert und über eine WLAN-Anbindung an den zentralen Server gesendet. Dadurch, dass das Lesegerät relativ nahe beim RFID-Tag

sein muss, ist gewährleistet, dass die Position mit ausreichender Genauigkeit vom GPS übernommen werden kann.

Vorteil dieses Systems ist, dass sehr kostengünstige passive RFID-Tags verwendet werden können. Die Anwendung dient zur Lokalisierung der Fahrzeuge im Freien. Vorausgesetzt wird dabei natürlich, dass jedes abgestellte Fahrzeug zuvor durch Auslesen des Tags verortet wurde. Im ERP-System ist dann der Lagerort verzeichnet. Mit dieser Lösung konnte das Auffinden der Fahrzeuge wesentlich beschleunigt werden. Zu jedem Zeitpunkt ist bekannt wo welches Fahrzeug steht und auch welche Stellplätze noch frei sind. Zeitaufwändige Suchvorgänge können vermieden werden.

Aufgrund des sehr einfachen Aufbaus dieses Systems könnte es kostengünstig auch für die Lagerprozesse bei Energieversorgungsunternehmen eingesetzt werden. Z.B. für Fragestellungen: Wo ist welcher Transformator gelagert, oder wo ist welche Kabeltrommel gelagert? Aufgrund der räumlichen Auflösung des GPS können nur relativ große Gegenstände hinreichend genau identifiziert werden.

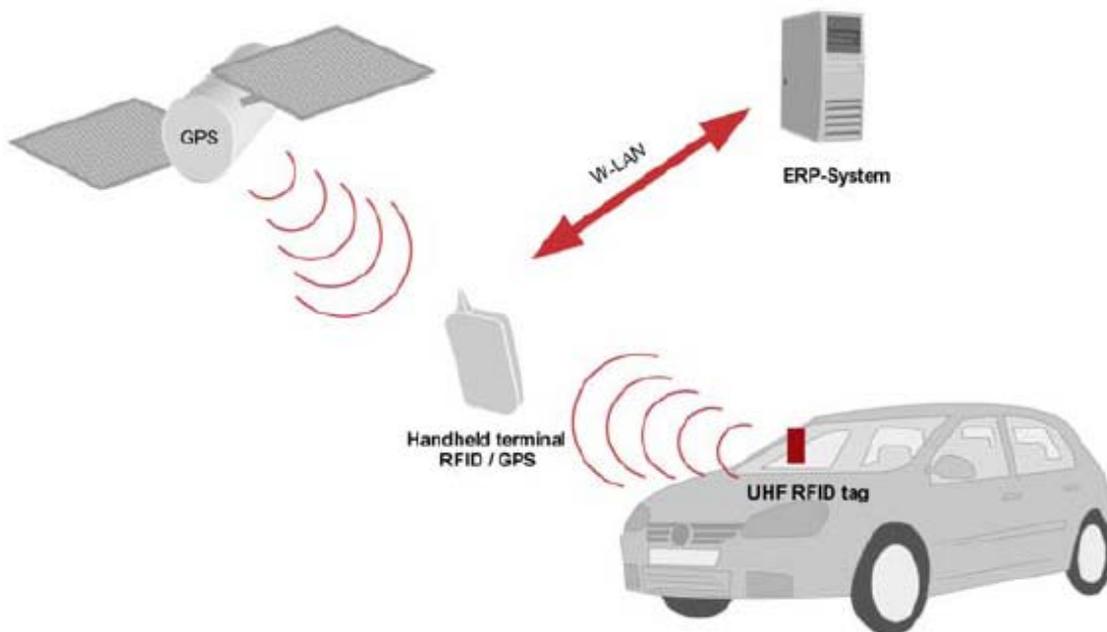


Abbildung 24: Hybrides RTLS mit RFID und GPS

Quelle: SCHOLZ-REITER, B. (2007)

4. Anwendungsszenarien in EVU

4.1. Grundsätzliche Anmerkungen

Nach Gesprächen mit Vertretern der Firmen Geodan und Ubisense, zwei namhaften Anbietern von RTLS-Lösungen im deutschsprachigen Raum, drängt sich der Eindruck auf, dass die Energieversorgungsbranche nicht zu den derzeitigen Hauptzielgruppen für RTLS-Lösungen gehört. Aus dem Studium der vorhandenen Lösungen ergeben sich aber doch auch einige interessante Einsatzgebiete in EVU. Dies sind z.B.:

- Kraftwerksbetrieb
- Lagerwirtschaft
- Asset-Management
- Workforce Management

4.2. Kraftwerksbetrieb

Die Aufgabenstellung im Kraftwerksbetrieb liegt darin, dass die Kraftwerksanlagen in täglichen Kontrollgängen auf ihre korrekte Funktion überprüft werden müssen. Diese Kontrollgänge sind auch außerhalb der üblichen Dienstzeiten, so in der Nacht und an Wochenenden sowie an Feiertagen durchzuführen. Der zunehmende Kostendruck bringt es mit sich, dass diese Kontrollgänge vorwiegend alleine durchgeführt werden. Dies birgt Risiken für die beteiligten Mitarbeiter im Falle eines Unfalles während des Kontrollganges. Dazu gibt es derzeit manuell auszuführende Meldevorgänge. RTLS können hier als Sicherheitssysteme wesentlich zur Erhöhung der Arbeitssicherheit beitragen. In den folgenden Kapiteln wurde eine solche Sicherheitslösung konzipiert.

Ein weiteres Einsatzgebiet ergibt sich nach Diskussion mit den Verantwortlichen im Bereich Kraftwerke in Zusammenhang mit Großrevisionen bei Kraftwerken oder bei Kraftwerksbaustellen. Bei diesen Einsatzszenarien sind zahlreiche Mitarbeiter von Fremdunternehmen auf dem Kraftwerksgelände. Der Überblick darüber, wer sich gerade auf dem Gelände befindet, und wo sich diese Personen aufhalten, ist oft nur nach zeitaufwändigen Rückfragen zu erhalten. Dies stellt eine Sicherheitslücke dar, sollte es zu einem Unglück (z.B. Brand) mit notwendiger Räumung des Geländes kommen.

RTLS könnten hier eine wesentliche Verbesserung bringen. Dazu müssten alle auf dem Kraftwerksgelände anwesenden Personen mit Tags ausgestattet werden, die über eine

geeignete Lösung geortet werden. Auf einer Visualisierungsoberfläche wird angezeigt, wie viele Personen sich auf dem Gelände befinden, und wo sich diese aufhalten.

Ähnliche Anwendungsszenarien sind z.B. für Raffinerien oder Hochofenbereiche beschrieben. Als Technologie könnte ein kombiniertes RTLS auf Basis von UWB und RFID eingesetzt werden, da eine größere Fläche mit zahlreichen metallischen Einbauten, wie z.B. Etagengänge auf Gitterrostbasis, Kesselanlagen, Rohrleitungen, usw. abzudecken wäre. Die UWB-Technologie ist in diesen Umgebungsbedingungen unempfindlicher gegenüber Multipath-Effekten. Aufgrund der Weitläufigkeit der Anlagen und der vielen unterschiedlichen Zugangsmöglichkeiten kann das Gelände alleine mit Chokepoints und Presence-Sensoren kaum wirkungsvoll abgedeckt werden.

4.3. Lagerwirtschaft

Die Lagerlogistik ist derzeit eines der häufigsten Einsatzgebiete für RTLS. Prinzipiell gelten für ein Lager eines EVU die gleichen logistischen Herausforderungen wie für andere Lager. Es gilt die Artikel möglichst platzsparend und effizient einzulagern und die Auslieferung der Waren ebenso effizient durchzuführen.

Von entscheidender Bedeutung ist dabei das Auffinden der eingelagerten Waren. Über eine Kombination von passiven RFID-Tags mit Positionsbestimmung durch RTLS können die Lagerprozesse wirkungsvoll unterstützt werden. Die Stapler-Fahrzeuge werden mit aktiven Tags ausgestattet (z.B. Wi-Fi-Tags, UWB-Tags, aktive RFID-Tags). Die Waren werden mit passiven RFID-Tags gekennzeichnet. Beim Ablegen der Artikel in die Lagerflächen registriert das System die Position des Staplers und übermittelt diese an ein zentrales Computersystem (über WLAN). Über das gleichzeitige Auslesen der passiven RFID-Tags kennt nun die Lösung, welche Artikel sich in welchen Lagerflächen befinden.

Eine Besonderheit bei EVU ist, dass auch viele größere, sperrige Artikel, in Freilandbereichen gelagert werden müssen. Dazu zählen z.B. Transformatoren und Kabeltrommeln. Über eine solche RTLS Lösung bestünde jederzeit der Überblick darüber, wo sich welche Transformatoren bzw. Kabeltrommeln befinden. Die Anwendung dieser Kennzeichnung macht allerdings nur ab einer bestimmten Lagergröße wirklich Sinn.

Ein weiteres Anwendungsgebiet könnte sein, die Kabeltrommeln mit aktiven Tags zu kennzeichnen und in ein Alarmierungssystem einzubinden, falls sie unbefugt entfernt

(gestohlen) werden, stellen doch die Kabeltrommeln in Zeiten hoher Metallpreise einen beträchtlichen finanziellen Wert dar.

Da es bei der „Diebstahlsicherung“ nicht auf eine hohe Genauigkeit ankommt, könnten kostengünstige Wi-Fi-Tags unter Anwendung der Presence-Methode eingesetzt werden. Die RFID-Technik ist jedenfalls bestens dazu geeignet, Warenflüsse zu automatisieren, vor allem einen medienbruchfreien Datenfluss über die Warenströme zu ermöglichen. So kann ein Material vom Lagerort bis zum Einbauort automatisiert verfolgt werden.

4.4. Asset-Management

Für die Unterstützung im Asset-Management bietet sich die Kennzeichnung der Betriebsmittel mit passiven RFID-Tags an. Diese Methode wird im Industriebereich schon häufig eingesetzt.

Unter Asset Management im EVU-Gebrauch wird im Allgemeinen die Wartung und Instandhaltung der Anlagen verstanden. Bedingt durch die Regulierung im Energiebereich und dem damit einhergehenden Kostendruck hat sich in den letzten Jahren ein beträchtlicher Wandel in den EVU vollzogen. Durch steigenden Kostendruck aufgrund sinkender Erlöse (z.B. im Stromnetzbereich durch die Vorgaben der ECG⁹⁶) haben sich die Instandhaltungs- und Wartungszyklen hin zur zustands- und risikoorientierten Instandhaltung verändert. Dadurch soll die Instandhaltung und Wartung nicht nur kostengünstiger werden, sondern die Mittel sollen dort eingesetzt werden, wo sie gebraucht werden. Ein wesentlicher Teil dabei ist die regelmäßige Begehung der Anlagen und die Bewertung der Zustände der Anlagen. Richtige Zustandsinformationen sind von entscheidender Bedeutung, wenn es darum geht mit entsprechender Softwareunterstützung langfristige Asset-Managementstrategien zu entwerfen, die die gesamten Lebenszykluskosten der Betriebsmittel berücksichtigen. Die effiziente Betriebsmittelbegehung ist eine Anforderung der Stunde. Die Kennzeichnung der Betriebsmittel mit RFID-Tags führt zu einer steigenden Effizienz durch folgende Nutzeneffekte:

- Betriebsmittel können automatisch identifiziert werden.
- Geringere Fehlerquote, weil Verwechslungsmöglichkeiten eliminiert werden, und das richtige Betriebsmittel auf der Erfassungsmaske für die Zustandsinformationen angezeigt wird.
- Zusätzliche Informationen sind vor Ort verfügbar.

⁹⁶ ECG = Energie-Control-GmbH
Manfred Farthofer

- Auf den Tags können Begehungs- Wartungs- und Instandhaltungsinformationen gespeichert werden, dadurch sind zusätzliche Information für die Vorort-Mitarbeiter verfügbar.
- Die Datenerfassung ist automatisiert, dadurch gibt es keine Medienbrüche.
- Bei Onlineverbindung stehen die Begehungsinformationen in Echtzeit zur Verfügung.
- Durchgehende Dokumentation des Begehungsvorganges und der Wartungs-und Instandhaltungstätigkeiten.
- Nachweis, dass man tatsächlich bei den Betriebsmitteln vor Ort war.
- Transparenz der Datenentstehung (Wer hat wann was erfasst?).
- Genau definierte Arbeitsprozesse und damit einheitliche Abläufe. Dies ist gerade bei auf mehreren Standorten verteilten Organisationseinheiten wichtig.
- Insgesamt weniger Aufwand bei der Begehung und dadurch niedrigere Kosten.

Neben der Unterstützung durch RFID-Tags bei der Identifikation der Betriebsmittel, könnten auch bewegliche Betriebsmittel von hohem Wert mit aktiven Tags gekennzeichnet und in Echtzeit getrackt werden. Dadurch sind Aussagen über den Inventarbestand in Echtzeit möglich. Für diese Anwendung ist wiederum der Aufbau einer eigenen Infrastruktur für die Ortung erforderlich. Dies könnte z.B. durch UWB-Systeme oder auch WLAN-basierte Systeme aber auch durch aktive RFID-Systeme erfolgen, weil dabei die Ortungsgenauigkeit eine untergeordnete Rolle spielt. Die Ortung erfolgt nach der Proximity- bzw. Presence-Methode.

Die Kennzeichnung der hochwertigen Betriebsmittel ist gerade im Kraftwerksbereich eine interessante Einsatzmöglichkeit, weil hier sehr viele teure Ersatzteile und teure Werkzeuge und Maschinen im Umlauf sind.

Ein weiterer Einsatzbereich für RFID ist die Kennzeichnung der Zähler mit passiven RFID-Tags. In der Zählerlogistik ist der wichtigste Punkt, dass die Stationen des Zählers genau verfolgt werden können. Es geht darum, dass zu jedem Zeitpunkt bekannt ist, wo sich ein Zähler gerade befindet. Der Lauf eines Zählers muss lückenlos dargestellt werden, ist doch der Zähler jenes Gerät, das die Basis für die Verrechnung der Entgelte an den Kunden darstellt. Die Kennzeichnung der Zähler mit RFID-Tags ermöglicht, dass beginnend vom Lagerort im Zentrallager bis zur Einbaustelle der Zähler getrackt werden kann. Dazu muss jede Ortsveränderung über RFID-Lesegeräte

abgewickelt werden. Dies kann über stationäre RFID-Reader und mobile Reader erfolgen. Diese übermitteln die jeweilige Zähler-Id ggf. mit weiteren Geräteinfos wie z.B. Zählerständen an eine zentrale Serverlösung für die Verwaltung der Zähler. Bei EVU ist dies häufig die Software SAP-ISU. Vorteile einer RFID-Lösung in diesem Zusammenhang sind:

- Lückenlose Erfassung der Zählerbewegungen, dadurch keine Fehlbestände mehr.
- Keine Eingabefehler bei den Zählernummern, weil keine Medienbrüche.
- Zählernummer kann ohne Sichtverbindung abgelesen werden.
- Schnellere Erfassung.
- Lückenlose Dokumentation.

Ein weiterer Einsatz für die RFID-Technologie in EVU stellt die Überprüfung von Werkzeugen und Maschinen dar. Viele Geräte für die Arbeiten in Zusammenhang mit Leitungsanlagen wie z.B. Hebezeuge wie Lugal, Werkzeuge für Arbeiten unter Spannung, elektrische Maschinen wie Bohrmaschinen, Winkelschleifer, usw. müssen in regelmäßigen Zeitintervallen geprüft werden. Die Kennzeichnung dieser Werkzeuge und Maschinen mit RFID-Tags erlaubt es, die Organisation der Überprüfung deutlich zu verbessern. So kann z.B. die Gerätebezeichnung automatisch ausgelesen werden. Ebenso ist es beispielsweise möglich das Datum der letzten Überprüfung und/oder den Namen des Prüfers auf den Tag zu schreiben. So ist im Anlassfalle jederzeit nachweisbar, wann und von wem das Gerät zuletzt überprüft wurde.

MANNEL, A. (2008) führt folgenden Nutzen (siehe Grafik) eines RFID-gestützten Asset-Managements in der Industrie an. Diese Nutzenpunkte sind im Wesentlichen auch für die EVU zutreffend und in der folgenden Auflistung durch eigene Überlegungen ergänzt:

- Erhöhung der Prozessqualität; durch festgelegte Abläufe; insbesondere bei Prozessen auf mehreren Standorten.
- Erhöhung der Prozesseffizienz; durch die Verbesserung des Handlings, Entfall von Dokumentationszeiten und weniger manuellen Eingaben.
- Besserer Lieferservice; bei Produkten die an Kunden ausgeliefert werden.
- Erhöhung der Kundenzufriedenheit; dies trifft auch für die internen Kunden zu, indem die vereinbarten Servicelevels besser eingehalten werden

- Erhöhung des Umsatzes; im internen Bereich erfolgt dies durch Verringerung der Fremdleistungen durch bessere interne Prozessabläufe
- Verringerung des Lagerbestandes; weil zeitaktueller auf die Anforderungen reagiert werden kann, und weil durch eine mit Zustandsinformationen hinterlegte Asset-Strategie der Bedarf genauer geplant werden kann.
- Damit weniger Kapitalbindung
- Weniger Schwund durch eine lückenlose Echtzeit-Verfolgung der Artikel. Dies ist vor allem im Zählerbereich eine zentrale Anforderung. Es ist der Weg vom Lager bis zum Einbauort lückenlos nach verfolgbar.
- Geringere Logistikkosten; infolge der definierten Prozessabläufe im Sinne standardisierter Prozesse und der Automatisierung der Abläufe und der Vermeidung von Medienbrüchen.
- Durch die vorgenannten Punkte insgesamt geringere Gesamtkosten.

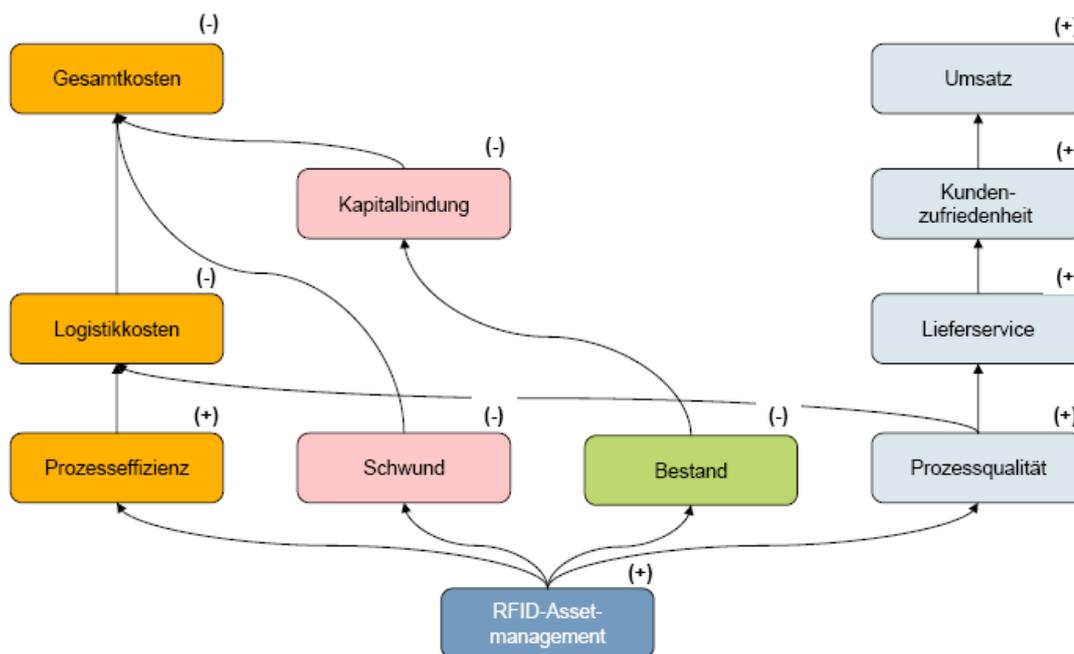


Abbildung 25: Nutzen RFID-gestütztes Asset Management

Quelle: MANNEL, A. (2008)

4.5. Workforce-Management (WFM)

Workforce Managementsysteme (WFMS) dienen zur Steuerung der Außendienst-Mitarbeiter im Servicebereich. Zentrale Elemente der WFMS sind:

- Serverapplikation
- Dispatching-Oberfläche für die Einteilung der Service-Mitarbeiter

- Optimierungskomponenten
- Mobile Komponente für Auftragsübermittlung und -rückmeldung
- Mobile Clientanwendung für die Mitarbeiter
- Integration mit den Vorsystemen

Ziel von WFM ist es, die richtigen Mitarbeiter zur richtigen Zeit mit der richtigen Ausstattung (Werkzeug, Material) am richtigen Ort einzusetzen.

In EVU gibt es eine relativ große Anzahl von Servicemitarbeitern. Zahlreiche Arbeiten sind in der „Fläche“ zu verrichten. Dazu gehören z.B. die Herstellung von Hausanschlüssen (Strom, Gas, FW, Telekom, Wasser), die Begehung von Leitungsanlagen, die Instandhaltung und Wartung von Stationen und Leitungen, die Leitungseinmessung, die Betriebsführungstätigkeiten wie Schaltungen, Zählerablesungen, Sperrungen, und andere.

Derzeit wird die Einteilung der Mitarbeiter meist manuell durchgeführt. Die Herausforderung bei der Einteilung ist dabei, eine unter Beachtung zahlreicher Nebenbedingungen optimale Einteilung der Mitarbeiter zu finden. Zu beachten sind Gesichtspunkte wie Qualifikationen, Einhaltung von Arbeitszeiten, Kundenanforderungen, örtliche Nähe, Gebietszuständigkeiten, gesetzliche Vorschriften, und Weitere.

Der Kostendruck aufgrund der Liberalisierung brachte es mit sich, dass die Kosten gerade im Servicebereich deutlich reduziert wurden und weiterhin reduziert werden. Dazu werden die Einsatzgebiete einerseits laufend vergrößert und andererseits die „fachliche Einsatzbreite“ durch Zusatzausbildungen verbreitert. Dies führt dazu, dass sowohl die Arbeitseinteiler (Dispatcher) als auch die Mitarbeiter im Außendienst zunehmend weniger Orts- und Anlagenkenntnisse haben. Es ist daher eine elektronische Unterstützung der Arbeitsprozesse durch geeignete Softwaresysteme erforderlich. Genau bei diesem Punkt setzten die WFMS an, indem unter Berücksichtigung der Qualifikationen und Auftragsanforderungen der „beste“ Mitarbeiter den Auftrag zugeteilt bekommt.

Üblicherweise landen dabei alle Arbeitsaufträge in einem Auftragspool und werden dann vom System unter Beachtung der Randbedingungen optimal auf die Ressourcen verteilt. Dies geschieht entweder automatisch, oder als Vorschlagswert für den Dispatcher, oder durch manuelle Zuordnung eines Auftrages auf eine Ressource. Eine grafische Benutzeroberfläche (z.B. GANNT-Darstellung) unterstützt den Dispatcher bei seiner Arbeit und warnt bei Regelverletzungen (z.B. wenn ein Auftrag einem

Mitarbeiter zugeordnet wurde, der nicht über die hierfür erforderliche Qualifikation verfügt).

Gerade in Zusammenhang mit Störungseinsätzen ist dabei von großer Bedeutung in Echtzeit zu wissen, wo sich welche Mitarbeiter befinden. Für diese Aufgabenstellung bietet das Tracking der Mitarbeiter (meist in Form vom Tracking der Fahrzeuge) eine wesentliche Entscheidungshilfe. Diese Aufgabe übernehmen z.B. Flottenmanagementsysteme oder auch Störungsmanagementsysteme als Teil der Gesamtlösung WFMS. Die Positionsbestimmung der Fahrzeuge erfolgt dabei meist über GPS. Die Positionsdaten werden über eine Kommunikationseinheit an den zentralen Server übertragen (z.B. beim System Tom Tom Work über eine eingebaute Linkbox⁹⁷). Die Position der Mitarbeiter (respektive der Fahrzeuge) wird auf einer Karte visualisiert. Ist nun eine Störung zu bearbeiten, ermittelt das System in Echtzeit den nächstgelegenen Mitarbeiter mit der erforderlichen Qualifikation und weist diesem entweder direkt den Störungsauftrag zu, oder schlägt dem Dispatcher den entsprechenden Mitarbeiter vor, der den Auftrag dann dem Mitarbeiter zuordnet und übermittelt. Dies erfolgt wiederum in Echtzeit über eine Telekommunikations-Verbindung, z.B. GPRS.

Der Mitarbeiter nimmt am mobilen Gerät den Auftrag dann entweder an, oder weist ihn zurück. Entsprechende Statusmeldungen gehen an den Server.

Vorteile dieser Lösungen:

- Wesentlich kürzere Reaktionszeiten bei Störungen.
- Besserer Überblick über die eingesetzten Mitarbeiter.
- Dokumentation aller wesentlichen Informationen, wie: Wann wurde der Auftrag zugewiesen? Wann wurde der Auftrag angenommen? Wann war die Störung beendet?
- Transparenz über die Abläufe.
- Ermittlung von Prozesskennzahlen, wie z.B. wie lange dauert welche Tätigkeit?
- Verringerung der Wegzeiten durch Zuweisung der nächstgelegenen Aufträge.
- Optimierung der Arbeitseinteilung z.B. über Routenoptimierung.

Als Technologie für die Positionsbestimmung kommt für die Auftragssteuerung in der „Fläche“ überwiegend die GPS-Technologie zum Einsatz. Aber auch die zellbasierte

⁹⁷ www.tomtomwork.com, zuletzt geprüft am 25.10.2009

Positionsbestimmung mittels Mobilfunk wäre eine Alternative, da die Positionsgenauigkeit in diesem Anwendungsszenario keine so große Rolle spielt.

Anders verhält es sich bei der räumlich optimierten Auftragseinteilung in Anlagen. Hier ist einerseits eine genauere Ortung erforderlich, weil zumindest auf Raumgenauigkeit festgestellt werden sollte, wer sich wo aufhält, und andererseits scheidet GPS als Ortungstechnologie im Innenraumbereich aus. Möglich wäre z.B. der Einsatz der Wi-Fi-Technologie oder auch der UWB-Technologie.

Studien zeigen auf, dass WFMS eine sehr gute Wirtschaftlichkeit mit kurzer ROI-Dauer aufweisen. Ein Beispiel hierfür sind die Studie der Aberdeen-Group (vgl. DUTTA, S. (2008)).

Entscheidend für die Wirtschaftlichkeit der WFM-Lösungen ist die Anzahl der mittels WFMS gesteuerten Mitarbeiter. Je größer die Mitarbeiterzahl, umso kürzer die ROI-Dauer. Erfahrung von Energieversorgern (Vgl. z.B. E.ON, MVV, RWE), die bereit WFM einsetzen ist, dass ein erheblicher Teil der Einsparungen in der Reduzierung der Wegekosten liegt. Schlüssel dafür ist, dass einerseits Routenoptimierung und andererseits GPS-Ortung eingesetzt werden. Aussage von Dr. Neumann, E.ON-Energie, im Rahmen eines Vortrages in Berlin am 29. Oktober 2009, war, dass schon durch die Einsparung bei den Wegekosten alleine die Lösung wirtschaftlich ist.

Im Rahmen einer Modellrechnung sieht der Autor die größten Einsparungen bei:

- Einsparung von Wegkosten durch Routenoptimierung, zeitnahe Nachsendung auf der Strecke liegender Aufträge, Anfahrt von Zu Hause weg (ca. 50% der Einsparungen)
- Reduktion der Aufwendungen durch automatisierte Arbeitseinteilung und effiziente Funktionen für die Arbeitseinteilung (ca. 15%)
- Reduktion von Mehrleistungen durch bessere Staffelung der Aufträge (ca. 5%)
- Reduktion von Aufwendungen durch bessere Steuerungsmöglichkeiten aufgrund der höheren Prozesstransparenz (ca. 10%)
- Reduktion von administrativen Aufwendungen durch Automatisierung der Datenflüsse (ca. 20%)

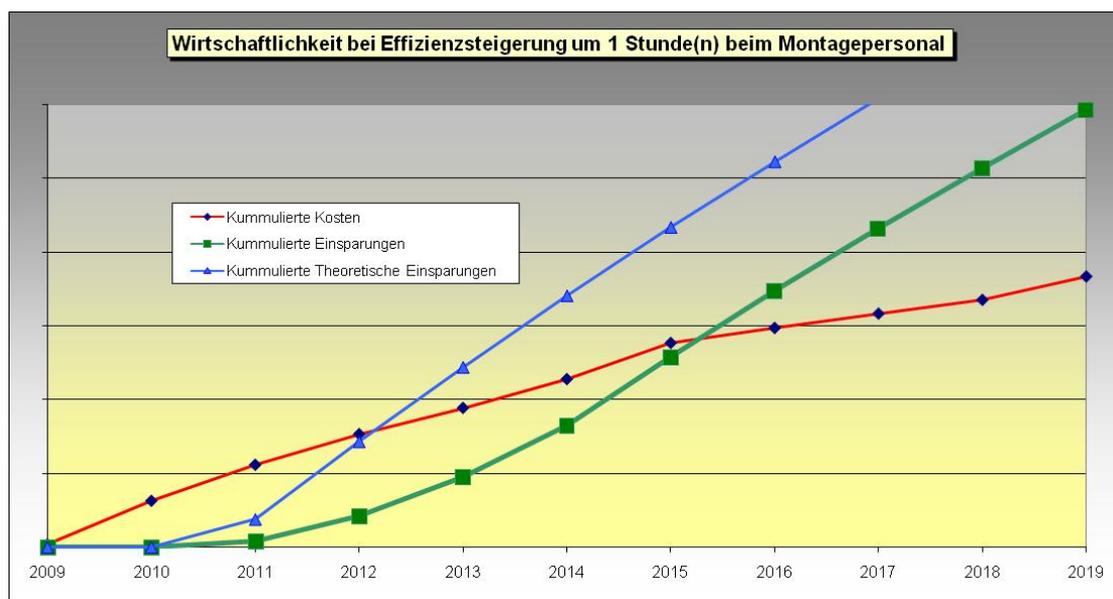


Abbildung 26: Wirtschaftlichkeitsberechnung, Darstellung ROI-Dauer

Dem oben angeführten Szenario liegen folgende Annahmen zugrunde:

- 200 Außendienst-Mitarbeiter
- Tägliche Einsparung von einer Stunde je Monteur
- Kosten je mobilen Arbeitsplatz ca. Euro 2.500
- Projektdauer von 2 Jahren
- Einsparungen werden erst in 3. Jahr voll wirksam

Unter diesen Annahmen ergibt sich eine ROI-Dauer zwischen 3,2 und 6,3 Jahren. Die Sensitivitätsanalyse zeigt, dass die Wirtschaftlichkeit ganz wesentlich von der Anzahl der eingebundenen Mitarbeiter bestimmt wird. Die ROI-Dauer ist relativ stabil gegenüber den Einmalkosten.

Ein Faktor, der nur schwer einzuschätzen ist, ist der Umstand der höheren Produktivität aufgrund der besseren Transparenz der Prozesse. Gerade die Echtzeitrückmeldung und speziell die Echtzeitortung bringt hier deutliche Verbesserungen in der Transparenz und aussagekräftigere Analysen.

4.6. Umfrage RTLS unter EVU in Österreich

Um zu hinterfragen, ob RTLS bereits bei Energieversorgern in Österreich praktisch eingesetzt werden, hat der Autor eine Umfrage unter Energieversorgungsunternehmen in Österreich durchgeführt. Dazu wurde ein 7-seitiger strukturierter Fragebogen auf Basis eines PDF-Formulars gestaltet, und an 28 Energieversorgungsunternehmen in Österreich versendet. Ziel war es mit dem Fragebogen folgende wesentlichen Fragestellungen zu beleuchten:

- Werden Ortungs- bzw. RTLS-Lösungen eingesetzt?
- In welchen Bereichen werden Ortungs- bzw. RTLS-Lösungen eingesetzt?
- Welche Ortungstechnologien werden eingesetzt?
- Welcher Nutzen wird gesehen?
- Welche Maßnahmen wurden in Bezug auf Privacy gesetzt?
- Welche Projekt- und Betriebserfahrungen gibt es?

Von diesen angefragten EVU haben 13, das sind 46% den ausgefüllten Fragebogen retourniert. Aufgrund der geringen Zahl der Angaben über praktisch umgesetzte Lösungen können die Aussagen nur als Beispielhaft gewertet werden. Eine allgemein gültige Schlussfolgerung lässt sich daraus nicht ziehen. In Bezug auf die oben angeführten Fragen lassen sich folgende Hauptaussagen aus der Auswertung ableiten:

Werden Ortungs- bzw. RTLS-Lösungen eingesetzt?

Der Großteil der Rückmeldungen ergab, dass derzeit keine entsprechenden Lösungen praktisch im Einsatz sind. Im Detail:

- Zwei Unternehmen setzen bereits eine Ortungslösung bzw. ein RTLS ein
- Zwei Unternehmen haben ein RTLS-Projekt in Einführung
- Ein Unternehmen hat eine Konzeptstudie erstellt
- Zwei Unternehmen haben konkrete Planungen für die nächsten beiden Jahre

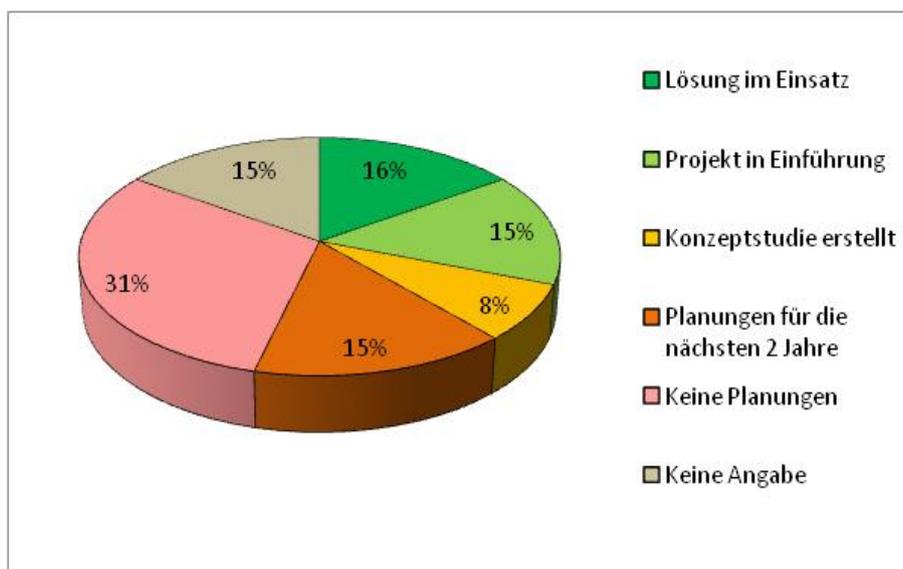


Abbildung 27: Umfrageergebnis Einsatz von RTLS-Lösungen in EVU in Österreich

In welchen Bereichen werden Ortungs- bzw. RTLS-Lösungen eingesetzt?

Die Lösungen werden vorrangig in der Fahrzeugsteuerung bzw. im Flottenmanagement und im Workforce Management verwendet.

- Es werden alle Fahrzeuge geortet
- Die Speicherung der Fahrzeugpositionen erfolgt mit Intervallen < 10 Sekunden
- Ein Unternehmen setzt das System in Verbindung mit passiver RFID-Technologie ein.
- Die Lösungen verwenden eine räumliche Auflösung von 30-100m
- Die Lösungen sind einerseits mit SAP und andererseits mit einem GIS bzw. Workforce Managementsystem gekoppelt.

Welche Ortungstechnologien werden eingesetzt?

In diesem Fragenblock wurden die verwendeten Technologien hinsichtlich Ortung, Telekommunikationsverbindung, Client- und Serverhardware hinterfragt.

- Für die Positionsbestimmung wird ausschließlich GPS verwendet.
- Ein Unternehmen hat eine Lösung mit Positionsbestimmung über Mobilfunk in Vorbereitung.
- Die Positionsbestimmung erfolgt am Client bzw. am Server.
- Als mobile Hardware werden PDAs und Laptops, sowie Navigationssysteme verwendet.
- Als Kommunikationsverbindung wird GPRS und UMTS sowie das eigene Betriebsfunknetz eingesetzt.
- Die Sicherheit der Datenübertragung wird mittels VPN gewährleistet.
- Die Server werden im eigenen Haus betrieben.

Welcher Nutzen wird gesehen?

Hier wurde hinterfragt, in welchen Bereichen die Unternehmen den Nutzen der Lösung sehen, und wie hoch sie ihn beurteilen. Dazu erfolgte eine Einteilung in vier Klassen (kein Nutzen, geringer Nutzen, mittlerer Nutzen, großer Nutzen).

- Der Nutzen wird von den Unternehmen wie folgt beurteilt:
 - Verbesserung Kundenservice: gering bzw. groß
 - Kostenreduktion: mittel bzw. groß
 - Personaleinsparungen: gering
 - Bessere Entscheidungsgrundlagen: mittel bzw. groß

- Schnellere Reaktionszeiten: groß
- Bessere Transparenz / Kenntnis der Prozesse: mittel bzw. groß
- Automatisierung von Abläufen: groß
- Vermeidung von Schnittstellen: mittel
- Mobile Erfassung von Daten: groß
- Verkürzung der Durchlaufzeiten: groß
- Erhöhung der Personensicherheit: kein bzw. mittel
- Der geplante Nutzen konnte überwiegend umgesetzt werden

Welche Maßnahmen wurden in Bezug auf Privacy gesetzt?

In diesem Fragenblock wurden der Zugriff auf die Standortinformationen, deren Speicherung, die unternehmensinternen Vereinbarungen dazu, und die Akzeptanz seitens der Mitarbeiter hinterfragt.

- Der Zugriff auf die Standortinformationen ist eingeschränkt.
- Die Ortungs-Positionsdaten werden gespeichert; bei einem Unternehmen für einen Monat.
- In allen Fällen wurde eine Betriebsvereinbarung abgeschlossen.
- Seitens der Mitarbeiter gibt es teilweise Vorbehalte hinsichtlich Kontrolle.

Welche Projekt- und Betriebserfahrungen gibt es?

In diesem Fragenblock wurden die Projekterfahrungen bei der Umsetzung der Projekte und die laufenden Betriebserfahrungen hinterfragt.

- Die Projektdauer der einzelnen Projekte betrug zwischen 50 und 104 Wochen.
- Es wurde jeweils ein Pilotprojekt durchgeführt. Die Einführung erfolgte jeweils stufenweise unter Einbindung von Praxismitarbeitern und des Betriebsrates.
- Die Lösungen sollen laufend weiterentwickelt werden.
- Als Lösungen wurden sowohl Standardlösungen als auch Individualentwicklungen umgesetzt.
- Die Ortungsgenauigkeit wird als ausreichend stabil gesehen.
- Der Ausfall der Kommunikationsverbindung wird einmal als einschränkender Faktor gesehen.
- Die Betriebsaufwendungen liegen bei 1,0 bzw. 0,3 Vollzeitkräften.

Zusammenfassung:

Die Ergebnisse der Umfrage passen gut zu den Rechercheergebnissen und Aussagen der beiden Hersteller, Geodan, und Ubisense, dass die EVU derzeit nicht als Hauptzielgruppe für den Einsatz der RTLS-Technologie gesehen werden können. Wenn die Echtzeitortung bereits praktisch eingesetzt wird, dann in Zusammenhang mit dem Tracking von Fahrzeugen und Personen für Flotten- bzw. Workforce Managementlösungen. Auch die Nutzenangaben decken sich gut mit den Ergebnissen die in der Literatur genannt werden.

5. Konkrete Lösung: Sicherheitslösung für Kraftwerksbegehungen

Das Kraftwerk Urstein der Salzburg AG ist ein Laufkraftwerk, das in Urstein nahe Hallein im Bundesland Salzburg liegt. Wie alle Wasserkraftwerke der Salzburg AG ist das KW Urstein im Regelfall unbesetzt. Zur Aufrechterhaltung des sicheren Betriebes sind aber regelmäßige Kontrollgänge vorgesehen, um wichtige technische Einrichtungen auf ihre Funktionstüchtigkeit zu überprüfen. Während der Wochentage Montag bis Freitag von 07:00 bis 17:00 Uhr erfolgen die Kontrollgänge vom Werkpersonal der Kraftwerksgruppe. Außerhalb dieser Zeit werden die Kontrollgänge von Bereitschaftsdienstmitarbeitern durchgeführt. Dabei sind diese Mitarbeiter alleine im Kraftwerksgelände unterwegs. Im Falle eines Unglücks könnte relativ lange Zeit vergehen, bis dieses bemerkt wird, und entsprechende Maßnahmen eingeleitet werden können. Die nachfolgende RTLS-Lösung soll die Sicherheit der Mitarbeiter erhöhen, indem schneller auf Ereignisse reagiert werden kann.

5.1. Informationen zum Kraftwerk Urstein

Das Kraftwerk Urstein wurde in den Jahren 1968 bis 1971 errichtet. Ausgangspunkt für den Kraftwerksbau war, dass sich die Salzach in diesem Bereich immer mehr eingetieft hatte, und deshalb eine Stabilisierung der Flusssohle erforderlich wurde um einen Sohldurchbruch zu vermeiden. Das Kraftwerk ist ein Laufkraftwerk mit zwei Kaplan-turbinen. Der Name des Kraftwerkes stammt von dem in der Nähe am rechten Salzachufer liegenden Schloss Urstein.

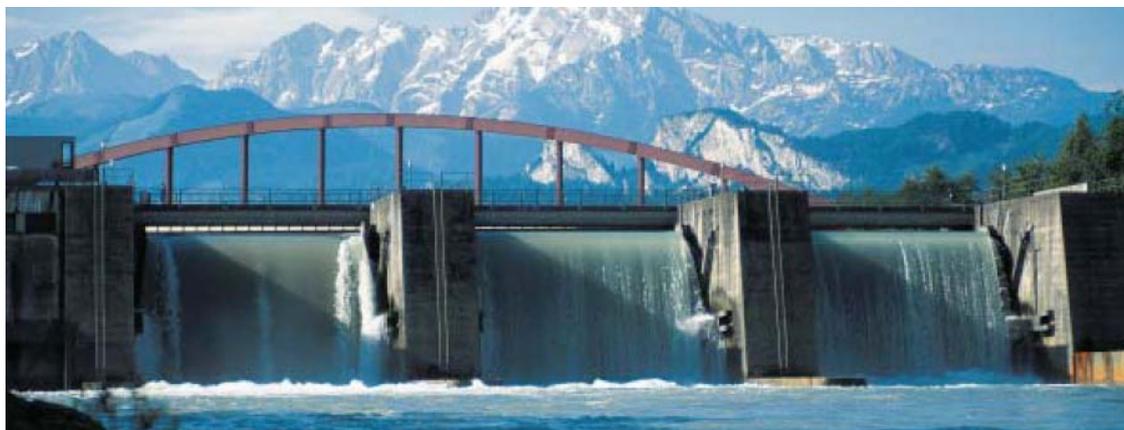


Abbildung 28: Kraftwerk Urstein

Quelle: Salzburg AG; Folder Kraftwerke_FlachgauTennengau.pdf

Kraftwerkstyp:	Laufkraftwerk
Gesamteinzugsgebiet:	4.383 km ²
durchschnittl. Jahreserzeugung:	120.000 MWh
Engpassleistung:	25.700 kW
Turbinen:	2 Kaplan Rohrturbinen mit 15° geneigten Wellen
Fallhöhe bei Ausbaumwassermenge:	11,15 m
Ausbaudurchfluss:	250 m ³ /s
Staulänge:	Salzach 5,3 km
	Königsseeache 0,9 km
Bauzeit:	Baubeginn 1968 - 1971

Tabelle 7: Technische Daten KW Urstein
Quelle: Salzburg AG

Lage:



Abbildung 29: Lage KW Urstein
Quelle: Google Earth 2009

5.2. Grundlegende Anforderungen an die Lösung

Im Rahmen einer Anforderungsanalyse (durchgeführt mit dem Kraftwerksgruppenleiter) wurden die grundlegenden Anforderungen an die Lösung erarbeitet. Folgende Rahmenbedingungen sind festzuhalten:

- Die Lösung soll die Sicherheit des eingesetzten Personals erhöhen, falls Unglücksfälle passieren.
- Verkürzung der Reaktionszeit bei Unglücksfällen.
- Die mobile Einheit soll als zentrales Gerät zur Mitnahme im Eingangsbereich aufgestellt werden.
- Die Reaktion des Systems soll unabhängig von einem Handyempfang erfolgen, da es zahlreiche Bereiche gibt, in denen kein Handyempfang möglich ist.
- Die Mitarbeiter in den Warten sollen feststellen können, in welchem Bereich sich der Mitarbeiter gerade befindet.
- Hinsichtlich der räumlichen Auflösung genügt es im Innenbereich zu wissen, in welchem Raum sich der Mitarbeiter aufhält. In den Freibereichen genügt die Info mit einer Positionsgenauigkeit von 10m.
- Die Information über den Standort soll zumindest bei jedem Raumwechsel und spätestens alle 10 Minuten erfolgen.
- Die Positionsinformationen sollen für die Mitarbeiter der KW-Einsatzleitstelle und im Kraftwerksgruppenleitstand verfügbar sein.
- Es soll eine automatische Meldung in der Kraftwerkseinsatzleitstelle erfolgen, falls über mehr als 10 Minuten keine aktualisierte Positionsmeldung erfolgt.
- Automatische Alarmierung der Einsatzleitwarte im Falle von Regelverletzungen.
- Automatischer Anruf beim Mitarbeiter im Falle von Regelverletzungen.
- Die Lösung ist so zu konzipieren, dass Fehlalarmierungen minimiert werden.
- Die Lösung soll auch für die Dokumentation der Kontrollgänge verwendet werden können.
- Die Lösung soll die Überwachung an verteilten Standorten ermöglichen
- Die Lösung soll kostengünstig sowohl in der Errichtung als auch im Betrieb sein.
- Die Server-Lösung soll im Sinne einer „Location-Plattform“ auch für andere Einsatzfälle geeignet sein.
- Die verwendete Hardware soll auch für andere Zwecke einsetzbar sein.

5.3. Prozess-Anforderungen an den Kontrollgang

5.3.1. Grundsätzlicher Prozessablauf

Der Mitarbeiter stellt nach dem Betreten des Kraftwerksgebäudes den Objektschutz ab und meldet sich telefonisch bei der Kraftwerkseinsatzleitstelle an. Danach geht er in die Maschinenhalle und stellt den Anwesenheitsschalter auf ein. Der Anwesenheitsschalter signalisiert in der KW-Einsatzleitstelle die Anwesenheit des Mitarbeiters.

Danach beginnt er den Rundgang, der wieder in der Maschinenhalle endet. Nach dem Rückstellen des Anwesenheitsschalters in die „Aus“-Position meldet sich der Mitarbeiter telefonisch in der KW-Einsatzleitstelle ab, aktiviert wieder den Objektschutz und verlässt das Kraftwerksgebäude.



Abbildung 30: Prozess Kontrollgang KW Urstein

Der derzeitige Prozessablauf hat aus sicherheitstechnischer Sicht folgende Schwachstellen:

- Wenn der Mitarbeiter anzurufen vergisst, erfolgt keine aktive Benachrichtigung, dass sich jemand im Kraftwerk aufhält.
- Wenn die Schalterstellung des Anwesenheitsschalters nicht verändert wird, ist keine Anzeige über die Anwesenheit im Kraftwerk vorhanden.

- Wenn der Mitarbeiter während des Kontrollganges verunglückt, kann mangels Information nicht darauf reagiert werden. Es verstreicht wertvolle Zeit.
- Keine Information in der KW-Leitstelle, wo innerhalb des Kraftwerks sich der Mitarbeiter aufhält.
- Keine aktive Benachrichtigung des Wartenpersonals.

5.3.2. *Kontrollgang*

Die Kontrollgänge sind erforderlich um die Betriebssicherheit des Kraftwerkes zu gewährleisten. Im Zuge der Kontrollgänge werden Anlagenteile auf ihre Funktionstüchtigkeit geprüft, Wasser- und Ölstände abgelesen, Dichtheitsüberprüfungen vorgenommen, sowie Meldungen überprüft.

Der Kontrollgang ist aus sicherheitstechnischer Sicht der kritische Punkt des Prozesses. Im Zuge des Kontrollganges erfolgen Abstiege in die Generator- und Turbinenschächte, die entsprechende Gefahrenquellen darstellen. Weiters müssen zahlreiche Bereiche betreten werden, in denen kein Handyempfang vorhanden ist, und somit auch keine aktive Alarmierung bei Unglücksfällen möglich ist. Allerdings wird zwischen den Bereichen ohne Handyempfang immer wieder einmal eine Zone mit Handyempfang betreten, sodass die maximale Zeit ohne Handyempfang ca. 5 Minuten beträgt. Die Gesamtdauer für einen Kontrollgang beträgt ca. 40 Minuten.

Ablauf Kontrollgang:

- 1) Betreten des Kraftwerksgebäudes
- 2) Ausschalten des Objektschutzes
- 3) Abgang in die Maschinenhalle
- 4) Anwesenheitsschalter an der Schalttafel auf „Ein“ stellen
- 5) Gang in den Leitstand und Überprüfen der Monitore des Leitrechners auf Meldungen
- 6) Abstieg in den ersten Generatorschacht. Der Abstieg ist ca. 8 m tief und erfolgt über eine steile enge Leiter. Im Generatorschacht müssen die Erregerbürsten und Kühlwasserpumpen kontrolliert werden. Dies ist ein kritischer Bereich, da einerseits Absturzgefahr besteht, und andererseits im Generatorschacht kein Handyempfang möglich ist.

- 7) Aufstieg in die Maschinenhalle und Abstieg in den zweiten Generatorschacht. Einrichtungen und Kontrollen, sowie Gefahrenquellen ident mit dem ersten Generatorschacht.
- 8) Aufstieg in die Maschinenhalle und Abstieg in den ersten Turbinenschacht. Kontrolle des Öldrucks und Kontrolle des Sperrwassers. Dies ist wiederum ein sicherheitskritischer Schritt, weil Absturzgefahr besteht. Der Turbinenschacht ist zur Gänze metallisch umschlossen, daher ist kein Handyempfang möglich.
- 9) Aufstieg in die Maschinenhalle und Abstieg in den zweiten Turbinenschacht. Einrichtungen und Kontrollen, sowie Gefahrenquellen ident mit dem ersten Turbinenschacht.
- 10) Aufstieg in die Maschinenhalle und Temperaturmessungen an der Schalttafel für die Hilfsbetriebe 1 und 2 kontrollieren
- 11) Weiter in den ersten Regler-Raum und Öldruck und Ölstand kontrollieren. Kein Handyempfang möglich.
- 12) Weiter in den ersten Hochspannungsraum; hier erfolgt die Kontrolle der Erregereinrichtung. Kein Handyempfang möglich.
- 13) Weiter in den zweiten Regler-Raum; Kontrolle Öldruck und Ölstand. Kein Handyempfang möglich.
- 14) Weiter in den zweiten Hochspannungsraum; Kontrolle der Erregereinrichtung. Kein Handyempfang möglich.
- 15) Abstieg in den Kühlwasserraum und Kontrolle des Wasserstandes und des Wasserdrucks. Kein Handyempfang möglich.
- 16) Kontrolle im Pumpenschacht (tiefster Punkt der Anlage) auf Ölaustritt (Ölfilm auf Wasseroberfläche). Kein Handyempfang möglich.
- 17) Weiter in den ersten Turbinenboden und Lagerölstand und Kühlwasserkreislauf kontrollieren. Kein Handyempfang möglich.
- 18) Weiter in den zweiten Turbinenboden und wiederum Lagerölstand und Kühlwasserkreislauf kontrollieren. Kein Handyempfang möglich.
- 19) Blocktrafo 1 kontrollieren auf Kühlwasserdruck
- 20) Blocktrafo 2 kontrollieren auf Kühlwasserdruck
- 21) Rückkehr in den Maschinenraum
- 22) Checkliste ausfüllen
- 23) Anwesenheitsschalter auf Stellung „Aus“ schalten
- 24) Außenbereich Rechenreinigungsanlage kontrollieren

- 25) Außenbereich Wehranlage kontrollieren
- 26) Ggf. Lagergebäude kontrollieren
- 27) Rückkehr ins Kraftwerkgebäude Checkliste vervollständigen
- 28) Telefonische Abmeldung bei der KW-Einsatzleitwarte
- 29) Aktivieren Objektschutz
- 30) Kraftwerksgebäude verlassen und Eingangstüre versperren

5.4. Konzipierte Lösung

5.4.1. Grundsätzliche Gesichtspunkte

Entsprechend dem erstellten Anforderungsprofil wurden verschiedene Lösungsvarianten betrachtet. Die Auswahl der Lösung erfolgte unter Bedachtnahme auf die geforderte räumliche und zeitliche Auflösung unter Berücksichtigung wirtschaftlicher Kriterien. Dabei sind sowohl die Serverkomponenten als auch die Clientkomponenten maßgeblich.

5.4.2. Variante WLAN-Lokalisierung

Grundsätzlich besteht die Möglichkeit die Lokalisierungstechnologie auf WLAN-Basis auszubilden. Dazu könnte z.B. eine Standardlösung von Ekahau auf Basis der Wi-Fi-Technologie (vgl. z.B. LARSSON, D.; SJÖDIN S. (2006)) eingesetzt werden. In den in Frage kommenden Bereichen ist überall ein Netzwerkanschluss möglich und eine Stromversorgung vorhanden. Durch Anordnung einer ausreichenden Anzahl an WLAN-Zugangspunkten wäre die vollständige Abdeckung des Areals möglich. Zur Anwendung käme vorwiegend die Presence-Methode in Kombination mit der Fingerprint-Methode. Auf Basis der WLAN-Technologie ergeben sich aber folgende Problempunkte:

- Da derzeit in dem Kraftwerk noch keine WLAN-Accesspoints vorhanden sind, müsste die Infrastruktur ausschließlich für die Ortung aufgebaut werden, was die Thematik doch aufwändig machen würde. Speziell müsste die Netzwerksverkabelung für die Anbindung der Accesspoints durchgeführt werden.
- Das Kraftwerksgelände erstreckt sich über 4 Ebenen, zahlreichen Halbstockwerken und ca. 40 Einzelräumen. Es müsste eine erhebliche Anzahl an Accesspoints aufgebaut werden. (Aufgrund der Verschachtelung der Räume und der relativ dicken Betonmauern ca. 20).

- Die Kalibrierung der Signalstärkenlandkarte („Fingerprint“) ist aufwändig (vgl. KARLSEN, B. (2006)) jedoch vorerst nur ein Einmalaufwand der durchgeführt werden müsste. Bei größeren Änderungen der Raumausstattungen und Umgebungen, Ausbauten müsste die Kalibrierung erneut durchgeführt werden.
- Es gibt mehrere Bereiche, die metallisch vollständig abgeschirmt sind (z.B. Turbinen und Generatorschächte). In diesen Bereichen müsste jedenfalls ein eigener Accesspoint oder eine Zusatztechnologie für die Ortung verwendet werden.
- Die Außenbereiche können mit WLAN-Accesspoints in den Innenräumen nicht mit ausreichender Genauigkeit abgedeckt werden. Es wäre daher auch hier der Aufbau von zusätzlichen Accesspoints erforderlich, oder GPS als Zusatztechnologie für die Ortung einzusetzen.
- Aufgrund des Positionsbestimmungsverfahrens mit WLAN und den Halbstockwerken ist eine stockwerksgenaue Zuordnung des Standortes zu einem bestimmten Raum schwierig. Die genaue Stockwerkszuordnung erfordert daher Zusatzverfahren.
- Viele metallische Einbauten und daher Störungseinflüsse durch Multipath-Effekte.

Neben den Nachteilen hätte die WLAN-Technologie bezogen auf das konkrete Einsatzszenario auch einige Vorteile:

- Möglichkeit Standardhardware in unterschiedlicher Ausprägung (PDA, Handheld, Laptop) einzusetzen.
- Voller Netzwerkzugriff am Client
- Hohe Datenübertragungsraten zwischen Clients und Server, damit Möglichkeit Zusatzinfos, wie z.B. Baupläne, direkt vom Server abzurufen.
- Keine Kommunikationskosten
- Robuste Positionsbestimmung, aufgrund der hohen Zahl an Accesspoints
- Gute Ortungsgenauigkeit im Bereich von 5 Meter
- Geringer Entwicklungsaufwand, weil Standardlösungen am Markt verfügbar
- Standardnetzwerktechnologie, daher intern sehr gut wartbar.

Aufgrund der angesprochenen Problempunkte und der Tatsache, dass die erzielbare Genauigkeit der Positionsbestimmung nicht benötigt wird, wurde diese Lösungsvariante nicht weiter verfolgt.

5.4.3. Variante UWB

Für das angestrebte Einsatzszenario im Kraftwerk mit vielen durch Betonwände abgeschlossenen Einzelräumen ist die UWB-Technologie aus Kostengründen nicht die optimale Technologie. Gründe hierfür sind:

- Die UWB-Signale durchdringen die Betonwände nicht
- Es wären sehr viele Sensoren erforderlich
- Teure Installationskosten, weil die Sensoren vernetzt werden müssen

Aufgrund der sehr guten Ortungsgenauigkeit und Robustheit der Positionsbestimmung gegenüber Störungseinflüssen würde diese Technologie aber auch einige Vorteile bringen:

- Für die Außenbereiche wären nur 4 UWB-Sensoren erforderlich.
- Die Positionsbestimmung ist damit in Submeter-Genauigkeit möglich.
- Es ist auch eine gute 3D-Genauigkeit gegeben.
- Die Technologie ist wenig anfällig gegenüber Multipath-Effekten.
- Es gibt Standard-Software für UWB-Technologie.
- Die Technologie ist sowohl für die Innenraumbereiche als auch die Außenbereiche geeignet.

Da im angestrebten Einsatz die hohe Genauigkeit der UWB-Variante nicht erforderlich ist, wurde aufgrund der hohen Kosten, diese Lösungsvariante nicht weiter verfolgt.

5.4.4. Gewählte Lösung

Aufgrund der verfügbaren Lösungsmöglichkeiten wurde unter Berücksichtigung der Anforderungen an die zeitliche und räumliche Auflösung und Beachtung der Kosten folgende Lösung ausgewählt:

- Softwarelösung Movidia der Fa. Geodan. Dies ist eine am Markt etablierte Standardlösung.
- Einsatz von passiven und aktiven RFID-Tags für die Positionsbestimmung und Ergänzung durch GPS.

- Einfache Telekommunikations-Hardware auf Basis GSM/GPRS/UMTS auf Clientseite mit eingebautem GPS und RFID-Leser.
- Clientlösung auf Basis PDA mit Windows Mobile Betriebssystem.

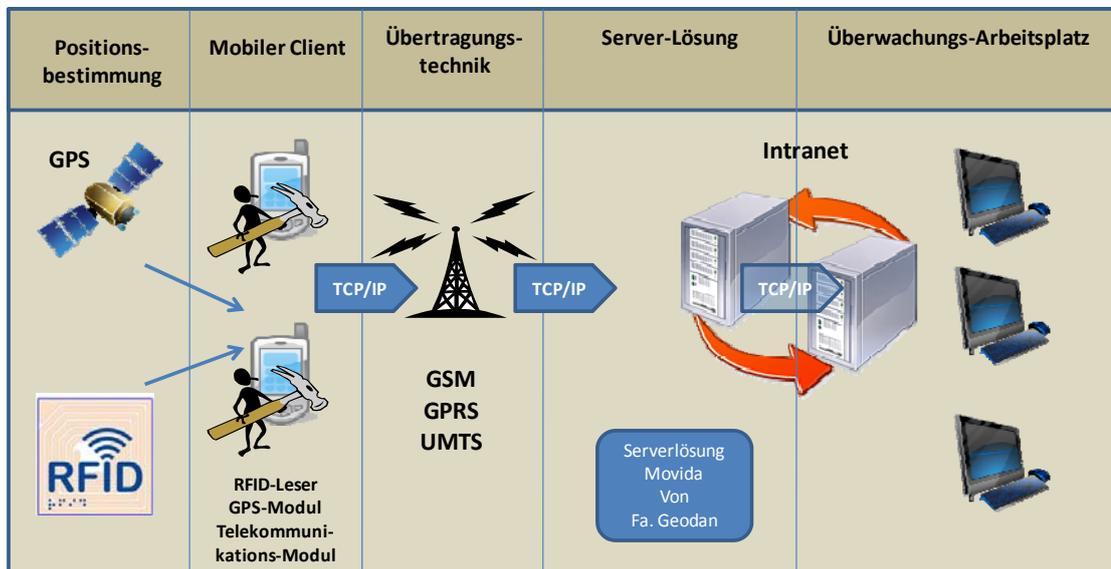


Abbildung 31: Grundsätzliche Lösung

Grundsätzlicher Ablauf:

In den Innenbereichen kommen die Ortungsverfahren „Chokepoints and Transit“, sowie „Proximity“ bzw. „Presence“ zur Anwendung (Geodan Movidia (2009))⁹⁸. Alle Durchgangstüren werden mit aktiven RFID-Tags gekennzeichnet (Verfahren Chokepoints and Transit). Die jeweiligen Tags haben eine eindeutige ID, sowie die Raumnummer bzw. den Raumteilbereich codiert. Die aktiven Tags werden auf eine Reichweite von 2 Meter ausgelegt. Damit ist sichergestellt, dass die Tags vom Lesegerät beim Durchgang durch die Türe automatisch ohne Zutun des Mitarbeiters ausgelesen werden.

Weiters werden besondere Arbeitsbereiche in größeren Räumen, wie z.B. die Anzeigetafel, bei der Messgeräte abgelesen werden müssen, mit passiven Tags gekennzeichnet (Verfahren „Proximity“). Diese Tags haben eine geringere Reichweite im Bereich von 10 cm. Damit muss der Auslesevorgang von den Mitarbeitern bewusst durchgeführt werden. Das Auslesen dieser Tags dient als Nachweis für die durchgeführte Kontrolltätigkeit. Die jeweilige Eingabemaske für den Messwert erscheint automatisch am Gerät. Daraufhin kann der jeweilige Messwert eingegeben

⁹⁸ Geodan Movidia (2009): indoor location | Geodan. Online verfügbar unter <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-indoor-location/>, zuletzt geprüft am 25.08.2009.

werden. Mit diesem Vorgehen ist es möglich, ohne Eingriff des Mitarbeiters jeweils die richtige Erfassungsmaske zu präsentieren („location awareness“).

Die Kennzeichnung der Türebereiche mit „Dual“-Tags dient dazu, dass aus den Sensorinformationen eindeutig bestimmt werden kann, ob ein Raum betreten oder verlassen wird. Damit ist die Raumzuordnung eindeutig möglich.

Die Client-Hardware besteht aus einem mobilen Handgerät, möglichst in PDA-Größe, mit eingebautem RFID-Leser und GPS-Modul sowie einem üblichen Telekommunikationsmodul auf GSM-Basis mit GPRS und UTMS-Möglichkeit. Je nach Verfügbarkeit eines integrierten Gerätes, könnte alternativ auch der RFID-Leser als externes Gerät an den PDA angebunden werden (z.B. über Bluetooth oder WLAN). Die Hardware läuft mit dem Betriebssystem Windows Mobil. Damit kann die Client-Lösung auf Basis eines Standardbetriebssystem entwickelt werden (= Zukunftssicherheit).

Nach dem Auslesen der Tags werden die Informationen über das Kommunikationsmodul automatisch zum Server gesendet. Diese Datensätze werden in einer Datenbank gespeichert und über Regeln prozessiert. Die Serverapplikation bereitet die Information für die grafische Darstellung bei den Überwachungsarbeitsplätzen auf. In Bereichen ohne Mobilfunkverbindung werden die Datensätze vorerst am Client zwischengespeichert, und nach Wiederherstellung der Kommunikationsverbindung automatisch zum Server gesendet.

5.4.4.1. Serverlösung⁹⁹

Ausgewählt wurde die Software „Movida“ der Fa. Geodan. Dabei handelt es sich um eine RTLS-Lösung, welche die Einbindung unterschiedlicher Sensortechniken ermöglicht. Diese Softwarelösung ist unabhängig von der eingesetzten Sensortechnologie. Es ist die Lokalisierung und Identifizierung über Dienste von Telekommunikationsdienstleistern (Cell-ID, AGPS), die Positionsbestimmung mit GPS, Wi-Fi und UWB sowie über RFID-Lösungen möglich.

Dies ermöglicht den Einsatz der für den jeweiligen Anwendungsfall am besten geeigneten Lokalisierungs-Technologie, ohne die Software daran ausrichten zu müssen.

⁹⁹ <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-key-features/>

Movida verwendet Konnektoren zur Übersetzung der proprietären Formate der Lokations-Hardware in ein standardisiertes Datenformat (OpenLS¹⁰⁰). Siehe dazu auch das Kapitel im Anhang.

Die Serversoftware erlaubt die Definition von Ereignissen, abhängig von der jeweiligen Position. So können Ereignisse (z.B. Alarmmeldungen, Auslösen von Aktionen) definiert werden, sobald ein Objekt sich einem definierten Bereich nähert, in diesen eintritt oder diesen verlässt. Dabei können die Ereignisse mit anderen Sensorinformationen bzw. Datenbankinformationen kombiniert werden, z.B. Alarmmeldung erfolgt, sobald ein Mitarbeiter einen bestimmten Bereich betritt, in dem die Schadstoffkonzentration einen bestimmten Wert überschreitet. Damit ist die Abbildung komplexer Ereignisbedingungen möglich.

Die Software erlaubt die simultane Beobachtung von mehreren Tausend Sensoren im Sekundentakt unter Berücksichtigung einer großen Anzahl von unterschiedlichen Regeln (ein Feature, das in der gegenständlichen Lösung nicht benötigt wird).

Die Visualisierung erfolgt einerseits auf Basis von Straßenkarten, digitalen Orthofotos bzw. beliebigen anderen geografischen Kartengrundlagen. Innenbereiche können über CAD-Zeichnungen oder auch andere Grafikformate visualisiert werden. Unterschiedliche Stockwerke können auch nebeneinander dargestellt werden.

Ausgesucht wurde die Lösung deshalb, weil es sich dabei um eine am Markt etablierte Standardsoftware handelt, welche entsprechend der jeweiligen Anforderungen skaliert werden kann. Damit ist es möglich eine Lösung zu implementieren, die laufend mitwächst. Ein weiterer Grund für die Wahl dieses Produktes ist der Umstand, dass die Software zentral betrieben werden kann, und innerhalb einer Lösung gleichzeitig unterschiedliche Standorte abbilden kann. Damit ist es möglich, die Überwachungsfunktion für alle Standorte im Bedarfsfalle auf einem Leitstand (der zentralen Leitwarte) zu konzentrieren. Der Überwachungsarbeitsplatz ist eine Web-Applikation und kann somit von jedem Arbeitsplatz im Netzwerk gestartet werden.

Die Software-Architektur der Lösung ist serviceorientiert (SOA¹⁰¹-Ansatz) und kann mit anderen Systemen, wie z.B. einem ERP-System – im Falle der Salzburg AG ist dies

¹⁰⁰ OpenLS = OpenGIS Location Service:

¹⁰¹ SOA = Service Oriented Architecture

SAP – gut integriert werden. Dazu steht ein API¹⁰² zur Verfügung um die Services aus anderen Applikationen heraus anzusprechen.

Die Lösung deckt folgende Funktionen ab:

- Einrichtung von Überwachungsstandorten auf Basis von CAD-Zeichnungen der Anlagenstandorte in den Innenräumen
- Einbindung von digitalen Orthofotos, die für die Außenbereiche verfügbar sind. In der Salzburg AG sind für alle Anlagen entsprechende Fotos vorhanden. Die Übersicht ist sowohl überregional (gesamtes Land Salzburg) als auch für bestimmte Anlagenbereiche (Kraftwerksstandorte, Umspannwerkstandorte) notwendig.
- Einbindung der Sensorinformationen
- Definition der Regeln für die Innenbereiche und die Außenbereiche
- Definition des Workflows für die Alarmierung
- Verteilte Überwachungsstandorte und Übergabe der Überwachungsfunktion an einen anderen Überwachungsstandort
- Systemadministrationsfunktionen wie die Einrichtung von Berechtigungen für die Datenbank der Sensorinformationen.
- Protokollierung der Sensorinformationen, welche die Anforderungen an Auditing erfüllt.

5.4.4.2. *Software-Architektur von Movida*¹⁰³

Movida ist eine modular aufgebaute Java-Plattform mit einer Anzahl von Core-Modulen und Schnittstellen zu externen Systemen. Die Komponenten sind:

- Die Server-Plattform: diese stellt alle Funktionalitäten von Geodan Movida zur Verfügung. Dabei kann diese entweder als einzelner Server oder als Server-Cluster¹⁰⁴ betrieben werden.

¹⁰² API = **A**pplication **P**rogramming **I**nterface: Entsprechend Wikipedia, http://en.wikipedia.org/wiki/Application_programming_interface, zuletzt geprüft am 25.10.2009, ist eine API eine Schnittstelle, die beschreibt wie Anwendungsprogramme auf Services einer Programmbibliothek und/oder des Betriebssystems zugreifen können.

¹⁰³ <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-software-architecture/> zuletzt geprüft am 25.10.2009

¹⁰⁴ Ein Server-Cluster ist eine Anzahl vernetzter Einzelservers, die von außen als ein Server angesprochen werden. Ein Server-Cluster dient zur Verteilung der Belastung auf mehrere Geräte, und damit besserer Performance, und zur Erhöhung der Ausfallsicherheit.

- Die „Location-Center“-Clients. Diese sind einsatzbereite Applikationen unterschiedlicher Ausprägung und Funktionalität für die gebräuchlichsten Anforderungen an Echtzeitortungssysteme.
- Die „Vertical-Clients“. Das sind spezialisierte Versionen von Movida für das Gesundheitswesen, Haftanstalten und Sicherheit in Industrie.
- Das Anwendungs-API: Wird von allen Anwendungen verwendet, die mit Geodan Movida kommunizieren.
- Das Verbindungs-API: wird von allen Lokalisierungs- und Identifikations-Geräten verwendet.
- Das Kommunikations-API: ermöglicht die Kommunikation mit Movida, um Alarmereignisse zu verarbeiten, und regelbasierende Anwendungen zu starten.
- Daten-Schnittstellen für die Anbindung von Geo-Datenbanken, Berechtigungssystem und anderen Datenbanken.

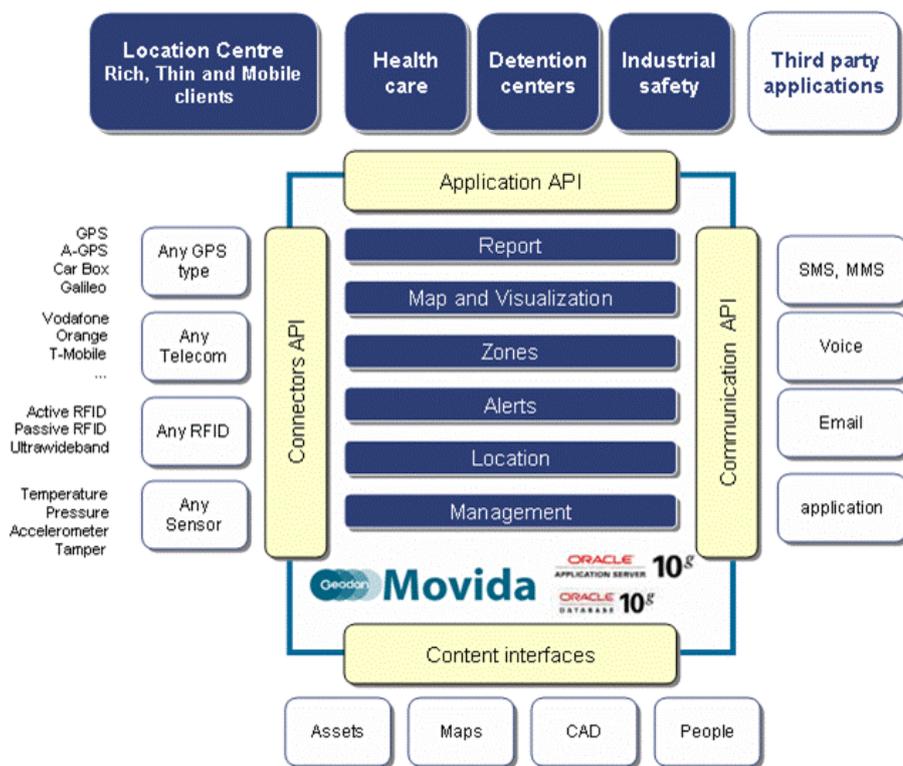


Abbildung 32: Movida Software-Architektur

Quelle: <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-software-architecture/>
zuletzt geprüft am 25.08.2009

Für die Telekommunikationsverbindung und Einbindung in das Firmennetzwerk wird der VPN-Dienst von T-Mobile (Vertragsunternehmen der Salzburg AG) verwendet. Damit ist die Übertragungssicherheit gewährleistet. Zusätzlich wird ein Verschlüsselungsverfahren eingesetzt.

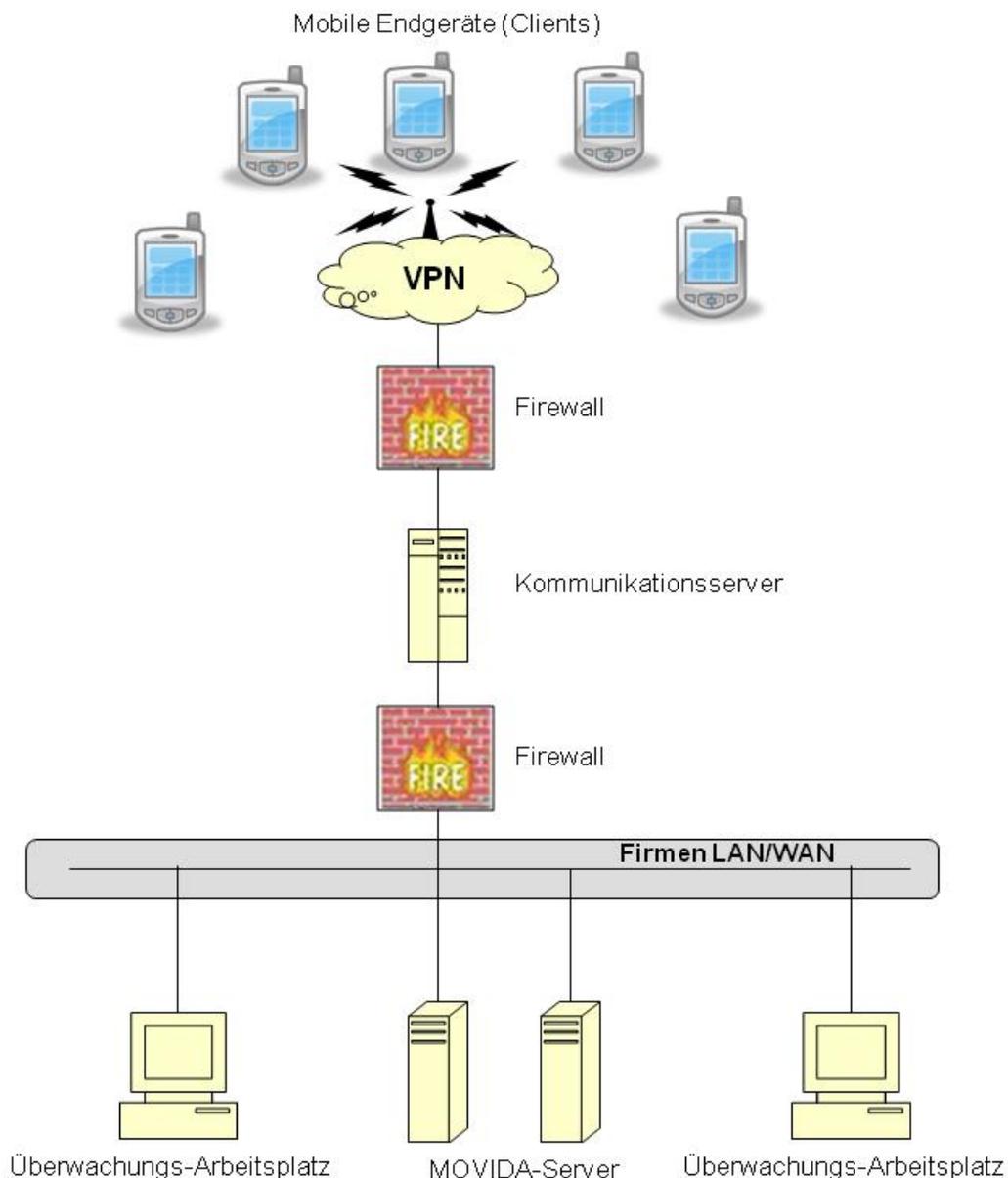


Abbildung 33: Sicherheitskonzept: VPN-Einbindung ins Firmennetzwerk

Quelle: angelehnt an das Kommunikationskonzept der Salzburg AG

5.4.4.3. Einrichtung der Überwachungsstandorte

Für alle zu überwachenden Standorte gibt es entsprechende AutoCAD-Zeichnungen. Diese Zeichnungen werden in das System eingecheckt, wobei zu beachten ist, dass es sich bei den Anlagen um räumlich sehr komplexe Gebilde handelt, mit unterschiedlichen Etagen und Halbetagen. Es gibt für jedes Stockwerk im Regelfall eine eigene CAD-Zeichnung.

Das Einchecken der Räume erfolgt in der Weise, dass die Sensorkennungen mit den jeweiligen Räumen „gebunden“ werden. Eine dreidimensionale „Eichung“ der CAD-Zeichnung ist aufgrund der verwendeten Sensortechnik nicht erforderlich. Sollte zu

einem späteren Zeitpunkt auf eine dreidimensionale Positionsbestimmung umgestellt werden, müssten die Gebäudepläne neu eingecheckt werden.

Eine Koordinatenbestimmung in Innenbereichen ist derzeit nicht vorgesehen. Es reicht die Bestimmung auf Raumgenauigkeit („Chokepoint and Transit“-Verfahren).

5.4.4.4. Einrichtung der Außenbereiche

Für die Außenbereiche werden die digitalen Orthofotos entsprechend dem für das Bundesland Salzburg festgelegten Koordinatenreferenzsystem referenziert. Dieses ist das Koordinatenreferenzsystem MGI (Ferro) M31, EPGS-Code 31289, genannt auch Österreichisches Bundesmeldenetz. Die Sensorinformationen werden vom GPS allerdings im Raumbezugssystem WGS 84 geliefert. Die Serversoftware muss daher eine Koordinatentransformation für die von den Sensoren gelieferten Koordinatenwerte vornehmen. Die Festlegung auf das Österreichische Bundesmeldenetz erfolgte aus Gründen der Kompatibilität zur GIS-Darstellung in der Salzburg AG. Damit ist es möglich, die Anlagendaten mit den Standortinformationen direkt in Beziehung zu setzen. Die eingesetzte GPS-Hardware liefert 3D-Koordinaten.

5.4.4.5. Einbindung der Sensorinformationen

Die Positionen der RFID-Tags sind alle koordinativ (in Gauß-Krüger-Koordinaten, Österreichisches Bundesmeldenetz, M31) bestimmt und dem Server bekannt. Damit ist gewährleistet, dass aus der Tag-Id die jeweilige Koordinate abgeleitet werden kann.

Die auf den mobilen Geräten installierte Software liefert die Sensorinformationen in Form von XML-Dateien (OpenLS), die über eine Telekommunikationsverbindung (GPRS) in festgelegten Intervallen bzw. bei festgelegten Ereignissen an den zentralen Server übertragen werden. Dabei wird unterschieden, ob sich das Gerät in den Innenbereichen oder in den Außenbereichen befindet.

Die Sensorinformationen werden als Datensätze in einer relationalen Datenbanktabelle gespeichert.

Innenbereiche

Der Mobile Client liefert, sobald ein RFID-Tag gelesen werden kann, die Geräte-ID, die Benutzer-ID, den Zeitstempel (Datum in JJJJ.MM.DD, Uhrzeit in HH:MM:SS in MEZ) sowie die Tag-ID. Die Serversoftware übersetzt die Tag-ID zusätzlich in geografische Koordinaten, damit alle Datensätze in einem einheitlichen Format abgespeichert

werden, und die Visualisierung der Standortposition in den eingebunden Karten erfolgen kann.

Der Auslesevorgang für die Tag-ID wird alle 10 Sekunden wiederholt.

Außenbereiche:

Sobald GPS-Empfang gegeben ist, liefert das Gerät im Abstand von 10 Sekunden die Geräte-ID, die Benutzer-ID, den Zeitstempel (Datum in JJJJ.MM.DD, Uhrzeit in HH:MM:SS in MEZ) sowie die geografische Position (in WGS84-Koordinaten).

Das System setzt für Außenbereiche die „Pseudo-Tag-ID“ Null als Kennung für Außenbereich.

5.4.4.6. Definition der Regeln für die Innen- und Außenbereiche

Ziel der Lösung ist es, die Sicherheit der eingesetzten Mitarbeiter zu erhöhen. Eine Überwachung der Arbeitsleistung ist kein Ziel der Lösung. Die Regeln sind daher so zu definieren, dass die Mitarbeiterstandorte überwacht werden können, die Privacy aber im größt möglichen Ausmaß gewährleistet bleibt.

Dazu gehört auch, dass das Gerät von den Mitarbeitern auf den Betriebsmodus „Privat“ gestellt werden kann. In diesem Fällen ist die Dauer der Abwesenheit über das Gerät bekanntzugeben. Nach Ablauf dieser Zeit wird das Gerät wieder automatisch in den Modus „Sicherheit“ gestellt, wenn nicht zuvor eine weitere Abwesenheit definiert wurde. Die Abwesenheitszeit muss aber nur definiert werden, wenn das mobile Gerät nicht in die Dockingstation zurückgesteckt wird. Im Modus „Privat“ werden keine Informationen an den zentralen Server übertragen.

5.4.4.6.1. Regeln für die Innenbereiche

Der mobile Client sendet, sobald ein RFID-Tag gelesen werden kann, die Tag-ID und die oben definierten Daten an den zentralen Server. Am zentralen Server ist ein Zeitintervall abhängig von der jeweiligen Tag-ID definiert, innerhalb dem ein weiterer Datensatz vom mobilen Client einlaufen muss. Das Zeitintervall ist dabei standortabhängig, weil die Verweildauer an den jeweiligen Standorten unterschiedlich ist.

Läuft innerhalb des Zeitintervalls + 10 Minuten „Zeitpolster“ kein weiterer Datensatz am zentralen Server ein, wird die Alarmierung ausgelöst. Der Zeitpolster wird in der Betriebsphase entsprechend der Erfahrungen angepasst, um Fehlalarmierungen möglichst zu vermeiden.

Alarmablauf:

- Automatische Warnmeldung am zentralen Überwachungsarbeitsplatz sowie Warnmeldung per E-Mail an das Postfach der zuständigen Mitarbeiter. System wird auf Alarmstatus 1 „Achtung“ gesetzt.
- Läuft nach weiteren 10 Minuten kein Datensatz vom Client ein wird die Kommunikationsverbindung geprüft, indem vom Server die Clientaktion „Kommunikationsverbindung prüfen“ ausgelöst wird.
- Ist keine Kommunikationsverbindung vorhanden, erfolgt eine detaillierte Warnmeldung über den Ausfall der Kommunikationsverbindung an das Überwachungspersonal.
- Besteht die Kommunikationsverbindung, wird ein automatischer Telefonanruf an den mobilen Client abgesetzt. Durch eine Quittierungsmeldung am Client kann dieser Anruf bestätigt werden. Der Alarmzustand wird dann aufgehoben.
- Erfolgt nach weiteren 2 Minuten keine Quittierung des Alarmanrufes wird automatisch Alarmstufe 2 „Erhöhte Aufmerksamkeit“ ausgelöst, und es erfolgt eine „Dringliche Warnmeldung“ unter Angabe der letzten registrierten Position an das Überwachungspersonal, mit der Aufforderung Aktionen vor Ort (Telefonische Verständigung von Mitarbeitern vor Ort bzw. Hinschicken von Mitarbeitern) einzuleiten. Der mobile Client wird dabei ebenfalls auf „Sicherheitsaktion“ gesetzt, d.h. die Client-Software erzeugt ein dauerndes Warnsignal am mobilen Gerät.
- Wird die Alarmstufe 2 nach weiteren 10 Minuten nicht quittiert, werden die Notdienste (Feuerwehr, Rettung) verständigt, und das System wird auf Alarmstatus 3 „Notfall“ gesetzt.

Alle Aktionen in Zusammenhang mit der Alarmierung werden entsprechend mit Zeitstempel protokolliert.

Mitführung des Alarmstatus am Client:

Auf dem mobilen Client soll immer der aktuelle Status bzw. Alarmierungsstatus mit geführt werden. Damit soll es dem Mitarbeiter möglich sein, den jeweiligen Überwachungsstatus zu erkennen, und rechtzeitig Maßnahmen zu setzen (z.B. wieder einen Bereich aufzusuchen, bei dem Handyempfang gegeben ist), falls das System in

den Alarmierungsstatus übergeht, wenn dies nicht erforderlich ist. Dazu ist vorgesehen, dass der Server, sobald ein neuer Kontrollgang begonnen wird, die vorgesehene Normalverweildauer plus die eingestellten Zeitpolster für die Überwachungsbereiche an den Client überträgt. Der Status wird über eine Farbkennzeichnung von grün, gelb, orange, rot deutlich am Client angezeigt. Zusätzlich erfolgt eine akustische Warnmeldung. Die Mitführung des Alarmstatus am Client gilt auch für die Außenbereiche.

Alarmablauf Flussdiagramm:

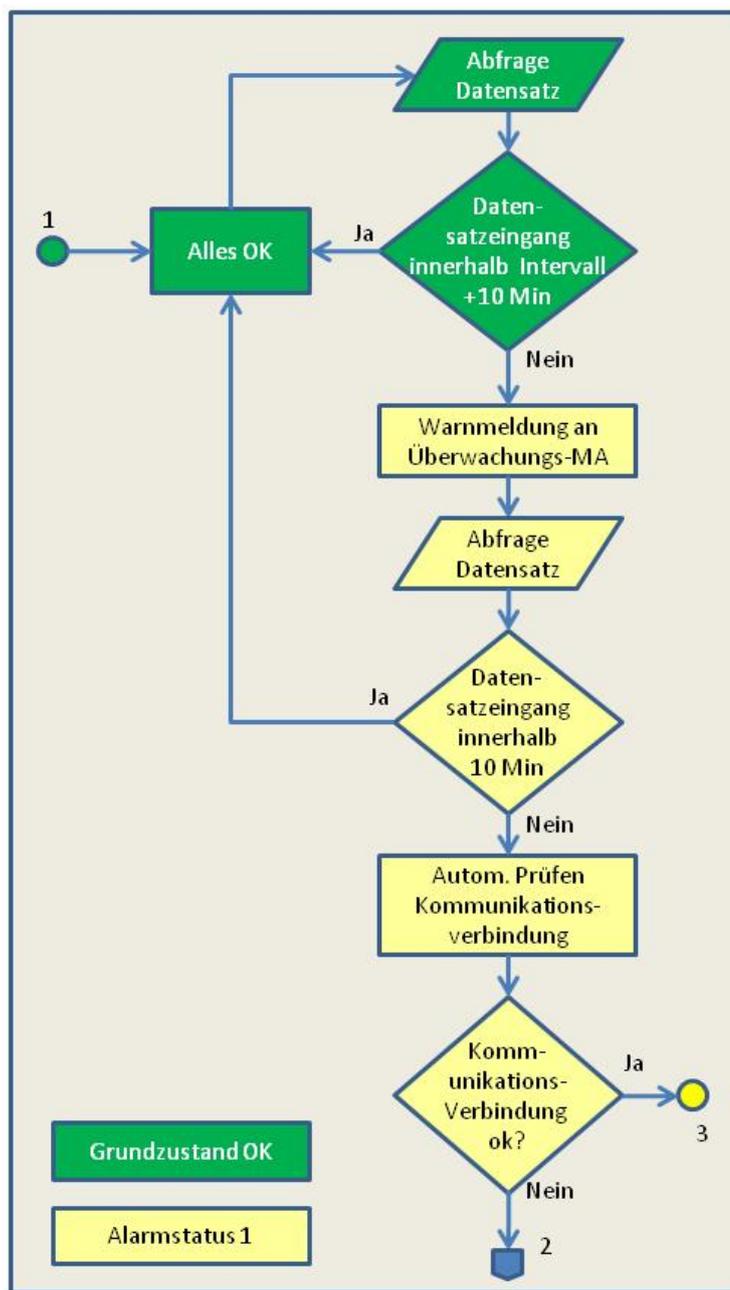


Abbildung 34: Alarmierung Flussdiagramm Teil 1

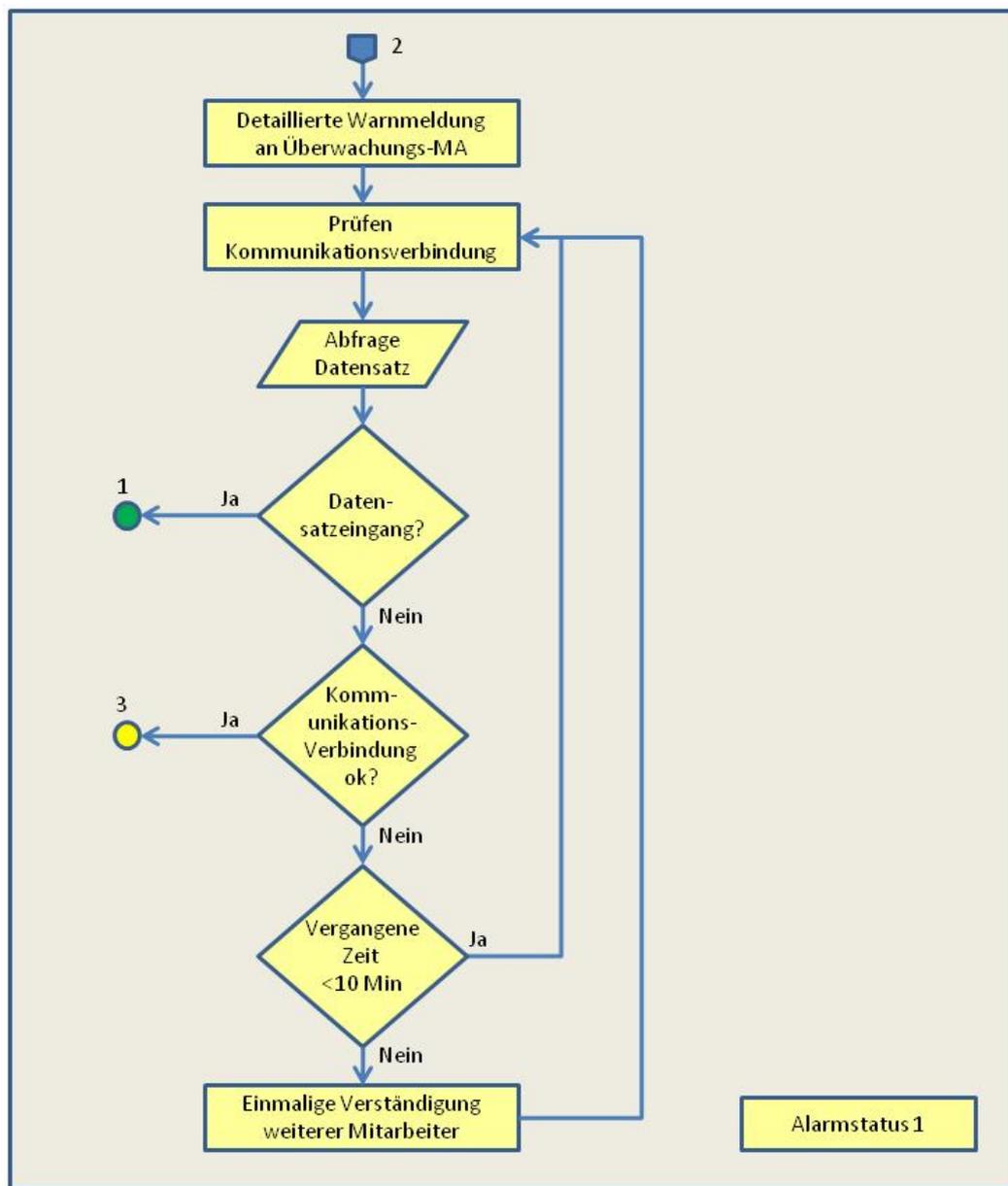


Abbildung 35: Alarmierung Flussdiagramm Teil 2

Rechnet man die verschiedenen Zeitdauern (inklusive der auf der nächsten Seite dargestellten Alarmierung) zusammen, so erfolgt im Alarmierungsfall eine Verständigung des Notdienstes nach längstens der Verweildauer + 42 Minuten. Geht man davon aus, dass die Verweildauer an einem Ort im Regelfall zwischen 5 und 10 Minuten beträgt, ist also Hilfe innerhalb etwa einer Stunde vor Ort. Das ist eine wesentliche Verkürzung der Reaktionszeiten gegenüber dem derzeitigen Stand, bei dem eine Hilfestellung im ungünstigen Fall erst 8 Stunden später erfolgen könnte.

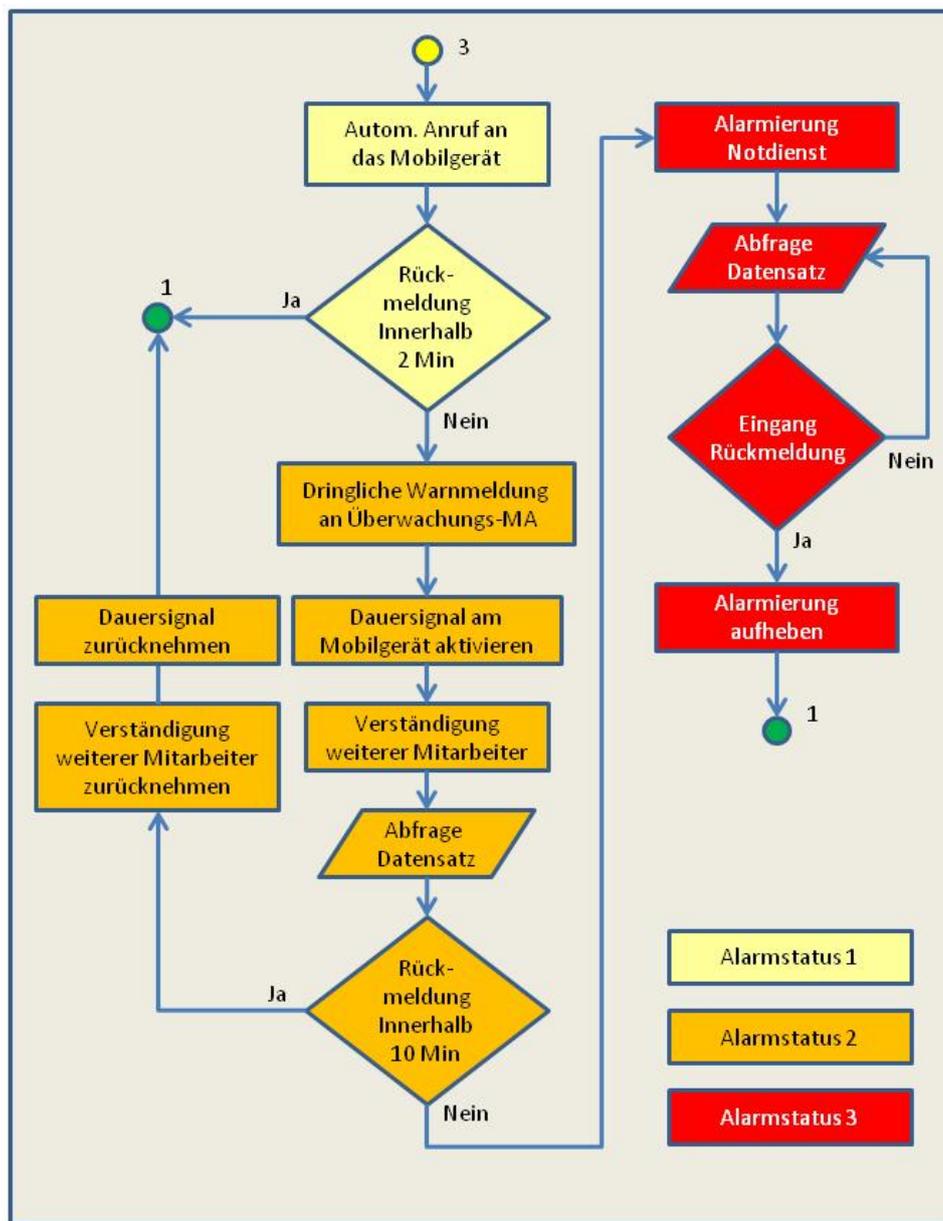


Abbildung 36: Alarmierung Flussdiagramm Teil 3

5.4.4.6.2. Regeln für die Außenbereiche

In den Außenbereichen wird für die Lokalisierung die GPS-Technik verwendet. Das eingesetzte GPS-Modul hat nur eine begrenzte Ortungsgenauigkeit. Die Fehler der Positionsbestimmung liegen im Bereich mehrerer Meter. In den Außenbereichen sind ebenso Regeln für bestimmte Arbeitsbereiche definiert. Das mobile Handgerät überträgt die Datensätze (ID-Daten und Positionsdaten) alle 10 Sekunden an den zentralen Server. Am Server werden jeweils zwei zeitlich aufeinanderfolgende Datensätze (die beiden letzten registrierten Positionen) verglichen und der Abstand zwischen den beiden Punkten errechnet. Dabei wird die euklidische 2D-Entfernung berechnet.

$$d = \sqrt{((x_2-x_1)^2 + (y_2-y_1)^2)}$$

Ist der Abstand größer als 10 Meter, so wird angenommen, dass sich die Position des Mitarbeiters verändert hat und somit alles ok ist. Als Ausgangswert wird jetzt die neue Position angesetzt. Ist der Abstand kleiner als 10 Meter (Bereich des Fehlers des GPS-Sensors), so wird angenommen, dass sich die Position nicht verändert hat.

Ändert sich die Position länger als das für den jeweiligen Bereich eingestellte Intervall + 10 Minuten nicht, wird der Alarmierungsvorgang ausgelöst, der analog der Innenbereiche abläuft.

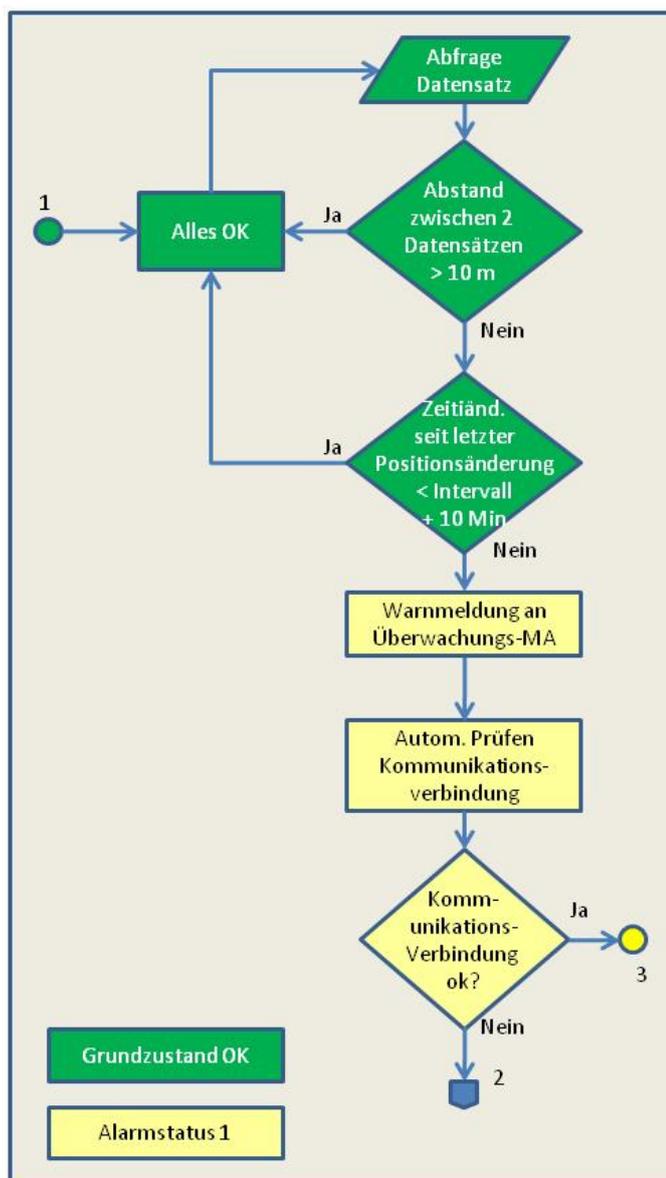


Abbildung 37: Flussdiagramm Auslöse Warnmeldung Außenbereich

5.4.4.7. Verteilte Überwachungsstandorte

Das System ist für die Überwachung, von wechselnden Standorten aus, auszulegen. Während der Normalarbeitszeit erfolgt die Überwachung im Regelfall vom zentralen Standort der jeweiligen Kraftwerksgruppe aus. Es sind in diesem Fall alle Überwachungsstandorte, die zu der jeweiligen Kraftwerksgruppe gehören, über den Überwachungsarbeitsplatz vor Ort abzudecken.

Die Überwachungsapplikation ist eine Webanwendung, daher ist die Überwachung von wechselnden Standorten aus einfach einzustellen.

Beim Aufruf der Überwachungsapplikation sind der Benutzername und das Passwort, sowie der Überwachungsstandort anzugeben. Das System prüft nun, ob der jeweilige User für die Überwachung des gewählten Standortes berechtigt ist. Wenn ja, startet die Überwachungsapplikation und das System visualisiert alle aktiven Überwachungsstandorte und listet alle aktiven mobilen Clients für die Überwachungsstandorte auf. Weiters werden eventuelle Warn- bzw. Alarmmeldungen angezeigt.

Möchte nun der regionale Überwachungsmitarbeiter, die Überwachung an einen anderen Standort übergeben (z.B. zentrale Leitwarte) so wird am regionalen Überwachungsarbeitsplatz dieser Vorgang ausgelöst. Die Übernahme der Überwachung ist vom „Übernehmer“ am System zu quittieren (dieser Vorgang wird auch mit Zeitstempel protokolliert). Alle Warn- und Alarmmeldungen laufen nun an dem neuen Überwachungsarbeitsplatz ein.

Außerhalb der Normalarbeitszeit schaltet das System automatisch auf zentrale Überwachung, d.h. von der zentralen Leitwarte aus, um. Eine Überwachung vor Ort ist wiederum nur mehr durch aktive Übergabe und ggf. Rückgabe möglich.

Die Webapplikation ermöglicht auch den Aufruf als Infoarbeitsplatz. In diesem Fall ist entsprechend dem eingestellten Berechtigungssystem nur die anonyme Visualisierung der aktuellen Position der jeweiligen aktiven mobilen Clients vorgesehen. Der Zugriff auf historische Daten ist nicht möglich. Warn- oder Alarmmeldungen werden nicht angezeigt.

5.4.4.8. Systemadministrations-Funktionen

Die Serversoftware kann über Administratorfunktionen eingestellt und konfiguriert werden. Die wichtigsten Administratorfunktionen sind:

- **Berechtigungssystem**
Das System unterstützt ein rollenbasiertes Berechtigungssystem. Berechtigungen können somit auf Ebene der Rolle (=Gruppe) und auf Ebene des Benutzers vergeben werden. Die Software unterstützt die Authentifizierung und Autorisierung zusätzlich zur eigenen Berechtigungsverwaltung auch über LDAP¹⁰⁵. LDAP hat sich als Standard in der allgemeinen IT für die Berechtigungsverwaltung durchgesetzt und eignet sich hervorragend zur Einbindung in ein übergeordnetes Sicherheitsframework (vgl. MÜHLEMANN, R. (2007)).
- Konfiguration der Software hinsichtlich Anwenderoberfläche und verfügbarer Funktionen.
- Definition eines anwenderspezifischen Datenmodelles.
- Einrichten von Reports.

5.4.4.9. Protokollierung der Sensorinformationen

Alle von den mobilen Geräten einlaufenden Informationen über Positionen und ausgelesene Tags und durchgeführte Aktionen am Client sollen so dokumentiert werden, dass die Anforderungen des Auditing erfüllt werden.

Wikipedia¹⁰⁶ definiert Auditing: „Bei Auditing geht es um das Protokollieren von Datensätzen, die angeben, welcher Nutzer bzw. welche Person (siehe Benutzer) in IT-Systemen zu welchem Zeitpunkt was getan hat.“

Dies ist insbesondere auch deshalb erforderlich, weil das System für den Nachweis der durchgeführten Überprüfungen bei den technischen Anlagen verwendet werden soll. Es ist daher sicherzustellen, dass gespeicherte Informationen nachträglich nicht verändert werden können, bzw. dass die Veränderungen nachvollziehbar dokumentiert werden.

¹⁰⁵ LDAP = Lightweight Directory Access Protocol. Dieses ist ein Anwendungsprotokoll (standardisiertes, erweiterbares Internetprotokoll) für den Zugriff auf Verzeichnisdienste, das z.B. die zentrale Verwaltung von Berechtigungen erlaubt. LDAP hat einen objektorientierten Ansatz und verwendet dazu ein hierarchisches Datenmodell (Baumstruktur). LDAP setzt auf das TCP/IP-Protokoll. Siehe auch http://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol, zuletzt geprüft am 25.10.2009. Über den Verzeichnisdienst können die entsprechenden Informationen von einem LDAP-Server (oder mehreren Servern) abgefragt werden.

¹⁰⁶ [http://de.wikipedia.org/wiki/Auditing_\(Informationstechnik\)](http://de.wikipedia.org/wiki/Auditing_(Informationstechnik)), zuletzt geprüft am 25.10.2009

Alle relevanten Daten werden in einer relationalen Datenbank gespeichert. Die Datenbank sollte nach Möglichkeit eine MS-SQL-Server-Datenbank sein, aber auch eine Oracle-Datenbank ist zulässig (festgelegt in der IT-Strategie der Salzburg AG). Die Datenbankgrundfunktionen stellen sicher, dass nur authentifizierte Benutzer Zugriff auf die Daten haben. Über das Berechtigungssystem kann gesteuert werden, wer welche Daten einsehen darf.

Das Datenmodell dazu kann individuell angepasst werden.

Folgende Informationen sollen aufgezeichnet werden:

- Wer hat wann welchen Sensor ausgelesen?
- Wer hat wann welche Überprüfungsaktion gesetzt?
- Wer hat wann welche Messwerte eingegeben?
- Wann wurde an wen welche Warnmeldung übermittelt?
- Wer hat wann welche Warnmeldung quittiert?
- Wer hat wann welche Daten abgefragt?

Da es sich bei den Daten, insbesondere bei den Bewegungsdaten, um personenbezogene Daten handelt, kommt der Aufzeichnung wer wann welche Daten abgerufen hat besondere Bedeutung zu. Der Zugang zu den Daten wird entsprechend eingeschränkt. Die Einsichtnahme in die Bewegungsdaten ist nur unter genau reglementierten Bedingungen erlaubt.

5.5. Kostenvergleich unterschiedlicher Lösungsvarianten für die Kraftwerksbegehung

Betrachtet man die unterschiedlichen Lösungen, so ist vorerst einmal fest zu stellen, dass die Einführungskosten von mehreren Komponenten abhängen, wobei die unterschiedlichen Lösungen auch unterschiedliche Kostenkomponenten beinhalten.

Wesentliche Kostenkomponenten sind:

- Kosten für die Serverapplikation und für die Clientapplikation
- Kosten für den Aufbau der Ortungsinfrastruktur (Sensoren)
- Kosten für die Vernetzung der Sensoren
- Kosten für die Tags
- Kosten für die Systemintegration
- Kosten für die Dienstleistung bei der Einführung

- Kosten für Projektarbeiten und Schulungen
- Laufende Betriebskosten wie Telekommunikationsgebühren, Wartungsgebühren für die Software, Kosten für den Softwarebetrieb

Je nach gewählter Technologie können die Kosten in weiten Bereichen schwanken. Im gegenständlichen Szenario der Sicherheitslösung für Kraftwerkskontrollgänge kommen mehrere Technologien in Frage. Die detaillierte Kostenbetrachtung dreier unterschiedlicher Technologien ergab dabei folgendes Bild:

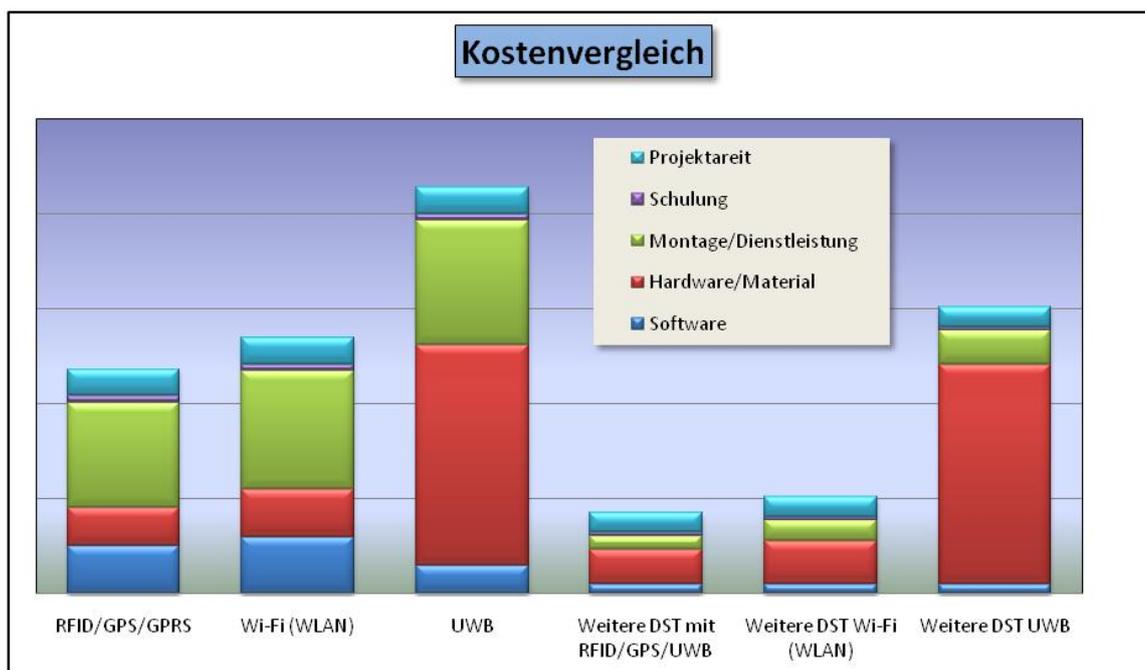


Abbildung 38: Kostenvergleich Sicherheitssystem

- RFID in Verbindung mit GPS und Mobilfunk mit Kosten von 100%
- Wi-Fi mit Kosten von 115%
- UWB mit Kosten von 180%

Im Kostenvergleich zeigt sich, dass die vorgeschlagene Lösung bei der Erstinstallation günstiger ist als die Variante WLAN (Wi-Fi) und deutlich günstiger als UWB. Die Ursache liegt darin, dass bei dieser Lösung die Hardware/Materialkosten deutlich niedriger sind. Dies trifft speziell für die UWB-Variante zu, bei der die Kosten für die Sensoren nahezu gleich hoch sind, wie die Gesamtkosten der ausgesuchten Lösung. Dabei ist zu beachten, dass der gegenständliche Kraftwerksbereich für eine UWB-Lösung, aufgrund der vielen durch Betonwände abgeschlossenen Einzelräume, schlecht geeignet ist, weil teure Sensoren für jeweils einen Raum aufgebaut werden müssen.

Vorteil von UWB und Wi-Fi gegenüber der kombinierten RFID/GPS-Lösung mit GPRS-Verbindung ist, dass keine laufenden Betriebskosten in Form von Telekommunikationsgebühren entstehen. Durch den vorhandenen Unternehmenstarif für den Mobilfunk fallen diese Kosten aber kaum ins Gewicht.

Deutlich zeigt sich auch, dass die Einbindung weiterer Standorte in die Sicherheitslösung wesentlich günstiger als die Erstinstallation ist, weil die Software-Entwicklungskosten für die Alarmierungsabläufe und die Clientanwendung nicht mehr anfallen. Bei den weiteren Standorten wirken sich die teuren Sensoren bei der UWB-Variante besonders ungünstig im Kostenvergleich aus.

Aus den Installationskosten für die Sicherheitslösung eine Wirtschaftlichkeit abzuleiten wird in diesem Zusammenhang nicht durchgeführt, weil keine monetäre Bewertung der körperlichen Unversehrtheit von Personen vorgenommen wird. Es können aber sehr wohl die Vorteile der Lösung für die Dokumentation der Kontrollgänge angeführt werden. Diese sind:

- Automatische Alarmierung unabhängig vom Zutun der Mitarbeiter.
- Kommunikationsmöglichkeit mit den Mitarbeitern
- Auditierbare Dokumentation der durchgeführten Kontrollen. Es kann jederzeit nachgewiesen werden, wer wann welche Kontrollen durchgeführt hat
- Effiziente Dokumentation, weil in vielen Fällen die Tags automatisch ohne notwendige Aktion der Mitarbeiter ausgelesen werden
- Unterstützung der Mitarbeiter, wenn Eingaben notwendig sind, weil automatisch die richtigen Eingabemasken vorausgefüllt erscheinen.
- Transparente Abläufe

5.6. Auswirkungen der Lösung auf die Privacy, Betriebsvereinbarung

Bei den Auswirkungen der Lösung auf die Privatsphäre der Mitarbeiter ist festzustellen, dass durch die permanente Übermittlung der tatsächlichen Aufenthaltsposition an einen zentralen Server ein wesentlicher Eingriff in die Privatsphäre erfolgt, der in einer entsprechenden Betriebsvereinbarung geregelt werden sollte.

Zum einen handelt es sich bei den Positionsdaten der einzelnen Mitarbeiter um personenbezogene Daten (Informationspflicht des Betriebsrates) und zum anderen liegen die Auswirkungen darin begründet, dass durch eine personenbezogene

Auswertung der Daten die genaue Beurteilung der individuellen Arbeitsleistung möglich wäre. Es könnten Vergleichswerte (Benchmarkwerte) für die Dauer bestimmter Tätigkeiten je Mitarbeiter ermittelt werden. Weiters wäre es z.B. möglich, genaue Bewegungsprofile zu erstellen, und daraus Rückschlüsse auf individuelle Verhaltensweisen zu ziehen (Wer hält sich wo wie lange, bzw. wie häufig auf? Wer trifft sich mit wem?).

Im österreichischen Arbeitsverfassungsgesetz ArbVG (2009) ist in § 96 geregelt, inwieweit Maßnahmen des Betriebsinhabers zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates bedürfen. Darin heißt es in Abs. 1, Ziffer 3:

„3. die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren;“

Weiters ist in § 96a angeführt:

„§ 96a. (1) Folgende Maßnahmen des Betriebsinhabers bedürfen zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates:

- 1. Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen. Eine Zustimmung ist nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben;*
- 2. die Einführung von Systemen zur Beurteilung von Arbeitnehmern des Betriebes, sofern mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind.“*

In einer Stellungnahme zum Thema Workforce Management vom Dezember 2009 teilt die Personalabteilung der Salzburg AG mit, dass laut herrschender Lehre von einer extensiven Auslegung der Begriffe Kontrollmaßnahmen und Menschenwürde auszugehen ist.

„Ein Mitbestimmungsrecht besteht laut hL nur hinsichtlich jener Kontrollmaßnahmen nicht, die die Menschenwürde nicht einmal berühren bzw. mit dieser nichts zu tun haben.“ und weiter:

„ ... ist ein Zustimmungserfordernis des BR spätestens dann gegeben, wenn das System ein arbeitnehmerbezogenes Bewegungsprofil während des ganzen Arbeitstags erlaubt,

was bei einer durchgehenden Kontrollmöglichkeit einzelner Arbeitsschritte anzunehmen ist.“

Übertragen auf die konkrete Sicherheitslösung erscheint es daher notwendig, vor Einführung der Sicherheitslösung eine entsprechende Vereinbarung mit dem Betriebsrat abzuschließen, zumal es sich um ein System handelt, das personenbezogene Daten speichert und die Überwachung der Arbeitnehmer ermöglicht, wenngleich auch aus Sicherheitsüberlegungen heraus (vgl. REIS (2008)).

Gemäß § 91, Ziffer 2, des ArbVG hat der Arbeitgeber den Betriebsrat jedenfalls über die Speicherung der personenbezogenen Arbeitnehmerdaten zu informieren.

„(2) Der Betriebsinhaber hat dem Betriebsrat Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht. Dem Betriebsrat ist auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen. Sofern sich nicht aus § 89 oder anderen Rechtsvorschriften ein unbeschränktes Einsichtsrecht des Betriebsrates ergibt, ist zur Einsicht in die Daten einzelner Arbeitnehmer deren Zustimmung erforderlich.“

Die Diskussion des Themas mit einem Vertreter des Betriebsrats hat gezeigt, dass gerade Anwendungen im Sicherheitsbereich vom Betriebsrat grundsätzlich positiv gesehen werden. Vorausgesetzt wird auch für diese Anwendungen, dass der Einsatz über entsprechende Betriebsvereinbarungen geregelt wird. Im Besonderen geht es dem Betriebsrat auch darum, dass aus den Aufzeichnungen keine Rückschlüsse über private Verhaltensweisen gezogen, oder gar Informationen über den Gesundheitszustand abgeleitet werden können (z.B. durch Auswertung wie lange sich ein Mitarbeiter an bestimmten Orten aufgehalten hat).

Beim Abschluss einer konkreten Betriebsvereinbarung sollten folgende Punkte angeführt und geregelt werden:

- Inhaltliche Beschreibung der Anwendung
- Für welchen Zweck wird die Anwendung betrieben?
- Welche personenbezogenen Daten werden in der Datenbank wie lange gespeichert?
- Wer darf Einsicht in welche Daten nehmen?
- Welche Sicherheitsvorkehrungen für den Datenzugriff werden angewendet?

- Welche Berichte dürfen erstellt werden?
- Allfällige Ausnahmen

Gerade auch für eine Sicherheitslösung ist die Akzeptanz seitens der Mitarbeiter eine Voraussetzung für ein klagloses Funktionieren. Gilt es doch die Lösung so zu gestalten, dass sie die Betriebsanforderungen bestmöglich abdeckt. Bei konkreter Umsetzung der Sicherheitslösung sollten daher schon in der Projektphase, einzelne Mitarbeiter und Vertreter des Betriebsrates in die Lösungsgestaltung miteinbezogen werden.

Zu hinterfragen ist auch, ob am Überwachungsarbeitsplatz eine Positionsdarstellung mit Raumgenauigkeit wirklich notwendig ist. So könnte z.B. eine Zusammenfassung der Rauminformationen auf bestimmte Bereichsinformationen (z.B. Geschoße) durchaus ausreichend sein, und damit das Thema Privacy deutlich entschärfen. Ein Zugriff auf die genaue Rauminformation wäre in diesem Fall nur im Alarmierungsfall und über ein besonders authentifiziertes Login möglich.

6. Ergebnisse und Schlussfolgerungen

6.1. Bewertung

Die nähere Beschäftigung mit dem Thema RTLS hat ergeben, dass es am Markt bereits eine Reihe von praktisch einsatzfähigen Lösungen gibt. Als Beispiele sollen hier die Lösungen der Firmen Geodan, Ubisense, und Ekahau angeführt werden. Im Gespräch mit Vertretern der Firmen Geodan und Ubisense hat sich gezeigt, dass die EVU-Branche derzeit noch nicht zu den Zielgruppen der RTLS-Hersteller gehört, wobei bei der Arbeit der Blick auf die EVU mit Netzaufgaben gerichtet ist, und weniger auf EVU mit Erzeugungsanlagen.

Dieses Bild deckt sich auch mit den Ergebnissen der Umfrage unter den Energieversorgern in Österreich. Auch hier kam deutlich zu Tage, dass sich erst einige wenige Unternehmen mit dem Thema RTLS auseinandergesetzt haben, wengleich aus den Umfrageergebnissen nur ein Stimmungsbild abgeleitet werden kann, da die Rücklaufquote keine Verallgemeinerung der Ergebnisse zulässt.

Das Studium von verschiedenen bestehenden Einsatzszenarien in anderen Branchen hat ergeben, dass es zahlreiche Anwendungsmöglichkeiten für RTLS auch in der EVU-Branche gibt, weil gerade die EVU-Branche zahlreiche Anforderungen anderer Branchen inkludiert. Als Beispiele werden hier angeführt, dass die EVU eine große Anzahl von Anlagen verteilt über das Versorgungsgebiet haben, die es zu warten und Instandzuhalten gilt. Das Asset-Management ist bei EVU jedoch mehr auf die „Fläche“ verteilt zu sehen und weniger auf große Anlagen. Ein möglicher Einsatz dabei ist die Kennzeichnung der Anlagen mit RFID-Tags und die Optimierung der Begehungsroutinen. Echtzeitinformationen, wie sie RTLS bereit stellen, können im Asset-Management der EVU eine nutzbringende Ergänzung sein, speziell wenn man die Prozesstransparenz betrachtet..

Etwas anders gelagert ist das Asset-Management in größeren Anlagen wie Schaltanlagen und Umspannwerken. Hier gibt es entsprechende Einsatzszenarien anderer Branchen, z.B. über die Wartung bzw. Inventur der Anlagenteile die fast 1:1 auf die Energieversorgungsbranche übertragen werden können (vgl. THIESSE, F. (2005), Dokumentation von Wartung und Reparaturarbeiten im Flughafen).

Jedes EVU hat in kleinerer oder größerer Ausprägung Anforderungen der Lagerwirtschaft, Lagerlogistik, zu erfüllen. Lagerlogistik stellt einen Kernbereich des Einsatzes von RFID- und RTLS-Lösungen dar. Hier können RTLS auch im EVU-Bereich zu deutlichen Prozessverbesserungen führen.

Zahlreiche EVU befassen sich derzeit mit dem Thema Workforce Management zur Verbesserung ihrer Service-Prozesse. Bei diesen Systemen ist die Echtzeitinformation über den Standort der Mitarbeiter eine wesentliche Information für die Optimierung des Arbeitseinsatzes. Hier kann die RTLS-Technologie einen wesentlichen Beitrag für die Prozessverbesserungen leisten, indem z.B. die Reaktionszeiten bei Störungen verkürzt werden können und Mitarbeiter in Echtzeit die nächstgelegenen Aufträge zugewiesen bekommen. Dieses ist ein Einsatzgebiet, das bereits mehrfach in konkreten Lösungen bei EVU umgesetzt ist.

Aus derzeitiger Sicht für EVU am Vielversprechendsten sind Einsatzszenarien im Sicherheitsbereich. Gerade der Kostendruck im Zuge der Liberalisierung des Energiemarktes brachte es mit sich, dass die Aufwendungen in den Servicebereichen laufend reduziert werden. Dort wo früher zwei Mitarbeiter gemeinsam tätig waren, verrichtet in vielen Fällen heute ein Mitarbeiter alleine die Arbeiten. Dies trifft im Besonderen für die Bereitschaftsdienste außerhalb der üblichen Dienstzeiten zu. Deshalb werden zunehmend Überlegungen angestellt, wie die Reaktionszeiten im Falle eines Unfalls der Mitarbeiter verkürzt werden können.

Das in der Arbeit dargestellte Einsatzszenario von RTLS in der Betriebsführung von Kraftwerksanlagen (Begehungen) stellt eine wesentliche Verbesserung gegenüber dem Istzustand dar, weil das System selbsttätig auf festgestellte Regelabweichungen reagiert, und die Mitarbeiter in den Warten von Kontroll- und Überwachungsarbeiten entlastet werden. Fehlerquellen und Lücken in den Überwachungsprozessen können mit diesem System vermieden, Reaktionszeiten auf Ereignisse können verkürzt werden. Die Anwendungen zur Verbesserung der Personensicherheit werden auch von der RTLS-Industrie als Markt mit wachsenden Einsatzmöglichkeiten gesehen (vgl. Presse-Aussendung der Fa. Ubisense vom 10.2.2009).

Besonderes Augenmerk ist bei der Einführung von RTLS-Lösungen auf das Thema Privacy zu richten. RTLS haben, wie in der Arbeit dargestellt, erheblichen Einfluss auf

die Privatsphäre der in das System eingebundenen Mitarbeiter, bedeutet es doch, dass der momentane Standort auf einem zentralen Serversystem sichtbar ist. Verbunden mit der Speicherung der Informationen und den Auswertemöglichkeiten lässt sich daraus ein Bewegungsprofil ermitteln, das geeignet ist, eine genaue Überwachung und Analyse der Arbeitsleistung durch zu führen. Auch wenn es nicht die Absicht des Arbeitgebers ist, die Systeme in diese Richtung einzusetzen, so stellen doch schon die Möglichkeiten dazu einen wesentlichen Eingriff dar, der jedenfalls mit dem Betriebsrat abzustimmen ist. Diesbezüglich sind die Rechtseinschätzungen jedenfalls ziemlich eindeutig (vgl. BIZER, J. et al (2006)). Der Gesetzgeber geht davon aus, dass Auswirkungen auf die Menschenwürde der Mitarbeiter gegeben sind, wenn aus den Kontrollsystemen ein Bewegungsprofil abgeleitet werden kann. Dies begründet eine Zustimmungspflicht des Betriebsrates für die Einführung dieser Systeme.

Mitarbeiter sind grundsätzlich skeptisch, wenn Systeme eingeführt werden, die ihre Privatsphäre betreffen. Hier gilt es durch vertrauensbildende Maßnahmen und vor allen durch klare transparente Regelungen entsprechendes Vertrauen zu schaffen. Sowohl Mitarbeiter als auch der Betriebsrat sollten schon bei der Planung der Systeme miteinbezogen werden.

Dem Interesse am Schutz der Privatsphäre, steht ein Interesse des Unternehmens an ausreichender Dokumentation der Abläufe gegenüber. Die gespeicherten Informationen, z.B. in Zusammenhang mit Wartungsarbeiten, müssen es zulassen, dass daraus der Nachweis geführt werden kann, wer welche Wartungsarbeiten wann durchgeführt hat. Hinsichtlich Speicherung der Ortsinformationen kann daher nicht nur auf Gesichtspunkte der Privatsphäre Rücksicht genommen werden.

Zusammenfassend kann festgestellt werden, dass die Einsatzmöglichkeiten der RTLS-Technologie in EVU vorhanden sind, und dass nach Meinung des Autors der Arbeit speziell für Sicherheitsanwendungen, die Systeme in den nächsten Jahren ihren Einsatz in EVU finden werden.

6.2. Grenzen und Einschränkungen

In Bezug auf die dargestellten Einsatzszenarien ist festzustellen, dass nicht alles was technisch machbar ist, auch wirtschaftlich sinnvoll ist. Von den in der Arbeit

dargestellten technischen Lösungen kommen für EVU vorwiegend Lösungen auf Basis von Mobilfunk, GPS, UWB und Wi-Fi, sowie RFID in Frage. Die Lösungen auf Infrarotbasis und Ultraschallbasis sind zwar technisch realisierbar, es fehlen aber die praktischen Einsatzszenarien.

Generell gilt, dass eher Lösungen erforderlich sind, die sowohl Innenbereiche als auch Freibereiche abdecken können. Die Anforderung hoher Positionsgenauigkeit ist ebenso kaum gegeben. In vielen Einsatzszenarien reicht es, die Position raumgenau zu kennen (z.B. im dargestellten Szenario für die Verbesserung der Arbeitssicherheit) oder z.B. beim Einsatzszenario Workforce Management die Position ortsteilgenau zu kennen.

Eine der wesentlichsten Anforderungen an die RTLS-Lösungen in EVU ist die Integration der Lösungen in die Gesamtsysteme. In EVU sind in der Regel zahlreiche Softwaresysteme im Einsatz, dies trifft im Besonderen für SAP zu, das bei vielen EVU ein zentrales System darstellt. Wesentliche Informationen, wie z.B. Auftragsdaten, Materialdaten, kommen aus dem SAP. Die RTLS sollten daher zur Vermeidung von Medienbrüchen und im Sinne eines Gesamtsystems in die vorhandene IT-Landschaft integriert werden können.

Auch haben viele EVU bereits Geografische Informationssysteme (GIS) im Einsatz. Für die Visualisierung von geografischen Informationen eignen sich diese Systeme hervorragend. Sie könnten daher in Zusammenhang mit Lösungen für RTLS als Visualisierungsoberfläche angebunden werden.

Bedingt durch die unterschiedlichen Einsatzszenarien bestehen auch unterschiedliche Anforderungen an die Visualisierung und die Prozessabbildung. Die RTLS-Lösungen sollten daher so konzipiert werden, dass nicht für jeden Anwendungsfall eine eigene Lösung entwickelt werden muss, sondern dass eine einheitliche „Location“-Plattform im Unternehmen entsteht, welche Informationen von unterschiedlichen Sensoren (UWB, Funk, Mobilfunk, Wi-Fi, RFID) verarbeiten und unterschiedliche Prozessabläufe abbilden kann. Dies ist eine zentrale Anforderung an die RTLS im EVU-Bereich.

6.3. Ausblick

Die dargestellte Lösung wurde in Diskussion mit der beteiligten Abteilung konzipiert. Die praktische Umsetzung dieser Lösung bedeutet, eine komplexe neue IT-Anwendung

in die bestehende Systemumgebung zu integrieren, die nicht nur dieses eine Anwendungsszenario, sondern auch weitere Anwendungsfälle im Sinne einer „Location“-Plattform unterstützen kann. Besonders interessant in diesem Zusammenhang ist der Einsatz von offenen Standards, in diesem Fall OpenLS, für die Ortungslösung und deren Einsatz in einer integrierten IT-Landschaft.

Es sollte geprüft werden, inwieweit OpenLS geeignet ist, weitere Anwendungsfälle mit Ortsinformationen, in EVU zu unterstützen. Eine Gelegenheit dazu würde sich bei Einführung einer Workforce Managementlösung bieten.

Hinsichtlich der Akzeptanz im Unternehmen sind die Auswirkungen auf die Privatsphäre der betroffenen Mitarbeiter von wesentlicher Bedeutung. Hier gilt es zu evaluieren, welche Regelungen andere Branchen, die RTLS einsetzen, getroffen haben. Nach Meinung des Autors werden RTLS ihr positives Potential nur dann entfalten können, wenn es gelingt die Auswirkungen auf die Privacy durch praxisgerechte Regelungen sowohl für die Mitarbeiter als auch für das Unternehmen zufriedenstellend zu regeln.

Am Ende bleibt der Wunsch, dass die konzipierte Sicherheitslösung nicht nur „Papier“ bleiben möge, sondern als praktisch eingesetzte Lösung die Sicherheit der Mitarbeiter verbessern hilft.

Anhang OpenLS¹⁰⁷

Die für das Sicherheitssystem ausgewählte Lösung, Movida, basiert auf OpenLS, daher soll dieser Standard an dieser Stelle erläutert werden.

OpenGIS Location Services (OpenLS) ist ein Standard des Open Geospatial Consortiums (OGC) und hat zum Ziel die Schnittstelle für den Zugriff auf die Kernfunktionen und die abstrakten Datentypen (Abstract Data Types, ADT) des GeoMobility Servers (GMS) zu definieren. Der GMS ist eine offene Plattform für Location Based Services (LBS). Das Zusammenwirken von OpenLS mit anderen Standards ist in der u.a. Grafik zu sehen.

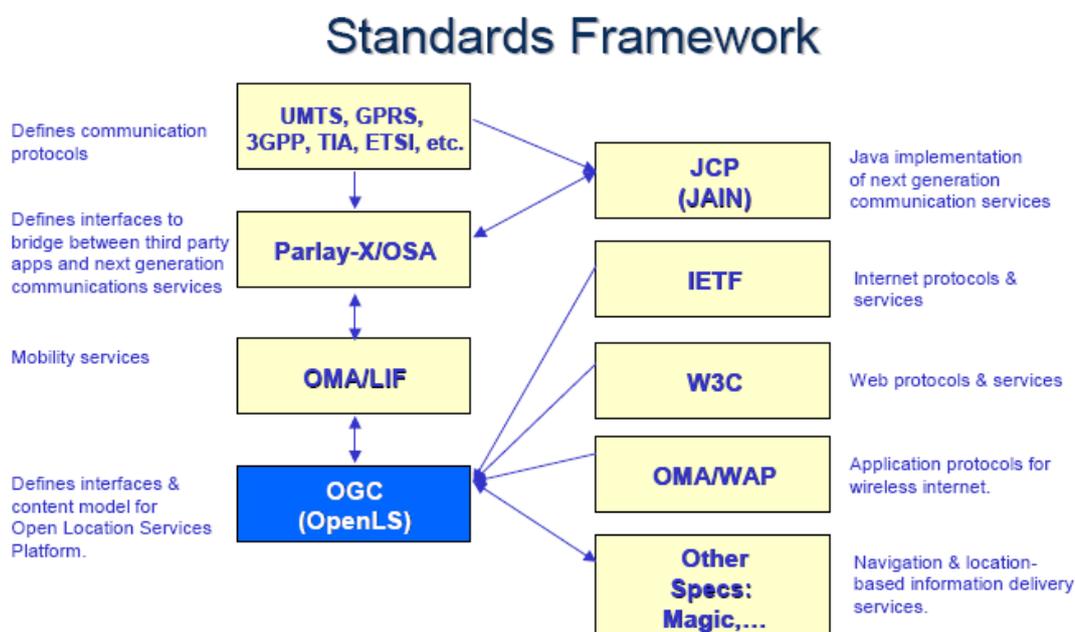


Abbildung 39: Zusammenhang OpenLS mit weiteren Standards

Quelle: OGC-Dokumentation. OGC 07-074. OpenGIS-Location Services (OpenLS): Core Services

Der GMS verwendet sogenannte Abstract Data Types (ADT) als Informationskonstrukt um auf seine Kern-Funktionen zugreifen zu können. ADTs sind wohldefinierte Datentypen und Strukturen für Location-Services. Die Definition erfolgt über ein eigenes XML-Schema für Location-Services (XLS).

Der GMS beinhaltet folgende Komponenten:

- Kern-Services und ihre OpenLS-Schnittstellen

¹⁰⁷ Siehe <http://www.opengeospatial.org/standards/ols>. Zuletzt geprüft am 24.10.2009

- Das OpenLS Informationsmodell; in Form von ADTs
- Optional eine Sammlung lokaler Applikationen (Zugriff über OpenLS-Schnittstellen)
- Inhalte wie Karten, Routen, Points of Interests
- Optional weitere Unterstützungsfunktionen für z.B. Verrechnung, Personalisierung, Logging

Allgemeiner Anwendungsfall einer OpenLS Anfrage und Antwort (Request/Response):

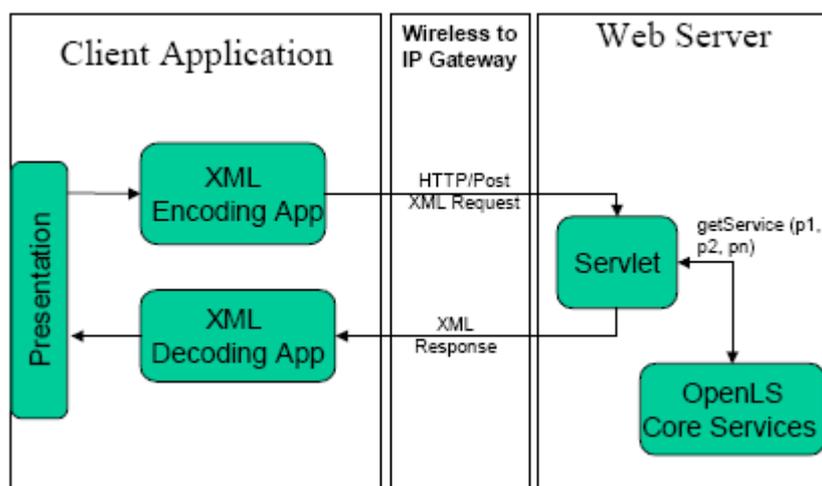


Abbildung 40: Grundsätzlicher Ablauf OpenLS Request/Response

Quelle: OGC 03-006r3, 16.01.2004: OpenGIS Location Services (OpenLS): Core Services

Die Client Anwendung führt eine Anfrage für einen Service aus. Diese Anfrage wird in der Client-Anwendung in XML übersetzt und über die HTTP/Post-Methode an ein Servlet übermittelt (Request). Das Servlet wandelt das XML in einen gültigen Funktionsaufruf für einen OpenLS-Core Service um. Der Core Service verarbeitet die Anfrage und gibt das Ergebnis an das Servlet zurück, welches wiederum ein XML daraus erzeugt und das XML an die Client-Anwendung übermittelt (Response). Die Client Anwendung decodiert das XML-File und führt die entsprechende Funktion für die Präsentation der Ergebnisse aus.

Beispiel für eine OpenLS Directory Service-Anfrage:

Welches Kino liegt innerhalb von 1000 m um das Hotel Sacher?

```

<DirectoryRequest>
  <POILocation>
    <WithinDistance>
      <POI ID="1">
        <POIAttributeList>
          <POIInfoList>

```

```

        <POIInfo name="POI Name" value="Hotel Sacher"/>
      </POIInfoList>
    </POIAttributeList>
  </POI>
  <MaximumDistance value="1000"/>
</WithinDistance>
</POILocation>
<POIProperties directoryType="Yellow Pages">
  <POIProperty name="NAICS_type" value="Kino"/>
</POIProperties>
</DirectoryRequest>

```

- **Gateway-Service:** Ist die Schnittstelle zwischen dem GMS und dem Location-Server. Sein Zweck ist es, die Positionsdaten für die mobilen Geräte abzufragen.
- **Location Utility Service:** Dieser Service liefert zu einer oder mehreren gegebenen geografischen Position die geocodierten Informationen in normierter Form (Ortsname oder Straßenadresse oder postalischer Code) bzw. umgekehrt zu geocodierten Informationen die geografische Position.
- **Presentation Service:** Liefert eine Karte für die Anzeige auf dem Client.
- **Route Service:** Bestimmt die Routeninformation beginnend von einem anzugebenden Startpunkt, über 0-n Zwischenpunkte bis zum Endpunkt.

Typischer Ablauf einer OpenLS-Serviceanfrage:

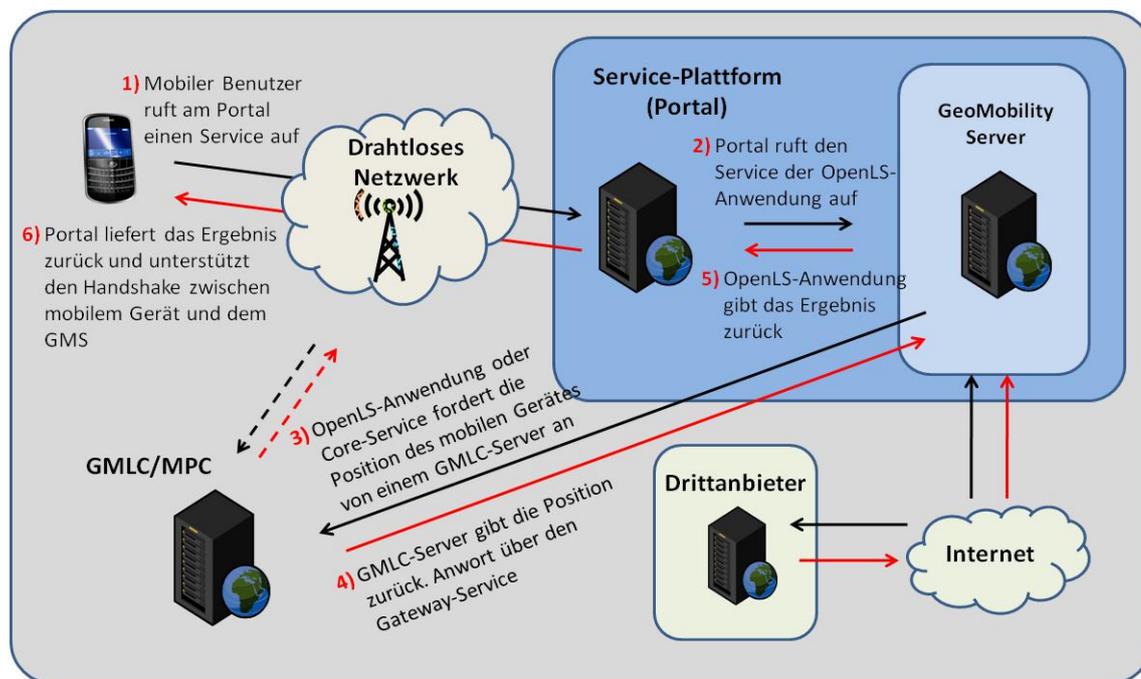


Abbildung 41: Verlauf einer OpenLS-Serviceanfrage

Quelle: angelehnt an Standard, OGC 07-074, 9 September 2008: OpenGIS Location Services (OpenLS): Core Services.

Literaturverzeichnis

- ABUSUBAIH, M.; RATHKE, B. (2008): Packet Loss Discrimination in Multi-Cell 802.11 Wireless LANs. Herausgegeben von Technische Universität Berlin. Online verfügbar unter <http://www.tkn.tu-berlin.de/publications/papers/LossDiscriminationAbusubaih1.pdf>, zuletzt geprüft am 05.10.2009.
- ArbVG (2009): Arbeitsverfassungsgesetz, ArbVG, BGBl. Nr. 22/1974, in der Fassung BGBl. I Nr. 74/2009. Online verfügbar unter <http://www.bmsk.gv.at/cms/site/attachments/3/8/4/CH0650/CMS1233229938197/arbeitsverfassungsgesetz.pdf>, zuletzt geprüft am 19.12.2009.
- ASHTON, S. (2009): ZigBee Technology Overview. Herausgegeben von ZigBee Alliance. Online verfügbar unter http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=16561, zuletzt geprüft am 19.10.2009.
- BEINAT, E. [1] (2008): Location Awareness and Privacy: Dataveillance. ZGIS LBS-Summer school 2008. Universität Salzburg.
- BEINAT, E. et al (2007): Location Awareness 2020. A foresight study on location and sensor services. Herausgegeben von Vrije Universiteit Amsterdam, Spatial Information Laboratory und Instituut voor Milieuvraagstukken. Amsterdam. Online verfügbar unter <http://www.oracle.com/global/it/mobility/events/ev-mov/2007/euro-beinat.pdf>, zuletzt geprüft am 16.10.2009.
- BIZER, J. et al (2006): Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des Bundesministeriums für Bildung und Forschung. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Kiel); Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (Berlin). Berlin.
Online verfügbar unter http://www.bmbf.de/pub/ita_taucis.pdf, zuletzt geprüft am 16.03.2009.
- DEY, A.K., ABOWD, G.D. (2000) Towards a Better Understanding of Context and Context Awareness.
- DOBSON, J.E., FISCHER P.F. (2003): Geoslavery, IEEE Technology and Society Magazine, 47–52
- DORNBUSCH, P., ZÜNDDT, M. (2002): Realisierung von Positionsortungen in WLAN. München. Online verfügbar unter <http://www.lkn.ei.tum.de/forschung/publikationen/dateien/Dornbusch2002RealisierungvonPositionsortungenin.pdf>, zuletzt geprüft am 24.10.2009.
- DUTTA, S. (2008): Field Service Scheduling and Routing. A Guide to Service Delivery Excellence. Herausgegeben von Aberdeen Group. Online verfügbar unter <http://resources.aberdeen.com/vault/pdfs/4897-RA-service-scheduling-routing.pdf>, zuletzt geprüft am 08.09.2009.

ECKERT, C. (2009): Vorlesung Sicher Mobile Systeme; Kapitel 5 Bluetooth (PAN). Technische Universität München. Online verfügbar unter <http://www20.informatik.tu-muenchen.de/assets/lehre/ss09/sms/sms-kap5-bluetooth.pdf>, zuletzt geprüft am 22.09.2009.

EKAHAU [1] (2009): Wi-Fi based RTLS Tracking And Communication Solutions. Online verfügbar unter http://www.aami.org/2009handouts/handouts/sunday/Kohonen_Sun_830.pdf, zuletzt geprüft am 18.10.2009.

EKAHAU [2] (2009). Wi-Fi RTLS; The myths vs. the facts. Online verfügbar unter http://www.ekahau.com/images/stories/products/ekahau_myth_vs_facts.pdf, zuletzt geprüft am 18.10.2009.

EPOF (2002): Comments on Review of the EU Data Protection Directive (Directive 95/46/EC). Herausgegeben von European Privacy Officers Forum (EPOF). Online verfügbar unter http://www.hunton.com/files/tbl_s47Details/FileUpload265/1738/epof_en2_7.31.02.pdf zuletzt geprüft am 04.05.2009.

EPOF (2003): EPOF'S Views on the Commission's Initiative on Employee Privacy. Herausgegeben von European Privacy Officers Forum (EPOF). Online verfügbar unter http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1748%5CEPOF_Employee_Privacy_12.03.pdf, zuletzt geprüft am 04.05.2009.

EU-Richtlinie (1995): Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995

EU-Richtlinie (2002): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Europäische Kommission (2007): 2007/131/EC. on allowing the use of the radio spectrum for equipment using ultra-wideband technology in a harmonised manner in the Community. Online verfügbar unter <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:055:0033:0036:EN:PDF>, zuletzt geprüft am 16.10.2009.

Europäische Union GD Binnenmarkt (2004): Europa Direkt Datenschutz in der Europäischen Union. Online verfügbar unter http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-austria_de.pdf; zuletzt geprüft am 30.03.2009

EPC Global (2009). The EPCglobal Architecture Framework. Version 1.3 vom 13.03.2009. Online verfügbar unter http://www.epcglobalinc.org/standards/architecture/architecture_1_3-framework-20090319.pdf; zuletzt geprüft am 20.06.2009

FISCHER, G. et al (2004): Bluetooth Indoor Localization System. Online verfügbar unter http://www2.informatik.hu-berlin.de/~fwinkler/publications/BILS_WPNC04.pdf, zuletzt geprüft am 25.10.2009.

FORGÒ, N. (2008): Forschungs- und Entwicklungsauftrag zum Thema Geoinformation und Datenschutz“ (GEODAT). Unter Mitarbeit von Tina Krügel und Nico Reiners. Herausgegeben von Leibnitz Universität Hannover. Hannover. Online verfügbar unter http://www.iri.uni-hannover.de/tl_files/pdf/Gutachten%20GEODAT.pdf; zuletzt geprüft am 03.05.2009.

GREGOR, S. (2006): Entwicklung einer Hardwareplattform für die Ermittlung von Positionsdaten innerhalb von Gebäuden. Bachelorarbeit. Hamburg. Hochschule für Angewandte Wissenschaften Hamburg, Technik und Informatik. Online verfügbar unter <http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/bachelor/gregor.pdf>, zuletzt geprüft am 14.10.2009.

HALLBERG, J., NILSSON, M. (2002): Positioning with Bluetooth, IrDA and RFID. Master Thesis. Lulea. Luleå University of Technology. Online verfügbar unter <http://epubl.luth.se/1402-1617/2002/125/LTU-EX-02125-SE.pdf>, zuletzt geprüft am 25.10.2009.

HEGLI, R. (2008): Whitepaper; From A to ZigBee... The Truth about Sensor Networks. Herausgegeben von Awarepoint Inc. Online verfügbar unter <http://www.awarepoint.com/documents/AtoZigbee-s.pdf>, zuletzt geprüft am 22.10.2009.

HERGLOTZ, A. (2006): Lokalisierung und Orientierung in Gebäuden - IMAPS und Headmounted Display im Einsatz als Museumsführer. Bachelorarbeit. Betreut von Dr. Gunter Klemke. Hamburg. Hochschule für Angewandte Wissenschaften Hamburg, Department Technik & Informatik. Online verfügbar unter <http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/bachelor/herglotz.pdf>, zuletzt geprüft am 11.10.2009.

HIGHTOWER, J. et al (2000): SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength. Online verfügbar unter <http://seattle.intel-research.net/people/jhightower/pubs/hightower2000indoor/hightower2000indoor.pdf>, zuletzt aktualisiert am 21.02.2000, zuletzt geprüft am 11.10.2009.

HOGREFE, D. (2009): Vorlesung Mobilkommunikation I. Online verfügbar unter <http://user.informatik.uni-goettingen.de/~elanmk/mk1/>, zuletzt geprüft am 10.03.2009.

HOPPER, A. (2003): Location Aware Computing. Herausgegeben von University of Cambridge. Online verfügbar unter <http://research.microsoft.com/en-us/um/cambridge/events/needhambook/videos/pdf/hopper.pdf>, zuletzt geprüft am 07.10.2009.

IBACH, P. et al (2005): Ortung drahtlos kommunizierender Endgeräte mit GRIPS/MagicMap. Berlin. Online verfügbar unter <http://subs.emis.de/LNI/Proceedings/Proceedings68/GI-Proceedings.68-111.pdf>, zuletzt geprüft am 12.10.2009.

ISO 19111 (2007) Geographic Information - Spatial referencing by coordinates

ISO/IEC 19762-5 (2008): Information technology -- Automatic identification and data capture (AIDC) techniques -- Harmonized vocabulary -- Part 5: Locating systems

JANSEN, R. (2004): Integration der Transpondertechnologie zur Erhöhung der Leistungsfähigkeit der operativen Produktionssteuerung. Heft 38. Herausgegeben von Technische Universität Chemnitz. Chemnitz. Online verfügbar unter http://archiv.tu-chemnitz.de/pub/2005/0009/data/Heft_38.pdf, zuletzt geprüft am 17.08.2009.

KUTTEROFF, A.; BEHRENS, P. (2008): JIM 2008 Jugend, Information, (Multi-)Media. Unter Mitarbeit von Tina König und Thomas Schmid. Herausgegeben von Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter http://www.mpfs.de/fileadmin/JIM-pdf08/JIM-Studie_2008.pdf, zuletzt geprüft am 12.09.2009.

LARSSON, D.; SJÖDIN S. (2006): Design, Implementation and Evaluation of a Self-controlled, Sensor-reading Scorpion Robot using Ekahau Positioning System, Wireless MICA2 Motes an a Bluetooth Mulle. Master Thesis. Luleå. Luleå University of Technology, Computer Science. Online verfügbar unter <http://epubl.ltu.se/1402-1617/2006/283/LTU-EX-06283-SE.pdf>, zuletzt geprüft am 16.08.2009.

LOSSAU, V. (2007): Verfügbare Tag-Typen. Herausgegeben von Nomina GmbH. (ISIS RFID Special 2007). Online verfügbar unter http://www.isis-specials.de/profile_pdf/1d226_ed_rfid0207.pdf, zuletzt aktualisiert am 17.10.2006, zuletzt geprüft am 22.03.2009.

MANNEL, A. (2008): Mehr Transparenz und höhere Effizienz durch RFID in der Intralogistik. Herausgegeben von Dematic GmbH. Online verfügbar unter http://www.rfid-nrw-nl.com/files/4_Transparenz_in_der_Intralogistik_Mannel.pdf, zuletzt geprüft am 17.10.2009.

MARKO, T.; SCHMIDLE, M. (2004): EAI-Nutzen ist messbar. (Netzwoche, 44/2004). Online verfügbar unter <http://www.bint.ch/files/EAI-Nutzen%20ist%20messbar.pdf>, zuletzt geprüft am 20.11.2009.

MATTERN, F. (2008): Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In: Alexander Rossnagel, Tom Sommerlatte, Udo Winand (Eds.): Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Springer, 3-29, Berlin Heidelberg New York, April 2008
Online verfügbar unter <http://www.vs.inf.ethz.ch/publ/ubicomp.html>; zuletzt geprüft am 15.03.2009

MÜHLEMANN, R. (2005): Konzeption eines Sicherheitsframeworks für eine Open Source- basierte Geodateninfrastruktur. Master Thesis. Betreut von Prof. Josef Strobl. Salzburg. Universität Salzburg.

OECD (Hg.) (2004): The Security Economy. Online verfügbar unter <http://www.oecd.org/dataoecd/14/17/16692437.pdf>, zuletzt geprüft am 14.03.2009

OOSTERLINCK, R. (2004): Tracking by Satellite, GALILEO; Beitrag in “The Security Economy”; OECD-Report; 77-90

Österreichisches Datenschutzgesetz "Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999"

PISCHEL, E. (2002): Architektur des Universal Mobile Telecommunications Systems. Herausgegeben von Humboldt Universität Berlin. Humboldt Universität Berlin. Berlin. Online verfügbar unter <http://www.epischel.de/studium/umts.pdf>, zuletzt geprüft am 16.09.2009.

PRIYANTHA, N. B. (2005): The Cricket Indoor Location System. Dissertation. Betreut von Hari Balakrishnan. Massachusetts Institute of Technology, S.M. Computer Science. Online verfügbar unter <http://nms.lcs.mit.edu/papers/bodhi-thesis.pdf>, zuletzt geprüft am 10.10.2009.

REIS, Martina (2008): Die Überwachung von Arbeitnehmern am Arbeitsplatz in Österreich. Betreut von Wolfgang Feiel. Eisenstadt. Fachhochschul-Studiengang Informationsberufe, Information & Knowledge Management. Online verfügbar unter <http://bibliothek.fh-burgenland.at/fileadmin/Download/bibliothek/diplomarbeiten/AC07075966.pdf>, zuletzt geprüft am 19.12.2009.

ROTH, J. (2005): Mobile Computing, dpunkt.verlag

SCHEURING, L. (2005): Verbesserung der Positionsbestimmung von PDA's für die kontextabhängige Interaktion mit einem fixen Anzeigesystem, Diplomarbeit, Universität Zürich

SCHOLZ-REITER, B.(2007): Tracking und Tracing in der Produktion mit passiven RFID Transpondern. Herausgegeben im ISIS Spezial RFID 2007 von Nomina GmbH, München

SHU, W. et al (2008): Location Based Services for Mobiles: Technologies and Standards - WCNC 2008 / ICC 2008. Herausgegeben von LG Electronic Mobile Research. Online verfügbar unter <http://to.swang.googlepages.com/ICC2008LBSforMobilesimplifiedR2.pdf>, zuletzt geprüft am 23.10.2009

Standard, OGC 07-074, (09.09.2008): OpenGIS Location Services (OpenLS): Core Services.

Standard, OGC 03-006r3, (16.01.2004): OpenGIS Location Services (OpenLS): Core Services

STEINBERG, T. (2007): Erstellung eines Frameworks für eine positionsabhängige Auftragsverwaltung in mobilen Netzwerken. Maser Thesis. Betreut von Gunter Klemke. Hamburg. Hochschule für Angewandte Wissenschaften Hamburg, Department Informatik. Online verfügbar unter <http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/master/steinberg.pdf>, zuletzt geprüft am 16.08.2009.

STERNIG, S. et al (2009): Robust Adaptive Classifier Grids for Object Detection from Static Cameras. Herausgegeben von Technische Universität Wien. Online verfügbar unter http://lrs.icg.tugraz.at/pubs/sternig_cvww_09.pdf, zuletzt geprüft am 07.10.2009.

TANNÒ, N.; TOMASONE, N. (2007): Positioning with Magic Map. Universität Freiburg, Institut für Informatik. Freiburg, Online verfügbar unter [http://diuf.unifr.ch/is/userfiles/file/studentprojects/reports/mBusiness_HS07_Positioning_with_Magic_Map_\(NinoTomasone_NataliaTanno\).pdf](http://diuf.unifr.ch/is/userfiles/file/studentprojects/reports/mBusiness_HS07_Positioning_with_Magic_Map_(NinoTomasone_NataliaTanno).pdf), zuletzt geprüft am 11.10.2009.

THIESSE, F. (2005): RFID-Technologie Anwendungen und technische Umsetzung. Herausgegeben von Universität St. Gallen und ETH Zürich. St. Gallen. Online verfügbar unter <http://akswt.uni-konstanz.de/docs/RFIDAnwendungen01FTH.pdf>, zuletzt geprüft am 17.10.2009.

VAN LIESHOUT, M. et al (2007): RFID Technologies: Emerging Issues, Challenges and Policy Options. Unter Mitarbeit von Marc van Lieshout, Luigi Grossi und Graziella VAN RIPER, D., WHITFIELD, T. (2004): Developing a Framework for Privacy in Location-Based Services (LBS), CSci 8715 – Group 3

WAGNER, R. et al (2005): Auswirkungen der Energiemarktregulierung. Herausgegeben von energate research und ConEnergy AG. Online verfügbar unter http://www.energate.de/download/Studie_05_1_Energiemarktregulierung.pdf, zuletzt geprüft am 19.11.2009.

WARD, A. et al (1997): A New Location Technique for the Active Office. Herausgegeben von AT&T Laboratories Cambridge. Online verfügbar unter <http://www.cl.cam.ac.uk/research/dtg/publications/public/files/tr.97.10.pdf>, zuletzt geprüft am 08.10.2009.

WESTIN, A. (1967): Privacy and Freedom, New York, Athenum

WILDE, G. et al (2002): Whitepaper: The Last Known Location of E-OTD. Herausgegeben von BWCS. Online verfügbar unter <http://www.bwcs.com/whitepapers/EOTD.pdf>, zuletzt geprüft am 23.10.2009.

WIPS (2000): WIPS Technical Documentation. Online verfügbar unter <http://www.tslab.ssvl.kth.se/csd/projects/0012/technical.pdf>, zuletzt geprüft am 19.10.2009.

YOUNG, T. (2008): Rosum FemtoSynch In-Building Timing and Location for Femtocells. Online verfügbar unter http://www.rosun.com/pdfs/Rosum_FemtoSynch_White_Paper_Oct08.pdf, zuletzt geprüft am 25.10.2009.

ZOGG, J.M. (2006): Grundlagen der Satellitennavigation, Users Guide, ublox AG Schweiz. Buch ist online verfügbar unter [http://www.ublox.de/customersupport/docs/GPS_Basics\(GPS-X-01006\).pdf](http://www.ublox.de/customersupport/docs/GPS_Basics(GPS-X-01006).pdf)

Internetquellen:

AT&T Laboratories Cambridge (Hg.) (2002): The Bat Ultrasonic Location System. Online verfügbar unter <http://www.cl.cam.ac.uk/research/dtg/attarchive/bat/>, zuletzt geprüft am 08.10.2009.

Balakrishnan, Hari (2006): The Cricket Indoor Location System: An NMS Project @ MIT CSAIL. Herausgegeben von Massachusetts Institute of Technology. Online verfügbar unter <http://cricket.csail.mit.edu/>, zuletzt geprüft am 08.10.2009.

Clarke's, Roger (2006): 'What's Privacy?'. Online verfügbar unter <http://www.rogerclarke.com/DV/Privacy.html>, zuletzt geprüft am 21.03.2009.

Clarke's, Roger (2006): Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Online verfügbar unter <http://www.rogerclarke.com/DV/Intro.html>, zuletzt geprüft am 21.03.2009.

Clarke's, Roger (2008): You Are Where You've Been Location Technologies' Deep Privacy Impact. Online verfügbar unter <http://www.rogerclarke.com/DV/YAWYB-CWP.html#P>, zuletzt geprüft am 21.03.2009.

DeCew, J. (2002, 2006): Privacy (Stanford Encyclopedia of Philosophy). Online verfügbar unter <http://plato.stanford.edu/entries/privacy/>, zuletzt geprüft am 21.03.2009.

EPCglobal (2005): Guidelines on EPC for Consumer Products. Online verfügbar unter http://www.epcglobalinc.org/public/ppsc_guide/, zuletzt geprüft am 09.04.2009

Fraunhofer IIS (2009): Lokalisierung in Kommunikationsnetzen. Online verfügbar unter <http://www.iis.fraunhofer.de/bf/nl/lik/index.jsp>, zuletzt geprüft am 20.12.2009.

Galileo EU Commission Transport (2009). Online verfügbar unter http://ec.europa.eu/transport/galileo/index_en.htm, zuletzt geprüft am 12.03.2009

Geodan Movida-Informationen: Online verfügbar unter <http://www.geodan.de/produkte/geodan-software/geodan-movida/geodan-movida-kernfunktionalitaeten/>, zuletzt geprüft am 10.08.2009

Geodan Movida (2009): indoor location | Geodan. Online verfügbar unter <http://www.geodan.com/products/geodan-software/geodan-movida/geodan-movida-indoor-location/>, zuletzt geprüft am 25.08.2009.

GSMWorld (2009): GSM Europäische Netzabdeckung 2009: Europa Technologies Limited for the GSM Association. Online verfügbar unter http://www.gsmworld.com/roaming/GSM_EuropePoster2009A.pdf, zuletzt geprüft am 12.09.2009.

Information and Service System for European Coordinate Reference Systems – CRS (2006). Online verfügbar unter <http://crs.bkg.bund.de/crs-eu/index.html>, zuletzt geprüft am 11.03.2009.

Kraftwerksgruppe Flachgau-Tennengau: Online verfügbar unter http://www.salzburg-ag.at/fileadmin/user_upload/Infomenu/Erzeugung/Wasserkraftwerke/Kraftwerke_FlachgauTennengau.pdf, zuletzt geprüft am 12.05.2009

KREMPL, S. (2003): heise mobil - 28.05.03 - Stille SMS. Online verfügbar unter <http://www.heise.de/mobil/artikel/ueberwachung-per-Mobilfunk-222789.html>, zuletzt geprüft am 23.10.2009.

OGP Surveying & Positioning Committee (2009). Online verfügbar unter <http://www.epsg.org/>, zuletzt geprüft am 11.03.2009.

Rosum (2009). Online verfügbar unter http://www.rosun.com/rosun_technology_tv-positioning.html, zuletzt geprüft am 25.10.2009.

Trusted-RFID (2006): Forschungsprojekt Trusted-RFID. Online verfügbar unter <http://www.trusted-rfid.de>, zuletzt geprüft am 09.04.2009.

UMTS-Link: Informationen zur Mobilfunktechnologie: Online verfügbar unter <http://www.umtslink.at/>, zuletzt geprüft am 18.09.2009.