

DIPLOMARBEIT

Gateway für ein Containerüberwachungssystem

ausgeführt zur Erlangung des akademischen Grades
eines Diplom-Ingenieurs unter der Leitung von

O. Univ. Prof. Dr. Dietmar Dietrich
Univ. Ass. Dr. Stefan Mahlknecht
Dipl.-Ing. Stefan Krywult

am

Institut für Computertechnik (E384)
der Technischen Universität Wien

durch

Bernd Schuster
Matr.Nr. 0225322
Am Berg 25, 2264 Sierndorf/March

Wien, im Oktober 2009

Kurzfassung

Diese Arbeit befasst sich mit dem Entwurf und der Realisierung eines Gateways für ein System zur drahtlosen Containerüberwachung. Die Überwachung von Containern gewinnt zunehmend an Bedeutung, da der globale Gütertransport größtenteils in Form von Transportcontainern erfolgt. Weltweit existieren mehr als 20 Millionen Container, die mit Lastkraftwagen, Schiffen und Zügen befördert werden. Auf dem Weg zu ihrem Zielort ist die Ware verschiedenen Risiken und unvorhersehbaren Ereignissen ausgesetzt. Drahtlose Überwachungssysteme sollen gewährleisten, dass die Ware qualitativ hochwertig und unverfälscht an ihrem Bestimmungsort ankommt. Diese Arbeit analysiert globale und lokale Kommunikationstechnologien, die eine wichtige Rolle bei der Überwachung von Containern spielen. Anhand marktreifer Produkte wird der Stand der Technik auf dem Gebiet der Containerüberwachung gezeigt. Aufbauend auf den Ergebnissen der Analyse wird ein Gateway implementiert, der Containern die globale Kommunikation über eine lokale Funkverbindung ermöglicht. Container in Funkreichweite des Gateways erhalten auf energiesparende Weise Zugriff auf ein globales Kommunikationsnetzwerk.

Abstract

This thesis deals with the design and the implementation of a gateway for a wireless container monitoring system. Container monitoring becomes more and more important because cargo containers are the most commonly used form of transportation in today's global economy. More than 20 million cargo containers are moved around the world by trucks, ships and trains. On the way to its destination, the cargo is exposed to various risks and unpredictable events. Wireless monitoring systems shall guarantee that the cargo reaches its destination in the highest quality and without damage. This thesis analyses global and local communication technologies which are important for wireless container monitoring systems. The state of the art for container monitoring systems is shown by the survey of products already available on the market. Considering the results of the analysis, a gateway is implemented which allows cargo containers to communicate globally through the use of local radio. Containers within the radio range of a gateway are therefore offered energy saving access to a global communication network.

Inhaltsverzeichnis

1	Einleitung	1
1.1	Wireless Cargo Monitoring System (WCMS)	1
1.2	Aufgabenstellung	2
1.2.1	Location-Service	3
1.2.2	SMS-Service	4
1.2.3	Stream-Service	5
1.2.4	Aufgabenliste	5
1.3	Aufbau der Arbeit	6
2	Drahtlose Containerüberwachung	7
2.1	Anforderungen und Umfeld	7
2.2	Globale Kommunikation	8
2.2.1	GSM	8
2.2.2	UMTS	12
2.2.3	GPS	14
2.3	Lokale Kommunikation	15
2.3.1	ZigBee	15
2.3.2	RFID	18
2.4	Produkte	21
2.4.1	Container Security Box	21
2.4.2	AIRSIS Express Trailer and Container Monitor	24
2.4.3	CommerceGuard	25
2.4.4	Smart Box	26
2.4.5	GlobalTrack	26
2.4.6	ORBCOMM	28
3	Problemanalyse	29
3.1	Mediumzugriff beim Funkprotokoll	29
3.2	Szenario - Lagerhalle	30
3.3	Szenario - Lagerplatz	33
3.4	Szenario - Eisenbahntransport	34
3.5	Durchsatzanalyse	36

4	Systemarchitektur	37
4.1	Wireless Cargo Monitoring System	37
4.2	Embedded Gateway	39
4.2.1	Gatewaycontroller	40
4.2.2	Funkcontroller	41
4.2.3	Funktransceiver	42
4.2.4	Lantronix-Modul	42
4.2.5	GSM-Modul	43
4.2.6	GPS-Modul	43
4.2.7	Speicher	44
4.2.8	Konsole	45
4.3	Schnittstellendefinition	45
5	Implementierung	48
5.1	Protokollstapel	48
5.2	Netzwerkanbindung	49
5.3	Funkanbindung	52
5.4	Gatewayapplikation	59
5.4.1	Anmeldung	60
5.4.2	Location-Service	61
5.4.3	SMS-Service	62
5.4.4	Stream-Service	64
6	Projektergebnisse	67
6.1	Testaufbau	67
6.2	Energiebilanz	69
6.3	Zusammenfassung	70
6.4	Ausblick	71
	Wissenschaftliche Literatur	72
	Internetreferenzen	74

Abkürzungen

3GPP	3rd Generation Partnership Project
AC	Authentication Center
AES	Advanced Encryption Standard
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Collision Avoidance
CAP	Contention Access Periode
CDB	Container Management Database
CEPT	European Conference of Postal and Telecommunications Administrations
CFP	Contention Free Periode
CGW	Container Management Gateway
COMA	Container Management
CRC	Cyclic Redundancy Check
CSB	Container Security Box
CSD	Container Security Device
CSMA	Carrier Sense Multiple Access
CSRV	Container Management Server
CTS	Clear to Send
DES	Data Encryption Standard
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data Rates for GSM Evolution
EEPROM	Electrically Erasable Programmable Read Only Memory
EGW	Embedded Gateway
EIR	Equipment Identify Register
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FTP	File Transfer Protocol
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Service Switching Center
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTS	Guaranteed Time Slot
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access

HTTP	Hypertext Transfer Protocol
ICT	Institut für Computertechnik
IEEE	Institute of Electrical and Electronics Engineers
IFF	Fraunhofer-Institut für Fabrikbetrieb und -automatisierung
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISM	Industrial Scientific Medical
ISO	International Organization for Standardization
IWF	Interworking Functions
LAN	Local Area Network
LEO	Low Earth Orbit
LSB	Least Significant Bit
MAC	Medium Access Control
MD5	Message Digest Algorithm 5
MSC	Mobile Service Switching Center
MTU	Main Telematics Unit
NACK	Not Acknowledged
OMC	Operation and Maintenance Center
OSI	Open Systems Interconnection
PAN	Personal Area Network
PCU	Packet Control Unit
PDA	Personal Digital Assistant
PDF	Portable Document Format
PSK	Phase Shift Keying
RAM	Random Access Memory
RC4	Ron's Code 4
RFID	Radio Frequency Identification
RNC	Radio Network Controller
RST	Request to Send
RTC	Real Time Clock
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Modul
SMS	Short Message Service
SMSC	Short Message Service Center
SNMP	Simple Network Management Protocol
SPI	Serial Peripheral Interface
SSH	Secure Shell
SSL	Secure Sockets Layer
SU	Sensor Unit
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TRAU	Transcoding and Rate Adaption Unit
UART	Universal Asynchronous Receiver Transmitter
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Network
VLR	Visitor Location Register
WCDMA	Wideband Code Division Multiple Access
WCMS	Wireless Cargo Monitoring System
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

1 Einleitung

Der globale Gütertransport erfolgt größtenteils in Form von Transportcontainern. Weltweit existieren mehr als 20 Millionen Container, die mit Lastkraftwagen, Schiffen oder Zügen an ihren jeweiligen Bestimmungsort befördert werden. Auf dem Weg zu ihrem Zielort ist die Ware verschiedenen Risiken und unvorhersehbaren Ereignissen ausgesetzt. Um zu gewährleisten, dass die Ware qualitativ hochwertig und unverfälscht an ihrem Bestimmungsort ankommt, hat sich in den letzten Jahren der Einsatz von Systemen zur Überwachung (Monitoring) und Verfolgung (Tracking) von Containern etabliert. Diese Systeme bieten Unternehmen einen ständigen Überblick über den aktuellen Zustand und die aktuelle geographische Position ihrer Container. Dadurch kann schnell und koordiniert auf unvorhergesehene Ereignisse reagiert werden. Die gesammelten Informationen können zu einer genauen Dokumentation und einer Optimierung der betriebswirtschaftlichen Prozesse genutzt werden.

Für die Ermittlung des aktuellen Containerzustands kommen unterschiedliche Sensoren zur Anwendung. Abhängig von der Sensorausstattung können die Umgebungsbedingungen der transportierten Ware laufend überwacht werden. Die Sensoren messen die Temperatur und Luftfeuchtigkeit sowie die Lichtverhältnisse im Container, Erschütterungen oder den Umgebungsdruck. Ebenso kann das Öffnen des Containers überwacht werden. Die gesammelten Daten werden in Folge über globale Kommunikationsnetze an ein Datacenter weitergeleitet, wo die Verarbeitung, Speicherung und Analyse der Daten erfolgt. Durch die laufende Überwachung der Container können Fehlleitungen frühzeitig aufgedeckt werden. Diebstähle und Manipulationen können erkannt und die Qualität der Ware hochgehalten werden. Systeme zur Containerüberwachung für den globalen Warenverkehr ermöglichen darüber hinaus eine lückenlose Aufzeichnung der Historie des Transports. Zur Dokumentation werden die gesammelten Daten oftmals in Datenbanken abgelegt. Autorisierte Personen können jederzeit aktuelle Informationen betreffend den Transport und die Ware in bestimmten Containern abrufen. Obwohl bereits mehrere Systeme zur Überwachung von Containern am Markt erhältlich sind, ist die Technologie noch nicht ausgereift. Es existieren noch einige Probleme, wie zum Beispiel die Energieversorgung am Container, an denen aktuell geforscht und entwickelt wird.

1.1 Wireless Cargo Monitoring System (WCMS)

Das Wireless Cargo Monitoring System (WCMS) ist ein System zur drahtlosen Überwachung von Transportcontainern. Dieses System ist noch nicht am Markt erhältlich. Es wird derzeit im Rahmen eines Forschungsprojekts an der Technischen Universität Wien entwickelt. Neben der

Technischen Universität Wien sind die Firmen Blue Technix, Rail Cargo Austria sowie LCM an diesem Projekt beteiligt. Ziel des Projekts ist die Entwicklung eines preiswerten Systems zur drahtlosen Überwachung und Verfolgung von Transportcontainern mit einem niedrigen Energieverbrauch.

Im Zuge des WCMS-Projekts werden Container mit Sensoren zur Erfassung des aktuellen Zustands und einem GPS-Empfänger (Global Positioning System) zur Ermittlung der aktuellen geographischen Position ausgestattet. Die zentrale Einheit am Container wird Main Telematics Unit (MTU) genannt. Diese Telematikbox beinhaltet den GPS-Empfänger, ein GSM-Modul (Global System for Mobile Communications) und einen Funktransceiver. Die durch den Funktransceiver erzielbare Funkreichweite von einigen 100 m wird im Folgenden als Lokalfunk bezeichnet. Darüber hinaus verfügt die MTU über Rechen- und Speicherkapazitäten. Die verschiedenen Sensoren sind auf Sensorknoten verteilt. Eine Sensor Unit (SU) kann direkt mit der MTU verbunden sein oder über Lokalfunk mit der MTU kommunizieren. Die gesammelten Daten werden von der Telematikbox über das GSM-Modul an das WCMS-Datencenter übertragen. Im Datencenter erfolgt die Speicherung, Analyse und Verarbeitung der Daten. Da die Kommunikation zwischen den Containern und dem WCMS-Datencenter über GSM erfolgt, können weltweit Daten ausgetauscht werden. Die Voraussetzung dafür ist die Verfügbarkeit eines GSM-Netzes. Periodische Statusmeldungen sowie spontane Alarmmeldungen werden in Form von SMS-Nachrichten von den Containern an das WCMS-Datencenter gesendet. In gleicher Weise erfolgt die Übermittlung von Konfigurationsänderungen in Form von SMS-Nachrichten vom Datencenter an die Container. Die Übertragung größerer Datenmengen erfolgt via GPRS (General Packet Radio Service). Anwendungsfälle sind die Übertragung neuer Firmware an die Container und das Senden von Logfiles an das Datencenter. Weitere Informationen über den WCMS-Aufbau finden sich in Abschnitt 4.1.

Eine Herausforderung im WCMS-Projekt ist die Bereitstellung einer passenden Energiequelle für die Elektronik an den Containern. Die Elektronik soll von keiner externen Versorgung abhängig sein, um an jedem beliebigen Container montiert werden zu können. Im Hinblick auf Wartungsfreiheit soll darüber hinaus eine hohe Betriebsdauer erreichbar sein. Im WCMS-Projekt wird eine Betriebsdauer von 5 Jahren angestrebt. Derzeit erfolgt die Versorgung durch Akkumulatoren oder Primärzellen. Als Energiequellen werden aber auch alternative Ansätze verfolgt, wie die Nutzung von Wind- und Sonnenenergie oder die Umwandlung von mechanischen Vibrationen in Energie. Das gesamte System wird im Hinblick auf einen niedrigen Energieverbrauch entwickelt. Eine andere Herausforderung sind die teilweise extremen Umwelteinflüsse beim Containertransport, welche ein robustes Design voraussetzen.

Bisher wurden derartige Überwachungssysteme in erster Linie für den Transport von wertvollen Gütern oder bei Containern mit integriertem Kühlsystem eingesetzt. Die Energieversorgung des Kühlsystems kann gleichzeitig für die Überwachungselektronik genutzt werden. Im Zuge des WCMS-Projekts soll eine Lösung gefunden werden, die ein preisgünstiges, wartungsfreies Produkt ermöglicht. Das Produkt soll auch für alltägliche Transporte eingesetzt werden können.

1.2 Aufgabenstellung

Diese Arbeit leistet einen Beitrag zur Entwicklung eines Gateways für die Anwendung in einem System zur drahtlosen Containerüberwachung. Der Gateway wird im Folgenden als Embedded Gateway (EGW) bezeichnet. Die Arbeiten finden im Rahmen des WCMS-Projekts (siehe Abschnitt 1.1) am Institut für Computertechnik (ICT) an der Technischen Universität Wien statt.

Im WCMS-Projekt erfolgt der Datenaustausch zwischen den Containern und dem Datacenter über das GSM-Netz. Diese Vorgehensweise ist während des Transports der Container sinnvoll. Auf Lagerplätzen oder in Lagerhallen, das heißt an Orten, an denen sich mehrere Container häufen, kann jedoch die lokal vorhandene Infrastruktur genutzt werden. Dazu zählen eine externe Energieversorgung und ein Internetzugang. Voraussetzung für die Nutzung der vorhandenen Infrastruktur ist die Aufstellung von stationären Gateways. Container in Reichweite sollen mit diesen Gateways über Lokalfunk kommunizieren. Die Gateways wiederum können über einen Internetzugang mit dem WCMS-Datacenter kommunizieren. Durch den Einsatz derartiger Gateways können energetische und wirtschaftliche sowie kommunikationstechnische Vorteile erzielt werden. Die Gateways können zusätzlich über die reine Weiterleitung von Nachrichten hinausgehende Dienste für die Container bereitstellen.

Diese Gedanken waren die Grundlage für den Beschluss, den Embedded Gateway für den Einsatz im WCMS-Projekt zu entwickeln. Der EGW soll in Zukunft drei wesentliche Dienste für die WCMS-Container zur Verfügung stellen, das Location-Service (siehe Abschnitt 1.2.1), das SMS-Service (siehe Abschnitt 1.2.2) und das Stream-Service (siehe Abschnitt 1.2.3). Alle Dienste verfolgen das Ziel, Arbeiten für die Container zu übernehmen und dadurch die Energieressourcen der Container zu schonen. Dadurch kann die Betriebsdauer der Containerelektronik verlängert werden. Zusätzlich soll der EGW die durchschnittliche Geschwindigkeit des Datenaustausches steigern und wirtschaftliche Vorteile im Vergleich zum bisherigen WCMS ohne EGW erzielen.

Die Entwicklung der Hardware für den EGW ist nicht Teil dieser Arbeit. Als Basis für die Entwicklung des EGW-Prototypen wird die neue Hardwaregeneration der MTU (Version 2.0) verwendet. Diese Plattform bietet alle notwendigen Voraussetzungen. Für den Testbetrieb des EGW-Prototypen muss die MTU-Hardware jedoch durch ein (W)LAN-Modul (Wireless Local Area Network) erweitert werden. Abbildung 1.1 zeigt die Vorgaben zum prinzipiellen Aufbau des EGW. Im Zuge dieser Arbeit soll die Gatewayapplikation am Gatewaycontroller implementiert werden. Darüber hinaus sollen die Schnittstellen zum Funkcontroller und zum (W)LAN-Modul definiert und implementiert werden. Zusätzlich sollen Funktionen zur Kommunikation mit dem GSM- und GPS-Modul bereitgestellt werden. Da der EGW auf der gleichen Hardware wie die MTU basiert, können einige Software-Module der MTU am EGW weiterverwendet werden. Die neue MTU-Hardwaregeneration verwendet jedoch einen anderen Mikrocontroller (STM32) als die Vorgängerversionen (LPC2114). Ein Bestandteil der Aufgabenstellung ist daher auch die Portierung der MTU-Software. Die Implementierung der Funkapplikation am Funkcontroller ist nicht Teil dieser Arbeit. In der schriftlichen Arbeit soll die Beschreibung des EGW erfolgen. Es sollen die Problemstellung und die Lösungsansätze diskutiert werden.

1.2.1 Location-Service

Um die aktuelle geographische Position eines WCMS-Containers zu ermitteln, werden mit Hilfe eines GPS-Moduls die GPS-Daten empfangen. Bisher wurde dabei ein containerinternes GPS-Modul verwendet. Da dieses Modul aufgrund energetischer Überlegungen zwischenzeitlich nicht versorgt wird, muss bei der Aktivierung zuerst eine gültige Verbindung mit den GPS-Satelliten aufgebaut werden. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen und verbraucht Energie. Um die Energieressourcen am Container zu schonen, soll daher ein Location-Service am EGW implementiert werden. Dieses Service soll den Containern die Möglichkeit bieten, die aktuellen GPS-Daten vom EGW abzufragen. Zur Kommunikation mit dem EGW soll der Lokalfunk verwendet werden. Durch dieses Vorgehen kann, vorausgesetzt ein EGW befindet sich in

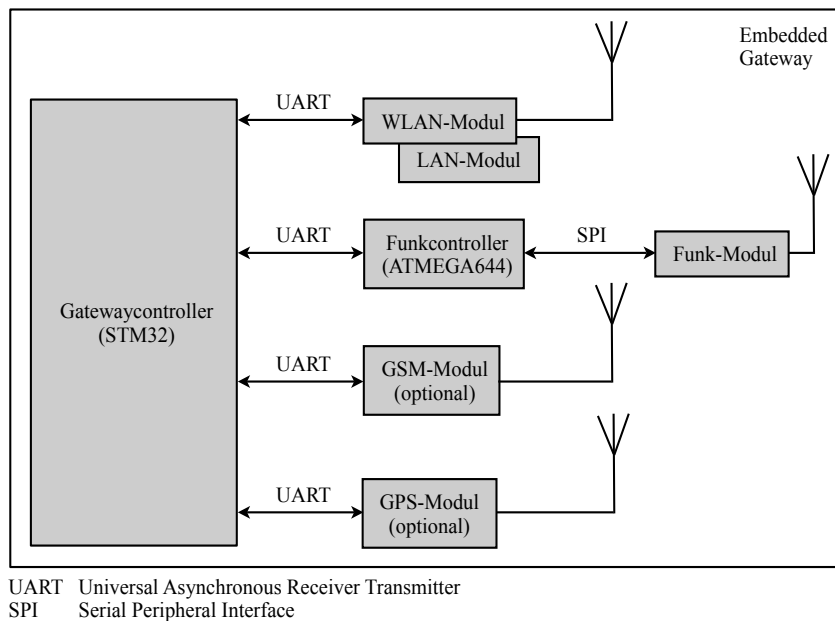


Abbildung 1.1: Vorgabe der prinzipiellen EGW-Architektur

Reichweite, die Inbetriebnahme des containerinternen GPS-Moduls entfallen. Die GPS-Daten des EGW sollen manuell sowie automatisch konfiguriert werden können. Die manuelle Konfiguration ermöglicht den Containern die Bestimmung der aktuellen Position auch innerhalb von Lagerhallen, wo keine Sichtverbindung zu den Satelliten gegeben ist. Wird der EGW im Freien montiert, so kann er mit einem GPS-Modul ausgestattet werden. Er soll daher die Funktion bereitstellen, aktuelle GPS-Daten auch automatisch empfangen zu können.

1.2.2 SMS-Service

Der Austausch von Status- und Alarmmeldungen sowie Konfigurationsänderungen zwischen dem WCMS-Datencenter und den WCMS-Containern erfolgt in Form von SMS-Nachrichten. Dazu wird ein GSM-Modul auf der MTU der Container verwendet. Dieses Modul wird genauso wie das GPS-Modul aus energetischen Gründen zwischenzeitlich nicht versorgt. Aus diesem Grund muss bei der Aktivierung zuerst ein GSM-Netz gesucht und die Verbindung hergestellt werden. Dieser Vorgang kann bis zu einer Minute in Anspruch nehmen. Zu beachten ist außerdem, dass das Versenden von SMS-Nachrichten kostenpflichtig ist. Durch die Implementierung eines bidirektionalen SMS-Services am EGW soll, vorausgesetzt ein EGW befindet sich in Reichweite, die Inbetriebnahme des containerinternen GSM-Moduls entfallen. Der Container soll dabei die Möglichkeit besitzen, Nachrichten über Lokalfunk an den EGW zu senden. Der EGW leitet die Nachrichten über einen WLAN- oder LAN-Zugang an das WCMS-Datencenter weiter. Empfängt der EGW eine Nachricht vom WCMS-Datencenter für einen dem EGW bekannten Container, so soll die Nachricht ebenfalls via Lokalfunk an den Container weitergeleitet werden. Das SMS-Service soll die Übermittlungszeit von SMS-Nachrichten verkürzen und die Kommunikation zwischen WCMS-Datencenter und den Containern auch ermöglichen, wenn kein GSM-Netz vorhanden ist.

1.2.3 Stream-Service

Für den Austausch von größeren Datenmengen zwischen dem WCMS-Datencenter und den WCMS-Containern wäre der Einsatz von SMS-Nachrichten nicht effizient, da pro SMS nur 140 Byte Nutzlast übertragen werden können. Aus diesem Grund werden im WCMS-Projekt Logfiles und Firmwareupdates (rund 100 kByte) mittels GPRS versendet. Hierbei gilt, wie beim Versenden von SMS-Nachrichten, dass der Betrieb des GSM-Moduls die Energieressourcen des Containers belastet und Kosten verursacht. Es soll daher am EGW ein bidirektionales Stream-Service implementiert werden, das den Austausch von großen Datenmengen ohne Zuhilfenahme des containerinternen GSM-Moduls ermöglicht. Voraussetzung ist, dass sich der Container in Reichweite eines EGW befindet. Die Daten sollen über Lokalfunk vom Container an den EGW gesendet und von diesem über einen WLAN- oder LAN-Zugang an die WCMS-Datenbank weitergeleitet werden. Empfängt der EGW Daten vom WCMS-Datencenter für einen dem EGW bekannten Container, so sollen diese ebenfalls via Lokalfunk an den entsprechenden Container weitergeleitet werden. Das Stream-Service soll neben der Übertragung von größeren Datenmengen zusätzlich eine interaktive Kommunikation mit den Containern ermöglichen. Ziel dabei ist, dass sich ein Benutzer über das Internet mit einem Container in Reichweite eines EGW verbinden kann. Mit Hilfe eines Konsolenprogramms können so Daten aus dem Container ausgelesen werden und Konfigurationseinstellungen in der Containersoftware geändert werden. Das Stream-Service am EGW soll es ermöglichen, die Verzögerung zwischen Absenden eines Kommandos und der zugehörigen Antwort gering zu halten.

1.2.4 Aufgabenliste

- Portierung der MTU-Software vom LPC2114 auf den STM32
- Definition der Schnittstellen vom Gatewaycontroller zum Funkcontroller und zum (W)LAN-Modul
- Implementierung eines Location-Services am Gatewaycontroller
- Implementierung eines bidirektionalen SMS-Services am Gatewaycontroller
- Implementierung eines bidirektionalen Stream-Services am Gatewaycontroller
- Implementierung mit Ausrichtung auf niedrigen Energieverbrauch
- Bereitstellung einer Konfigurationsmöglichkeit des EGW
- Bereitstellung von Funktionen zur Kommunikation mit einem optionalen GPS-Modul
- Bereitstellung von Funktionen zur Kommunikation mit einem optionalen GSM-Modul
- Bereitstellung eines Testaufbaus zur Verifizierung der Gatewayapplikation
- Unterstützung von bis zu 100 Containern pro EGW
- Beschreibung und Diskussion des EGW

1.3 Aufbau der Arbeit

Diese Arbeit beschäftigt sich mit dem Entwurf und der Realisierung eines Gateways für ein System zur drahtlosen Überwachung von Transportcontainern. In Kapitel 2 werden die Anforderungen und das Umfeld beim globalen Containerverkehr behandelt. Danach folgt ein Überblick über globale und lokale Kommunikationstechnologien, die bei der Containerüberwachung eingesetzt werden. Darüber hinaus wird an Hand marktreifer Produkte der Stand der Technik bei der Containerüberwachung betrachtet. Aufbauend auf diese Kenntnisse erfolgt in Kapitel 3 die Analyse der Anforderungen und Probleme beim Einsatz des EGW im WCMS-Projekt. Dabei wird der EGW-Einsatz anhand realitätsnaher Szenarien betrachtet. Kapitel 4 liefert einen Einblick in die WCMS-Architektur sowie detaillierte Informationen über die EGW-Architektur und die Schnittstellendefinitionen. Kapitel 5 widmet sich der Implementierung am Gatewaycontroller. Es werden die definierten Kommunikationspakete sowie die angebotenen Gateway-Dienste im Detail beschrieben. Kapitel 6 beschreibt den Testaufbau zur Verifizierung der Gatewayapplikation. Es werden die Projektergebnisse zusammengefasst und ein Ausblick auf künftige Möglichkeiten durch den Einsatz des EGW im WCMS gegeben.

2 Drahtlose Containerüberwachung

Auf dem Gebiet der drahtlosen Überwachung und Verfolgung von Transportcontainern wurden in den letzten Jahren einige Fortschritte erzielt. Wesentlich daran beteiligt sind die laufende Miniaturisierung und Optimierung elektronischer Komponenten sowie die Entwicklung und Verbesserung der Kommunikationstechnologien. Preisgünstige elektronische Komponenten bilden die Basis dafür, zukünftig auch alltägliche Transporte und Waren überwachen zu können. Dieses Kapitel zeigt die Anforderungen an Systeme zur Verfolgung und Überwachung von Transportcontainern. Es werden globale und lokale Kommunikationstechnologien vorgestellt, die für die Containerüberwachung relevant sind. Anhand marktreifer Produkte werden Lösungen gezeigt und Einblicke in den Stand der Technik gegeben.

2.1 Anforderungen und Umfeld

Die meisten Güter werden in genormten Containern transportiert, die im Normalfall aus Stahl bestehen. Die am weitesten verbreiteten Container sind die nach ISO 668:1995 genormten 40-beziehungsweise 20-Fuß-Großraumbehälter. Tabelle 2.1 zeigt einen Ausschnitt der genormten Abmessungen. Es sind jedoch auch viele andere Containertypen für den allgemeinen Transport sowie für Spezialanwendungen im Umlauf. Aufgrund der genormten Abmessungen können die Container platzsparend gestapelt werden. Die Stapelung von Containern wird vor allem beim Transport mit Containerschiffen oder auf Lager- beziehungsweise Be- und Entladeplätzen genutzt. Beim Transport mit der Eisenbahn werden die Container in einer Reihe sequentiell auf die Waggons verladen. Beim Transport mit dem Lastkraftwagen besteht eine Ladung im üblichen Fall höchstens aus zwei Containern, die ebenfalls hintereinander angeordnet werden. Die Art der Stapelung kann bereits wesentliche Auswirkungen auf ein Überwachungssystem haben. Dabei kann die Funkverbindung von Containern gestört oder unterbrochen werden [MM07]. Darüber hinaus werden eventuell Solarzellen abgedunkelt oder andere Komponenten zur Nutzung alternativer Energiequellen behindert.

Die Anforderungen an Überwachungssysteme für den globalen Containerverkehr werden in [MM07] aufgelistet. Dazu zählt die Verfolgung der geographischen Position der Container vom Be- bis zum Entladezeitpunkt. Es soll das unautorisierte Eindringen in Container registriert werden sowie ein Diebstahlreport für ein rechtzeitiges Eingreifen erfolgen. Darüber hinaus sollen rechtzeitig Informationen über die Beschädigung von Container und Ware erhältlich sein. Der Einsatz im rauen Umfeld des Containertransports fordert ein robustes Design und Gehäuse. Aus diesem Grund

Tabelle 2.1: Containerabmessungen nach ISO688 [1]

Typ	Länge	Breite	Höhe	Gesamtgewicht
20 ft	6,058 m	2,438 m	2,591 m	24000 kg
40 ft	12,192 m	2,438 m	2,591 m	30480 kg

sind zuverlässige, preiswerte Lösungen mit niedrigem Energieverbrauch und langer Betriebsdauer gefragt.

Voraussetzung für ein System zur drahtlosen Verfolgung und/oder Überwachung von Transportcontainern ist die Ausstattung der Container mit Sensoren, Kommunikationseinrichtungen und anwendungsabhängigen Prozessor- und Speicherkapazitäten. Das zentrale Element an einem Container ist eine Telematikbox. Diese Box besitzt in den meisten Fällen keine externe Versorgung und muss daher unter Berücksichtigung eines niedrigen Energieverbrauchs entwickelt werden. Die Erfassung des Containerzustands wird durch Sensoren ermöglicht. Die Sensoren können in der Telematikbox inkludiert sein oder auf eigenen Sensoreinheiten im oder am Container verteilt angebracht werden. Die Telematikbox kann Technologien zur globalen und lokalen Kommunikation umfassen. Eine globale Infrastruktur wird zum Datenaustausch zwischen Telematikbox und dem Datacenter des Systems benötigt. Das Datacenter umfasst Datenbanken, Server sowie weitere Einrichtungen zur Analyse, Verarbeitung und Visualisierung der Daten. Die lokale Kommunikation umfasst den Datenaustausch zwischen der Telematikbox und einer Einheit im Umkreis von bis zu einigen 100 m. Lokale Technologien werden für den Datenaustausch zwischen der Telematikbox und stationär montierten Geräten sowie mobilen Geräten genutzt. Stationär montierte Geräte werden zur laufenden, automatischen Erfassung von Daten eingesetzt. Mobile, tragbare Geräte werden von Personen für die Überprüfung und Konfiguration eines Containers vor Ort benutzt. Abschnitt 2.4 liefert detaillierte Informationen über den Aufbau verschiedener Überwachungssysteme.

2.2 Globale Kommunikation

In Systemen zur drahtlosen Überwachung und Verfolgung von Transportcontainern werden Container mit Telematikboxen ausgestattet. Diese Boxen verfügen über globale und/oder lokale Kommunikationseinrichtungen. Die globale Kommunikationsinfrastruktur wird für den Datenaustausch mit dem Leitstand, Datenbanken und Servern im Internet sowie anderen entfernten informationstechnischen Einrichtungen benötigt. Aktuelle Überwachungssysteme verwenden dabei zelluläre Mobilfunknetze oder Satellitennetzwerke.

2.2.1 GSM

GSM wurde mit dem Ziel entwickelt, ein digitales europäisches Mobilfunknetz zu etablieren, das länderübergreifend nutzbar ist. Die Anfänge von GSM liegen bei einer Arbeitsgruppe (Groupe Spéciale Mobile) innerhalb der CEPT (European Conference of Postal and Telecommunications Administrations) [3]. Im Jahr 1989 wurde die Standardisierung vom ETSI (European Telecommunications Standards Institute) [4] übernommen. Seit diesem Zeitpunkt steht GSM für „Global

System for Mobile Communications“ [MS01]. Mittlerweile hat sich der GSM-Standard nicht nur in Europa verbreitet, sondern weltweit durchgesetzt. Terrestrische GSM-Netze decken bereits mehr als 80% der heutigen Weltbevölkerung ab. Weltweit gibt es 3,5 Milliarden GSM-Nutzer, die auf 1050 Netzwerke in 220 Ländern und Regionen verteilt sind [2]. GSM ohne Erweiterungen ermöglicht mobile Sprachkommunikation und leitungsgebundene Datenkommunikation mit einer maximalen Datenrate von 9,6 kBit/s. Darüber hinaus wird ein Dienst zur Übertragung von Kurznachrichten (Short Message Service - SMS) angeboten. GSM zählt zur zweiten Generation von Mobilfunkstandards.

Nach dem GSM-Standard setzt sich ein Mobilfunknetz aus unterschiedlichen Komponenten zusammen (siehe Abbildung 2.1). Das Mobilfunknetz ist dabei aus sich überlappenden Funkzellen aufgebaut. Dadurch können in Summe große Areale abgedeckt werden. Eine Zelle kann einen Bereich mit einem Radius von bis zu 35 km umfassen. Da die Anzahl der gleichzeitig nutzbaren Endgeräte je Zelle beschränkt ist, sind die Abmessungen mancher Zellen, vor allem im städtischen Bereich, aber wesentlich kleiner [Sau08].

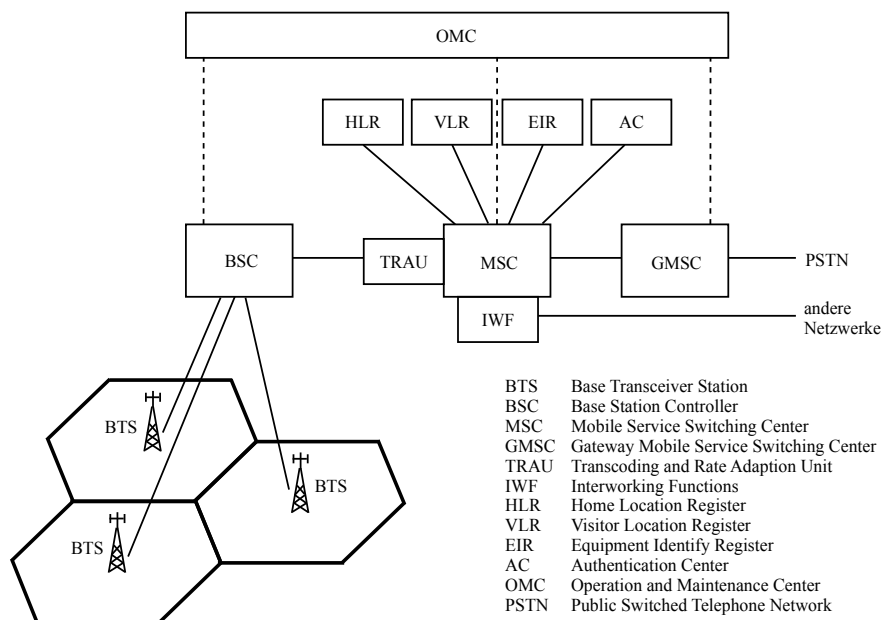


Abbildung 2.1: GSM-Architektur [MS01, Sau08, Sie03]

Mobile Endgeräte kommunizieren über Funk mit der Basisstation, auch Funkfeststation oder Base Transceiver Station (BTS) genannt. Das durch die BTS abgedeckte geographische Gebiet wird als Zelle bezeichnet. Um gegenseitigen Störungen mit Nachbarzellen vorzubeugen, werden benachbarten Zellen unterschiedliche Frequenzen zugewiesen. Infolgedessen sinkt die mögliche Anzahl an Sendefrequenzen je BTS. Um die Kapazität einer BTS besser zu nutzen, wird die Zelle in mehrere Sektoren unterteilt. Jeder Sektor wird von einer eigenen Empfangs- und Sendehardware versorgt. Meist wird eine Zelle in 2 oder 3 Sektoren unterteilt [Sau08].

Mehrere BTS werden von einer gemeinsamen Kontrolleinheit, dem Base Station Controller (BSC), verwaltet. Der BSC ist für die Überwachung und Aufrechterhaltung der Verbindungen in seinem Bereich verantwortlich. Darüber hinaus ist der BSC für das Handover beim Wechsel eines mobilen Endgerätes zwischen benachbarten Zellen (in seinem Bereich) zuständig. Der Anschluss an das

Kernnetzwerk erfolgt über die Transcoding and Rate Adaption Unit (TRAU). Diese Umwandlungseinheit ist für die Komprimierung und Dekomprimierung von Sprachdaten verantwortlich. Dabei werden die unterschiedlichen Übertragungsarten zwischen Luftschnittstelle und Kernnetzwerk angepasst. Die TRAU bietet unterschiedliche Methoden zur Sprachkomprimierung [Sau08].

Für die Kontrolle der Verbindungen sind Vermittlungsstellen, die Mobile Service Switching Center (MSC), zuständig. Darunter fallen Verbindungen zwischen Endgeräten im eigenen Netzwerk sowie zu Endgeräten in anderen Netzwerken. Die notwendigen Informationen bezieht ein MSC aus verschiedenen Datenbanken. Dazu zählen das Home Location Register (HLR), das Visitor Location Register (VLR), das Authentication Center (AC) und das Equipment Identify Register (EIR). Das HLR enthält Informationen über fest zugeordnete Benutzer. Darunter fallen die Rufnummer, Berechtigungen, Dienste und der momentane Aufenthaltsort des Teilnehmers. Als Schlüssel zu den Daten dient die International Mobile Subscriber Identity (IMSI). Diese weltweit eindeutige Kennung ist auf der SIM-Karte (Subscriber Identity Modul) des Teilnehmers und im HLR gespeichert. Ein Teilnehmer kann somit anhand der IMSI identifiziert und den Informationen im HLR zugeordnet werden. Durch die zentrale Ablage der teilnehmerspezifischen Informationen im HLR und die eindeutige Identifizierung durch die IMSI kann eine aufwändige Suche in den Datenbanken aller MSC entfallen. Jedem MSC ist zusätzlich ein VLR zugewiesen, das als lokale Ablage dient. Die Datenbank enthält Informationen über Benutzer, die sich aktuell im zugeordneten geographischen Bereich des MSC aufhalten. Diese Daten sind als temporäre Kopie der Originaldaten im HLR zu interpretieren. Die Daten werden, sobald ein Teilnehmer in den Zuständigkeitsbereich eines MSC wechselt, vom HLR kopiert und lokal abgelegt. Dadurch kann in Folge der Signalisierungs- und Kommunikationsaufwand verringert werden. Wenn der Teilnehmer den Bereich des MSC verlässt, werden die Einträge im VLR wieder gelöscht. Die Daten im VLR sind dynamisch und werden durch die Kommunikation des MSC mit den Endgeräten und dem HLR aktualisiert. Im EIR können eindeutige Gerätenummern abgelegt werden. Die Informationen ermöglichen den Ausschluss bestimmter Geräte vom GSM-Netz. Das AC ist wie das HLR eine zentrale Funktion. In dieser Datenbank ist für jeden Benutzer ein eigener Schlüssel abgelegt, der auch auf der SIM-Karte gespeichert ist. Der Schlüssel wird zur Authentifikation des Teilnehmers benötigt. Der Übergang vom MSC zu anderen Netzen erfolgt durch spezielle Übersetzungseinrichtungen, die Interworking Functions (IWF). Der Anschluss des Mobilfunknetzes an das Festnetz erfolgt über spezielle Gateway-Vermittlungsstellen, den Gateway Mobile Service Switching Center (GMSC). Alle Arbeiten für die Wartung und den Betrieb des Mobilfunknetzes werden von einer Verwaltungsstelle, dem Operation and Maintenance Center (OMC), geleistet. Detaillierte Informationen finden sich in [MS01, Sau08, Sie03].

Der Kurznachrichtendienst fordert eine weitere Einheit, das Short Message Service Center (SMSC). Das SMSC ist für die Weiterleitung und die Zwischenspeicherung von Kurznachrichten zuständig. Eine SMS-Nachricht wird vom Absender an das zuständige MSC gesendet und von dort zum SMSC weitergeleitet. Das SMSC bestätigt den Empfang, speichert die Nachricht und sucht im HLR nach dem derzeitigen Aufenthaltsort des Empfängers. Die Nachricht wird an das zuständige MSC weitergeleitet. Kann das entsprechende MSC die Nachricht dem Empfänger zustellen, erhält das SMSC eine Bestätigung und löscht die Nachricht. Ist der Empfänger nicht erreichbar, wird im VLR des zuständigen MSC und im HLR ein Flag gesetzt. Die Nachricht bleibt am SMSC gespeichert. Sobald der Empfänger wieder erreichbar ist, informiert das MSC aufgrund des gesetzten Flags das SMSC. Die Nachricht wird in Folge erneut zugestellt. Befindet sich der Empfänger bei der nächsten Aktivierung seines Endgeräts bereits im Bereich eines anderen MSC, werden die Teilnehmerinformationen aus dem HLR ins VLR des aktuell zuständigen MSC kopiert. Dadurch wird das Flag ebenfalls registriert und die Nachricht korrekt zugestellt [Sau08].

Der Übertragungsweg zwischen BTS und den Endgeräten wird als Luftschnittstelle bezeichnet. Es gibt länderabhängig teilweise verschiedene Trägerfrequenzen. Europäische GSM-Netze arbeiten auf 900 MHz und 1800 MHz. In Nordamerika wird auf 850 MHz und 1900 MHz kommuniziert. Um eine gleichzeitige Kommunikation mehrerer Teilnehmer mit der BTS zu ermöglichen, wird eine Kombination aus Frequency Division Multiple Access (FDMA) und Time Division Multiple Access (TDMA) angewendet (siehe Abbildung 2.2). Für den Uplink und den Downlink werden unterschiedliche Frequenzbänder verwendet, die in verschiedene Kanäle unterteilt sind. Jeder Kanal ist dabei nummeriert und hat einen Gegenpart im anderen Band. Die Frequenzkanäle sind in Zeitschlitz unterteilt, wobei ein TDMA-Rahmen 8 Zeitschlitz umfasst. Dadurch wird pro Trägerfrequenz 8 Teilnehmern ein gleichzeitiges Kommunizieren gestattet. Um die Auswirkung schmalbandiger Störungen zu verringern, kann während einer Verbindung periodisch die Frequenz gewechselt werden (Frequency Hopping). Die Nutzung dieser Option ist eine Entscheidung des Netzbetreibers. Als Modulationsverfahren wird Gaussian Minimum Shift Keying (GMSK) eingesetzt.

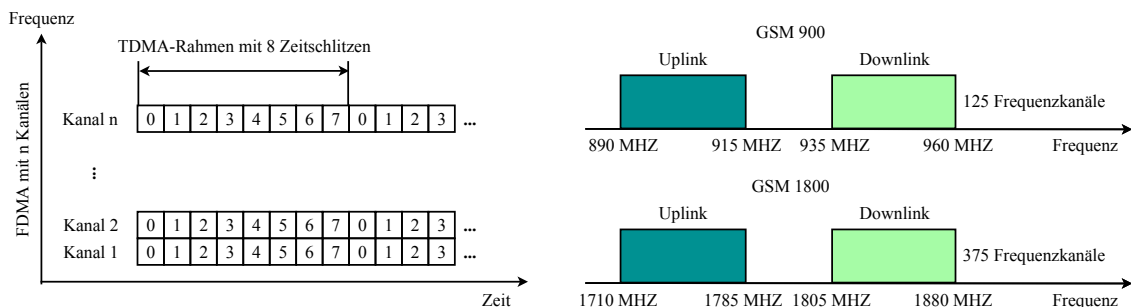


Abbildung 2.2: FDMA und TDMA im GSM-Standard [MS01, Sau08]

GSM wurde ursprünglich für die Übertragung von Sprachkommunikation konzipiert und optimiert. Darüber hinaus ermöglichen GSM-Netze leitungsgebundene Datenkommunikation, wobei ohne Erweiterungen eine maximale Datenrate von 9,6 kBit/s erreicht werden kann. Auf Kosten der Fehlerkorrektur kann die Datenrate teilweise auf 14,4 kBit/s gesteigert werden. Seit dem weltweiten Durchbruch des Internets spielt die Datenübertragung jedoch eine immer größere Rolle, was Erweiterungen und Anpassungen an den GSM-Netzen fordert. Um die Datenübertragungsraten zu steigern, wurden deshalb High Speed Circuit Switched Data (HSCSD), das General Packet Radio Service (GPRS) und Enhanced Data Rates for GSM Evolution (EDGE) eingeführt. HSCSD ermöglicht die Bündelung von bis zu 8 physikalischen Kanälen für die leitungsvermittelnde Datenübertragung. Dadurch sind nur geringe Änderungen, ausschließlich die Funkübertragung betreffend, erforderlich. Die Erweiterung kann somit als Softwareerweiterung betrachtet werden.

Die Einführung von GPRS fordert im Vergleich zu HSCSD neue Netzwerkkomponenten. Durch die infrastrukturelle Erweiterung des GSM-Netzwerks kann eine paketorientierte Datenübertragung angeboten werden. Alle Nutzer einer Mobilfunkzelle müssen sich dabei die Übertragungskapazität teilen. Leitungsvermittelnde und paketvermittelnde Kanäle können parallel genutzt werden, jedoch haben erstere gegenüber GPRS-Kanälen Vorrang. Die Erweiterungen in der Infrastruktur umfassen zusätzliche Komponenten für die Vermittlung und Anbindung von GPRS-Datenverkehr an andere paketvermittelnde Netze (siehe Abbildung 2.3). Der BSC ist Teil des leitungsvermittelnden GSM-Netzwerkes und ist deshalb nicht für GPRS geeignet. Aus diesem Grund wird eine neue Komponente, die Packet Control Unit (PCU), eingeführt. Diese Komponente ermöglicht den Einsatz der Funkfeststationen für GPRS. Die Anbindung an andere Netze wird durch spe-

zielle Gateways, die Gateway GPRS Support Nodes (GGSN), vollzogen. Sie sind somit für die Interoperabilität zu anderen paketvermittelnden Netzen, wie dem Internet, verantwortlich. Die Mobilität von GPRS-Endgeräten wird durch spezielle Vermittlungsknoten, die Serving GPRS Support Nodes (SGSN), ermöglicht. Ein SGSN übernimmt bei GPRS die Aufgabe eines MSC bei der leitungsvermittelnden Datenübertragung beziehungsweise der Sprachkommunikation [Sau08].

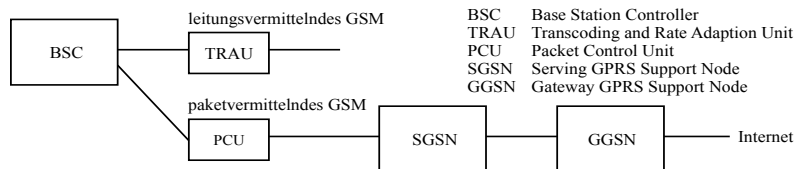


Abbildung 2.3: GPRS-Erweiterungen im GSM-Netzwerk [Sau08]

Um die Übertragungsrate der paketvermittelnden GPRS-Datenübertragung weiter zu steigern, wird mit EDGE ein neues Modulationsverfahren für die Luftschnittstelle eingeführt. Dabei wird die GMSK-Modulation durch das Modulationsverfahren 8-Phase Shift Keying (8PSK) ersetzt. Die Umstellung erfordert im Wesentlichen nur Änderungen in der Basisstation [MS01].

Die terrestrischen GSM-Netzwerke decken weltweit riesige Gebiete (mehr als 220 Länder) ab. Durch Roaming-Abkommen zwischen den Netzbetreibern kann somit eine flexible, mobile und globale Kommunikation ermöglicht werden. Aus diesem Grund wird die Kommunikation über GSM unter anderem für die drahtlose Verfolgung und Überwachung von Containern oder Objekten eingesetzt (siehe Abschnitt 2.4). GPRS und EDGE ermöglichen den Datenaustausch zwischen den mobilen Komponenten und Servern oder Datenbanken im Internet. Die mobilen Komponenten werden dazu mit GSM-Modulen, wie dem GPRS-M2M-Modul von SAGEM [Sag09], ausgerüstet. Dieses Modul, das auch im WCMS-Projekt auf der MTU und optional am EGW zum Einsatz kommt, weist Abmessungen von nur 27 mm x 27 mm x 3,6 mm auf. Es ist für den Einsatz auf 850/900/1800/1900 MHz geeignet und unterstützt GPRS. Mit dem Modul werden über GPRS Datenraten von bis zu 85,6 kBit/s im Download und 42,8 kBit/s im Upload erreicht. Darüber hinaus wird auch das Versenden von SMS-Nachrichten ermöglicht. Die technische Entwicklung führt dazu, dass zukünftig alltägliche Objekte mit kleinen preiswerten Kommunikationsmodulen ausgestattet werden können.

2.2.2 UMTS

Der nächste Evolutionsschritt nach GSM und GPRS ist die Einführung vom Universal Mobile Telecommunications System (UMTS). UMTS zählt zur dritten Generation von Mobilfunkstandards. Der Übergang von GSM zu UMTS erfolgt dabei in Schritten, so genannten Releases. Für die Festlegung der einzelnen Releases ist das Standardisierungsgremium 3rd Generation Partnership Project (3GPP) [5] zuständig. Die Releases wurden anfangs nach der Jahreszahl bezeichnet, bekamen später aber eine laufende Nummer. Im Gegensatz zu GSM wurde bei der Spezifikation von UMTS von Beginn an der Datenverkehr berücksichtigt. Die ständige Steigerung von Prozessor- und Speicherkapazitäten seit Inbetriebnahme der ersten GSM-Netzwerke ermöglicht bei UMTS eine Verbesserung der Übertragung durch den Einsatz von komplexeren und rechenintensiveren Verfahren [Sau08].

Release 99 enthält die Spezifikation für die erste Ausbaustufe von UMTS (siehe Abbildung 2.4). Dabei wird ein neues Zugangnetzwerk mit der Bezeichnung UMTS Terrestrial Radio Network

(UTRAN) eingeführt. Das bei GSM eingesetzte Zeit- und Frequenzmultiplexverfahren (siehe Abschnitt 2.2.1) wird durch das Codemultiplexverfahren Wideband Code Division Multiple Access (WCDMA) ersetzt. Dadurch kann die Übertragungsrates im Vergleich zu GSM/GPRS gesteigert werden. Das Konzept der Funkfeststationen und Kontrollenheiten wird von GSM übernommen, wobei UMTS die Bezeichnung BTS durch Node-B und BSC durch RNC (Radio Network Controller) ersetzt. Das leitungsvermittelnde und paketvermittelnde Kernnetzwerk von GSM/GPRS wird in Release 99 bis auf Softwareänderungen übernommen. Dadurch kann die Einführung von UMTS gleichzeitig neben dem laufenden Betrieb eines GSM/GPRS-Netzwerkes erfolgen. Die Abdeckung des vorhandenen GSM-Netzwerkes bleibt somit erhalten. Die Vorteile von UMTS können jedoch nur in den bereits ausgebauten Regionen genutzt werden. Das Hauptziel von Release 99 ist die Einführung von schnellen Paketdatendiensten [Sau08].

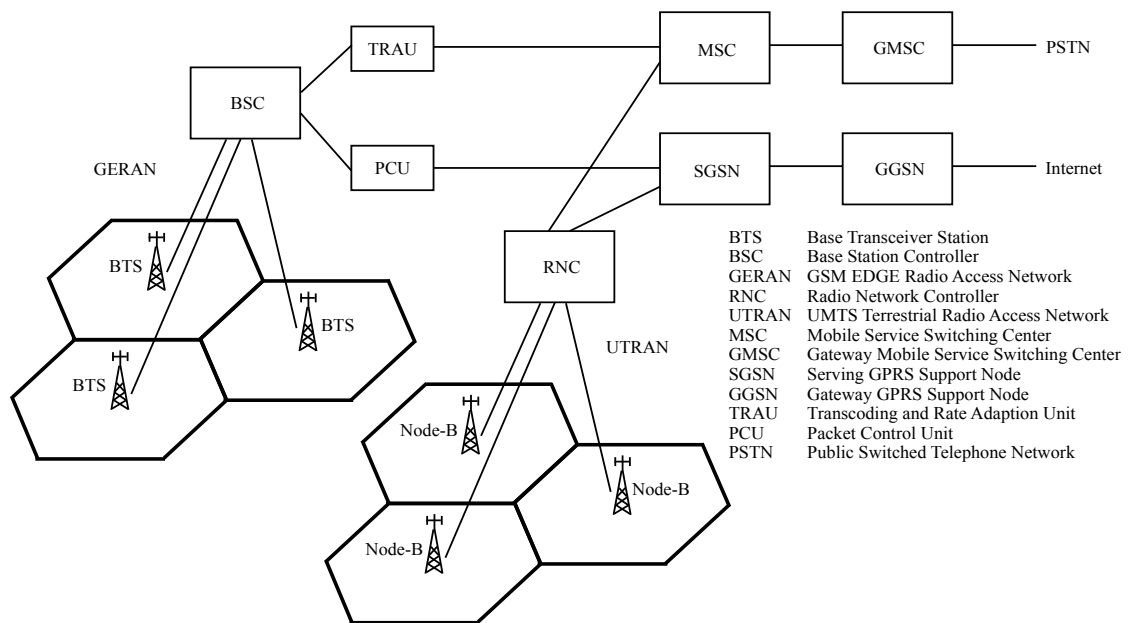


Abbildung 2.4: UMTS-Architektur nach Release 99 [Sau08]

Das UMTS-Zugangnetzwerk nach Release 99 arbeitet auf verschiedenen Trägerfrequenzen (siehe Abbildung 2.5). Diese sind wie bei GSM länderspezifisch. Um die gleichzeitige Kommunikation zwischen Node-B und mehreren Endgeräten zu ermöglichen, wird WCDMA [GG04] eingesetzt. Bei diesem Verfahren arbeiten alle Teilnehmer auf der gleichen Frequenz. Die Trennung der Kanäle wird durch individuelle Codes erreicht, während im GSM-System unterschiedliche Frequenzen und Zeitschlitze eingesetzt werden (siehe Abbildung 2.2). Um das gleichzeitige Senden vom Node-B und den Endgeräten zu ermöglichen, werden zwei Betriebsarten definiert, der FDD-Betrieb (Frequency Division Duplex) und der TDD-Betrieb (Time Division Duplex). Im FDD-Betrieb werden wie bei GSM zwei unterschiedliche Frequenzbänder für den Uplink und den Downlink eingesetzt. Dabei wird für die Verbindung vom Endgerät zum Node-B sowie für die Verbindung vom Node-B zum Endgerät eine unterschiedliche Frequenz benutzt. Im TDD-Betrieb verwenden Uplink und Downlink die gleichen Frequenzen. Endgeräte und Node-B senden dabei auf der gleichen Frequenz, aber zu unterschiedlichen Zeiten. Dazu wird der Frequenzkanal in Zeitschlitze unterteilt, die auf Uplink und Downlink aufgeteilt werden. Jeder Zeitschlitz ist durch WCDMA in verschiedene Funkkanäle unterteilt. Dabei kann eine asymmetrische Aufteilung der Übertragungskapazität auf Uplink und Downlink erfolgen.

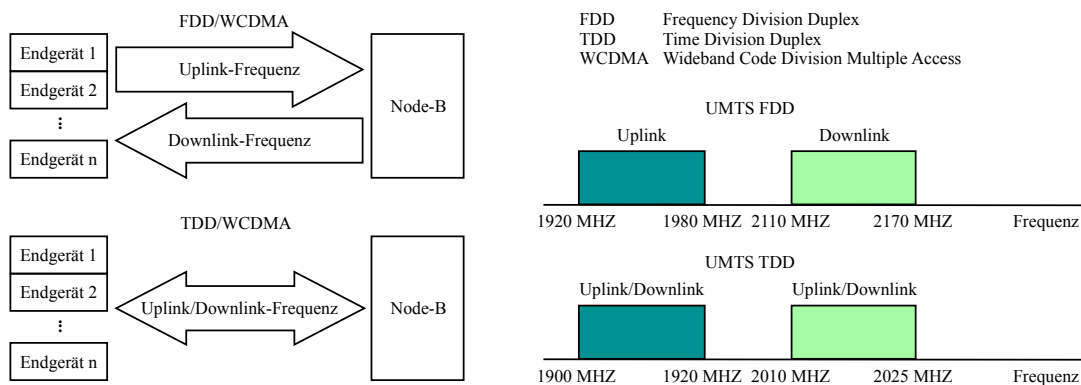


Abbildung 2.5: FDD und TDD im UMTS-Funkzugangsnetzwerk nach Release 99 [5]

Release 4 legt die Basis für die Zusammenführung der Übertragung von Sprach- und Datendiensten. Das Ziel ist die Verschmelzung des leitungsvermittelnden und des paketvermittelnden Kernnetzwerks. Durch die Neuerungen in Release 4 können leitungsvermittelnde Dienste im Kernnetzwerk in IP-Paketen übertragen werden. Mit Release 5 wird ein weiterer Schritt in Richtung eines auf IP basierenden Netzwerks gemacht. Ab diesem Release können Sprachverbindungen nicht mehr nur im Kernnetzwerk, sondern von Endgerät zu Endgerät über IP transportiert werden. Release 5, 6 und 7 führen ein neues Übertragungsverfahren im Funknetzwerk ein. Für die Übertragung vom Endgerät zum Node-B wird High Speed Uplink Packet Access (HSUPA) eingesetzt, während für die Übertragung vom Node-B zum Endgerät High Speed Downlink Packet Access (HSDPA) angewendet wird. Dabei können laut [Sau08] Übertragungsraten von mehreren MBit/s erreicht werden. Weitere Optimierungen und Erweiterungen im UMTS-Netzwerk werden vom 3GPP laufend in Releases definiert. Die aktuellste Version ist derzeit Release 10.

In Systemen zur Überwachung von Containern sind Kommunikationsmodule, die UMTS unterstützen, noch wenig verbreitet (siehe Abschnitt 2.4). Hauptgrund ist wahrscheinlich die derzeit noch geringere globale Abdeckung als bei GSM-Netzwerken. Sobald der Ausbau der UMTS-Netzwerke aber weiter fortgeschritten ist, werden die Vorteile, die diese Technologie bietet, auch zum Einsatz in der Containerüberwachung führen.

2.2.3 GPS

Das Global Positioning System (GPS) ist ein satellitengestütztes System zur drahtlosen, globalen Positionsbestimmung [6, TVS07]. Das System wird in drei Segmente unterteilt, das Space-Segment, das Control-Segment und das User-Segment. Das Space-Segment umfasst 24 Satelliten, wobei jeder Satellit in einer Entfernung von rund 20000 m die Erde innerhalb von 12 Stunden einmal umkreist. Das GPS-Projekt wurde bereits 1978 gestartet. Im Jahr 1994 wurde das primäre System durch Positionierung des 24. Satelliten einsatzbereit. Ein Satellit ist mit bis zu 4 Atomuhren ausgestattet, sodass globale Positionierungs-, Navigations- und Zeitdienste angeboten werden können. Das Control-Segment besteht aus mehreren Kontroll- und Überwachungsstationen. Diese Einrichtungen sind für Bahnkorrekturen der Satelliten verantwortlich und sorgen dafür, dass die Satelliten auf den vorgesehenen Umlaufbahnen bleiben. Darüber hinaus liegt die laufende Nachstellung und Kalibrierung der Atomuhren auf den Satelliten in ihrem Zuständigkeitsbereich. Das

User-Segment umfasst die GPS-Empfänger. GPS-Empfänger empfangen Daten von den GPS-Satelliten und ermitteln daraus die dreidimensionale Position und die Uhrzeit. Manche GPS-Receiver unterstützen auch die Berechnung der aktuellen Geschwindigkeit und der Bewegungsrichtung.

GPS wurde ursprünglich von den USA für militärische Zwecke entwickelt, ist aber mittlerweile auch für zivile Anwendungen weltweit frei nutzbar. Die angebotenen Dienste sind für zivile Nutzungen jedoch beschränkt. Die volle Leistungsfähigkeit von GPS ist weiterhin dem US-Militär und US-Regierungsbehörden vorbehalten. Trotzdem wird GPS weltweit für die Navigation im Luft-, Schiff- und Straßenverkehr eingesetzt.

GPS-Satelliten senden kontinuierlich ihre aktuelle Position, wobei die Nachrichten mit einem lokalen Zeitstempel versehen werden. Diese Nachrichten können von GPS-Empfängern empfangen werden. Die Bestimmung der Position anhand der empfangenen GPS-Daten erfolgt durch Triangulation. Für die exakte Bestimmung müssen die Distanzen zwischen dem GPS-Receiver und mindestens 4 Satelliten bekannt sein. Die Ermittlung der Distanzen erfolgt durch Laufzeitmessung. Es werden 4 Satelliten benötigt, da neben den 3 unbekannt Koordinaten noch die Abweichung der Empfängeruhr von den Satellitenuhren als zusätzliche Unbekannte in das Gleichungssystem eingeht [YT06, TVS07]. Die empfangene Zeitinformation kann von den GPS-Empfängern zur Synchronisierung von verteilten Systemen genutzt werden [TVS07].

Der technologische Fortschritt und die Miniaturisierung in der Elektronik ermöglichen, dass derzeit bereits preiswerte GPS-Empfänger, wie das UC322 OEM GPS Receiver Module von Fastrax [Fas08], erhältlich sind. Dieses Modul ermöglicht eine globale Positionsbestimmung und Zeitalisierung. Das Modul weist Abmessungen von lediglich 10,4 mm x 30,0 mm x 2,9 mm auf, wobei die Antenne bereits integriert ist. Die kleinen Bauformen aktueller GPS-Empfänger eignen sich daher für den Einsatz in Überwachungs- und Verfolgungssystemen für Objekte wie Container. Wie in Abschnitt 2.4 gezeigt wird, setzen aktuell am Markt erhältliche Produkte zur drahtlosen Containerüberwachung vorwiegend GPS zur Positionsbestimmung ein.

2.3 Lokale Kommunikation

In Systemen zur drahtlosen Überwachung und Verfolgung von Transportcontainern werden Container mit Telematikboxen ausgestattet. Diese Boxen verfügen über globale und/oder lokale Kommunikationseinrichtungen. Die lokale Kommunikationsinfrastruktur wird für den Datenaustausch mit stationären oder mobilen Einheiten im Umkreis von bis zu einigen 100 m eingesetzt. Aufgrund der meist beschränkten Energieressourcen am Container steht ein niedriger Energieverbrauch im Vordergrund. Zwei Technologien zur lokalen Kommunikation, die in den letzten Jahren an Bedeutung und allgemeiner Bekanntheit gewonnen haben, sind ZigBee und RFID.

2.3.1 ZigBee

ZigBee ist eine Funktechnologie für die Datenübertragung über kurze Distanzen (bis 100 m). Die Technologie zeichnet sich durch eine einfache Architektur und geringen Energieverbrauch aus. Die Datenübertragungsrate ist mit maximal 250 kBit/s gering. Durch den niedrigen Energieverbrauch können batteriegespeiste Funkknoten mit einer Betriebsdauer von Monaten bis Jahren hergestellt werden [PFGM08]. ZigBee ermöglicht dabei kleine und billige Bauformen der Kommunikationsmodule. Zu den Anwendungsgebieten von ZigBee zählen vorwiegend die Heim- und

Gebäudeautomation sowie industrielle Steuerungs- und Überwachungsaufgaben. Die Funktechnologie dient auch der Realisierung drahtloser Sensornetzwerke und Personal Area Networks (PAN). Im Vergleich mit Bluetooth hat ZigBee eine geringere Übertragungsrate, einen niedrigeren Energieverbrauch und eine größere Reichweite. Darüber hinaus kann die Funktionalität nach Aufwachen aus einem Energiesparmodus schneller wieder hergestellt werden [Sch08]. ZigBee ermöglicht den automatischen und dynamischen Aufbau von Netzwerken mit mehreren 100 Knoten. Daten werden von Knoten zu Knoten weitergereicht, bis sie am Empfänger eintreffen. Der Zickzack-Kurs, den die Daten zurücklegen, zeigt Ähnlichkeit mit dem Flug einer Biene, wodurch der Name der Technologie abgeleitet wurde [Dem07].

In Anlehnung an das OSI-Referenzmodell (Open Systems Interconnection) baut der ZigBee-Protokollstapel (siehe Abbildung 2.6) auf dem IEEE 802.15.4-Standard auf. Der IEEE 802.15.4-Standard definiert die Bitübertragungsschicht sowie die Mediumzugriffsschicht für drahtlose PAN mit niedriger Datenrate. Die Schichten darüber werden von der ZigBee-Allianz definiert. Die ZigBee-Allianz ist ein Zusammenschluss von Firmen, die gemeinsam einen offenen Standard für drahtlose Überwachungs- und Steuersysteme entwickeln. Eine Auflistung aller aktuellen Mitglieder findet sich unter [7]. Die ZigBee-Allianz unterstützt die Realisierung von preisgünstigen, drahtlos vernetzbaren Produkten mit niedrigem Energieverbrauch. Dadurch soll der Einbau von drahtloser Kommunikationstechnik in alltägliche Produkte ermöglicht werden. Die ZigBee-Allianz ist verantwortlich für die Definition der Netzwerkschicht sowie der Anwendungsschicht. Darüber hinaus erstellt die ZigBee-Allianz Spezifikationen für Interoperabilitäts- und Konformitätstests. Zu den weiteren Aufgaben zählen die weltweite Bekanntmachung von ZigBee, die Aufmerksamkeit neuer Märkte zu gewinnen und die Leitung der zukünftigen Weiterentwicklung der Technologie [7].

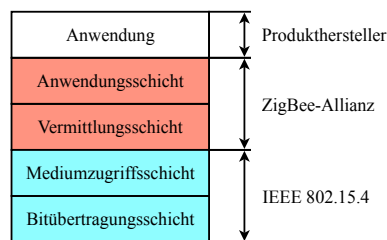


Abbildung 2.6: ZigBee-Protokollstapel [LLF07]

ZigBee nutzt verschiedene Frequenzbereiche (siehe Tabelle 2.2), wobei die maximale Datenrate bei 250 kBit/s liegt. Es stehen insgesamt 27 Kanäle zur Verfügung. Bei Nutzung des 2,4 GHz Frequenzbandes kann es zu Störungen mit Bluetooth und WLAN kommen. Zur Reduzierung der Störungen wird das Frequenzspreizverfahren Direct Sequence Spread Spectrum (DSSS) eingesetzt. Das zu übertragende Signal wird dabei auf einen größeren Frequenzbereich verteilt. Die im Normalfall schmalbandigen Störsignale wirken sich in Folge nicht mehr so stark aus [GG04]. ZigBee zeigt dadurch eine höhere Robustheit als vergleichbare Technologien.

Zur Regelung des Mediumzugriffs wird Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) angewendet. Dabei überprüft jedes Gerät, bevor es sendet, ob der Kanal belegt ist. Nur bei einem freien Kanal, beginnt das Gerät zu senden. Da ZigBee auf dem IEEE 802.15.4-Standard aufbaut, kann durch die dort definierte Superframe-Struktur Slotted- und Unslotted-CSMA/CA angewendet werden. Beim Unslotted-CSMA/CA wird kein Beacon-Paket vom Koordinator ausgesendet. Alle Geräte können zu jeder Zeit versuchen, unter Beachtung von CSMA/CA, zu senden. Dabei wartet ein Gerät eine zufällige Zeit, bevor es den Kanal abhört. Ist der Kanal

Tabelle 2.2: Trägerfrequenzen von ZigBee [GG04]

Frequenz	Abdeckung	Bitrate	Kanäle	Kanalabstand
2,4 GHz	weltweit	250 kBit/s	16	5 MHz
868 MHz	Europa	20 kBit/s	1	-
915 MHz	Amerika	40 kBit/s	10	2 MHz

frei, wird gesendet. Im Fall, dass gerade ein anderes Gerät sendet, wird eine weitere zufällige Zeit gewartet und der Kanal erneut abgehört. Beim Slotted-CSMA/CA [KAT06] werden periodisch Beacon-Pakete vom Koordinator ausgesendet. Das Beacon wird dazu genutzt, das Netzwerk zu identifizieren und andere Knoten zu synchronisieren. Das Zeitintervall zwischen zwei Beacons (siehe Abbildung 2.7) unterteilt sich dabei in eine aktive und optional eine inaktive Zone. In der aktiven Zone findet die Kommunikation zwischen den Knoten statt, während die inaktive Zone zur Schonung der Energieressourcen genutzt werden kann. Die Knoten dürfen in dieser Zeit in einen Schlafmodus wechseln. Die aktive Zone wird in 16 gleichbreite Zeitschlitze unterteilt, wobei Zeitschlitz 0 für das Beacon reserviert ist. In der aktiven Zone konkurrieren alle Knoten im Sinne von CSMA/CA um das Senderecht. Dabei besteht die Möglichkeit, Zeitschlitze für bestimmte Knoten zu reservieren. Dazu kann die aktive Zone optional in eine Periode mit und ohne konkurrierendem Zugriff unterteilt werden. Im Gegensatz zur Periode mit konkurrierendem Zugriff (Contention Access Periode - CAP) können in der Periode ohne konkurrierendem Zugriff (Contention Free Periode - CFP) Zeitschlitze reserviert werden. In diesen besetzten Zeitschlitzen (Guaranteed Time Slots - GTS) darf nur der Besitzer des Zeitschlitzes senden. Die Reservierung von Zeitschlitzen kann dazu genutzt werden, rundenbasiert bestimmte Knoten ohne Konflikte abzufragen. Die Reservierung gilt jedoch nur für das betrachtete Netzwerk. Andere Netzwerke in der Umgebung können den Funkverkehr innerhalb eines reservierten Zeitschlitzes weiterhin stören. Der IEEE 802.15.4-Standard definiert darüber hinaus 4 Rahmentypen für die Mediumzugriffsschicht: Beacon-Rahmen, Acknowledge-Rahmen, Datenrahmen und Kommandorahmen. Für nähere Informationen sei auf den IEEE-Standard verwiesen.

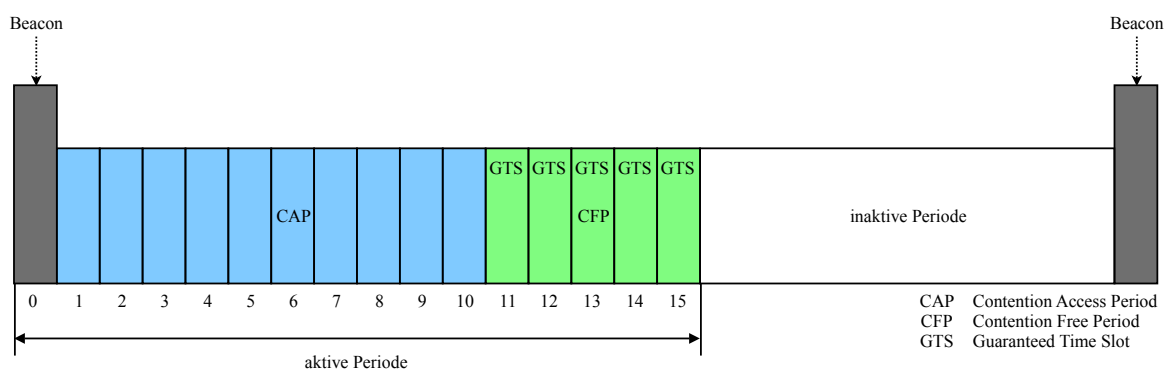


Abbildung 2.7: Superframe-Struktur nach IEEE 802.15.4 [KAT06]

ZigBee definiert drei Gerätetypen: Koordinator, Router (Full Function Device) und Endgerät (Reduced Function Device). Endgeräte implementieren nur einen Teil des ZigBee-Protokolls. Diese Geräte kommunizieren mit Routern, besitzen selbst jedoch keine Routingkapazitäten. Dadurch weisen Endgeräte den geringsten Energieverbrauch auf. Als Router werden Geräte bezeichnet,

die Routingaufgaben übernehmen, gleichzeitig aber auch als Endgerät fungieren können. Da der Empfänger für Routingaufgaben ständig aktiviert ist, verbrauchen diese Knoten mehr Energie als reine Endgeräte. Ein Router im Netzwerk übernimmt die Rolle des Koordinators. In einem ZigBee-Netzwerk gibt es genau einen Koordinator, der das Netzwerk aufbaut und verwaltet. Da der Koordinator Informationen über die anderen Geräte im Netzwerk lokal speichern muss, benötigt er mehr Speicher- und Prozessorkapazitäten. Zusätzlich weist der Koordinator einen höheren Energiebedarf auf [PFGM08, LLF07].

Mit ZigBee können verschiedene Netzwerktopologien realisiert werden: Stern, Cluster-Baum und vermaschte Netzwerke. Bei der Sterntopologie kann ein Koordinator aufgrund der 16 Bit breiten Netzwerkadressen theoretisch bis zu 65536 Endgeräte erfassen. Es findet dabei keine direkte Kommunikation zwischen zwei Endgeräten statt. Alle Knoten kommunizieren stets mit oder über den Koordinator. Der Koordinator wird bei der Sterntopologie meistens extern versorgt, während die restlichen Knoten batteriebetrieben sind. Beim Cluster-Baum muss eine Nachricht eventuell über mehrere Knoten weitergegeben werden, wodurch Verzögerungen entstehen können. Es können jedoch größere Areale abgedeckt werden, wobei der Koordinator nicht an jeder Kommunikation beteiligt sein muss. Ein vermaschtes Netz bietet verschiedene Wege vom Sender zum Empfänger, wodurch die Robustheit der Kommunikation erhöht wird. Bei Ausfall eines Knotens kann durch entsprechende Routingalgorithmen ein alternativer Weg gefunden werden. Es können dadurch selbstkonfigurierende und selbstheilende Netzwerke gebildet werden [LLF07].

2.3.2 RFID

Die Abkürzung RFID (Radio Frequency Identification) bezeichnet eine Technologie zur automatischen Identifikation von Objekten. Dabei wird im Allgemeinen eine Seriennummer auf einem so genannten RFID-Transponder (RFID-Tag) gespeichert. Die gespeicherte Information (Seriennummer, ID) kann von RFID-Lesegeräten über Funk ausgelesen werden. Die Vorteile der RFID-Technologie gegenüber anderen Identifikationsmöglichkeiten, wie zum Beispiel Barcodes, liegen in der Möglichkeit gleichzeitig mehrere Transponder erfassen zu können (Pulkerfassung), wobei keine Sichtverbindung notwendig ist. Dadurch muss der Transponder nicht an der Oberfläche des Trägerobjekts befestigt werden, sondern kann in Objekte eingebettet beziehungsweise eingegossen werden. Die Umhüllung ermöglicht den Einsatz der Transponder auch unter extremen Umweltbedingungen wie Hitze oder Schmutz [FM05].

Die wesentlichen Komponenten eines RFID-Systems sind RFID-Transponder, Lesegeräte und ein Rechner zur Verarbeitung der Daten. RFID-Transponder bestehen im einfachsten Fall aus einem Mikrocontroller und der Kopplungseinheit zur Kommunikation. Dabei gibt es eine Vielzahl an unterschiedlichen Bauformen, wie zum Beispiel RFID-Transponder im Chipkartenformat oder aufgedruckt auf Klebefolien. Die Transponder können mit stationären oder mobilen Lesegeräten ausgelesen werden. Bei mobilen Geräten ist der Rechner mit dem Lesegerät in einem Gehäuse integriert. Stationäre Lesegeräte sind mit einem externen Rechner verbunden, wobei der Rechner wiederum mit einer Datenbank oder Applikationen auf anderen Rechnern kommunizieren kann. Nur bei weniger umfangreichen Anwendungen wird ein isolierter Rechner zum Einsatz kommen. Der Rechner kann Kommandos an das Lesegerät senden und ausgelesene Daten empfangen. Manche Transponder unterstützen auch das Schreiben von Daten über das Lesegerät. Für die Übertragung an einen Transponder moduliert das Lesegerät Kommandos und Daten vom Rechner auf ein magnetisches beziehungsweise elektromagnetisches Wechselfeld [FM05].

Zum Betrieb des Mikrocontrollers und zur Kommunikation mit dem Lesegerät benötigt ein RFID-Transponder Energie. In [FM05] werden Transponder anhand der Energiequellen klassifiziert, wobei zwischen passiven, semiaktiven und aktiven Transpondern unterschieden wird. Passive Transponder beziehen die gesamte benötigte Energie aus dem Feld des Lesegeräts. Semiaktive Transponder versorgen den Mikrocontroller über eine integrierte Batterie und nutzen die Feldenergie des Lesegeräts nur für die Kommunikation. Aktive Transponder beziehen die gesamte benötigte Energie aus einer integrierten Batterie.

Die meisten RFID-Systeme arbeiten mit Frequenzen in den lizenzfreien ISM-Bändern¹. Ausnahmen bilden Systeme, die um 135 kHz und 900 MHz herum kommunizieren. Laut [FM05] lassen sich folgende typische Frequenzbereiche für RFID-Systeme angeben:

- 100 kHz bis 135 kHz (Niederfrequenz)
- 13,56 MHz (Hochfrequenz)
- 868 MHz Europa, 915 MHz USA (Ultrahochfrequenz)
- 2,45 GHz und 5,8 GHz (Mikrowelle)

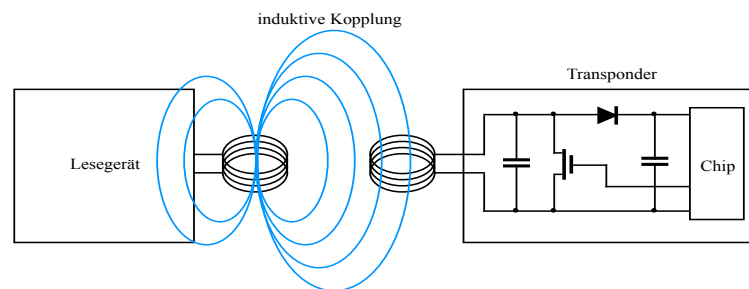


Abbildung 2.8: RFID-System mit induktiver Kopplung [FM05]

Die Energie- und Datenübertragung zwischen Lesegerät und RFID-Transponder kann durch induktive oder elektromagnetische Kopplung erfolgen. Systeme die mit 135 kHz oder 13,56 MHz arbeiten, basieren auf der induktiven Kopplung (siehe Abbildung 2.8). Das Lesegerät erzeugt über eine Spule ein magnetisches Wechselfeld, auf dem die Daten moduliert werden. Das magnetische Wechselfeld induziert eine Wechselspannung in die Spule des RFID-Transponders. Nach Gleichrichtung der induzierten Spannung wird damit ein Kondensator geladen, über den der Mikrocontroller auf passiven Transpondern versorgt werden kann. Um die induzierte Spannung zu erhöhen, ist der Spule am Transponder üblicherweise ein Kondensator parallel geschaltet. Dieser Parallelschwingkreis wird für eine Resonanzfrequenz ausgelegt, die der Sendefrequenz des Lesegeräts entspricht. Bei Resonanz kann somit eine höhere induzierte Spannung erreicht werden. Das führt zu einer größeren Reichweite. Die induktive Kopplung funktioniert jedoch nur im so genannten Nahfeld, wodurch die maximale theoretische Reichweite durch die Grenze des Nahfeldes beschränkt wird. Die Realität zeigt jedoch, dass die induzierte Spannung an den Grenzen des Nahfeldes nicht mehr ausreicht, um den Mikrocontroller auf passiven Transpondern zu versorgen. Die Grenze zwischen Nah- und Fernfeld einer Antennenspule kann in einer Näherung

¹Als ISM-Bänder (Industrial Scientific Medical) werden Frequenzbereiche bezeichnet, die in Industrie, Wissenschaft, Medizin und im häuslichen Bereich lizenzfrei genutzt werden können.

nach Formel 2.1 berechnet werden, wobei c die Lichtgeschwindigkeit und f die Trägerfrequenz ist. Zur Übertragung von Daten zum Lesegerät wird Lastmodulation eingesetzt. Über den digitalen Datenstrom wird dabei ein Lastwiderstand ein- und ausgeschaltet. Der Lastwiderstand liegt parallel zur Spule des Transponders und verändert dadurch die Induktivität. Am Lesegerät werden die Änderungen der Gegeninduktivität als Spannungsänderungen erkannt. Dadurch kann das übertragene Signal ermittelt und weiterverarbeitet werden.

$$d = \frac{c}{2\pi f} \quad (2.1)$$

Systeme die mit 868 MHz, 915 MHz, 2,45 GHz und 5,8 GHz arbeiten, nutzen das Prinzip der elektromagnetischen Kopplung (siehe Abbildung 2.9). Das Lesegerät und der Transponder benötigen dafür Antennen. Die Antenne des Lesegeräts erzeugt eine elektromagnetische Welle, die sich im Raum ausbreitet und in der Antenne des Transponders eine Wechselspannung induziert. Die induzierte Spannung wird gleichgerichtet und bei passiven Systemen über einen Kondensator zur Versorgung des Mikrocontrollers genutzt. Die Reichweite hängt unter anderem von der Sendeleistung am Lesegerät ab. Die zugelassene Sendeleistung ist jedoch abhängig von den verwendeten Frequenzbereichen gesetzlich beschränkt. Passive Systeme können eine Reichweite von bis zu 3 m erzielen. Semiaktive Transponder erzielen eine Reichweite von bis zu 15 m und aktive Transponder von bis zu 100 m [FM05]. Zur Übertragung von Daten zum Lesegerät wird, wie bei der induktiven Kopplung, ein Lastwiderstand in Abhängigkeit vom zu übertragenden digitalen Datensignal ein- oder ausgeschaltet. Dadurch werden bei elektromagnetischer Kopplung die Eigenschaften der Antenne und somit die reflektierte elektromagnetische Welle verändert. Das Lesegerät empfängt die reflektierte Welle und kann aus den Änderungen die Daten ermitteln und weiterverarbeiten.

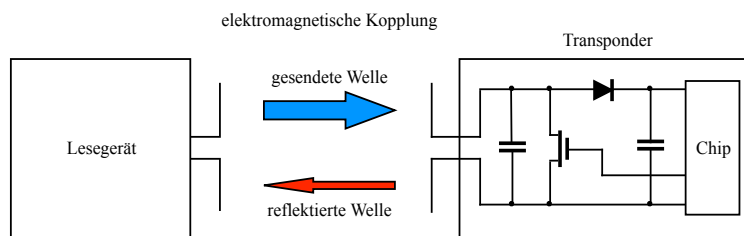


Abbildung 2.9: RFID-System mit elektromagnetischer Kopplung [FM05]

Die Speicherung zusätzlicher Informationen über ein Objekt, das mit einem RFID-Tag ausgestattet ist, kann in einer Datenbank oder lokal am RFID-Tag erfolgen. Im einfachsten Fall werden einmalig Daten, zum Beispiel eine Seriennummer, auf dem RFID-Transponder gespeichert und in Folge nur mehr ausgelesen. Die ausgelesene ID oder Seriennummer dient nicht nur zur reinen Identifikation, sondern ist oft gleichzeitig eine Referenz auf weitere Daten in einer Datenbank. RFID-Transponder, die einen zusätzlichen Datenspeicher besitzen, können relevante Informationen lokal speichern, sodass der Zugriff auf eine Datenbank entfallen kann. Dabei gibt es Transponder, die über das Lesegerät sowohl gelesen, als auch beschrieben werden können. Ein Schreibzugriff benötigt im Normalfall jedoch mehr Energie, was bei passiven Systemen zu einer Verminderung der erzielbaren Reichweite führt [FM05].

Die Kosten für passive RFID-Tags, die nur eine Seriennummer speichern, liegen im Zig-Cent-Bereich [FM05]. Diese preiswerten Transponder ermöglichen den Einsatz der RFID-Technologie

für alltägliche Produkte und Massenwaren. In logistischen und betriebswirtschaftlichen Prozessen gewinnt RFID daher immer mehr an Bedeutung. Waren können durch den Einsatz von RFID-Technologie auf dem Weg durch die innerbetriebliche Prozesskette verfolgt werden. Die gesammelten Daten ermöglichen eine Optimierung der betriebswirtschaftlichen Prozesse. RFID wird auch in der Lagerhaltung eingesetzt, wodurch eine lückenlose Erfassung des aktuellen Lagerstands erfolgen kann. Die automatische Erfassung des Lagerstands liefert stets aktuelle Daten und schließt Fehler, wie bei der manuellen Eingabe in Datenbanken aus. Daraus folgt, dass zum Beispiel Engpässe rechtzeitig erkannt werden können [Sch08].

Die zunehmenden Anwendungsbereiche und die Bekanntheit der RFID-Technologie fordern eine Regelung. Aus diesem Grund gibt es Standards und Normen, die die Kommunikation zwischen RFID-Transpondern und RFID-Lesegeräten verschiedener Hersteller gewährleisten sollen. Dabei werden unter anderem Trägerfrequenz, Kodierung, Timing, Modulationsverfahren, Datenübertragungsraten, Vielfachzugriffsverfahren (Pulkerfassung) und Befehlsumfang festgelegt. Eine Auflistung der wichtigsten Standards und Normen im RFID-Bereich findet sich in [FM05].

2.4 Produkte

Die Entwicklung der drahtlosen Überwachung und Verfolgung von Transportcontainern hat in den letzten Jahren einige Fortschritte erzielt. Wesentlich daran beteiligt sind die laufende Miniaturisierung und Optimierung elektronischer Komponenten sowie die Entwicklung und Verbesserung der Kommunikationstechnologien. Preisgünstige elektronische Komponenten bilden die Basis dafür, zukünftig auch alltägliche Transporte und Waren überwachen zu können. Dabei gibt es aber noch einige Gebiete, wie zum Beispiel die Energieversorgung, die noch verbessert werden müssen. Bei vielen der bereits eingesetzten Systeme handelt es sich daher um Prototypen oder Versuchsaufbauten. Trotz der teilweise noch ungelösten Probleme sind bereits marktreife Produkte erhältlich.

2.4.1 Container Security Box

Die Container Security Box (CSB) [8] ist ein System zur Überwachung von Transportcontainern. Die CSB wurde von der Rainer Koch Kommunikation GmbH entwickelt und wird seit 2005 kommerziell eingesetzt. Seit 2008 wird die CSB von der CSB Technologies GmbH vermarktet. Abbildung 2.10 zeigt die Grundausstattung des Systems. Die CSB wurde unter Berücksichtigung des „One-Way-Verkehrs²“ von Containern entwickelt und kann daher auch als mobiles System betrachtet werden. Mobil bedeutet dabei, dass das System leicht an einen Container an- und abmontierbar sein muss, sodass die Container immer wieder gewechselt werden können. Die schnelle und leichte An- und Abmontage wird durch die Befestigung mit einem Magneten erreicht. Durch diese Montagetechnik ist der Diebstahl beziehungsweise das Entfernen der Box nicht ausgeschlossen. Die CSB ist ein GPS-GSM-gestütztes System. Container, die mit einer CSB ausgestattet werden, können somit GPS-Daten empfangen und ihre geographische Position feststellen. Die Positionsdaten sowie andere Meldungen können via GSM an eine Zentrale weitergeleitet werden. Die Zentrale kann dabei eine anwenderspezifische Einrichtung sein oder eine externe Partei, welche internationale Interventionsmöglichkeiten besitzt. Die Betriebsdauer einer CSB liegt laut

²Viele Container werden nur für den Transport von Punkt A nach Punkt B angemietet. Der Container wird danach nicht mehr zu Punkt A retourniert, sondern wird für andere Transporte weiterverwendet.

Hersteller bei bis zu 80 Tagen. Diese im Vergleich zu anderen Lösungen kurze Betriebsdauer verursacht laufende Kosten für die Wartung und das Wiederaufladen des Energiespeichers der CSB.



Abbildung 2.10: CSB-Equipment: 1-Basisgerät, 2-Transportbox, 3-Innenraumsensor, 4-Ladegerät [8]

Da viele Container nur für den Transport von Punkt A nach Punkt B gemietet werden, muss die CSB beim Empfänger wieder vom Container demontiert werden. Danach muss das CSB-Equipment an den Versender der Ladung retourniert werden. Dazu wird der Fracht im Container eine spezielle Transportbox für die CSB beigelegt. Nach der Demontage wird das CSB-Equipment in dieser Transportbox verstaut. Die CSB deaktiviert sich automatisch in der Transportbox und kann somit auch ohne Probleme mit dem Flugzeug an den Ausgangsort der Ladung retourniert werden.

Das CSB-System am Container besteht aus zwei Teilen, dem Basisgerät und der Innenraumsensoreinheit. Das Basisgerät wird in einer Mulde an der Containeroberseite mit einem Magneten fixiert. Die Sensoreinheit wird ebenfalls magnetisch im Containerinnenraum montiert. Für nicht-magnetische Behälter werden spezielle Halterungen bereitgestellt. Die Kommunikation zwischen Basisgerät und Sensoreinheit erfolgt per Funk. Alle Sensoren besitzen einen programmierbaren eindeutigen Code, durch den sie identifiziert werden können. Die Sensoreinheit der Grundausstattung (Innenraumsensor) registriert das Öffnen und Schließen der Türen, die Bewegung von Personen im Innenraum des Containers sowie Lichteinfall bei geschlossenen Türen. Im Basisgerät ist darüber hinaus ein Stoßsensor enthalten.

Das System unterstützt die Anbindung von zusätzlichen Sensoren. Dadurch können optional Sensoren zur Messung von zum Beispiel Temperatur, Feuchtigkeit oder Radioaktivität eingesetzt werden. Die zusätzlichen Sensoren sind jedoch nicht in der Grundausstattung enthalten, sondern müssen kundenspezifisch entwickelt werden. Weiters wird ein Anschluss für ein externes RFID-Lesegerät über eine RS232-Schnittstelle bereitgestellt. In Entwicklung ist darüber hinaus ein Sensor, der den Containerinhalt registriert. Die einzelnen Waren sollen dabei mit RFID-Tags ausgestattet werden und beim Be- und Entladen des Containers vom Sensor registriert werden.

Das Basisgerät wird durch einen Li-Ion-Akkumulator mit einer Kapazität von 3,6 Ah versorgt. Dieser Akku wird vor dem Transport mit einem externen Ladegerät aufgeladen. Während des

Transports kann der Akku über eine Solarzelle mit 4 Wp geladen werden. Ohne Sonneneinstrahlung bleibt die CSB 80 Tage betriebsbereit. Die Sensoreinheit wird durch Li-Ion-Primärzellen mit 2,25 Ah versorgt. Tabelle 2.3 zeigt einen Überblick der technischen Daten.

Tabelle 2.3: Technische Daten des CSB-Equipments [8]

	Basisgerät	Sensoreinheit
Abmessungen	780 mm x 128 mm x 27 mm	153 mm x 87 mm x 83 mm
Gewicht	2,25 kg	820 g
Versorgung	Li-Ion-Akku 3,6 Ah; Solarzelle 4 Wp	Li-Ion-Primärzellen 2,25 Ah

Bei der typischen Betriebsweise der CSB wird periodisch, in Abständen von 8 Stunden, die geographische Position mittels GPS-Koordinaten ermittelt. Einmal täglich wird ein Report an die Zentrale gesendet. Die Konfiguration der Betriebsweise kann automatisch oder manuell durch die Zentrale erfolgen. Somit kann zum Beispiel auf bestimmten Transportabschnitten die Periode der Positionsmeldungen verkürzt werden. Ereignismeldungen werden, sofern eine Kommunikationsverbindung besteht, sofort an die Zentrale weitergeleitet. Jede Meldung enthält neben der Information über das eingetretene Ereignis die aktuelle geographische Position sowie einen Zeitstempel. In der Zentrale kann definiert werden, ob eine eintreffende Meldung als Alarm, Ereignis oder Logbucheintrag behandelt werden soll. Bei einem Alarm wird der festgelegte Alarmplan angezeigt und die Alarmmeldung als SMS oder E-Mail an verantwortliche Personen weitergeleitet. Das System unterstützt folgende Typen von Ereignismeldungen:

- CSB-Basisgerät am Container befestigt/entfernt
- Unterschreitung des Akkusollwertes im Basisgerät
- Sensor im Container befestigt/entfernt
- Batteriestatus der Sensoren
- Türen geöffnet/geschlossen
- Bewegung von Personen im Innenraum
- Lichteinfall im geschlossenen Container
- Überschreitung der Beschleunigungsgrenzen
- Über-/Unterschreiten von Grenzwerten
- Stapelzustand des Containers
- Erreichen/Verlassen vordefinierter Adressen/Areale
- Verlassen vorgegebener Routen
- täglicher Report mit Position, Akkuspannung, Providercode des GSM-Netzes
- Information über die ordnungsgemäße Be-/Entladung der Ware (RFID)

2.4.2 AIRSIS Express Trailer and Container Monitor

AIRSIS Express Trailer and Container Monitor [9] ist ein vom amerikanischen Unternehmen AIRSIS Inc. entwickeltes System zur Überwachung von Containern. Dieses System ermöglicht es, Container via Satellitenkommunikation und Internet rund um die Uhr zu verfolgen. Das integrierte System ist in einem widerstandsfähigen Gehäuse (siehe Abbildung 2.11) eingebaut, wodurch der Einsatz in einer rauen Umgebung ermöglicht wird. Das System besteht aus einem Teil und muss an einer Position mit direkter Sicht zu den Satelliten montiert werden. Das Gerät kann an den Container geschraubt werden oder mit Hilfe eines Industrieklebers befestigt werden. Da das Gerät durch eine austauschbare Batterie gespeist wird, entfällt die externe Versorgung. Es werden darüber hinaus keine externen Antennen oder sonstigen Verkabelungen benötigt. Aktiviert wird das System durch Betätigen eines Knopfes auf dem Gerät oder per Personal Digital Assistant (PDA). Je nach Betriebsmodus (Übertragungen/Tag) kann das System eine Betriebsdauer von 3 bis 7 Jahren ohne Wartung erreichen.



Abbildung 2.11: AIRSIS-Überwachungseinheit am Container [9]

Die Visualisierung der erfassten Daten erfolgt über das AIRSIS Vision Service. Dieser Dienst basiert auf einer Webanwendung. Dem Kunden wird eine eigene Website zur Verfügung gestellt, über die er seine Container von jedem Internetzugang 24 Stunden am Tag überwachen kann. Das AIRSIS Vision Service ermöglicht den Überblick über die geographische Position aller mit AIRSIS-Hardware ausgestatteten Container. Die Darstellung erfolgt auf einer Landkarte mit verschiedenen Abstraktionsstufen bis hinunter auf Straßenniveau. Es können die Historie der Container sowie eingegangene Statusmeldungen abgefragt werden. Alarmmeldungen können per SMS oder E-Mail weitergeleitet werden. Das System ermöglicht darüber hinaus die Integration der gesammelten Daten in kundenspezifische Anwendungen.

AIRSIS Express Trailer and Container Monitor wird in erster Linie für die grundlegende Positionsbestimmung der Container angewendet. Dabei werden typischerweise 1 bis 4 Reportmeldungen täglich abgesetzt. Die Sendeintervalle der Positionsmeldungen können jedoch variiert werden, wobei die Umstellung zum Beispiel nach geographischen Arealen erfolgen kann. Zusätzlich wird die Anbindung externer Sensoren angeboten, die im Normalfall jedoch nicht vorgesehen ist. Das System kommuniziert mit Hilfe eines globalen Satellitennetzwerks. Die Abmessungen des Gehäuses am Container betragen rund 280 mm x 100 mm x 25 mm.

2.4.3 CommerceGuard

Das CommerceGuard-System [10] wird von General Electric und Siemens gemeinsam vertrieben. Container werden dabei mit einem Container Security Device (CSD) ausgestattet (siehe Abbildung 2.12). Das System besteht darüber hinaus aus mobilen und fixen Lesestationen sowie einem Datencenter. Das CSD wird magnetisch an der Innenseite des Türrahmens befestigt. Diese Position schützt das Gerät vor äußeren Einwirkungen wie Sabotage oder Beschädigung während des Transports. Durch die platzsparende Montage geht kein Ladeplatz verloren. Das CSD ist mit einem Näherungssensor ausgestattet, womit das Öffnen der Türen überwacht werden kann. Das Gerät ist weiters mit einem seriellen Port für Erweiterungen ausgestattet, wodurch zusätzliche anwendungsspezifische Sensoren nachgerüstet werden können. Das CSD kommuniziert über Funk auf 2,4 GHz mit stationären und mobilen Lesestationen, wobei die Datenkommunikation im CommerceGuard-System durch den Advanced Encryption Standard (AES) verschlüsselt wird. Das batterieversorgte CSD erreicht eine Betriebsdauer von 6 Jahren.



Abbildung 2.12: Container Security Device (CSD) [10]

Stationäre Lesestationen werden an Schlüsselstellen in der Transportkette, wie zum Beispiel Ein- und Ausfahrten von Häfen, Depots oder Fabriksarealen montiert. Die Reichweite der stationären Lesegeräte beträgt rund 30 m. Dabei können die Container das Lesegerät mit einer maximalen Geschwindigkeit von 36 km/h passieren. Die Lesestationen werden extern versorgt und besitzen einen LAN-Anschluss. Mit Hilfe einer Zusatzbox, der so genannten COM-Unit, kann die stationäre Lesestation auch drahtlos über GPRS kommunizieren. Zur Steigerung der Flexibilität sind mobile Lesegeräte erhältlich. Mobile Lesegeräte, auch als Handheld Reader bezeichnet, haben eine Reichweite von rund 10 m. Der Zugang zum globalen Informationsnetz erfolgt über eine direkte Verbindung mit einem ans Internet angeschlossenen Computer. Das mobile Lesegerät kann mit einem zusätzlichen GPRS-Modem nachgerüstet werden.

Zu Beginn eines Transports wird das CSD nach Verschluss der Containertüren mit Hilfe eines mobilen Lesegeräts aktiviert. Von diesem Zeitpunkt an wird jedes unautorisierte Öffnen des Containers sowie jede unautorisierte Kommunikation mit dem CSD registriert und aufgezeichnet. Mit mobilen Lesegeräten können autorisierte Personen jederzeit während des Transports Daten vom CSD abrufen und den Türalarm für Inspektionszwecke zwischenzeitlich deaktivieren. Erkannte Alarmereignisse werden mit einem Zeitstempel versehen und lokal abgespeichert. Zusätzlich zu

Alarmmeldungen werden während des Transports Zeit, Datum und Reader-ID der passierten stationären Lesegeräte gespeichert. Kommt ein Container in Reichweite einer Lesestation, so werden die abgespeicherten Informationen übertragen. Die registrierten Ereignisse und Daten werden gemeinsam mit der Position beziehungsweise der ID der Lesestation an das Datacenter übermittelt. Die Informationen werden verschlüsselt über das Internet übertragen. Im Datacenter erfolgt die entsprechende Aufbereitung der Daten. Zuständige Behörden, Frächter, Eigentümer sowie andere autorisierte Personen können die Daten der Container in Folge über jeden beliebigen Internetzugang rund um die Uhr abrufen.

2.4.4 Smart Box

Smart Box nennt sich eine Überwachungslösung, die vom Fraunhofer-Institut für Fabrikbetrieb und -automatisierung (IFF) [11] in Kooperation mit dem DHL Innovation Center der Deutschen Post [12] entwickelt wurde. Die Smart Box kombiniert GSM, GPS, Sensorik und RFID-Technologie. Dadurch ist die Smart Box in der Lage, Informationen über den Zustand der enthaltenen Ware sowie die aktuelle Position der Box zu erfassen und weiterzuleiten. Die Smart Box ist mit einem RFID-Lesegerät ausgestattet, wobei drei Antennen in den Seitenwänden und dem Boden integriert sind. Das RFID-Lesegerät arbeitet auf einer Frequenz von 13,56 MHz und kann passive RFID-Transponder auf eine Entfernung von bis zu 80 cm pro Antenne auslesen. Dadurch kann jede Ware, die in die Box gelegt beziehungsweise aus der Box entfernt wird, registriert werden. Voraussetzung ist die Bestückung der Warengüter mit RFID-Transpondern. Es kann somit laufend der aktuelle Inhalt der Box ermittelt werden. Die Visualisierung der Daten kann über eine an der Box angebrachte Anzeige oder einen Leitstand erfolgen. Zu diesem Zweck ist die Smart Box mit einem GSM-Modul ausgestattet. Mit Hilfe dieses Moduls können Daten zur Speicherung, Analyse und Bearbeitung an ein entferntes Datacenter übertragen werden. Darüber hinaus verfügt die Smart Box über einen GPS-Empfänger, der die Positionsbestimmung der Box ermöglicht. Die Smart Box kann optional mit zusätzlicher Sensorik zur Überwachung von Druck, Temperatur oder Vibration ausgerüstet werden. Für die Stromversorgung gibt es mehrere Varianten. Die Versorgung kann über einen optionalen Netzanschluss (220 V AC) erfolgen, einen KFZ-Bordanschluss (9 bis 36 V DC) oder über Akkumulatoren (9 bis 36 V DC). Mögliche Anwendungsgebiete werden in der Überwachung und Steuerung logistischer Güter in komplexen Logistikketten und einer laufenden Inventur gesehen.

2.4.5 GlobalTrack

GlobalTrack [13] ermöglicht die globale Lokalisierung von Objekten wie Containern. Das Unternehmen wurde 2001 gegründet und bietet unterschiedliche Tracking-Hardware an. Die passende Hardware wird dabei durch die Anforderungen des Kunden und der Einsatzumgebung bestimmt. Jedes GlobalTrack-Produkt ist, um die eigene Position bestimmen zu können, mit einem GPS-Empfänger ausgestattet. Abhängig vom eingesetzten Produkt werden die Positionsdaten über ein Mobilfunknetz oder über einen der vier Kommunikationssatelliten von GlobalTrack weitergeleitet. Die vier Satelliten von GlobalTrack ermöglichen eine globale Abdeckung. Es werden auch Produkte angeboten, die beide Kommunikationstechnologien unterstützen. Dadurch können die Vorteile zellulärer Mobilfunknetze sowie der Satellitenverbindung genutzt werden. Über die gewählte Infrastruktur werden die Positionsdaten in Folge an die Server von GlobalTrack gesendet und verarbeitet.

GlobalTrack bietet darüber hinaus eine Visualisierungssoftware mit dem Namen WebTrack an. Die Software ermöglicht die Visualisierung aller mit entsprechender Tracking-Hardware ausgerüsteten Objekte auf ständig aktualisierten Straßenkarten und Satellitenbildern. Dabei kann die Vergrößerung einer Lokalität bis auf Straßenniveau erfolgen. Die Historie der überwachten Objekte kann über den Karten dargestellt werden oder zur genaueren Analyse in Reportform angezeigt werden. Die Meldungen können anhand von Kriterien geordnet werden und graphisch mit Diagrammen aufbereitet werden. Reporte können in benutzerdefinierten Intervallen oder per Anfrage erfolgen. Darüber hinaus kann bei eintreffenden Meldungen eine Weiterleitung über SMS oder E-Mail eingerichtet werden. Um WebTrack zu nutzen, wird nur ein Browser, ein Internetzugang und ein Passwort benötigt. Es muss keine Software installiert werden. Der Benutzer muss sich daher nicht um Softwareupdates und das Speichern der Daten kümmern. Daten können in verschiedenen Formaten exportiert werden. Dadurch können die ermittelten Daten in anwenderspezifische Systeme importiert und weiterverarbeitet werden. Das System unterstützt bei mehreren Benutzern auch unterschiedliche Authentifizierungsstufen. Abbildung 2.13 gibt einen Überblick über die Infrastruktur und Architektur von GlobalTrack.

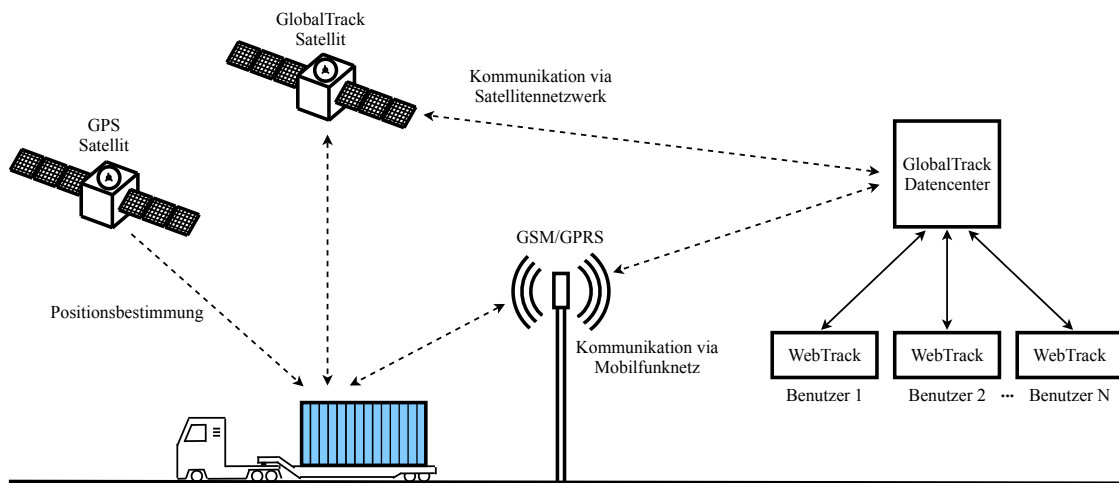


Abbildung 2.13: Infrastruktur und Architektur von GlobalTrack [13]

GlobalTrack bietet Produkte für unterschiedliche Anforderungen an. Die Tracking-Hardware SAT-340 kommuniziert über die Satelliten von GlobalTrack und ermöglicht dadurch die globale Lokalisierung von Objekten. Das Produkt benötigt eine externe Versorgung und wird bevorzugt im Marine- und Luftfahrtbereich eingesetzt. Die Tracking-Hardware DUO-900 nutzt während des Aufenthalts in einem durch GSM/GPRS abgedeckten Bereich das lokale Mobilfunknetz zur Kommunikation. In Gebieten ohne GSM/GPRS-Netze erfolgt der Datenaustausch automatisch über die Kommunikationssatelliten von GlobalTrack. Auch dieses Produkt benötigt eine externe Versorgung. Die Tracking-Hardware BAT-340 wird von einer auswechselbaren Batterie gespeist und benötigt daher keine externe Versorgung. Dabei kann eine Betriebsdauer von bis zu 3 Jahren erreicht werden. Diese Hardware wird bevorzugt zur Überwachung von Containern und Trailern eingesetzt. Die Einheit wird durch einen externen Magneten aktiviert, wodurch unnötiger Energieverbrauch beim Lagern vermieden wird. Die Kommunikation erfolgt über die GlobalTrack-Satelliten. Neben den Tracking-Produkten bietet GlobalTrack auch ein Terminal für die Kommunikation mit dem Fahrer des überwachten Transports an. Das Produkt nennt sich Message Terminal und wird im Führerhaus montiert. Das Message Terminal ermöglicht die direkte Kommunikation zwischen

Fahrer und einem WebTrack-Benutzer. Dabei können bidirektional Textnachrichten ausgetauscht werden. Der Fahrer bekommt zusätzlich GPS-Daten, Geschwindigkeit und Richtung angezeigt. Darüber hinaus können von einem WebTrack-Benutzer Geschwindigkeitslimits festgelegt werden. Der Fahrer wird bei einer Überschreitung akustisch und optisch darauf aufmerksam gemacht. Durch Betätigung eines Notfall-Knopfes am Message Terminal kann WebTrack eine SMS oder E-Mail mit den letzten GPS-Koordinaten an definierte Personen versenden. Die Hardware bietet zusätzliche Ein- und Ausgänge sowie 2 serielle Ports für künftige Erweiterungen. Das Message Terminal muss extern versorgt werden. Detaillierte Informationen zu den Produkten finden sich unter [13].

2.4.6 ORBCOMM

ORBCOMM [14] ist ein Unternehmen in der Telekommunikationsbranche, das globale drahtlose bidirektionale Datenkommunikationsdienste sowie Positionierungsdienste anbietet. Der Fokus wird dabei auf die Kommunikation zwischen Maschinen gelegt. Der Hauptsitz des Unternehmens befindet sich in Fort Lee (New Jersey). ORBCOMM betreibt ein eigenes LEO-Satellitennetzwerk (Low Earth Orbit), wodurch eine globale Abdeckung erreicht wird. Die terrestrische Infrastruktur besteht aus über die ganze Welt verteilten Gateways und einem Kontrollzentrum in Dulles (Virginia). Die Gateways sind für die Anbindung an terrestrische Netze sowie den Zugang zum Satellitennetzwerk verantwortlich. Das Kontrollzentrum überwacht die Satellitenkonstellation und die Umlaufbahnen. ORBCOMM-Produkte ermöglichen den Kunden einen weltweiten Zugang zu privaten und öffentlichen Netzen, wie dem Internet. Es werden auch Produkte angeboten, die sowohl über GSM/GPRS/EDGE als auch über das ORBCOMM-Satellitennetzwerk kommunizieren können. Eine Liste verfügbarer Produkte findet sich unter [14]. Die Produktpalette reicht von einer einfachen Modemfunktionalität über programmierbare Geräte für spezifische Anwendungen bis hin zu voll ausgestatteten Systemen. Letztere verfügen über einen integrierten GPS-Empfänger, zusätzliche Ein- und Ausgänge sowie Komponenten zur GSM- und Satellitenanbindung. ORBCOMM-Produkte werden unter anderem für Überwachungszwecke an Lastkraftwagen, Containern oder Trailern montiert.

3 Problemanalyse

Im Zuge der Problemanalyse werden die geplanten Einsatzumgebungen des EGW analysiert und diskutiert. Da sich diese Arbeit mit der Implementierung der Gatewayapplikation am Gatewaycontroller beschäftigt, wird nicht näher auf die Funkapplikation am Funkcontroller eingegangen. Die Regelung des Mediumzugriffs beim Lokalfunk hat jedoch direkte Auswirkungen auf die Gatewayapplikation. Aus diesem Grund wird die Zugriffsregelung eingangs beschrieben. Die eigentliche Problemanalyse wird an Hand praxisnaher Szenarien durchgeführt. Das Szenario Lagerhalle dient der Analyse der grundlegenden Abläufe und Probleme beim Einsatz eines EGW in einem System zur drahtlosen Containerüberwachung. Es wird eine Lokalität mit nur einem EGW und geringer bis mittlerer Auslastung betrachtet. Aufbauend auf dieser Basisanalyse folgt die Analyse eines Systems mit mehreren EGW und hoher Auslastung. Dabei dient ein Lagerplatz als Szenario. Die Einsatzmöglichkeiten in einer dynamischen Umgebung werden am Beispiel eines Eisenbahntransports analysiert. Die Container befinden sich dabei in Bewegung, während der EGW stationär montiert ist.

3.1 Mediumzugriff beim Funkprotokoll

Die Kommunikation zwischen dem EGW und Containern in Reichweite erfolgt über Lokalfunk. Da die Energieressourcen am Container beschränkt sind und die MTU dadurch auf den Energieverbrauch achten muss, kann der Funktransceiver nicht ständig aktiv betrieben werden. Aus diesem Grund wird eine im Zuge des WCMS-Projekts entwickelte Regelung für den Mediumzugriff angewendet. Dabei werden zwei Betriebsmodi unterschieden, der passive Empfangsbetrieb und der aktive Empfangsbetrieb. Solange keine Kommunikation stattfindet, wird der passive Empfangsbetrieb ausgeführt. In diesem energieschonenden Betrieb (siehe Abbildung 3.1) wird periodisch alle 10 s der Funktransceiver auf der MTU aktiviert und für 4,4 ms am Funk gehört. Darüber hinaus wird von der MTU periodisch alle 100 s ein Beacon-Paket gesendet. Das Paket dient dazu, vorhandene EGW in Funkreichweite auf die MTU aufmerksam zu machen. Mit dem Beacon-Paket sendet die MTU neben ihrer ID auch Timinginformationen. Dadurch weiß ein EGW, der das Beacon empfängt, wann die MTU am Funk hört. Der Empfangszeitanschlit nach dem Beacon ist für die Antwort auf das Beacon vorgesehen, vorausgesetzt ein EGW befindet sich in Reichweite. Wenn die MTU innerhalb des periodischen Empfangszeitanschlitzes die definierte Preamble eines Kommunikationspakets empfängt, wird in den aktiven Empfangsbetrieb gewechselt. Dabei bleibt der Funktransceiver solange auf Empfang, bis die gesamte Nachricht empfangen wurde. Da der eingesetzte Funktransceiver den IEEE 802.15.4-Standard (siehe Abschnitt 2.3.1)

unterstützt, kann im Fall, dass die MTU eine Nachricht an einen EGW senden möchte, zu einem beliebigen Zeitpunkt unter Beachtung des CSMA/CA-Mechanismus gesendet werden. Der EGW kann, da er extern versorgt wird, ständig am Funk hören, außer, wenn er selbst gerade sendet. Nach Beendigung einer Kommunikation wird wieder in den passiven Empfangsmodus gewechselt.

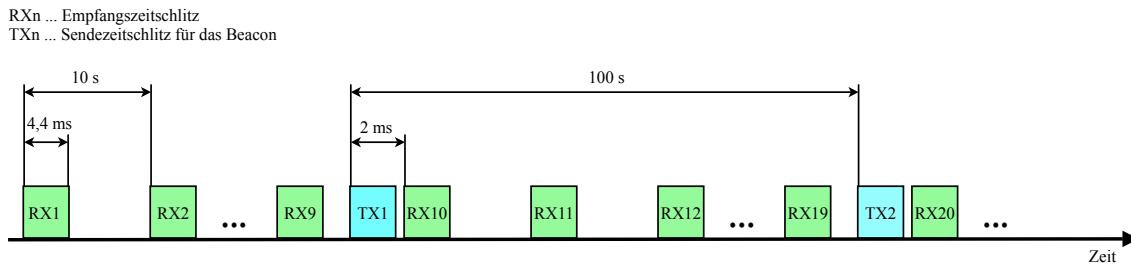


Abbildung 3.1: Sende- und Empfangszeit slots im passiven Empfangsbetrieb der MTU

3.2 Szenario - Lagerhalle

Das Szenario Lagerhalle dient zur Analyse der grundlegenden Abläufe und Probleme beim Einsatz eines EGW in einem System zur drahtlosen Containerüberwachung. Es wird eine Lokalität mit nur einem EGW und geringer bis mittlerer Auslastung betrachtet. Objekt der Annahme ist eine Lagerhalle, in der Container abgestellt werden. Abbildung 3.2 veranschaulicht die Sachverhalte.

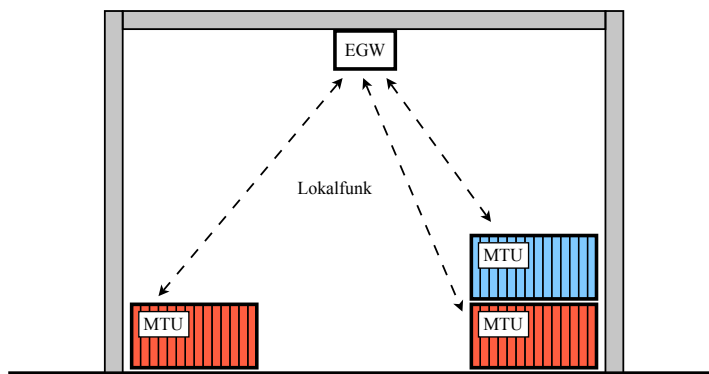


Abbildung 3.2: Lagerhalle mit einem EGW

Da nur ein EGW vorhanden ist, muss die Montage an einem Ort erfolgen, der sich in Reichweite aller Container befindet. Kann das Areal der Halle nicht mit einem EGW abgedeckt werden, müssen mehrere EGW montiert werden. Als Alternative können Lagerplätze außerhalb der EGW-Reichweite für Container ohne Überwachungsausstattung vorbehalten werden. Die Stapelung der Container ist zu beachten, da sie zu Problemen bei der Funkkommunikation führen kann. Der EGW muss darüber hinaus an eine externe Stromversorgung angeschlossen werden. Für die Kommunikation mit dem Datacenter benötigt der EGW einen Internetzugang. Dazu kann der EGW alternativ zum LAN-Modul auch mit einem WLAN-Modul ausgerüstet werden. Da der EGW einen niedrigen Energieverbrauch anstrebt, werden der Gateway- sowie der Funkcontroller so oft wie möglich in einen energiesparenden Schlafmodus versetzt. Deshalb muss vor

einer Datenübertragung zuerst sichergestellt werden, dass die Gegenstelle aktiv ist. Aus diesem Grund wird das im Rahmen des WCMS-Projekts entwickelte Extended Protocol angewendet. Dieses Protokoll wurde ursprünglich für die serielle Kommunikation zwischen dem zentralen Controller auf der MTU und anderen Microcontrollern entwickelt. Nähere Informationen finden sich in Abschnitt 4.3. Der Gatewaycontroller am EGW muss sowohl mit dem Funkcontroller als auch mit dem LAN-Modul kommunizieren. Um Problemen mit den eventuell unterschiedlichen Übertragungsgeschwindigkeiten vorzubeugen, wird eine Flusskontrolle eingesetzt. Darüber hinaus werden alle Kommunikationspakete mit zusätzlichen Informationen zur Erkennung von Übertragungsfehlern ausgestattet.

Um die Dienste am EGW zu nutzen, muss sich ein Container anmelden. Bei der Anmeldung werden die Kennungen sowie Informationen zu den Empfangszeit slots der MTU ausgetauscht (siehe Abschnitt 3.1). Das Datacenter muss über neu angemeldete Container informiert werden. Nur so können Daten an die Container über den korrekten EGW weitergeleitet werden. Sobald sich ein Container nicht mehr in Reichweite des EGW befindet, muss das Datacenter ebenfalls informiert werden. Dadurch werden zukünftige Nachrichten an den Container nicht mehr über den EGW, sondern über einen alternativen Kommunikationsweg (GSM) gesendet. Der Funkcontroller muss daher den Gatewaycontroller stets über Änderungen bei den angemeldeten Containern informieren. Der Gatewaycontroller leitet die Informationen über das LAN-Modul an das Datacenter weiter.

Das Location-Service soll Containern in Reichweite eines EGW die Ermittlung der GPS-Koordinaten über Lokalfunk ermöglichen. Dazu müssen die aktuellen GPS-Koordinaten dem EGW bekannt sein. Da der EGW stationär montiert wird, ändert sich seine geographische Position nicht. Aus diesem Grund können die GPS-Koordinaten fest konfiguriert werden. Dieser Vorgang kann automatisch, mit Hilfe eines GPS-Moduls oder manuell erfolgen. Da in einer Lagerhalle keine direkte Sichtverbindung zu den GPS-Satelliten gegeben ist, wird der GPS-Empfänger kein Signal empfangen. Deshalb wird in Lagerhallen die manuelle Konfiguration vorgezogen. Im einfachsten Fall werden die Koordinaten über ein Konsolenprogramm an den EGW übermittelt. Dazu muss eine Konsole für den EGW implementiert werden. Alternativ kann die Übermittlung der GPS-Koordinaten auch über die LAN-Anbindung oder das optionale GSM-Modul erfolgen. Die Koordinaten werden vom Gatewaycontroller verwaltet, da er das zentrale Element am EGW ist und Zugriff auf das optionale GPS-Modul und das optionale GSM-Modul hat. Da die Abfrage der Koordinaten über Lokalfunk direkt vom Funkcontroller beantwortet werden kann, müssen die GPS-Koordinaten an den Funkcontroller weitergeleitet werden. Dadurch muss nicht bei jeder Abfrage der Gatewaycontroller kontaktiert werden. Die festen GPS-Koordinaten müssen dabei nur einmalig vom Gatewaycontroller an den Funkcontroller übergeben werden. Im Rahmen einer Konfigurationsrunde, beim Einschalten des EGW, können so die Koordinaten mit anderen Parametern an den Funkcontroller übermittelt werden. Im Fehlerfall muss es jedoch eine Möglichkeit geben, mit der der Funkcontroller die GPS-Koordinaten explizit vom Gatewaycontroller abfragen kann. Container in Reichweite eines EGW können die GPS-Koordinaten explizit über Lokalfunk abfragen. Die Antwort erfolgt vom Funkcontroller ohne Umweg über den Gatewaycontroller. Da die Abfrage der GPS-Koordinaten stets vom Container initiiert wird und Verzögerungen bei der Antwort zulässig sind, kann die MTU im passiven Empfangsmodus arbeiten. Eine Anmeldung an den EGW ist Voraussetzung für die Nutzung der Dienste. Dadurch können die GPS-Koordinaten auch einmalig im Zuge der Anmeldung übertragen werden. So entfallen weitere Abfragen und der Funkverkehr wird entlastet.

Das SMS-Service soll Containern in Reichweite eines EGW das Empfangen und Senden von Kurznachrichten über Lokalfunk ermöglichen. Dabei handelt es sich um unabhängige Nachrichten mit

einer maximalen Nutzdatenmenge von 140 Byte. Die Nachrichten haben Meldungscharakter (Status, Alarm, Konfiguration) und verlangen keine unmittelbare Antwort. Dadurch kann die MTU im energieschonenden, passiven Empfangsmodus arbeiten. Die eventuell auftretende Wartezeit, bis die MTU in einen Empfangszeit slot wechselt, wird dabei toleriert. Der extern versorgte EGW hört ständig am Funk, falls er nicht selbst sendet. Die Nachrichten müssen zusätzlich zu den Nutzdaten auch eine Kennung des beteiligten Containers enthalten. Die Kennung dient bei Nachrichten an einen Container für die korrekte Adressierung über Funk und bei Nachrichten von einem Container für die Zuordnung im Datencenter. Der Gatewaycontroller leitet Nachrichten, die er vom Funkcontroller erhält, an das LAN-Modul weiter und Nachrichten vom LAN-Modul an den Funkcontroller. Je nach festgelegtem Protokoll muss ein Umbau der Kommunikationspakete erfolgen. Im Problemfall werden Hochlasten durch Eingangspuffer abgefangen. Im Fall, dass Probleme bei der Weiterleitung von Nachrichten an den Funkcontroller oder am Funk auftreten, muss es eine Möglichkeit geben, das Datencenter zu informieren. Wenn eine Nachricht über Funk nicht abgesetzt werden kann, muss der Funkcontroller daher den Gatewaycontroller informieren. Der Gatewaycontroller informiert wiederum das Datencenter. Die unmittelbare Gegenstelle ist dabei der Container Management Gateway (CGW). Er ist für die Wahl des Kommunikationswegs zu den Containern zuständig. Wenn der CGW eine Fehlermeldung vom EGW erhält, kann er künftige Nachrichten über einen alternativen Weg (GSM) an die Container weiterleiten. Dabei ist es sinnvoll, mit der Fehlermeldung die unzustellbare Nachricht zu retournieren. Dadurch müssen die gesendeten Nachrichten nicht am CGW gespeichert werden. Für den Fall, dass die LAN-Verbindung kurzzeitig unterbrochen wird, kann der Gatewaycontroller einige Nachrichten zwischenspeichern. Bei längerem Verbindungsausfall muss eine Möglichkeit zur Verfügung gestellt werden, die den Funkcontroller informiert, damit dieser keine Nachrichten mehr an den Gatewaycontroller weiterleitet.

Das Stream-Service soll Containern in Reichweite eines EGW das Empfangen und Senden von größeren Datenmengen über Lokalfunk ermöglichen. Voraussetzung ist eine Anmeldung des Containers am EGW. Ein typischer Anwendungsfall ist die Übertragung von Logfiles und Firmwareupdates. Die Datenmenge beträgt dabei durchschnittlich bis zu 100 kByte. Daraus folgt, dass die Datenmenge in mehreren Teilen übertragen werden muss. Darüber hinaus soll das Stream-Service eine interaktive Konsolenverbindung zwischen einem Benutzer im Internet und einem Container ermöglichen. Die Konsolenverbindung fordert kurze Antwortzeiten. Diese Anforderungen können nicht durch den passiven Empfangsbetrieb der MTU erfüllt werden, da die Verzögerungen gering gehalten werden müssen. Die MTU muss daher während einer Stream-Verbindung im aktiven Empfangsbetrieb gehalten werden, wodurch sie ständig erreichbar ist. Aus diesem Grund muss ein Verfahren für das Öffnen und Schließen einer Stream-Verbindung sowie für die Übertragung zusätzlicher Streaminformationen bereitgestellt werden. Wie beim SMS-Service, muss auch beim Stream-Service die MTU-Kennung mit den Stream-Daten übertragen werden. Um mehrere gleichzeitige Stream-Verbindungen mit einem Container zu ermöglichen, kann zusätzlich eine Kanalnummer eingeführt werden. Das Schließen einer Streamverbindung muss im Fehlerfall durch ein Timeout sichergestellt werden. Dadurch wird verhindert, dass die MTU im aktiven Empfangsmodus verbleibt. Für den Fall, dass Probleme bei der Weiterleitung von Daten an den Funkcontroller oder am Funk auftreten, muss es eine Möglichkeit geben, das Datencenter zu informieren. Wenn ein Container über Funk nicht erreicht werden kann, muss der Funkcontroller daher den Gatewaycontroller informieren. Der Gatewaycontroller leitet die Fehlermeldung an den CGW weiter. Im Fall, dass die LAN-Verbindung unterbrochen ist, muss der Gatewaycontroller den Funkcontroller informieren. Im Fehlerfall muss eine Streamverbindung immer geschlossen werden. Wie mit Datenmengen verfahren wird, die aufgrund einer Verbindungsunterbrechung nur teilweise

empfangen wurden, fällt nicht in die Zuständigkeit des Gatewaycontrollers. Er bietet lediglich die Transportdienste an.

Der EGW muss über eine einfache Möglichkeit zur manuellen Konfiguration verfügen. Die Konfiguration erfolgt dabei über den Gatewaycontroller, da er das zentrale Element am EGW ist und Zugriff auf das optionale GSM-Modul sowie die LAN-Anbindung hat. Die Kommunikation mit dem Benutzer kann im einfachsten Fall über ein Terminalprogramm auf einem beliebigen Computer erfolgen. Alternativ können SMS-Nachrichten oder der LAN-Zugang genutzt werden.

3.3 Szenario - Lagerplatz

Das Szenario Lagerplatz dient zur Analyse der Problematik beim parallelen Einsatz mehrerer EGW in einem System zur drahtlosen Containerüberwachung. Es wird eine Lokalität mit mehreren EGW und hoher Auslastung betrachtet. Objekt der Annahme ist ein Lagerplatz, auf dem Container zwischengelagert werden. Abbildung 3.3 veranschaulicht die Sachverhalte. Alle Überlegungen betreffend die grundlegenden Abläufe und Probleme beim Einsatz eines EGW aus Abschnitt 3.2 gelten auch für dieses Szenario. Es werden lediglich Erweiterungen erarbeitet beziehungsweise Spezialfälle analysiert.

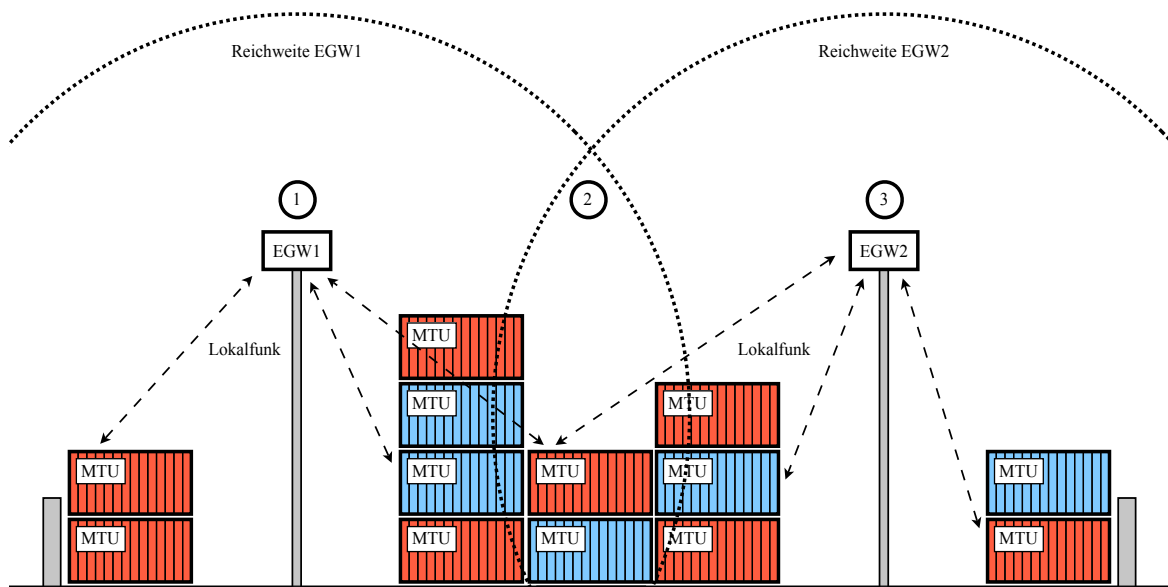


Abbildung 3.3: Lagerplatz mit mehreren EGW

Um die Anzahl der Container, die EGW-Dienste nutzen dürfen, zu steigern (maximal 100 Container je EGW) und ein größeres Areal abdecken zu können, müssen mehrere EGW eingesetzt werden. Damit sichergestellt ist, dass sich jeder Container am Lagerplatz in Reichweite eines EGW befindet, müssen die EGW mit überlappender Reichweite montiert werden. Einige MTU befinden sich daher in einem Bereich, der von unterschiedlichen EGW abgedeckt wird (siehe Bereich 2 in Abbildung 3.3). Als Folge werden die Datenpakete jener MTU von mehreren EGW empfangen. Um das Auftreten von Inkonsistenzen zu verhindern, darf eine MTU stets nur an einem EGW angemeldet sein. Es muss daher ein Verfahren zur Auswahl des zuständigen EGW entwickelt werden. Die Selektion kann vom CGW durchgeführt werden, da er Informationen über

alle EGW und die angemeldeten MTU besitzt. Die Selektion muss bereits während der Anmeldung erfolgen. Ein neuer Container in Reichweite wird vom EGW an den CGW gemeldet. Wenn mehrere EGW den neuen Container erkennen, werden in Folge mehrere Meldungen am CGW eingehen. Der CGW wählt einen EGW aus und retourniert das Ergebnis an die anfragenden EGW. Nur der ausgewählte EGW darf die Anmeldung der MTU durchführen. Dazu muss der Funkcontroller dem Gatewaycontroller neben der Kennung des neuen Containers auch Kriterien für die Selektion übermitteln. Der Gatewaycontroller leitet die Informationen an den CGW weiter. Das Ergebnis der Selektion wird vom CGW an den Gatewaycontroller gesendet, der wiederum den Funkcontroller informiert. Als Kriterien für die Selektion bieten sich die Empfangssignalstärke über Funk und die Anzahl der bereits am EGW angemeldeten Container an. Bei der Selektion kann dadurch auch eine Lastverteilung erfolgen.

3.4 Szenario - Eisenbahntransport

Das Szenario Eisenbahntransport dient der Problemanalyse einer dynamischen Umgebung in einem System zur drahtlosen Containerüberwachung. Es wird eine Lokalität mit einem EGW neben einem Bahngleis betrachtet. Die Container befinden sich dabei in Bewegung, während der EGW stationär montiert ist. Objekt der Annahme ist ein Eisenbahntransport, der einen EGW passiert. Abbildung 3.4 veranschaulicht die Sachverhalte. Alle Überlegungen betreffend die grundlegenden Abläufe und Probleme beim Einsatz eines EGW aus Abschnitt 3.2 gelten auch für dieses Szenario. Es werden lediglich Erweiterungen erarbeitet beziehungsweise Spezialfälle analysiert.

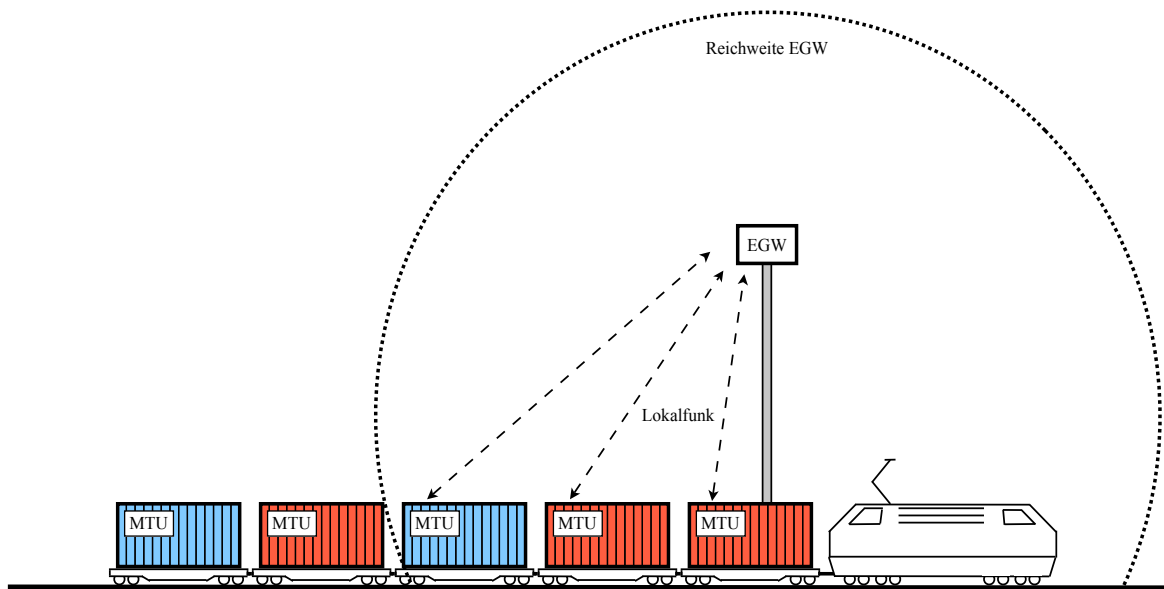


Abbildung 3.4: Eisenbahntransport beim Passieren eines EGW

Der Einsatz von EGW ist für Lokalitäten mit gehäuftem Containerverkehr geplant. Dazu zählen neben Lagerhallen und Lagerplätzen auch Verschubbahnhöfe und bestimmte Gleisabschnitte der Bahn. Bei den dynamischen Umgebungen ist entscheidend, mit welcher Geschwindigkeit die Container den EGW passieren. Ist die Geschwindigkeit zu hoch, so ist die Zeit, die sich ein Container

in Reichweite des EGW befindet, eventuell zu kurz. Dabei muss beachtet werden, dass die MTU im passiven Empfangsmodus (siehe Abschnitt 3.1) arbeitet. Ein EGW neben einem Bahngleis kann für das Absetzen eines Lifesigns genutzt werden. Dabei wird das Datacenter darüber informiert, ob die MTU am Container noch funktioniert und wo sich der Container im Augenblick befindet.

Erfahrungswerte aus Feldversuchen im Rahmen des WCMS-Projekts zeigen, dass der Lokalfunk im Freien eine Reichweite von rund 300 m erzielt. Wird der EGW direkt neben einem Bahngleis montiert, befindet sich ein Container daher beim Vorbeifahren für etwa 600 m in Reichweite. Die geringste Kommunikationsdauer zwischen einem Container und dem EGW wird erreicht, wenn lediglich das Beacon abgesetzt wird. Der EGW informiert in Folge den CGW, der anhand des EGW erkennt, wo sich der Container gerade befindet. Dadurch kann das so genannte Lifesign an das Datacenter übertragen werden. Nach Absetzen des Beacons kann der Container die Reichweite des EGW bereits verlassen haben. Da die MTU im passiven Empfangsmodus arbeitet, wird nur alle 100 s ein Beacon gesendet. Daraus folgt, dass sich ein Container im schlechtesten Fall für mindestens 100 s in Reichweite des EGW befinden muss. Bei 600 m Funkabdeckung und einer minimalen Aufenthaltsdauer von 100 s ergibt sich eine maximale Geschwindigkeit von 6 m/s oder 21,6 km/h.

Ein EGW kann laut Spezifikation maximal 100 Container unterstützen. In einem weiteren Gedankenexperiment wird daher ein Güterzug mit 100 Containern betrachtet. Dabei wird es beim Absetzen der Beacons aufgrund des eingesetzten CSMA/CA-Mechanismus zu Kollisionen kommen. Ein Beacon umfasst laut Funkspezifikation maximal 20 Byte. Der derzeit eingesetzte Funktransceiver arbeitet auf 2,4 GHz und ermöglicht eine Datenrate von 250 kBit/s. Dadurch kann ein Beacon innerhalb von 640 μ s abgesetzt werden. Wenn davon ausgegangen wird, dass keine Kollisionen auftreten, benötigt das Absetzen aller Beacons der 100 Container 64 ms. Auf das Beacon-Intervall von 100 s bezogen, werden dabei lediglich 0,064% belegt. Da das Timing der MTUs nicht absolut synchron verläuft, ist die Kollisionswahrscheinlichkeit nach diesem Gedankenexperiment eher gering. Es kann jedoch zu Kollisionen kommen, die eventuell verhindern, dass einige Container ein Beacon absetzen. Tabelle 3.1 fasst die Ergebnisse zusammen. Neben dem derzeit eingesetzten Transceiver mit einer Datenrate von 250 kBit/s wird ein pinkompatibler Transceiver mit einer Datenrate von 100 kBit/s betrachtet. Die Auslastung entspricht der Dauer von 100 Beacons ohne Kollisionen, bezogen auf das Beacon-Intervall.

Tabelle 3.1: Eignung des EGW zum Einsatz in einer dynamischen Umgebung

Funktransceiver	Frequenz	Datenrate	Beacon	Auslastung ^[1]	Geschwindigkeit
AT86RF230	2,4 GHz	250 kBit/s	640 μ s	0,064%	max. 21,6 km/h
AT86RF212	868 MHz	100 kBit/s	1600 μ s	0,160%	max. 21,6 km/h

[1] Dauer von 100 Beacons bezogen auf ein Beacon-Intervall von 100 s

Die errechneten maximalen Geschwindigkeiten sind für Güterzüge im Freiland sehr niedrig. Um den Transport nicht zu verzögern, können EGW daher vorwiegend an Gleisabschnitten montiert werden, an denen die Umgebungsbedingungen eine Verringerung der Geschwindigkeit fordern. Eine weitere Möglichkeit ist die Montage von EGW in Bahnhofsabschnitten. Eine Alternative besteht darin, zu tolerieren, dass einige Container kein Beacon absetzen können und den EGW am Gleisrand lediglich als zusätzliche Meldemöglichkeit zu betrachten. Umfangreichere Dienste, wie das Versenden einer SMS-Nachricht, sind prinzipiell für einzelne Container denkbar. Bei einem

großen Transport steigt jedoch aufgrund des erhöhten Funkverkehrs die Kollisionswahrscheinlichkeit. Darüber hinaus muss das Beacon kurz nach Eintritt in die Reichweite des EGW erfolgen, da für das Nutzen der EGW-Dienste eine abgeschlossene Anmeldung erforderlich ist.

3.5 Durchsatzanalyse

Für eine genaue Durchsatzanalyse werden detaillierte Informationen über den Funk sowie über die Funkapplikation am Funkcontroller benötigt. Da die Funkapplikation nicht Teil dieser Arbeit ist, sind die folgenden Überlegungen als Abschätzungen zu verstehen. Dadurch soll die prinzipielle Tauglichkeit des EGW für die vorgesehenen Aufgaben betrachtet werden. Die Überlegungen finden in einem stationären Umfeld statt.

Laut Abschnitt 3.1 sendet die MTU eines Containers alle 100 s ein Beacon, wobei ein Beacon laut Funkspezifikation maximal 20 Byte beträgt. Der eingesetzte Funktransceiver arbeitet auf 2,4 GHz mit einer Datenrate von 250 kBit/s. Dadurch kann ein Beacon innerhalb von $640 \mu\text{s}$ abgesetzt werden. Im Fall, dass die maximale Anzahl von 100 Containern an einem EGW angemeldet ist und keine Kollisionen auftreten, werden für die Übertragung aller Beacons 64 ms benötigt. Das entspricht, bezogen auf das Beacon-Intervall von 100 s, einer Auslastung von 0,064%. Aufgrund des eingesetzten CSMA/CA-Mechanismus wird es jedoch zu Kollisionen kommen. Durch die geringe Auslastung und die Tatsache, dass die einzelnen MTU nicht exakt synchron arbeiten, stellen auftretende Kollisionen aber kein Problem dar. Die geringe Auslastung zeigt, dass noch ausreichend Zeit für den weiteren Funkverkehr bleibt. Darunter fällt die Nutzung der EGW-Dienste. Treten keine Alarmmeldungen auf, so sendet ein Container lediglich eine SMS-Nachricht pro Tag an das Datacenter. Dieses Lifesign informiert das Datacenter über den Aufenthaltsort des Containers und das korrekte Arbeiten der MTU. Dazu kommt noch der Datenverkehr bei der Anmeldung am EGW. Das Verkehrsaufkommen am Funk ist daher auch von der Häufigkeit der Containerwechsel an einem EGW abhängig. Eine SMS-Nachricht kann 140 Byte an Nutzdaten transportieren. Mit einem Overhead von geschätzten 10 Byte müssen 150 Byte übertragen werden. Bei einer Datenrate von 250 kBit/s dauert die Übertragung 4,8 ms. Dazu kommen noch Verzögerungen durch eventuelle Kollisionen. Da das genaue Funkprotokoll nicht bekannt ist, müssen noch zeitliche Reserven berücksichtigt werden. Dennoch sollte es möglich sein, eine SMS-Nachricht in etwa 10 ms zu übertragen. Logfiles oder Firmwareupdates werden mit dem Stream-Service übertragen. Die durchschnittliche Datenmenge liegt bei 100 kByte. Da die genaue Aufteilung der Daten auf die Funkpakete nicht bekannt ist, werden die 100 kByte für die Abschätzung auf die Größe von SMS-Nachrichten unterteilt. Dabei wird wieder ein Overhead von 10 Byte berücksichtigt. Somit müssen rund 715 Nachrichten zu je 150 Byte übertragen werden. Bei einer Datenrate von 250 kBit/s dauert die Übertragung 3,5 s. Dazu kommen noch Verzögerungen durch eventuelle Kollisionen. Da das genaue Funkprotokoll nicht bekannt ist, müssen wieder zeitliche Reserven berücksichtigt werden. Dennoch sollte es möglich sein, eine Datenmenge von 100 kByte in rund 5 s zu übertragen. Die Abschätzungen zeigen, dass ein EGW im Normalfall durchaus Dienste für 100 Container unterstützen kann. Solange keine Dienste angefordert werden und sich kein neuer Container anmeldet, beträgt die Auslastung am Funk bei 100 Containern lediglich 0,064%. Die Überlegungen zeigen, dass innerhalb einer Sekunde rund 100 SMS-Nachrichten abgesetzt werden können. Auch die Übertragung von größeren Datenmengen ist durchführbar, solange nicht alle Container gleichzeitig ihr Logfile senden beziehungsweise ein Firmwareupdate nicht gleichzeitig an alle Container erfolgt.

4 Systemarchitektur

Der EGW wird für den Einsatz im WCMS (siehe Abschnitt 1.1) entwickelt. Aus diesem Grund gibt dieses Kapitel einen Überblick über den Aufbau und das Zusammenspiel der einzelnen Komponenten beim WCMS. Dabei wird gezeigt, welche Rolle der EGW im Gesamtsystem spielt. Im Anschluss wird der Aufbau des EGW im Detail beschrieben. Aufbauend auf den Ergebnissen der Problemanalyse wird die gewählte Architektur erklärt. Es werden die Schnittstellen zwischen Gatewaycontroller und Funkcontroller sowie zwischen Gatewaycontroller und (W)LAN-Modul definiert.

4.1 Wireless Cargo Monitoring System

Das WCMS dient der drahtlosen Überwachung von Transportcontainern. Abbildung 4.1 zeigt den prinzipiellen Aufbau des Systems sowie das Zusammenspiel der einzelnen Komponenten. Die Container werden mit einer Telematikbox (MTU) und verschiedenen Sensoren ausgerüstet. Die MTU am Container verfügt über ein GSM-Modul, ein GPS-Modul sowie über einen Lokal-funktransceiver. Um die Daten der Container speichern, verwalten, analysieren und verarbeiten zu können, werden die gesammelten Daten von den Containern an das Datencenter übermittelt. Das Datencenter besteht aus der COMA-Datenbank (CDB), dem COMA-Server (CSRV) und dem COMA-Gateway (CGW). Die Abkürzung COMA steht für Container Management. Der CSRV ist ein Rechner im Netz mit Zugriff auf die CDB. Auf dem CSRV läuft die COMA-Applikation. Der CSRV sendet und empfängt Nachrichten im XML-Format (Extensible Markup Language). Der Leitstand kann sich mit dem CSRV verbinden und liefert eine graphische Benutzerschnittstelle. Über den Leitstand hat der Benutzer Zugriff auf das gesamte System. Der Leitstand kann auf einem beliebigen Rechner im Netz eingerichtet werden, der sich mit „NET Remoting“ mit dem CSRV verbindet. Der Leitstand ermöglicht den Zugriff auf alle in der Datenbank gespeicherten Informationen der Container sowie das Senden von Daten an Container. Es kann die zurückgelegte Route eines Containers auf einer Landkarte visualisiert werden und die aktuelle geographische Position ermittelt werden.

Die Kommunikation zwischen CSRV und den Containern erfordert verschiedene infrastrukturelle Einrichtungen. Der CSRV ist mit dem CGW verbunden. Der CGW ist ein Rechner im Netz, der die Anbindung von verschiedenen Kommunikationstechnologien an das WCMS ermöglicht. Empfangene Daten von Containern werden am CGW aus den spezifischen Formaten in ein XML-Format umgesetzt und an den CSRV weitergeleitet. Daten vom CSRV an die Container werden vom

XML-Format in das Format der gewünschten Kommunikationstechnologie umgesetzt und versendet. Development-Tools greifen direkt über die XML-Schnittstelle auf den CGW zu. Der Zugriff auf die unterstützten Frontends am CGW wird dadurch ohne Umweg über den CSRV ermöglicht. Dieses Vorgehen erleichtert die Entwicklung und die Fehlersuche. Zur Kommunikation mit den Containern verfügt der CGW über eine GSM-, eine SMSC- und eine TCP/IP-Schnittstelle. Als GSM-Schnittstelle wird das GSM-Modul verwendet, das auch auf der MTU zum Einsatz kommt. Das Modul wird über einen seriellen Port angesprochen. Über das GSM-Modul kann der CGW mit den Containern und mit EGW kommunizieren, die mit einem GSM-Modul ausgerüstet sind. Die SMSC-Schnittstelle dient der Kommunikation mit dem Gateway eines Telekommunikationsunternehmens. Die Kommunikation mit dem Gateway erfolgt über HTTP (Hypertext Transfer Protocol). Der Gateway leitet die Nachrichten an das SMSC weiter (siehe Abschnitt 2.2.1), wo auch Nachrichten landen, die über ein GSM-Modul versendet wurden. Die Vorteile der SMSC-Schnittstelle am CGW gegenüber der GSM-Schnittstelle liegen in der Einfachheit und der Geschwindigkeit. Das SMSC des Telekommunikationsunternehmens dient zum SMS-Austausch mit den Containern über das GSM-Netz. Der Vorteil liegt darin, dass SMS-Nachrichten zwischengespeichert werden, bis der Empfänger erreichbar ist. Im WCMS-System ist dieser Punkt wichtig, da das GSM-Modul auf der MTU der Container aus energetischen Gründen zwischenzeitlich nicht versorgt wird. Über die TCP/IP-Schnittstelle kann sich der CGW über das Internet mit den (W)LAN-Modulen auf den EGW verbinden. Besteht eine Verbindung, so können Daten ausgetauscht werden. Die TCP/IP-Schnittstelle dient darüber hinaus zur Anbindung eines TCP/IP-Servers an den CGW. Dieser Server ist für die Verwaltung des Stream-Dienstes verantwortlich. Um eine interaktive Konsolenverbindung mit einem Container aufzubauen, kann sich ein Benutzer von einem beliebigen Rechner im Netz am TCP/IP-Server anmelden. Der TCP/IP-Server baut auf Anfrage über den CGW die Stream-Verbindung mit dem Container auf. Als weiteres Anwendungsbeispiel kann der TCP/IP-Server zusätzlich über eine FTP-Bridge (File Transfer Protocol) mit einem Massenspeichermedium verbunden werden. Dadurch können an einem EGW angemeldete Container mit Hilfe des Stream-Dienstes Logfiles über den CGW an den TCP/IP-Server senden. Größere Datenmengen können auf diese Weise extern gespeichert beziehungsweise ausgelagert werden.

Die EGW werden an Örtlichkeiten mit gehäuftem Containervorkommen stationär montiert. Einsatzorte sind zum Beispiel Lagerplätze sowie Be- und Entladeplätze. Es können auch mehrere EGW parallel eingesetzt werden. Dadurch kann ein größeres Areal abgedeckt werden und mehrere Container bedient werden. Die maximale Anzahl an angemeldeten Containern pro EGW ist auf 100 Container festgelegt. Die Standardausführung ist mit einem (W)LAN-Modul und einem Lokalfunktransceiver ausgestattet. Ausführungen mit einem GSM-Modul anstelle eines Lantronix-Moduls sind derzeit nur für Spezialanwendungen geplant, wo keine externe Stromversorgung und kein Internetzugang verfügbar sind. Der EGW kann optional auch mit einem GPS-Modul ausgestattet werden. Der CGW ist mit den einzelnen EGW über das Internet verbunden. Container, die sich in Reichweite eines EGW befinden, können sich über Lokalfunk anmelden. Nach erfolgreicher Anmeldung bei einem EGW können dessen Dienste über Lokalfunk in Anspruch genommen werden. Container können dadurch über den EGW SMS-Nachrichten senden und empfangen, die GPS-Koordinaten abfragen sowie größere Datenmengen übertragen beziehungsweise empfangen. Ist ein Container an einen EGW angedockt, kann darüber hinaus eine interaktive Konsolenverbindung zwischen dem Container und einem Benutzer im Netz (Console Client) hergestellt werden. Dadurch besteht die Möglichkeit, aus der Ferne Konfigurationsparameter der MTU manuell abzuändern und Daten der MTU abzurufen. Die Konsole kann, bis auf die längeren Antwortzeiten, so verwendet werden, als wäre eine direkte Verbindung zum Container vorhanden.

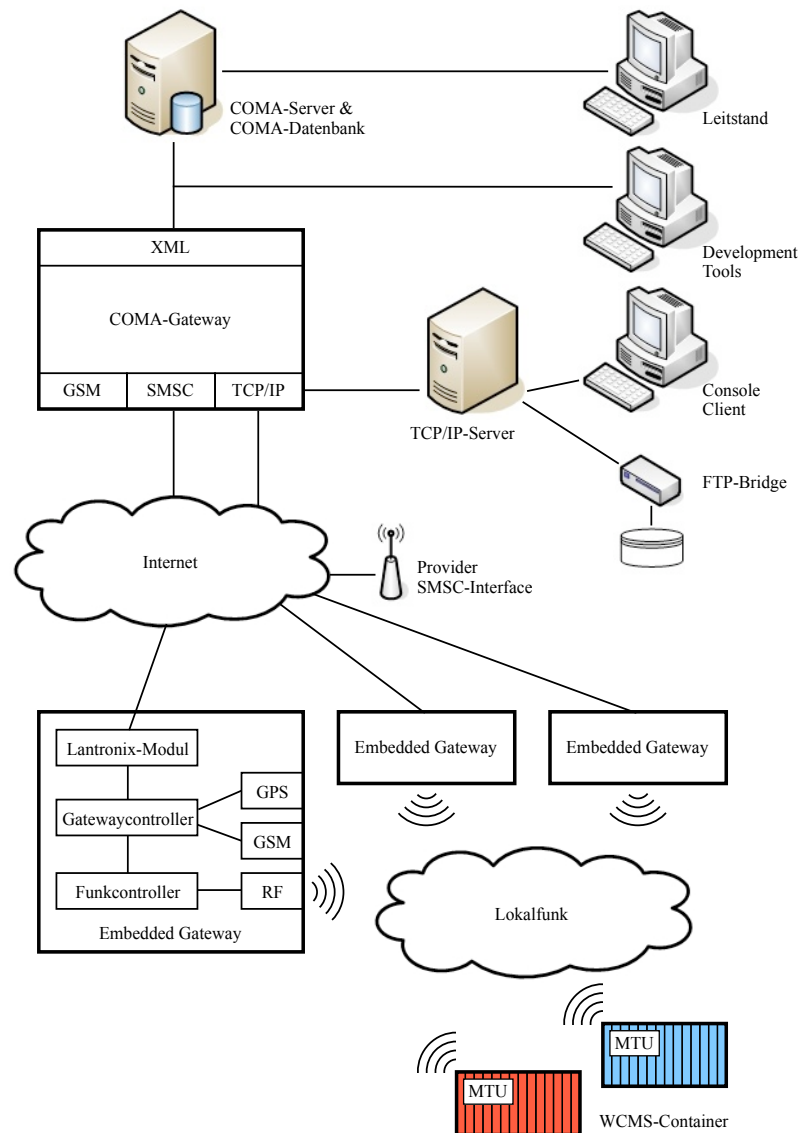


Abbildung 4.1: WCMS-Architektur

4.2 Embedded Gateway

Da der EGW auf Basis der neuen MTU-Hardware (Version 2.0) entwickelt wird, zeigt sich in der Systemarchitektur große Ähnlichkeit (siehe Abbildung 4.2). Der Hauptunterschied liegt in der Erweiterung der Hardware um ein (W)LAN-Modul. Dabei kommt ein Modul von Lantronix zum Einsatz. Im Gegensatz zu vorhergehenden MTU-Versionen kommt am EGW, wie auch bei der neuen MTU-Version, bereits ein STM32-Mikrocontroller von STMicroelectronics zum Einsatz. Ältere MTU-Versionen verwendeten einen LPC2114 von NXP Semiconductors. Weitere Unterschiede liegen in der Optionalität von GPS- und GSM-Modul. Während die Module auf jeder MTU vorhanden sind, wird ein EGW nur für Spezialanwendungen damit ausgerüstet.

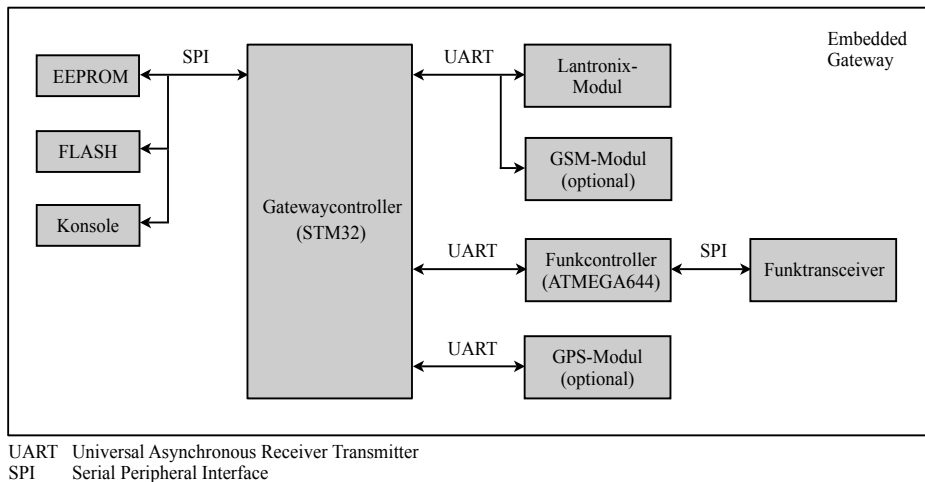


Abbildung 4.2: EGW-Architektur

Der EGW verfügt über zwei Mikrocontroller, den Gatewaycontroller (STM32) und den Funkcontroller (ATMEGA644). Der Gatewaycontroller ist die zentrale Komponente am EGW. Er verwaltet alle anderen Komponenten und ist für die eigentliche Gatewayfunktionalität verantwortlich. Der Funkcontroller steuert den Funktransceiver und implementiert das Funkprotokoll. Der EGW verfügt darüber hinaus über verschiedene nichtflüchtige Speicherbausteine, ein EEPROM und ein FLASH. Eine Konsole ermöglicht die manuelle Konfiguration des EGW über den Gatewaycontroller. Das Lantronix-Modul ist für die Verbindung mit dem Internet verantwortlich. Das Modul ist in einer WLAN- und einer LAN-Ausführung erhältlich. Die Kommunikation über Lokalfunk wird durch einen Funktransceiver ermöglicht. GPS- und GSM-Modul sind optional. Das GSM-Modul kann anstelle des Lantronix-Moduls verwendet werden. Die Internetanbindung erfolgt dabei über GPRS. Ist kein GPS-Modul vorhanden, so kann die geographische Position des EGW manuell über die Konsole konfiguriert werden.

4.2.1 Gatewaycontroller

Die Gatewayapplikation läuft auf einem Mikrocontroller vom Typ STM32F101RBT6 der Firma STMicroelectronics. Dieser Mikrocontroller wird seit der neuen MTU-Generation (Version 2.0) auch als Hauptcontroller der Telematikbox an den Containern eingesetzt. Ältere MTU-Versionen waren mit einem LPC2114 von NXP Semiconductors ausgestattet. Da der EGW auf Basis der MTU-Hardware entwickelt wird, wurden im Zuge dieser Arbeit sämtliche Treiber zur Kommunikation und Steuerung der Peripherie vom LPC2114 auf den STM32 portiert. Durch die Portierung wird die Wiederverwendung einiger Software-Module der MTU am EGW ermöglicht. Darüber hinaus ist die MTU-Applikation mit den neuen Treibern ohne Änderung der höheren Programmschichten am STM32 lauffähig. Dadurch wird der Wechsel auf die neue MTU-Version erleichtert. Der Gatewaycontroller übernimmt am EGW die Aufgabe des Hauptcontrollers, der alle Komponenten verbindet und somit die Gesamtfunktion ermöglicht. Der Gatewaycontroller ist über eine SPI-Schnittstelle mit dem EEPROM, dem FLASH und der Konsole verbunden. Über UART-Schnittstellen kommuniziert der Mikrocontroller mit dem Funkcontroller, dem Lantronix-Modul, dem GSM-Modul (optional) und dem GPS-Modul (optional).

Der STM32 basiert auf einem 32 Bit ARM-Prozessor, dem Cortex-M3. Genaue Informationen über den Prozessor sowie über den Mikrocontroller finden sich in [Hit08]. Der Mikrocontroller wurde unter anderem wegen seiner Eignung für Low-Power-Anwendungen ausgewählt. Der STM32 kann in verschiedene Energiesparmodi versetzt werden und bietet so, in Kombination mit der integrierten Real Time Clock (RTC), die Basis für einen energieeffizienten Betrieb der MTU und des EGW. Es wird mit abnehmendem Energieverbrauch zwischen dem Running-, Sleep-, Stop- und Standby-Modus unterschieden. Im Sleep-Modus wird der Prozessor gestoppt, was zur Folge hat, dass der Applikationscode nicht weiter abgearbeitet wird. Es läuft nur mehr die Peripherie. Aus diesem Modus kann der Mikrocontroller durch einen beliebigen Interrupt geweckt werden. Im Stop-Modus wird zusätzlich zum Prozessor die Peripherie gestoppt, mit Ausnahme der Peripherie für externe Interrupts. Der Zustand bleibt erhalten, da FLASH und RAM (Random Access Memory) weiter versorgt werden. Aus diesem Modus kann der Mikrocontroller nur durch einen externen Interrupt oder einen Alarm der RTC, die einen externen Interrupt auslösen kann, geweckt werden. Da die RTC einen eigenen Oszillator und eine eigene Versorgung besitzt, kann der Mikrocontroller periodisch aus dem Sleep-Modus geweckt werden. Im Standby-Modus ist der Mikrocontroller nahezu abgeschaltet. Der Prozessor und die Peripherie werden gestoppt, der Zustand geht verloren. Dieser Modus kann nur durch einen Alarm der RTC, einen externen Reset, einen Reset durch den Watchdog-Timer oder eine steigenden Flanke am Wakeup-Pin verlassen werden. Das Verlassen des Standby-Modus kommt einem Programmneustart gleich. Die einzige Region des Mikrocontrollers, die in allen Modi versorgt wird, ist die Backup-Region. Sie beinhaltet die RTC, den Watchdog-Timer und zehn 16 Bit breite Speicherregister. Die Backup-Region verfügt über einen eigenen Versorgungsanschluss, sodass sie mit Hilfe einer Batterie, unabhängig von den restlichen Regionen, versorgt werden kann. Der tatsächlich erreichbare Stromverbrauch ist anwendungsspezifisch, da er von der Taktfrequenz des Prozessors sowie von der aktivierten Peripherie abhängt. Der STM32F101RTB6 kann mit bis zu 36 MHz betrieben werden. In den aktuellen Tests wurde die Taktrate auf 24 MHz festgelegt. Folgende Werte beziehen sich auf eine Versorgungsspannung von 3,3 V und wurden aus [Hit08] entnommen. Im Standby-Modus kann der Stromverbrauch auf $1,4 \mu\text{A}$ gesenkt werden, während im Stop-Modus bereits rund $15,4 \mu\text{A}$ benötigt werden. Beim Sleep- und Running-Modus richtet sich der Verbrauch nach der eingestellten Taktfrequenz und der aktivierten Peripherie. Im Sleep-Modus kann bei 24 MHz ein Verbrauch zwischen 2,3 mA und 5,3 mA erreicht werden. Im Running-Modus beträgt der Stromverbrauch bei 24 MHz knapp unter 20 mA.

4.2.2 Funkcontroller

Die Funkapplikation ist auf einen eigenen Mikrocontroller ausgelagert. Für die Aufgabe kommt ein ATMEGA644P von Atmel zum Einsatz. Der Funkcontroller implementiert die zeitkritische Funkapplikation sowie die Treibersoftware zur Ansteuerung des Funktransceivers. Der Funkcontroller kommuniziert mit dem Gatewaycontroller über eine UART-Schnittstelle. Der Datenaustausch erfolgt mit folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit, kein Paritätsbit und keine Flusskontrolle. Die Baudrate beträgt 125000 Bit/s. Das LSB (Least Significant Bit) wird zuerst übertragen. Die Kommunikation erfolgt nach dem im Zuge des WCMS-Projekts entwickelten Extended Protocol. Für den EGW wurde dieses Protokoll um ein neues Profil erweitert (siehe Abschnitt 4.3). Zur Umsetzung dieses Protokolls werden neben den Datenleitungen zwei zusätzliche Handshake-Leitungen benötigt. Der Datenaustausch zwischen dem Funkcontroller und dem Funktransceiver erfolgt über eine SPI-Schnittstelle. Der Funkcontroller kann darüber hinaus den Funktransceiver in einen Schlafmodus versetzen und einen Reset auslösen. Der Transceiver kann am Funkcontroller einen Interrupt auslösen.

4.2.3 Funktransceiver

Die Kommunikation via Lokalfunk erfolgt am EGW mit Hilfe eines Funktransceivers vom Typ AT86RF230 der Firma Atmel. Container in Reichweite eines EGW können über Lokalfunk die Dienste des Gateways in Anspruch nehmen. Nach der erfolgreichen Anmeldung an einen EGW kann ein Container über Lokalfunk SMS-Nachrichten empfangen und versenden, aktuelle GPS-Daten abfragen und größere Datenmengen über den Stream-Dienst austauschen. Der Transceiver unterstützt den IEEE 802.15.4-Standard. Er eignet sich daher auch für die Implementierung von ZigBee-Applikationen. Im Rahmen des WCMS-Projekts setzt jedoch ein spezifisches Protokoll auf den Schichten des IEEE 802.15.4-Standards auf. Der Transceiver arbeitet auf einer Frequenz von 2,4 GHz mit einer Übertragungsrate von 250 kBit/s. Der Funktransceiver wird vom Funkcontroller über eine SPI-Schnittstelle gesteuert. Der Funkcontroller implementiert die Treibersoftware sowie das restliche Funkprotokoll. Der Transceiver wird permanent versorgt, kann jedoch vom Funkcontroller in einen Schlafmodus versetzt werden. Aufgrund des geringen Leistungsverbrauchs (siehe Tabelle 4.1) eignet sich der Transceiver für den Einsatz in Low-Power-Anwendungen.

Tabelle 4.1: Der Funktransceiver AT86RF230 von Atmel eignet sich aufgrund des niedrigen Leistungsverbrauchs für Low-Power-Anwendungen [Atm07].

	Schlafmodus	Empfangsmodus	Sendemodus
Versorgungsspannung	1,8 V bis 3,6 V	1,8 V bis 3,6 V	1,8 V bis 3,6 V
Stromverbrauch	20 nA	15,5 mA	16,5 mA ^[1]
Leistungsverbrauch ^[2]	60 nW	46,5 mW	49,5 mW

[1] bei einer maximalen Sendeleistung von 3 dBm

[2] bei einer Versorgungsspannung von 3 V

4.2.4 Lantronix-Modul

Der EGW wird mit einem WLAN- beziehungsweise LAN-Modul an das Internet angebunden. Bei den bisherigen Tests wurde dabei ein Modul vom Typ MatchPort AR des Herstellers Lantronix verwendet. Das Modul übernimmt das gesamte Netzwerkmanagement und sendet beziehungsweise empfängt Daten über Ethernet. Der Gatewaycontroller kommuniziert mit dem Lantronix-Modul über eine UART-Schnittstelle. Der Datenaustausch erfolgt mit folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit und kein Paritätsbit. Die Flusskontrolle erfolgt über RTS/CTS-Leitungen. Die Baudrate beträgt 115200 Bit/Sekunde. Das LSB wird zuerst übertragen. Der Gatewaycontroller besitzt weiters die Möglichkeit, den Verbindungsstatus (verbunden/nicht verbunden) des Lantronix-Moduls über eine zusätzliche Leitung abzufragen. Der Datenaustausch zwischen CGW und Lantronix-Modul erfolgt über TCP/IP. Das Lantronix-Modul verfügt über einen Web-Server und kann über einen Web-Browser oder alternativ über eine Telnet-Verbindung konfiguriert werden. Darüber hinaus unterstützt das Modul SNMP (Simple Network Management Protocol). Im Hinblick auf Security bietet das Modul SSL (Secure Sockets Layer) und SSH (Secure Shell). Bei der Verschlüsselung kann zwischen AES, 3DES und RC4 in Kombination mit SHA-1-, MD5- oder Base-64-Authentifizierung gewählt werden. Die Schlüssellänge kann bis zu 1024 Bit betragen. Der Leistungsverbrauch liegt bei einer Versorgung mit 3,3 V im Durchschnitt bei 0,67 W und ist somit im Ruhezustand rund 150 mal höher als der des GSM-Moduls (siehe Abschnitt 4.2.5) [Lan09].

Aus diesem Grund besteht die Option, den EGW anstelle des Lantronix-Moduls mit einem GSM-Modul auszustatten. Diese Option ist derzeit jedoch nur für Low-Power-Anwendungen geplant, welche über keine zusätzliche Versorgungsinfrastruktur verfügen.

4.2.5 GSM-Modul

Die Ausstattung des EGW mit einem GSM-Modul ist als Option definiert. Für die Tests bei der Entwicklung wird ein Modul vom Typ HiLo des Herstellers SAGEM verwendet. Dieses Modul wird auch auf der MTU eingesetzt. Das GSM-Modul wird zum Versenden und Empfangen von SMS-Nachrichten benutzt (SMS-Service) und soll via GPRS die Schnittstelle zum Internet bilden (Stream-Service). Ein EGW verfügt entweder über ein GSM-Modul oder ein LAN- beziehungsweise WLAN-Modul. Es werden nicht beide Module auf einem EGW eingebaut. Die GSM-Option des EGW ist im Hinblick auf eine Low-Power-Ausführung des EGW gedacht, da der durchschnittliche Leistungsverbrauch des getesteten Lantronix-Moduls deutlich über dem des GSM-Moduls liegt. Ein EGW mit der GSM-Option kann zum Beispiel auf Masten im Freien montiert werden und seine Versorgung über Solarzellen beziehen. Die derzeitige Standardausführung des EGW besitzt kein GSM-Modul, sondern wird über ein Lantronix-Modul an das Internet angebunden. Die Abmessungen des GSM-Moduls betragen 27 mm x 27 mm x 3,6 mm. Aufgrund der Quad-Band-Unterstützung kann das Modul auf 850, 900, 1800 sowie 1900 MHz kommunizieren [Sag09]. Der Gatewaycontroller ist mit dem GSM-Modul über eine UART-Schnittstelle verbunden. Der Datenaustausch erfolgt mit folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit, kein Paritätsbit und RTS/CTS-Flusskontrolle. Die Baudrate beträgt 115200 Bit/Sekunde. Das LSB wird zuerst übertragen. Der Gatewaycontroller kann aus energetischen Gründen die Versorgung des Moduls ein- und ausschalten. Die Versorgungsspannung des Moduls kann zwischen 3,2 V und 4,5 V liegen, wobei der nominale Wert 3,6 V beträgt. Tabelle 4.2 gibt einen Überblick des typischen Stromverbrauchs bei einer Versorgung mit 3,6 V. Zu beachten ist, dass im Standby-, COM- und GPRS-Modus Bursts mit bis zu 1,7 A bei 850/900 MHz und bis zu 1,5 A bei 1800/1900 MHz auftreten [Sag09].

Tabelle 4.2: Stromverbrauch des GSM-Moduls bei einer Versorgungsspannung von 3,6 V [Sag09]

Frequenz	Off-Modus	Standby-Modus	COM-Modus	GPRS-Modus ^[1]
850 MHz	35 μ A	1,25 mA	220 mA	360 mA
900 MHz	35 μ A	1,25 mA	220 mA	360 mA
1800 MHz	35 μ A	1,25 mA	160 mA	245 mA
1900 MHz	35 μ A	1,25 mA	160 mA	245 mA

[1] bei der Nutzung von 2 Sendezeitschlitzen und 3 Empfangszeitschlitzen

4.2.6 GPS-Modul

Das GPS-Modul ist als Option für den EGW definiert. Aktuell wird ein GPS-Modul vom Typ UC322 der Firma Fastrax für die Tests während der Entwicklung verwendet. Im Normalfall wird der EGW stationär montiert, sodass sich die geographischen Koordinaten nicht verändern. In diesem Fall ist es ausreichend, die GPS-Daten einmalig bei Inbetriebnahme des EGW zu konfigurieren. Die manuelle Konfiguration der GPS-Daten erfolgt über die Konsole. Im Fall, dass

der EGW mit einem GSM-Modul ausgestattet ist, kann die Konfiguration alternativ über GSM in Form einer SMS-Nachricht durchgeführt werden. Ist ein EGW mit einem GPS-Modul ausgestattet, so kann die Konfiguration der GPS-Daten auch automatisch erfolgen. Zu beachten ist, dass alle Container in Reichweite eines EGW durch das Location-Service identische GPS-Daten erhalten. Die räumliche Anordnung der Container kann daher ohne zusätzliche Ressourcen nicht ermittelt werden. Der Gatewaycontroller kommuniziert mit dem GPS-Modul über eine UART-Schnittstelle. Der Datenaustausch erfolgt mit folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit, kein Paritätsbit und keine Flusskontrolle. Die Baudrate beträgt 4800 Bit/Sekunde. Das LSB wird zuerst übertragen. Aus energetischen Gründen kann der Gatewaycontroller die Versorgung des Moduls ein- und ausschalten. Der Gatewaycontroller besitzt weiters die Möglichkeit, das GPS-Modul in den so genannten Hibernate-Modus zu versetzen. In diesem Modus werden nur mehr das interne RAM und die RTC versorgt. Das GPS-Modul unterstützt das NMEA- sowie das SiRF-Format [Fas08].

4.2.7 Speicher

Der EGW verfügt über verschiedene nichtflüchtige Speicherbausteine (siehe Tabelle 4.3). Für die Speicherung größerer Datenblöcke steht ein FLASH zur Verfügung und für die Speicherung von Konfigurations- oder Bootparametern ein EEPROM. Beide Speicher werden vom Gatewaycontroller über dieselbe SPI-Schnittstelle angesprochen. Durch Chip-Enable-Leitungen kann der gewünschte Speicher ausgewählt werden. Da die MTU sowie der EGW im Hinblick auf geringsten Leistungsverbrauch entwickelt werden, kann der Gatewaycontroller die Versorgung beider Speicherbausteine ein- und ausschalten. Die Versorgung der Speicher kann jedoch nicht für jeden Baustein individuell, sondern nur für beide gemeinsam geschaltet werden.

Tabelle 4.3: Vergleich der technischen Daten von FLASH und EEPROM am EGW [SST06, Atm05]

	FLASH	EEPROM
Typ	SST25VF080B	AT25640A
Versorgungsspannung	2,7 V bis 3,6 V	2,7 V bis 5,5 V
Kapazität	8 MBit	64 kBit
Schreibzyklen	typ. 100000	typ. 1000000
Taktfrequenz ^[1]	max. 50 MHz	max. 5 MHz

[1] serielle Übertragungsrate auf der SPI-Schnittstelle

Als FLASH wird ein IC vom Typ SST25VF080B der Firma SST (Silicon Storage Technologie Inc.) verwendet. Dieser Speicherbaustein stellt ein serielles 4-Draht-Interface zur Verfügung, das über eine SPI-Schnittstelle des Gatewaycontrollers angesprochen wird. Das FLASH kann komplett oder in einzelnen Blöcken zu 4, 32 oder 64 kByte gelöscht werden. Der Speicher hat eine Kapazität von rund 8 MBit (8388600 Bit) und ist in 1048575 Speicheradressen zu je 8 Bit organisiert [SST06]. Als EEPROM wird ein IC vom Typ AT25640A der Firma Atmel verwendet. Der Speicherbaustein stellt, wie der FLASH-IC, ein serielles 4-Draht-Interface zur Verfügung, das über eine SPI-Schnittstelle des Gatewaycontrollers angesprochen wird. Der Speicher hat eine Kapazität von rund 64 kBit (65536 Bit) und ist in 8192 Speicheradressen zu je 8 Bit organisiert. Im Gegensatz zum FLASH werden keine separaten Löschyklen vor einem Schreibzyklus benötigt [Atm05].

4.2.8 Konsole

Der EGW stellt über den Gatewaycontroller eine Konsole zur Verfügung, die während der Entwicklung für Debug-Zwecke verwendet werden kann. Im Betrieb kann der EGW über die Konsole konfiguriert werden sowie interne Informationen ausgeben. Das eigentliche Interface für das Konsolen-Modul am Gatewaycontroller ist eine SPI-Schnittstelle des Mikrocontrollers. Dieselbe SPI-Schnittstelle wird auch zur Kommunikation mit den beiden Speicherbausteinen benutzt, weshalb mit Hilfe von Chip-Enable-Leitungen die gewünschte Gegenstelle ausgewählt werden muss. Die Leitungen der SPI-Schnittstelle sind über eine Steckverbindung an der EGW-Platine zugänglich. Um ein beliebiges Terminal- oder Konsolenprogramm für die Interaktion mit dem Gatewaycontroller und somit dem EGW verwenden zu können, muss mit zusätzlicher Hardware eine Verbindung zwischen der SPI-Schnittstelle am EGW und einem PC hergestellt werden (siehe Abbildung 4.3). Aktuell wird eine externe Platine verwendet, die eine SPI/UART-Bridge und eine UART/USB-Bridge zur Verfügung stellt. Diese Platine wird über eine Flachbandleitung mit der EGW-Platine verbunden. Mit Hilfe eines handelsüblichen USB-Kabels kann die Platine mit jedem Notebook oder PC, der über eine USB-Schnittstelle verfügt, verbunden werden. Am PC oder Notebook erscheint die UART/USB-Bridge als virtueller COM-Port. Bei den Tests wurde das Terminalprogramm HTerm eingesetzt. Dieses Programm kann kostenlos aus dem Internet bezogen werden.

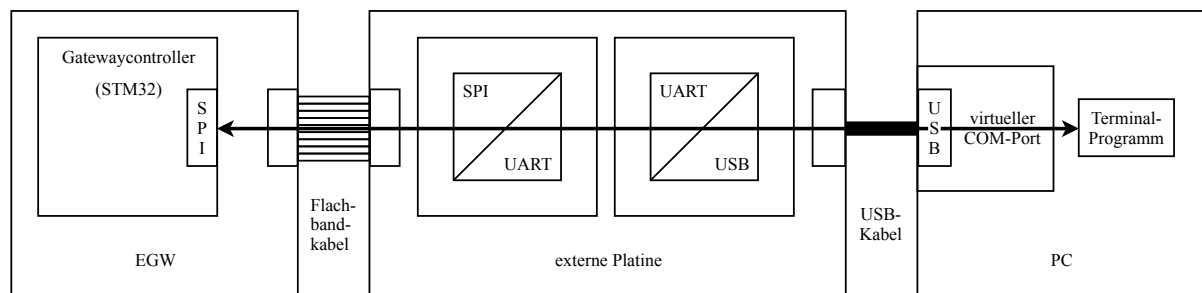


Abbildung 4.3: Verbindung der Konsole am Gatewaycontroller mit einem Terminalprogramm am PC

Um sich mit dem Konsolen-Modul am Gatewaycontroller über ein Terminalprogramm verbinden zu können, sind folgende Parameter zu verwenden: 1 Startbit, 8 Datenbits, 1 Stoppbit, kein Paritätsbit und keine Flusskontrolle. Die Baudrate beträgt 38400 Bit/Sekunde. Das LSB wird zuerst übertragen. Besteht eine Verbindung, so können EGW-interne Informationen im Terminalfenster angezeigt werden und Befehle über die Tastatur an den Gatewaycontroller gesendet werden.

4.3 Schnittstellendefinition

Der EGW besitzt über den Funkcontroller und den Funktransceiver einen Lokalfunkzugang und über das Lantronix-Modul einen Internetzugang. Zwischen diesen beiden Anbindungen sitzt der Gatewaycontroller, der für die Gatewayfunktion verantwortlich ist. Der Gatewaycontroller ist mit dem Lantronix-Modul und mit dem Funkcontroller über eine UART-Schnittstelle verbunden.

Die Schnittstelle zum Lantronix-Modul besteht aus der Sende- und Empfangsleitung, zwei Leitungen für die Flusskontrolle und einer Statusleitung (siehe Abbildung 4.4). Der Datenaustausch erfolgt mit den folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit und kein Paritätsbit.

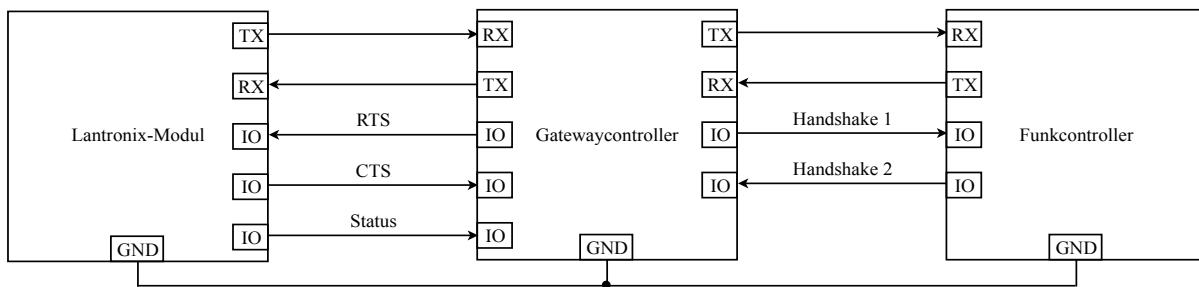


Abbildung 4.4: Schnittstellen zwischen Gatewaycontroller, Funkcontroller und Lantronix-Modul

Die Flusskontrolle erfolgt über RTS/CTS-Leitungen. Die Baudrate beträgt 115200 Bit/s. Das LSB wird zuerst übertragen. Der Gatewaycontroller besitzt weiters die Möglichkeit, den Verbindungsstatus (verbunden/nicht verbunden) des Lantronix-Moduls über eine zusätzliche Leitung abzufragen. Die Kommunikationspakete, die zwischen Lantronix-Modul und Gatewaycontroller ausgetauscht werden, besitzen den gleichen grundlegenden Aufbau (siehe Abbildung 4.5). Jedes Paket setzt sich aus zwei Startbytes, einem Längenbyte, den Nutzdaten und einer CRC8-Checksumme (Cyclic Redundancy Check) zusammen. Die Startbytes dienen der Kennung des Paketanfangs und ermöglichen im Fehlerfall eine Resynchronisierung beim Empfang der Datenpakete. Das Längenfeld gibt die Länge der Nutzdaten in Byte an. Mit dem letzten Byte jedes Kommunikationspakets wird eine CRC8-Checksumme übertragen. Sie dient der Erkennung von Übertragungsfehlern. Die CRC8-Checksumme wird nur über die Nutzdaten gebildet. Die maximale Länge eines Datenpakets beträgt 259 Byte, wobei maximal 255 Byte Nutzdaten übertragen werden können. Das erste Byte der Nutzdaten ist für den Nutzdatentyp reserviert.

generisches Kommunikationspaket

Byte	1	2	3	4	5	...	n	n+1
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdaten				CRC8
Wert	0x7E	0xDB	-	-	-	-	-	-

Abbildung 4.5: Aufbau der Kommunikationspakete zwischen Gatewaycontroller und Lantronix-Modul

Da der EGW einen niedrigen Energieverbrauch anstrebt, werden der Gateway- und der Funkcontroller so oft wie möglich in einen energiesparenden Schlafmodus versetzt. Dadurch muss vor einer Datenübertragung zuerst sichergestellt werden, dass die Gegenstelle aktiv ist. Aus diesem Grund wird das im Rahmen des WCMS-Projekts entwickelte Extended Protocol (EXTPROTO) angewendet. Dieses Protokoll wurde ursprünglich für die serielle Kommunikation zwischen externen Einheiten und dem zentralen Controller der MTU entwickelt. Dabei wird durch ein Handshake-Verfahren vor der Übertragung sichergestellt, dass beide Einheiten für die Kommunikation bereit sind. Abbildung 4.6 zeigt das Handshake-Verfahren. Die Kommunikation zwischen zwei Einheiten wird durch das High-Setzen einer Handshake-Leitung eingeleitet (1). Der Empfänger setzt sobald er bereit ist die andere Handshake-Leitung auf High-Pegel (2). Der Sender beginnt danach mit der Datenübertragung. Der Empfänger setzt seine Handshake-Leitung wieder auf Low-Pegel (3). Sender und Empfänger bleiben, solange eine Handshake-Leitung auf High-Pegel liegt, kommunikationsbereit (4). Die Kommunikation wird beendet, wenn beide Leitungen wieder auf Low-Pegel liegen (5). Das EXTPROTO definiert darüber hinaus, dass jede Datenübertragung vom zentralen Controller eingeleitet wird. Externe Einheiten müssen, falls sie mit dem zentralen Con-

troller kommunizieren möchten, das Handshake-Verfahren beginnen. Sie dürfen danach aber nicht sofort Daten übertragen, sondern werden vom zentralen Controller abgefragt. Im Fall des EGW ist der Gatewaycontroller der zentrale Controller und der Funkcontroller die externe Einheit.

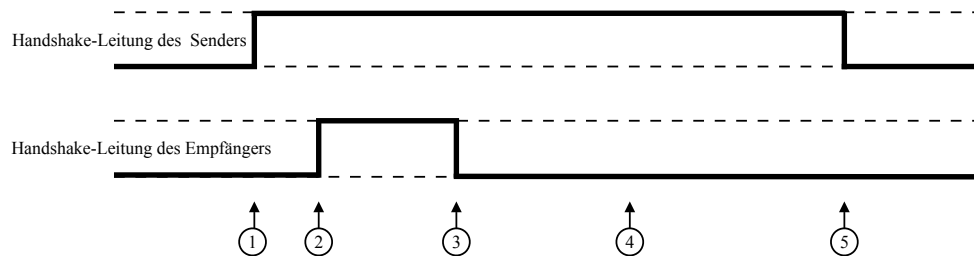


Abbildung 4.6: Handshake-Verfahren nach dem Extended Protocol (EXTPROTO)

Die Schnittstelle zum Funkcontroller besteht aus der Sende- und Empfangsleitung und zwei Leitungen für das Handshake-Verfahren nach dem EXTPROTO (siehe Abbildung 4.4). Der Datenaustausch erfolgt mit folgenden Parametern: 1 Startbit, 8 Datenbits, 1 Stoppbit, kein Paritätsbit und keine Flusskontrolle. Die Baudrate beträgt 125000 Bit/s. Das LSB wird zuerst übertragen. Die Kommunikationspakete, die zwischen Gatewaycontroller und Funkcontroller ausgetauscht werden, besitzen den gleichen grundlegenden Aufbau (siehe Abbildung 4.7). Jedes Paket setzt sich aus einem Längenbyte, den Nutzdaten und einer XOR-Checksumme zusammen. Die maximale Länge eines Datenpakets beträgt 257 Byte, wobei maximal 255 Byte an Nutzdaten übertragen werden können. Ein Byte wird jeweils für das Längenfeld und die XOR-Checksumme benötigt. Das erste Byte der Nutzdaten ist für den Nutzdatentyp reserviert. Die XOR-Checksumme wird nur über die Nutzdaten gebildet. Das Längenfeld gibt die Länge der Nutzdaten in Byte an. Mit dem letzten Byte jedes Kommunikationspakets wird die XOR-Checksumme übertragen. Sie dient der Erkennung von Übertragungsfehlern.

Byte	1	2	3	4	5	...	n	n+1
Bezeichnung	Länge	Nutzdaten						XOR
Wert	-	-	-	-	-	-	-	-

Abbildung 4.7: Aufbau der Kommunikationspakete zwischen Gatewaycontroller und Funkcontroller

5 Implementierung

Der EGW besitzt zwei Mikrocontroller, den Gatewaycontroller und den Funkcontroller. Dieses Kapitel beschreibt die Gatewayapplikation am Gatewaycontroller. Die Funkapplikation am Funkcontroller ist nicht Teil dieser Arbeit. Die Applikation am CGW und die Funkapplikation werden nur allgemein berücksichtigt, um die Rolle der Gatewayapplikation im Gesamtsystem zu beschreiben. Dieses Kapitel gibt einen Überblick über den implementierten Protokollstapel. Es werden die definierten Kommunikationspakete im Detail erklärt und ihre Anwendung gezeigt. Darüber hinaus werden die implementierten Dienste beschrieben.

5.1 Protokollstapel

Am EGW findet die Umsetzung von einem lokalen Funkprotokoll auf TCP/IP statt (siehe Abbildung 5.1). Dadurch wird Containern in EGW-Reichweite die Kommunikation mit dem Datacenter ermöglicht. Die Container kommunizieren über den energiesparenden Lokalfunk und können über die Netzwerkanbindung des EGW auf ein globales Informationssystem zugreifen. Die Protokollumsetzung erfolgt durch den Gatewaycontroller, den Funkcontroller und das Lantronix-Modul.

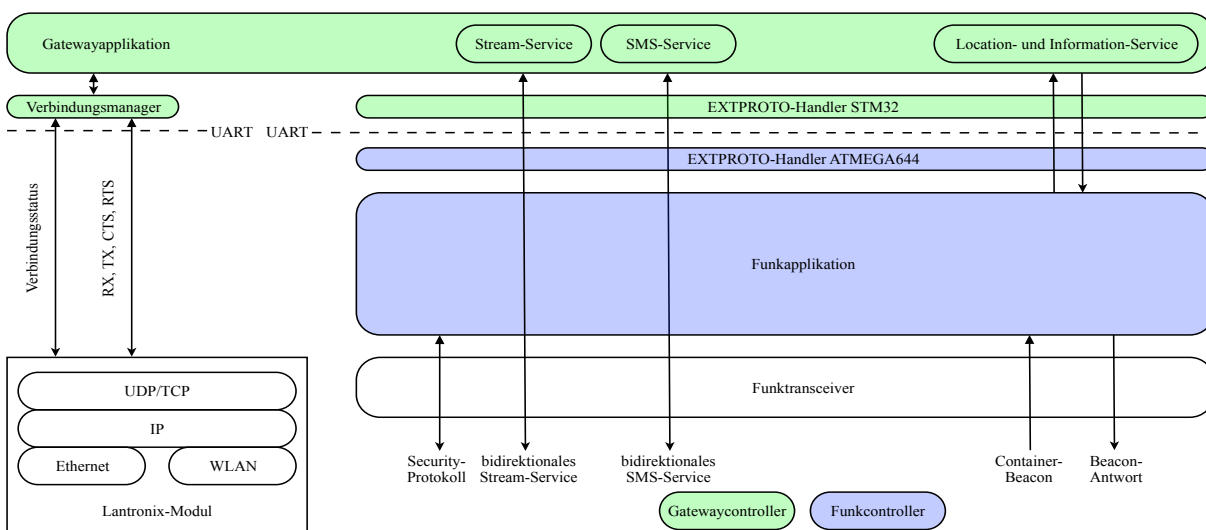


Abbildung 5.1: EGW-Protokollstapel

Die Gatewayapplikation stellt die definierten Dienste zur Verfügung. Dazu zählen das SMS-, das Stream- und das Location-Service. Das Location-Service ist in Abbildung 5.1 als Location- und Information-Service dargestellt, da neben den GPS-Daten auch noch andere Konfigurationsparameter abgefragt werden können. Der Verbindungsmanager ist für die Kommunikation mit dem Lantronix-Modul zuständig. Die Kommunikation zwischen Gatewaycontroller und Lantronix-Modul erfolgt über eine UART-Schnittstelle. Das Lantronix-Modul ist für die (W)LAN-Anbindung verantwortlich. Das Modul setzt das UART-Protokoll auf TCP/IP um. Über einen Internetanschluss kann dadurch die Kommunikation mit dem CGW erfolgen. Der EXTPROTO-Handler am Gatewaycontroller dient zur Anbindung an den Funkcontroller. Dieses Modul implementiert das Extended Protocol. Der Handler ist für die Kommunikation mit dem Funkcontroller über eine UART-Schnittstelle zuständig. Die Funkapplikation implementiert das Funkprotokoll und stellt die Treiber für den Funktransceiver zur Verfügung. Darüber hinaus ist sie für die Verarbeitung der empfangenen Beacons von den Containern zuständig. Die Sicherheit und die kryptographische Absicherung des Funkverkehrs werden hier verwaltet. Die Funkapplikation umfasst ebenfalls einen EXTPROTO-Handler für die Kommunikation mit dem Gatewaycontroller.

5.2 Netzwerkanbindung

Der Zugang zum lokalen Netzwerk erfolgt über das Lantronix-Modul. Es sind LAN- und WLAN-Ausführungen erhältlich. Über die lokale Infrastruktur und einen Internetzugang kann der EGW mit dem Datacenter kommunizieren. Die Daten zwischen Gatewaycontroller und Lantronix-Modul werden über eine UART-Schnittstelle ausgetauscht. Die genauen Betriebsparameter, die physikalischen Anschlüsse und der allgemeine Aufbau der Kommunikationspakete finden sich in Abschnitt 4.3. Aufbauend auf den Ergebnissen der Problemanalyse wurden verschiedene spezifische Pakettypen festgelegt.

SMS-Paket

Das SMS-Paket (siehe Abbildung 5.2) dient der Übertragung von Kurznachrichten. Es beinhaltet als Nutzdaten den Datentyp (0x00), die MTU-ID und die eigentliche Nachricht. Die MTU-ID ist 32 Bit breit, wobei das MSB (Most Significant Byte) zuerst übertragen wird. Sie dient dazu, den Container, der das Paket empfangen soll beziehungsweise versendet hat, eindeutig zu identifizieren. Die SMS-Daten sind projektspezifisch auf maximal 140 Byte je SMS-Paket festgelegt. Theoretisch können 250 Byte SMS-Daten je SMS-Paket übertragen werden.

SMS-Paket								
Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	MTU-ID			
Wert	0x7E	0xDB	-	0x00	-	-	-	-

Byte	9	...	n	n+1
Bezeichnung	SMS			CRC8
Wert	-	-	-	-

Abbildung 5.2: Aufbau eines SMS-Pakets

NACK-Paket

Das NACK¹-Paket (siehe Abbildung 5.3) dient der Information im Fehlerfall. Kann ein SMS-Paket vom EGW nicht an den Container weitergeleitet werden, wird ein NACK-Paket an den Absender retourniert. Dieses Paket gleicht dem ursprünglichen SMS-Paket bis auf den Nutzdatentyp (0x01). Der Empfang eines NACK-Pakets bedeutet, dass das SMS-Paket auf dem gewählten Weg nicht zugestellt werden konnte. Als Reaktion kann ein alternativer Kommunikationsweg (GSM) gewählt werden oder die Information an eine höhere Instanz weitergeleitet werden.

NACK-Paket

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	MTU-ID			
Wert	0x7E	0xDB	-	0x01	-	-	-	-

Byte	9	...	n	n+1
Bezeichnung	SMS			CRC8
Wert	-	-	-	-

Abbildung 5.3: Aufbau eines NACK-Pakets

Stream-Data-Paket

Das Stream-Data-Paket (siehe Abbildung 5.4) dient der Übertragung von Stream-Daten. Es ist für die Übertragung größerer Datenmengen (Logfiles, Firmwareupdates) und die Implementierung einer interaktiven Konsolenverbindung vorgesehen. Bevor Stream-Daten übertragen werden können, muss ein Kanal geöffnet werden (siehe Stream-Information-Paket). Mit einem Paket können maximal 249 Byte Stream-Daten übertragen werden. Der gewünschte Kanal wird im Service-ID-Feld angegeben. Eine Streamverbindung wird durch Schließen des Kanals beendet (siehe Stream-Information-Paket). In den Nutzdaten sind zusätzlich der Nutzdatentyp (0x02) und die MTU-ID enthalten.

Stream-Data-Paket

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	MTU-ID			
Wert	0x7E	0xDB	-	0x02	-	-	-	-

Byte	9	10	...	n	n+1
Bezeichnung	Service-ID	Streamdaten			CRC8
Wert	-	-	-	-	-

Abbildung 5.4: Aufbau eines Stream-Data-Pakets

¹NACK steht in der Informatik für „not acknowledged“. Die Abkürzung wird verwendet, wenn eine Anfrage negativ beantwortet werden soll.

Stream-Information-Paket

Das Stream-Information-Paket (siehe Abbildung 5.5) dient der Steuerung des Stream-Dienstes. Es wird zum Öffnen und Schließen einer Verbindung und zur Übertragung weiterer Steuerinformationen genutzt. Im Service-ID-Feld wird der betreffende Kanal angegeben und im Status-Feld die zu übertragende Information: 0x00 - Öffnen eines Stream-Kanals, 0x01 - Schließen eines Stream-Kanals, 0x02 - Schließen eines Stream-Kanals (Fehlerfall), 0x03 - Stream-Kanal offen. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. In den Nutzdaten sind zusätzlich der Nutzdatentyp (0x03) und die MTU-ID enthalten.

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	MTU-ID			
Wert	0x7E	0xDB	0x07	0x03	-	-	-	-

Byte	9	10	11
Bezeichnung	Service-ID	Status	CRC8
Wert	-	-	-

Abbildung 5.5: Aufbau eines Stream-Information-Paketes

Identification-Paket

Das Identification-Paket (siehe Abbildung 5.6) dient der Ermittlung der Gegenstellen-ID. Das Status-Feld wird zur Übertragung von Steuerinformationen genutzt: 0x00 - Anfrage, 0x01 - Antwort. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. Das Paketformat wird für die Anfrage und die Antwort verwendet. Bei der Anfrage werden die ID-Felder leer gelassen. Der Empfänger fügt seine ID ein, ändert das Status-Feld und retourniert das Paket. Der CGW kann mit diesem Paket zum Beispiel die ID eines EGW feststellen. In den Nutzdaten ist zusätzlich der Nutzdatentyp (0x04) enthalten.

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	Status	ID		
Wert	0x7E	0xDB	0x06	0x04	-	-	-	-

Byte	9	10
Bezeichnung	ID	CRC8
Wert	-	-

Abbildung 5.6: Aufbau eines Identification-Paketes

Membership-Information-Paket

Das Membership-Information-Paket (siehe Abbildung 5.7) wird zur Übertragung von Informationen über die Mitgliedschaft eines Containers bei einem EGW genutzt. Das Status-Feld enthält

die eigentliche Steuerinformation: 0x00 - Anfrage auf Mitgliedschaft, 0x01 - Mitgliedschaft gestattet, 0x02 - Container ignorieren, 0x03 - Mitgliedschaft beendet. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. In den Nutzdaten sind zusätzlich der Nutzdatentyp (0x05), die EGW-ID, die MTU-ID sowie Felder zur Übertragung zusätzlicher Informationen enthalten. Nicht verwendete Felder werden leer gelassen. Im Signalstärke-Feld kann eine Wertung der Funkempfangssignalstärke am EGW eingetragen werden. Im Mitglieder-Feld kann die Anzahl der bereits am EGW angemeldeten Container eingetragen werden. Die Informationen können zur EGW-Selektion am CGW genutzt werden.

Membership-Information-Paket

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Startbyte 1	Startbyte 2	Länge	Nutzdatentyp	Status	EGW-ID		
Wert	0x7E	0xDB	0x0C	0x05	-	-	-	-

Byte	9	10	11	12	13	14	15	16	
Bezeichnung	EGW-ID	MTU-ID				Signalstärke	Mitglieder	CRC8	
Wert	-	-	-	-	-	-	-	-	

Abbildung 5.7: Aufbau eines Membership-Information-Pakets

5.3 Funkanbindung

Der Zugang zum Lokalfunk erfolgt über den Funkcontroller und den Funktransceiver. Über Lokalfunk kann der EGW mit den Containern in Funkreichweite kommunizieren. Die Daten zwischen Gatewaycontroller und Funkcontroller werden über eine UART-Schnittstelle ausgetauscht. Die genauen Betriebsparameter, die physikalischen Anschlüsse und der allgemeine Aufbau der Kommunikationspakete finden sich in Abschnitt 4.3. Aufbauend auf den Ergebnissen der Problemanalyse wurden verschiedene spezifische Pakettypen festgelegt.

Report-Paket

Die Kommunikation zwischen Gatewaycontroller und Funkcontroller baut auf dem Extended Protocol auf (siehe Abschnitt 4.3). Eine Kommunikation besteht immer aus Anfrage und Antwort. Die Datenübertragung muss vom Gatewaycontroller gestartet werden. Im Fall, dass der Funkcontroller Daten übertragen möchte, muss er den Gatewaycontroller über das Handshake-Verfahren informieren. Dieser fragt in Folge mit einem Report-Paket (siehe Abbildung 5.8) die Daten ab. Der Nutzdatentyp wird alternierend mit 0x60 und 0x61 codiert. Dadurch kann festgestellt werden, ob es sich um eine neue Anfrage oder die Wiederholung der vorhergehenden Anfrage handelt. Als Antwort auf ein Report-Paket stehen mehrere Pakettypen zur Verfügung.

Der Nutzdatentyp eines Response-Pakets wird aus dem zugehörigen Request-Paket übernommen (0x60 oder 0x61). Im Request-Feld wird die Forderung codiert. Je nach Forderung unterscheidet sich der Aufbau der Pakete. Wenn die Kommunikation versehentlich eingeleitet wurde oder keine Forderung ansteht, kann mit einem Report-Response-Paket mit Request 0x00 geantwortet werden (siehe Abbildung 5.9).

Report-Paket (Request)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x60/0x61	0x60/0x61

Abbildung 5.8: Aufbau eines Report-Request-Pakets

Report-Paket (Response): kein Request

Byte	1	2	3	4
Bezeichnung	Länge	Nutzdatentyp	Request	XOR
Wert	0x02	0x60/0x61	0x00	0x60/0x61

Abbildung 5.9: Aufbau eines Report-Response-Pakets ohne Request

Um SMS-Daten vom Funkcontroller an den Gatewaycontroller zu übertragen, werden die Daten in die Antwort auf das Report-Paket hineingepackt (siehe Abbildung 5.10). Der Request für das SMS-Service wird mit 0x01 codiert. Die SMS-Daten sind projektspezifisch auf maximal 140 Byte je Paket festgelegt. Theoretisch können 249 Byte an SMS-Daten mit einem Paket übermittelt werden. Das Paket enthält zusätzlich die MTU-ID zur eindeutigen Kennung des Absenders.

Report-Paket (Response): SMS-Request

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Request	MTU-ID				SMS
Wert	-	0x60/0x61	0x01	-	-	-	-	-

Byte	...	n	n+1
Bezeichnung	SMS		XOR
Wert	-	-	-

Abbildung 5.10: Aufbau eines Report-Response-Pakets mit SMS-Request

Um Stream-Daten vom Funkcontroller an den Gatewaycontroller zu übertragen, sind zusätzliche Steuerinformationen notwendig (siehe Abbildung 5.11). Der Request für das Übermitteln von Stream-Informationen wird mit 0x02 codiert. Im Service-ID-Feld wird der betreffende Kanal angegeben. Das Status-Feld enthält die Steuerinformation: 0x00 - Öffnen eines Stream-Kanals, 0x01 - Schließen eines Stream-Kanals, 0x02 - Schließen eines Stream-Kanals (Fehlerfall), 0x03 - Stream-Kanal offen. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. Das Paket enthält zusätzlich die MTU-ID des Absenders.

Stream-Daten vom Funkcontroller an den Gatewaycontroller werden, wie SMS-Daten, mit der Antwort auf ein Report-Paket mitgesendet (siehe Abbildung 5.12). Bevor Daten übertragen werden können, muss ein Kanal geöffnet werden (siehe Paket mit Stream-Information). In der Antwort auf ein Report-Paket können maximal 248 Byte Stream-Daten übertragen werden. Der Request für das Stream-Service wird mit 0x03 codiert. Der gewünschte Kanal wird im Service-ID-Feld angegeben. Eine Streamverbindung wird durch Schließen des Kanals beendet (siehe Paket mit Stream-Information). In den Nutzdaten ist zusätzlich die MTU-ID des Absenders enthalten.

Report-Paket (Response): Stream-Information-Request

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Request	MTU-ID				Service-ID
Wert	0x08	0x60/0x61	0x02	-	-	-	-	-

Byte	9	10
Bezeichnung	Status	XOR
Wert	-	-

Abbildung 5.11: Aufbau eines Report-Response-Pakets mit Stream-Information-Request

Report-Paket (Response): Stream-Data-Request

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Request	MTU-ID				Service-ID
Wert	-	0x60/0x61	0x03	-	-	-	-	-

Byte	9	...	n	n+1
Bezeichnung	Streamdaten			XOR
Wert	-	-	-	-

Abbildung 5.12: Aufbau eines Report-Response-Pakets mit Stream-Data-Request

Informationen über die Mitgliedschaft von Containern bei einem EGW werden in der Antwort auf ein Report-Paket mit Request 0x04 codiert (siehe Abbildung 5.13). Im Status-Feld wird die Steuerinformation codiert: 0x00 - Anfrage auf Mitgliedschaft, 0x01 - Mitgliedschaft gestattet, 0x02 - Container ignorieren, 0x03 - Mitgliedschaft beendet. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. In den Nutzdaten sind zusätzlich die MTU-ID und Felder zur Übertragung weiterer Informationen enthalten. Nicht verwendete Felder werden leer gelassen. Im Signalstärke-Feld kann eine Wertung der Funkempfangssignalstärke am EGW eingetragen werden. Im Mitglieder-Feld kann die Anzahl der bereits am EGW angemeldeten Container eingetragen werden. Die Informationen können zur EGW-Selektion am CGW genutzt werden.

Report-Paket (Response): Membership-Information-Request

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Request	Status	MTU-ID			
Wert	0x09	0x60/0x61	0x04	-	-	-	-	-

Byte	9	10	11
Bezeichnung	Signalstärke	Mitglieder	XOR
Wert	-	-	-

Abbildung 5.13: Aufbau eines Report-Response-Pakets mit Membership-Information-Request

Um Konfigurationsparameter vom Gatewaycontroller abzufragen, wird in der Antwort auf ein Report-Paket der Request 0x05 gesendet (siehe Abbildung 5.14). Der Funkcontroller kann da-

durch Konfigurationsparameter, wie die fixen GPS-Koordinaten, explizit abfragen. Mit einem Request können mehrere Parameter gleichzeitig abgefragt werden. Die jeweilige Parameter-ID muss bekannt sein. Die Werte der angeforderten Parameter werden in Folge mit einem Configure-Paket an den Funkcontroller übermittelt.

Report-Paket (Response): Get-Configuration-Request

Byte	1	2	3	4	5	...	n	n+1
Bezeichnung	Länge	Nutzdatentyp	Request	ID 1	ID2	...	ID n-3	XOR
Wert	-	0x60/0x61	0x05	-	-	-	-	-

Abbildung 5.14: Aufbau eines Report-Response-Pakets mit Get-Configuration-Request

Ein NACK-Request wird in der Antwort auf ein Report-Paket mit 0x06 codiert (siehe Abbildung 5.15). Der Request dient zur Information im Fehlerfall. Kann ein SMS-Paket vom EGW nicht an einen Container weitergeleitet werden, wird mit einem NACK-Request die ursprüngliche SMS-Nachricht an den Absender retourniert. Der Empfang eines NACK-Requests bedeutet allgemein, dass eine SMS-Nachricht auf dem gewählten Weg nicht zugestellt werden konnte. Als Reaktion kann ein alternativer Kommunikationsweg gewählt werden oder die Information an eine höhere Instanz weitergeleitet werden. Im vorliegenden Fall konnten SMS-Daten vom Funkcontroller nicht über Funk abgesetzt werden. Sie werden mit dem NACK-Request an den Gatewaycontroller retourniert. In den Nutzdaten sind neben dem Requestcode die MTU-ID und die SMS-Daten enthalten.

Report-Paket (Response): NACK-Request

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Request	MTU-ID				SMS
Wert	-	0x60/0x61	0x06	-	-	-	-	-

Byte	...	n	n+1
Bezeichnung	SMS		XOR
Wert	-	-	-

Abbildung 5.15: Aufbau eines Report-Response-Pakets mit NACK-Request

Configure-Paket

Mit dem Configure-Paket (siehe Abbildung 5.16) können Konfigurationswerte vom Gatewaycontroller an den Funkcontroller übermittelt werden. Der Nutzdatentyp wird mit 0x62 codiert. Mit einem Paket können gleichzeitig mehrere Konfigurationswerte gesendet werden. Die jeweilige Parameter-ID muss bekannt sein. Die Länge der Konfigurationswerte ist variabel und wird implizit mit den untersten 2 Bits der Parameter-ID angegeben: 00 - 1 Byte, 01 - 2 Byte, 10 - 4 Byte, 11 - 8 Byte. Im fehlerfreien Fall wird mit dem Antwortpaket 0x00 im Error-Feld retourniert. Bei einem Fehler wird die ID des ersten fehlgeschlagenen Parameters eingetragen.

Configure-Paket (Request)

Byte	1	2	3	4	5	6	...	n
Bezeichnung	Länge	Nutzdatentyp	ID 1	Wert 1	ID 2	Wert 2	...	XOR
Wert	-	0x62	-	-	-	-	-	-

Configure-Paket (Response)

Byte	1	2	3	4
Bezeichnung	Länge	Nutzdatentyp	Error	XOR
Wert	0x02	0x62	-	-

Abbildung 5.16: Aufbau eines Configure-Pakets (Anfrage und Antwort)

Get-Configuration-Paket

Mit dem Get-Configuration-Paket (siehe Abbildung 5.17) kann der Gatewaycontroller Konfigurationswerte vom Funkcontroller abfragen. Der Nutzdatentyp wird mit 0x63 codiert. Mit einem Paket können gleichzeitig mehrere Konfigurationswerte abgefragt werden. Die jeweilige Parameter-ID muss bekannt sein. In der Antwort wird die Parameter-ID mit dem zugehörigen Parameterwert retourniert. Die Länge der Konfigurationswerte ist variabel und wird implizit mit den untersten 2 Bits der Parameter-ID angegeben: 00 - 1 Byte, 01 - 2 Byte, 10 - 4 Byte, 11 - 8 Byte.

Get-Configuration-Paket (Request)

Byte	1	2	3	4	5	...	n	n+1
Bezeichnung	Länge	Nutzdatentyp	ID 1	ID2	ID 3	...	ID n-2	XOR
Wert	-	0x63	-	-	-	-	-	-

Get-Configuration-Paket (Response)

Byte	1	2	3	4	5	6	...	n
Bezeichnung	Länge	Nutzdatentyp	ID 1	Wert 1	ID 2	Wert 2	...	XOR
Wert	-	0x63	-	-	-	-	-	-

Abbildung 5.17: Aufbau eines Get-Configuration-Pakets (Anfrage und Antwort)

SMS-Paket

Mit dem SMS-Paket (siehe Abbildung 5.18) können Kurznachrichten vom Gatewaycontroller an den Funkcontroller gesendet werden. Es beinhaltet als Nutzdaten den Datentyp 0x64, die MTU-ID des Empfängers und die eigentliche SMS-Nachricht. Die maximale Länge von SMS-Daten ist auf 140 Byte festgelegt. Theoretisch können mit einem Paket 250 Byte SMS-Daten übertragen werden. Das Status-Feld in der Antwort enthält Informationen über den Erfolg der Übertragung: 0x00 - OK, 0x01 - BUSY. Mit BUSY kann der Funkcontroller signalisieren, dass er im Moment keine SMS-Daten annehmen kann. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar.

Byte	1	2	3	4	5	6	7	...
Bezeichnung	Länge	Nutzdatentyp	MTU-ID				SMS	
Wert	-	0x64	-	-	-	-	-	-

Byte	n	n+1
Bezeichnung	SMS	XOR
Wert	-	-

Byte	1	2	3	4
Bezeichnung	Länge	Nutzdatentyp	Status	XOR
Wert	0x02	0x64	-	-

Abbildung 5.18: Aufbau eines SMS-Pakets (Anfrage und Antwort)

Stream-Information-Paket

Das Stream-Information-Paket (siehe Abbildung 5.19) dient zur Steuerung des Stream-Dienstes. Es wird zum Öffnen und Schließen einer Stream-Verbindung sowie zur Übertragung weiterer Informationen genutzt. Der Nutzdatentyp wird mit 0x65 codiert. Im Service-ID-Feld wird der Kanal angegeben und im Status-Feld die zu übertragende Steuerinformation: 0x00 - Öffnen eines Stream-Kanals, 0x01 - Schließen eines Stream-Kanals, 0x02 - Schließen eines Stream-Kanals (Fehlerfall), 0x03 - Stream-Kanal offen. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. Das Paket enthält zusätzlich die MTU-ID des Empfängers. Die Antwort enthält keine neuen Informationen. Sie dient ausschließlich zur Bestätigung des Paketempfangs.

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	MTU-ID				Service-ID	Status
Wert	0x07	0x65	-	-	-	-	-	-

Byte	9
Bezeichnung	XOR
Wert	-

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x65	0x65

Abbildung 5.19: Aufbau eines Stream-Information-Pakets (Anfrage und Antwort)

Stream-Data-Paket

Mit dem Stream-Data-Paket (siehe Abbildung 5.20) werden Stream-Daten vom Gatewaycontroller zum Funkcontroller übertragen. Bevor Stream-Daten übertragen werden können, muss ein Kanal geöffnet werden (siehe Stream-Information-Paket). Der Nutzdatentyp wird mit 0x66 codiert. Der gewünschte Kanal wird im Service-ID-Feld angegeben. Die MTU-ID dient zur eindeutigen Kennung des Empfängers. Mit einem Paket können maximal 249 Byte Stream-Daten übertragen werden. Eine Stream-Verbindung wird durch Schließen des Kanals beendet (siehe Stream-Information-Paket). Das Status-Feld in der Antwort enthält Informationen über den Erfolg der Übertragung: 0x00 - OK, 0x01 - BUSY. Mit BUSY kann der Funkcontroller signalisieren, dass er im Moment keine Stream-Daten annehmen kann. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar.

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	MTU-ID				Service-ID	Streamdaten
Wert	-	0x66	-	-	-	-	-	-

Byte	...	n	n+1
Bezeichnung	Streamdaten		XOR
Wert	-	-	-

Byte	1	2	3	4
Bezeichnung	Länge	Nutzdatentyp	Status	XOR
Wert	0x02	0x66	-	-

Abbildung 5.20: Aufbau eines Stream-Data-Pakets (Anfrage und Antwort)

Start-Sending-Paket

Mit dem Start-Sending-Paket (siehe Abbildung 5.21) kann der Gatewaycontroller dem Funkcontroller die Empfangsbereitschaft mitteilen. Dadurch kann der Gatewaycontroller in Kombination mit dem Stop-Sending-Paket die Datenpaketannahme zwischenzeitlich stoppen. Das Überlaufen des Eingangspuffers kann im Fehlerfall so verhindert werden. Der Nutzdatentyp wird mit 0x67 codiert. Die Antwort enthält keine neuen Informationen. Sie dient ausschließlich zur Bestätigung des Paketempfangs.

Stop-Sending-Paket

Mit dem Stop-Sending-Paket (siehe Abbildung 5.22) kann der Gatewaycontroller dem Funkcontroller das Senderecht entziehen. Dadurch kann ein Überlaufen des Eingangspuffers im Fehlerfall verhindert werden. Der Nutzdatentyp wird mit 0x68 codiert. Die Antwort enthält keine neuen Informationen. Sie dient ausschließlich zur Bestätigung des Paketempfangs.

Start-Sending-Paket (Request)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x67	0x67

Start-Sending-Paket (Response)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x67	0x67

Abbildung 5.21: Aufbau eines Start-Sending-Pakets (Anfrage und Antwort)

Stop-Sending-Paket (Request)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x68	0x68

Stop-Sending-Paket (Response)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x68	0x68

Abbildung 5.22: Aufbau eines Stop-Sending-Pakets (Anfrage und Antwort)

Membership-Information-Paket

Das Membership-Information-Paket (siehe Abbildung 5.23) wird zur Übertragung von Informationen über die Mitgliedschaft eines Containers bei einem EGW genutzt. Der Nutzdatentyp wird mit 0x69 codiert. Das Status-Feld enthält die eigentliche Steuerinformation: 0x00 - Anfrage auf Mitgliedschaft, 0x01 - Mitgliedschaft gestattet, 0x02 - Container ignorieren, 0x03 - Mitgliedschaft beendet. Im zukünftigen Betrieb ist die Erweiterung der Steuerinformationen denkbar. Die MTU-ID dient zur eindeutigen Kennung des betreffenden Containers. Die Antwort enthält keine neuen Informationen. Sie dient ausschließlich zur Bestätigung des Paketempfangs.

5.4 Gatewayapplikation

Die Gatewayapplikation stellt die definierten Dienste zur Verfügung. Dabei handelt es sich um das SMS-, das Stream- und das Location-Service. Dazu muss eine korrekte Kommunikation mit dem Lantronix-Modul und dem Funktransceiver bereitgestellt werden. Zusätzlich müssen die Datenpakete an die spezifizierten Vorgaben angepasst werden. Es wird eine Konsole für die manuelle Interaktion mit dem EGW bereitgestellt und die Möglichkeit der Anbindung eines optionalen GPS- und GSM-Moduls geboten.

Membership-Information-Paket (Request)

Byte	1	2	3	4	5	6	7	8
Bezeichnung	Länge	Nutzdatentyp	Status	MTU-ID				XOR
Wert	0x06	0x69	-	-	-	-	-	-

Membership-Information-Paket (Response)

Byte	1	2	3
Bezeichnung	Länge	Nutzdatentyp	XOR
Wert	0x01	0x69	0x69

Abbildung 5.23: Aufbau eines Membership-Information-Pakets (Anfrage und Antwort)

5.4.1 Anmeldung

Voraussetzung für die Nutzung der Dienste am EGW ist eine erfolgreiche Anmeldung der MTU. Die MTU am Container sendet periodisch ein Beacon-Paket aus (siehe Abschnitt 3.1). Solange das Paket nicht beantwortet wird, nutzt die MTU die containerinternen Ressourcen. Empfängt ein EGW das Beacon einer unbekanntenen MTU, meldet er den erkannten Container mit zusätzlichen Informationen (Signalstärke, Anzahl der bereits angemeldeten Container) an den CGW. Dazu leitet der Funkcontroller das Handshake-Verfahren ein. Der Gatewaycontroller bestätigt den Handshake und sendet ein Report-Paket. In der Antwort auf das Report-Paket sendet der Funkcontroller seinen Request (Membership Information) und die MTU-ID. Es können auch zusätzliche Informationen für die Selektion am EGW mitgesendet werden. Der Gatewaycontroller bringt die Daten in die definierte Paketform für die Netzwerkanbindung. Die Daten werden mit einem Membership-Information-Paket an das Lantronix-Modul gesendet. Das Lantronix-Modul leitet das Paket unverändert an den CGW weiter. Am CGW wird die EGW-Selektion durchgeführt. Im Fall, dass mehrere EGW den neuen Container melden, wird ein zuständiger EGW bestimmt. Die Auswahl erfolgt anhand der mitgesendeten Informationen. Im Zuge der Selektion kann auch eine Lastverteilung erfolgen. Der CGW sendet das Ergebnis der Selektion an die EGW zurück. Das Ergebnis für den jeweiligen EGW wird mit einem Membership-Information-Paket an das Lantronix-Modul gesendet. Das Modul leitet das Paket an den Gatewaycontroller weiter. Dort wird das Paket in die definierte Paketform für die Funkanbindung gebracht. Der Gatewaycontroller aktiviert den Handshake. Nach der Bestätigung des Handshakes wird ein Membership-Information-Paket an den Funkcontroller gesendet. In der Antwort auf das Paket wird der Empfang bestätigt. Ein EGW erhält den Zuspruch zur Kommunikation mit der MTU, die anderen erhalten die Anweisung die MTU zu ignorieren. Die abgewiesenen EGW antworten daher nicht auf das aktuelle und zukünftige Beacons dieser MTU. Der ausgewählte EGW führt die Anmeldung der MTU durch. Dafür ist die Funkapplikation zuständig. Es werden Informationen über die Empfangszeitpunkte der MTU (siehe Abschnitt 3.1) und die GPS-Koordinaten vom EGW ausgetauscht. Die MTU kann von diesem Zeitpunkt an die Dienste am EGW nutzen. Der EGW hört ständig am Funk, falls er nicht selbst sendet. Dadurch kann die MTU nach der Anmeldung jederzeit versuchen mit dem EGW über CSMA/CA zu kommunizieren. Der EGW weiß durch die Anmeldung, wann die MTU am Funk hört.

Es gibt keine explizite Abmeldung vom EGW. Solange die MTU glaubt, eine gültige Anmeldung an einem EGW zu besitzen, versucht sie bei Bedarf die Kommunikation. Kann der EGW nach mehreren Versuchen nicht kontaktiert werden, löscht die MTU die EGW-Einträge. Danach wer-

den die lokalen MTU-Ressourcen genutzt, bis wieder ein EGW auf das Beacon antwortet. Der EGW löscht die MTU-Einträge, wenn sich eine MTU über mehrere Beacon-Perioden nicht mehr gemeldet hat. Die Information wird wie bei der Anmeldung an den CGW weitergeleitet. Dadurch leitet der CGW künftige Nachrichten an die MTU nicht mehr an den EGW weiter. Der CGW gibt die zuvor abgewiesenen EGW wieder für die MTU frei.

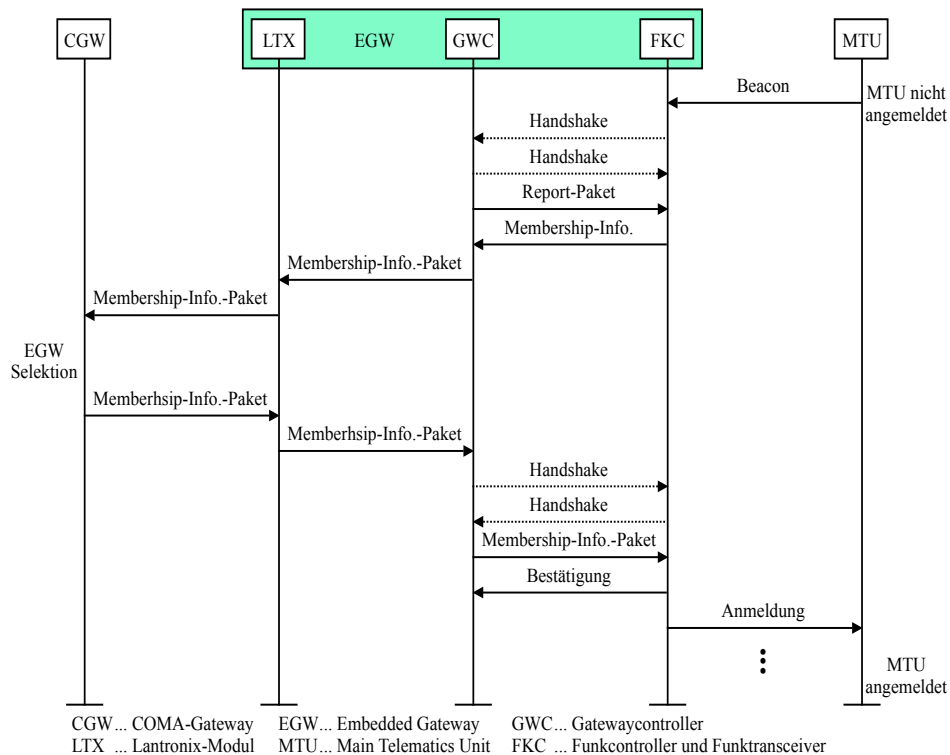


Abbildung 5.24: Anmeldung einer MTU an einen EGW

5.4.2 Location-Service

Das Location-Service (siehe Abschnitt 1.2.1) am EGW ermöglicht angemeldeten Containern die Abfrage der GPS-Koordinaten über Lokalfunk. Die Koordinaten können am EGW mit Hilfe der Konsole am Gatewaycontroller manuell konfiguriert werden. Bei Ausführungen mit GPS-Modul kann die Ermittlung der aktuellen Koordinaten auch automatisch erfolgen. Die GPS-Daten werden von der Gatewayapplikation verwaltet. Der Funkcontroller kann die GPS-Daten explizit anfordern. Die Anforderung (siehe Abbildung 5.25) wird vom Funkcontroller durch Aktivieren der Handshake-Leitung initiiert. Der Gatewaycontroller aktiviert in Folge seine Handshake-Leitung. Dadurch ist die Verbindung bestätigt und beide Mikrocontroller befinden sich in der Kommunikationsphase. Da jede Kommunikationsrunde (Request-Response) laut Definition vom Gatewaycontroller eröffnet werden muss, sendet dieser ein Report-Paket an den Funkcontroller. In der Antwort auf das Report-Paket sendet der Funkcontroller seinen Request (Get-Configuration) und die ID des gewünschten Konfigurationsparameters. In diesem Fall die ID der GPS-Koordinaten. Danach ist die Kommunikationsrunde beendet. Der Gatewaycontroller holt die GPS-Koordinaten aus dem Speicher und sendet sie in einer weiteren Kommunikationsrunde an den Funkcontroller. Das Handshake-Verfahren wird dieses Mal vom Gatewaycontroller eingeleitet. Danach werden mit

einem Configure-Paket die GPS-Koordinaten übermittelt. In der Antwort auf das Configure-Paket kann der Funkcontroller eventuell aufgetretene Fehler melden. Damit ist die zweite Kommunikationsrunde abgeschlossen. Mit diesem Vorgehen kann der Funkcontroller jederzeit die GPS-Daten abfragen. Um die Abfrage der GPS-Daten nicht gesondert durchführen zu müssen, können sie gemeinsam mit anderen Konfigurationswerten beim Start der Funkapplikation vom Gatewaycontroller abgerufen werden. Dieser Vorgang muss nur einmal bei einem Neustart oder Reset durchgeführt werden. Die Übertragung der GPS-Koordinaten über Funk ist Teil der Funkapplikation. Ein Container erhält die GPS-Koordinaten bei der Anmeldung. Sie können aber auch explizit abgefragt werden.

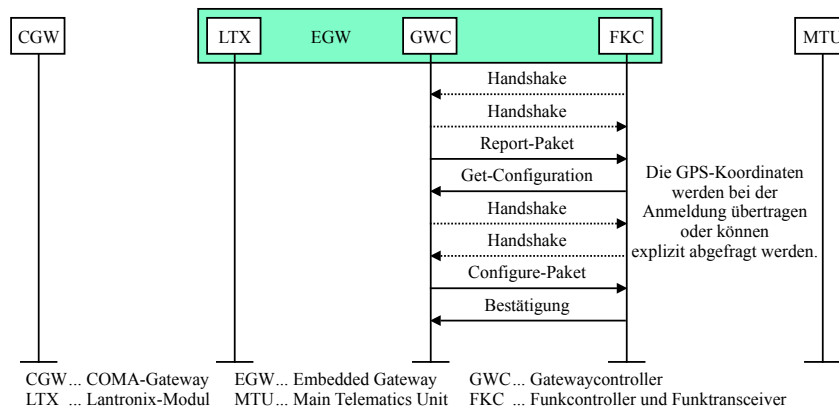


Abbildung 5.25: Location-Service am EGW

5.4.3 SMS-Service

Das SMS-Service (siehe Abschnitt 1.2.2) am EGW ermöglicht angemeldeten Containern das Versenden und Empfangen von SMS-Nachrichten über Lokalfunk. Im Fall, dass eine Nachricht vom Datacenter an einen Container gesendet werden soll, wird die Nachricht vom CSRV an den CGW gesendet. Dort wird überprüft, ob der Empfänger derzeit an einem EGW angemeldet ist. Befindet sich der Container nicht in Reichweite eines EGW, wird die Nachricht über die GSM- oder die SMSC-Schnittstelle weitergeleitet. Ist der Container an einem EGW angemeldet, wird die SMS-Nachricht in Form eines SMS-Pakets an das Lantronix-Modul am entsprechenden EGW gesendet (siehe Abbildung 5.26). Die Übertragung erfolgt über TCP/IP. Das Lantronix-Modul sendet das SMS-Paket unverändert über eine UART-Schnittstelle an den Gatewaycontroller. Dort wird die Nachricht an den spezifizierten Paketaufbau für die Funkanbindung angepasst. Der Gatewaycontroller startet das Handshake-Verfahren mit dem Funkcontroller. Nach erfolgreichem Handshake wird die Nachricht mit einem SMS-Paket übertragen. In der Antwort auf das SMS-Paket können aufgetretene Fehler an den Gatewaycontroller gemeldet werden. Danach ist die Kommunikationsrunde abgeschlossen. Der Funkcontroller weiß durch die Anmeldung, wann der Container seinen Empfänger aktiviert. Dadurch kann er zum richtigen Zeitpunkt die SMS-Daten senden. Der genaue Ablauf ist von der Funkapplikation abhängig.

Um auf Probleme bei der Übertragung von SMS-Nachrichten gezielt reagieren zu können, wurde ein NACK-Verfahren implementiert (siehe Abbildung 5.27). Die Übertragung vom CGW zum Lantronix-Modul erfolgt über eine TCP-Verbindung, die bereits dafür sorgt, dass keine Daten verloren gehen. Das Lantronix-Modul sendet die Daten weiter an den Gatewaycontroller. Dort erfolgt

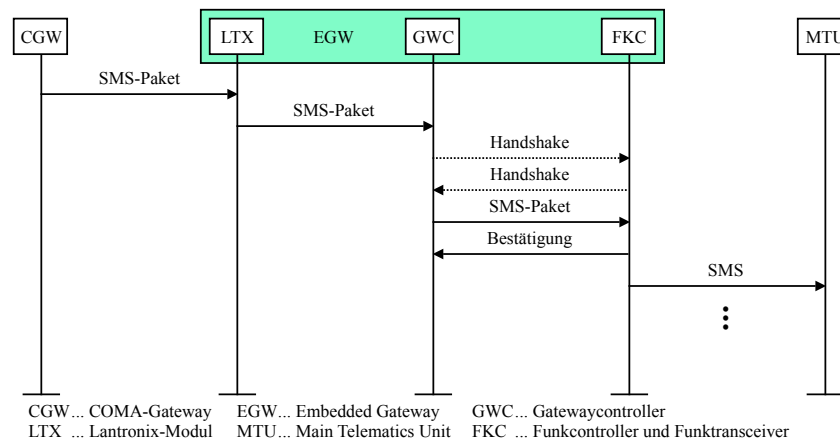


Abbildung 5.26: Übertragung einer SMS-Nachricht vom CGW an einen Container

die Überprüfung der CRC8-Checksumme. Derzeit werden fehlerhafte Pakete verworfen. Dadurch wird eine Falschinterpretation verhindert. In Zukunft könnte auch eine Meldung über den aufgetretenen Fehler an den CGW erfolgen. Fehlerfreie Pakete werden verarbeitet und an den Funkcontroller weitergesendet. Reagiert der Funkcontroller nicht auf die Handshake-Aufforderung, wird die Aufforderung bis zu drei Mal wiederholt. Nach erfolgreichem Handshake wird das SMS-Paket an den Funkcontroller gesendet. Wenn keine Antwort auf das gesendete Paket empfangen wird, wird das Senden der SMS-Daten bis zu drei Mal wiederholt. Die Anzahl der Wiederholungen beim Handshake und beim Versenden der Daten kann manuell festgelegt werden. Kann das SMS-Paket nicht an den Funkcontroller übermittelt werden, wird der Kommunikationsversuch abgebrochen und ein NACK-Paket an das Lantronix-Modul gesendet. Das Lantronix-Modul leitet das NACK-Paket an den CGW weiter. Am CGW wird über das weitere Vorgehen entschieden. Entweder wird die Nachricht über einen alternativen Kommunikationsweg (GSM, SMSC) gesendet oder die Fehlermeldung an den CSRV weitergeleitet. Kann die Nachricht erfolgreich an den Funkcontroller übertragen werden, erfolgt dort die Überprüfung der XOR-Checksumme. Bei einem fehlerhaften Paket kann eine Neusendung vom Gatewaycontroller veranlasst werden. Tritt ein Problem bei der Funkübertragung auf, kann der Funkcontroller ein NACK-Paket an den Gatewaycontroller senden. Das NACK-Paket wird an den CGW weitergeleitet. Die genaue Vorgehensweise bei einem Funkproblem ist Teil der Funkapplikation.

Im Fall, dass eine Nachricht von einem Container an das Datacenter gesendet werden soll, sendet die MTU die Nachricht über Lokalfunk an den EGW (siehe Abbildung 5.28). Die Kommunikation erfolgt über CSMA/CA. Der EGW hört ständig am Funk, sofern er nicht selbst gerade sendet. Die genaue Implementierung ist Teil der Funkapplikation. Der Funkcontroller leitet den Handshake mit dem Gatewaycontroller ein. Der Gatewaycontroller bestätigt den Handshake und sendet ein Report-Paket. In der Antwort auf das Report-Paket sendet der Funkcontroller seinen Request (SMS-Service) und die Nachricht. Danach ist die Kommunikationsrunde beendet. Am Gatewaycontroller wird die Nachricht in das vorgegebene Format für die Netzwerkanbindung umgewandelt. Die Nachricht wird in Form eines SMS-Pakets an das Lantronix-Modul gesendet. Das Lantronix-Modul leitet das SMS-Paket unverändert über eine TCP/IP-Verbindung an den CGW weiter. Fehler oder Probleme, die bei der Funkübertragung oder am Funkcontroller auftreten, müssen von der Funkapplikation und der MTU-Applikation behandelt werden. Bei Nachrichten, die am Gatewaycontroller empfangen werden, wird die XOR-Checksumme überprüft. Bei einem

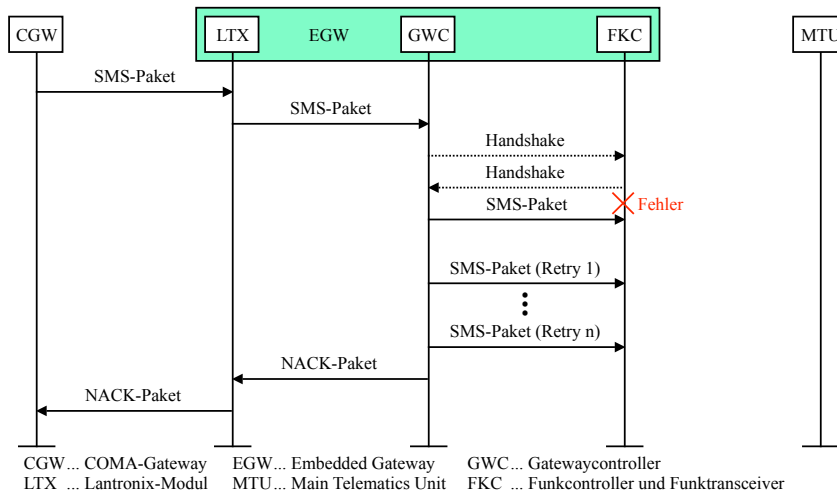


Abbildung 5.27: Fehlerhafte Übertragung einer SMS-Nachricht vom CGW an einen Container

Übertragungsfehler wird eine Neusendung vom Funkcontroller angefordert. Dabei werden maximal drei Wiederholungen angefordert. Danach bricht der Gatewaycontroller die Kommunikation ab. Der Funkcontroller kann in einer neuen Kommunikationsrunde erneut versuchen, die Nachricht abzusetzen. Wird die Nachricht fehlerfrei am Gatewaycontroller empfangen, wird sie verarbeitet. Die Nachricht wird für die Weiterleitung vorbereitet und mit einer CRC8-Checksumme versehen. Das Lantronix-Modul sendet die Nachricht über TCP an den CGW. Im Fall, dass die Netzwerkverbindung unterbrochen wird und der Eingangspuffer am Gatewaycontroller ein definiertes Level erreicht, sendet der Gatewaycontroller ein Stop-Sending-Paket an den Funkcontroller. Danach werden keine Pakete Richtung Datencenter mehr angenommen. Sobald die Netzwerkverbindung wieder hergestellt ist, wird der Funkcontroller mit einem Start-Sending-Paket informiert.

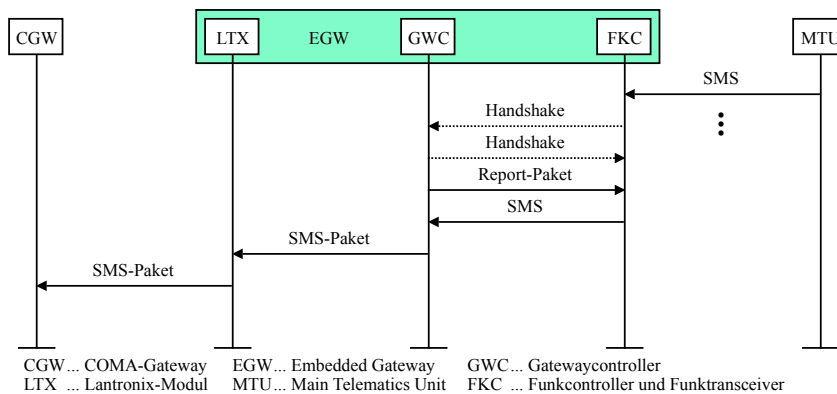


Abbildung 5.28: Übertragung einer SMS-Nachricht von einem Container an den CGW

5.4.4 Stream-Service

Das Stream-Service (siehe Abschnitt 1.2.3) am EGW ermöglicht angemeldeten Containern das Versenden und Empfangen von größeren Datenmengen über Lokalfunk. Darüber hinaus wird das

Service zur Realisierung einer Konsolenverbindung zwischen einem Benutzer im Internet und einem Container benötigt. Bevor Daten über eine Streamverbindung gesendet werden können, muss ein Kanal geöffnet werden. Dadurch wechselt die MTU in den aktiven Empfangsmodus bis der Kanal geschlossen wird. Der Kanal kann dabei von der MTU oder vom CGW (siehe Abbildung 5.29) geöffnet werden. Im Fall, dass der CGW das Öffnen initiiert, wird ein Stream-Information-Paket mit dem Request Kanal öffnen, der Kanalnummer und der MTU-ID an den EGW gesendet. Das Paket wird vom Lantronix-Modul unverändert an den Gatewaycontroller weitergeleitet. Dort wird das Paket in die definierte Form für die Funkanbindung gebracht. Der Gatewaycontroller startet das Handshake-Verfahren. Nachdem der Funkcontroller den Handshake bestätigt hat, sendet der Gatewaycontroller das Stream-Information-Paket. Mit der Antwort auf das Paket wird der Empfang bestätigt. Der Funkcontroller sendet die Stream-Informationen in einem Empfangszeit slot der MTU an den Container. Der genaue Ablauf am Funk ist Teil der Funkapplikation. Die MTU wechselt in den aktiven Empfangsmodus und sendet ein Stream-Information-Paket mit einer Bestätigung an den EGW. Der Funkcontroller startet das Handshake-Verfahren. Der Gatewaycontroller bestätigt den Handshake und sendet ein Report-Paket. In der Antwort auf das Report-Paket sendet der Funkcontroller seinen Request (Stream-Information) und die Information (Kanal offen). Der Gatewaycontroller wandelt das Paket in die definierte Form für die Netzwerkanbindung und sendet ein Stream-Information-Paket an das Lantronix-Modul. Das Lantronix-Modul leitet das Paket an den CGW weiter. Der Kanal ist dadurch geöffnet und es können Daten übertragen werden.

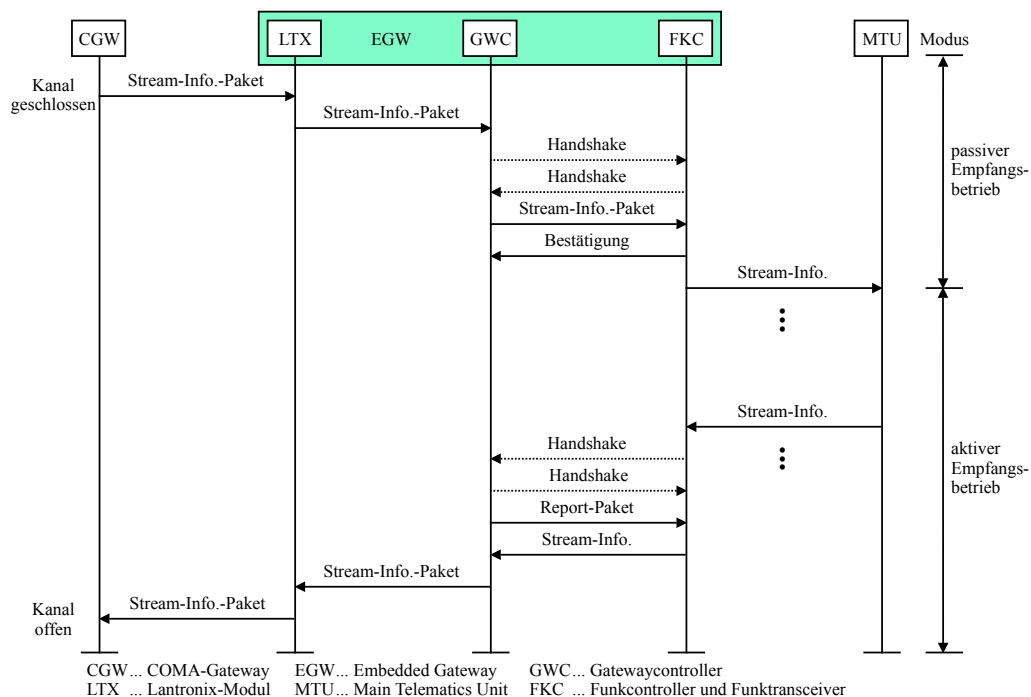


Abbildung 5.29: Öffnung eines Stream-Kanals

Die Übertragung der Stream-Daten (siehe Abbildung 5.30) erfolgt nach dem gleichen Prinzip wie die Übermittlung von Stream-Informationen. Für den Datentransport wird das Stream-Data-Paketformat benutzt. Eine Stream-Verbindung wird durch das Schließen des Kanals beendet. Dazu wird ein Stream-Information-Paket mit dem Request Kanal schließen gesendet. Die MTU

wechselt danach wieder in den passiven Empfangsmodus. Mit den Paketen wird genauso verfahren wie beim SMS-Service. Auch das Verhalten im Fehlerfall ist gleich. Anstelle des NACK-Pakets wird jedoch ein Stream-Information-Paket mit Request Kanal schließen (Fehlerfall) gesendet. Dadurch wird sichergestellt, dass keine unbenutzten offenen Kanäle entstehen.

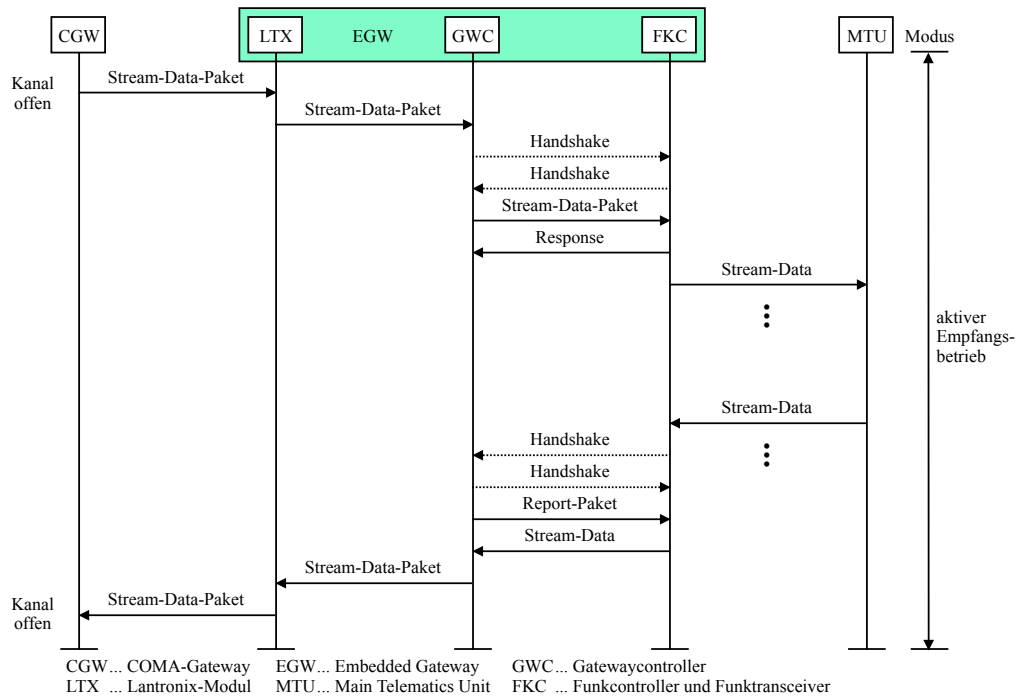


Abbildung 5.30: Übertragung von Stream-Daten

6 Projektergebnisse

Der EGW-Prototyp wurde im Labor in Betrieb genommen und mit Hilfe eines speziell entworfenen Testsystems getestet. Im Zuge der Tests wurde die Gatewayapplikation am Gatewaycontroller verschiedenen Testfällen ausgesetzt. Darüber hinaus erfolgte ein Testlauf der Infrastruktur vom CGW bis zum Funkcontroller. Die Funkapplikation am Funkcontroller konnte noch nicht in die Tests einbezogen werden, da derzeit noch keine lauffähige Version existiert. Aus diesem Grund wurde der Funk durch eine Testapplikation am Funkcontroller simuliert. Dieses Kapitel beschreibt das aufgebaute Testsystem und die Ergebnisse. Nach einer Zusammenfassung der Arbeit wird ein Ausblick auf die zukünftige Verwendung des EGW gegeben.

6.1 Testaufbau

Die Entwicklung des EGW, vor allem der Software-Module, ist auf mehrere Personen aufgeteilt. Im Zuge dieser Arbeit wurde die Gatewayapplikation am Gatewaycontroller (STM32) implementiert. Die Implementierung der Funkapplikation am Funkcontroller (ATMEGA644) sowie die Implementierung am CGW wird von zwei weiteren Studenten der Technischen Universität Wien bearbeitet. Durch die Definition der Schnittstellen und Kommunikationspakete konnten die einzelnen Module unabhängig entwickelt werden. Zur Aufgabenstellung dieser Arbeit zählt auch die Bereitstellung eines Testsystems, um die Gatewayapplikation am Gatewaycontroller verifizieren zu können. Die entwickelte Testumgebung ermöglicht die Simulation des EGW-Betriebs, ohne dass die fehlenden EGW- beziehungsweise WCMS-Komponenten benötigt werden. Dadurch kann die Gatewayapplikation verschiedenen Tests ausgesetzt werden. Das Testsystem (siehe Abbildung 6.1) setzt sich im Wesentlichen aus vier Komponenten zusammen, der EGW-Platine, der externen Platine für die Konsole (siehe Abschnitt 4.2.8), der Test-Platine und einem PC. Die Test-Platine wurde im Zuge dieser Arbeit eigens für den Testaufbau entwickelt. Das gesamte Testsystem kann über ein Terminalprogramm von einem beliebigen PC aus bedient werden.

Um die Gatewayapplikation testen zu können, werden die Leitungen der Schnittstellen zum Funkcontroller und zum Lantronix-Modul (siehe Abschnitt 4.3) am Rand der EGW-Platine herausgeführt. Von dort werden sie über Flachbandkabel mit der Test-Platine verbunden. Eine UART/USB-Bridge ermöglicht den Anschluss der UART-Leitungen Richtung Lantronix-Modul an den USB-Port eines PC. Mit Hilfe eines Terminalprogramms kann so der Datenverkehr vom Gatewaycontroller Richtung Lantronix-Modul beobachtet werden und Daten an den Gatewaycontroller gesendet werden. Die Statusleitung, über die der Gatewaycontroller im Betrieb den Verbindungsstatus des Lantronix-Moduls abfragen kann, wird über einen Schalter gesteuert. Die

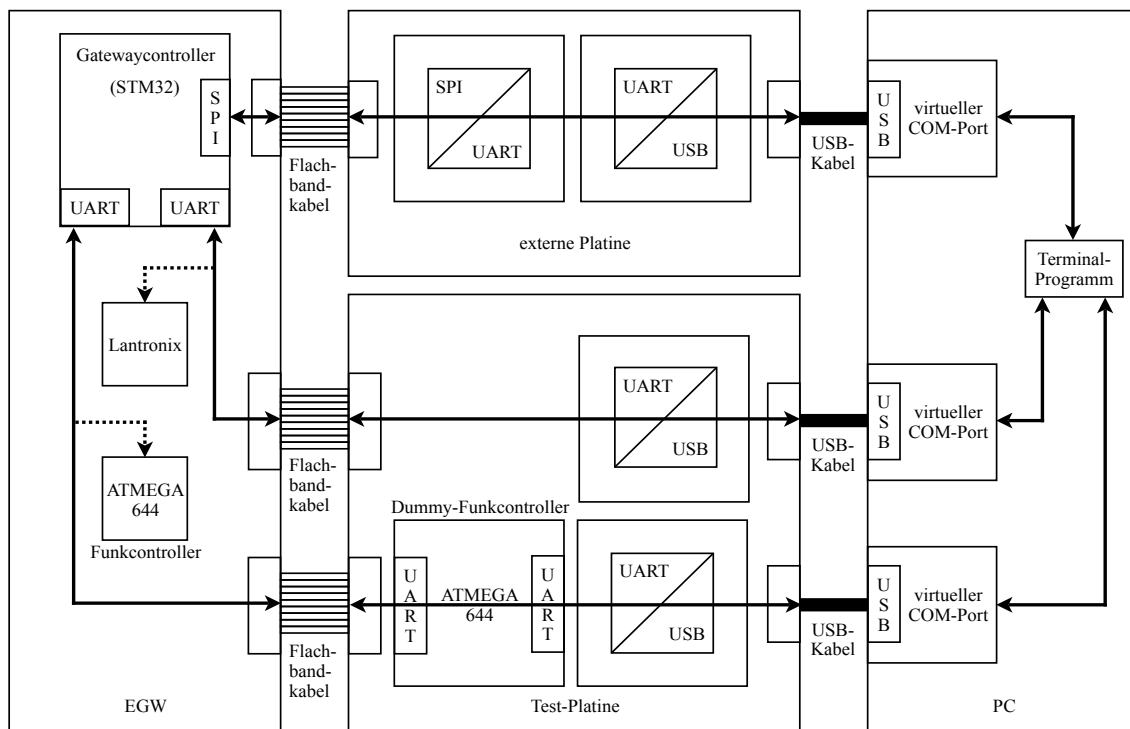


Abbildung 6.1: Testsystem zur Überprüfung der Gatewayapplikation

Leitungen Richtung Funkcontroller werden auf der Test-Platine mit einem Dummy-Funkcontroller verbunden. Auf dem Controller läuft eine Testapplikation. Über eine UART-Schnittstelle des Dummy-Funkcontrollers und eine weitere UART/USB-Bridge wird, nach gleichem Prinzip wie beim Gatewaycontroller, eine Konsole realisiert. Der Dummy-Funkcontroller kann daher ebenfalls mit dem Terminalprogramm am PC gesteuert werden. Dadurch wird die Beobachtung der Pakete vom Gatewaycontroller Richtung Funk ermöglicht. Mit Hilfe verschiedener Konsolenbefehle können Testpakete über den Dummy-Funkcontroller an den Gatewaycontroller gesendet und Testfälle durchgespielt werden.

Die Test-Platine in Kombination mit einem Terminalprogramm am PC ermöglicht die Beobachtung der Datenpakete, die vom Gatewaycontroller an das Lantronix-Modul oder an den Funkcontroller gesendet werden. Darüber hinaus können über das Terminalprogramm Datenpakete vom Lantronix-Modul oder vom Funkcontroller an den Gatewaycontroller simuliert werden. Der Benutzer kann mit dem Testsystem von jedem PC über ein beliebiges Terminalprogramm interagieren. Bei den durchgeführten Tests wurde das Programm HTerm benutzt. Es werden drei USB-Anschlüsse am PC benötigt. Im Terminalprogramm werden drei Fenster geöffnet. Ein Fenster dient zur Kommunikation mit dem Gatewaycontroller, das zweite zur Kommunikation mit dem Dummy-Funkcontroller und das dritte Fenster zur Simulation des Lantronix-Moduls. Durch das Testsystem kann die Einhaltung der spezifizierten Paketformate sowie das korrekte Weiterleiten und Verarbeiten der empfangenen Pakete am Gatewaycontroller überprüft werden. Da das Lantronix-Modul und der echte Funkcontroller parallel zum Testsystem angeschlossen sind, dürfen sie während eines aktiven Tests nicht versorgt werden. Sie können auch von den entsprechenden Leitungen getrennt werden. Mit dem Testsystem wurde der Gatewaycontroller mehreren Tests ausgesetzt. Die Gatewayapplikation zeigte ein stabiles Verhalten und konnte alle Testfälle

korrekt bearbeiten. In einem erweiterten Testlauf wurde die gesamte Infrastruktur vom CGW über das Lantronix-Modul und den Gatewaycontroller bis zum Dummy-Funkcontroller überprüft. Dieser Testlauf zeigte, dass die einzelnen Komponenten und Module wie geplant zusammenarbeiten. Sobald eine lauffähige Version der Funkapplikation verfügbar ist, können Tests mit dem vollständigen EGW durchgeführt werden. Die bisherigen Tests verliefen bezogen auf das Grundkonzept EGW vielversprechend.

6.2 Energiebilanz

Durch den Einsatz des EGW im WCMS kann die MTU ihre beschränkten Energieressourcen besser nutzen. Dadurch wird die Betriebsdauer verlängert. Eine Abschätzung des Energieverbrauchs der MTU mit und ohne EGW soll die Verbesserungen hervorheben. Dabei wird die Abfrage der GPS-Daten über das GPS-Modul der MTU mit der Abfrage über den EGW (Lokalfunk) verglichen. Beim SMS-Service wird das Absetzen einer SMS mit 140 Byte über das GSM-Modul der MTU mit der Absetzung über den EGW (Lokalfunk) verglichen. Beim Stream-Service wird die Übertragung von 100 kByte betrachtet. Die Alternativen sind GPRS über das GSM-Modul der MTU oder Lokalfunk über den EGW. Die Leistungsdaten wurden aus den Datenblättern der Hersteller entnommen beziehungsweise im WCMS gemessen. Sie geben typische Werte wieder. Die Zeiten ohne EGW sind Erfahrungswerte aus dem WCMS. Die Zeiten mit EGW können ohne genaue Kenntnis der Funkapplikation nur abgeschätzt werden (siehe Abschnitt 3.5). Dennoch ist anhand der Größenordnungen erkennbar, dass der Einsatz des EGW die Betriebsdauer einer MTU verlängern kann. Voraussetzung ist, dass sich die Container regelmäßig in Reichweite eines EGW befinden. Tabelle 6.1 zeigt den durchschnittlichen Leistungsverbrauch und die Zeiten für die Erfüllung der gestellten Aufgaben in einem System ohne EGW. Tabelle 6.2 zeigt den durchschnittlichen Leistungsverbrauch und die Zeiten für die Erfüllung der gestellten Aufgaben in einem System mit EGW.

Tabelle 6.1: Leistungsverbrauch und Zeitbedarf der MTU ohne EGW

	Location-Service ^[1]	SMS-Service ^[2]	Stream-Service ^[3]
Leistung	90 mW	850 mW	1030 mW
Zeit	60 bis 180 s	4 bis 17 s	50 s

[1] Abfrage der GPS-Koordinaten über das GPS-Modul

[2] Senden einer SMS mit 140 Byte über das GSM-Modul

[3] Übertragung von 100 kByte über das GSM-Modul (GPRS - 1 TX-Slot)

Tabelle 6.2: Leistungsverbrauch und Zeitbedarf der MTU mit EGW

	Location-Service ^[1]	SMS-Service ^[2]	Stream-Service ^[3]
Leistung	50 mW	50 mW	50 mW
Zeit	4 ms	10 ms	5 s

[1] Abfrage der GPS-Koordinaten über Lokalfunk (EGW)

[2] Senden einer SMS mit 140 Byte über Lokalfunk (EGW)

[3] Übertragung von 100 kByte über Lokalfunk (EGW)

6.3 Zusammenfassung

Der globale Gütertransport erfolgt größtenteils in Form von Transportcontainern. Dadurch existieren weltweit mehr als 20 Millionen Container. Diese Container werden mit Lastkraftwagen, Schiffen oder Zügen an ihren jeweiligen Bestimmungsort befördert. Auf dem Weg zu ihrem Zielort ist die Ware verschiedenen Risiken und unvorhersehbaren Ereignissen ausgesetzt. Um zu gewährleisten, dass die Ware qualitativ hochwertig und unverfälscht an ihrem Bestimmungsort ankommt, hat sich in den letzten Jahren der Einsatz von Überwachungssystemen für Container etabliert. Diese Systeme bieten Unternehmen einen ständigen Überblick über den aktuellen Zustand sowie die aktuelle geographische Position ihrer Container. Dadurch kann schnell und koordiniert auf unvorhergesehene Ereignisse reagiert werden. Die gesammelten Informationen können für eine genaue Dokumentation und für eine Optimierung der betriebswirtschaftlichen Prozesse genutzt werden.

An der Technischen Universität Wien wird aus diesem Grund im Rahmen eines Forschungsprojekts das Wireless Cargo Monitoring System (WCMS) entwickelt. Die vorliegende Arbeit beschäftigt sich mit dem Entwurf und der Realisierung eines Gateways zum Einsatz im WCMS. Der Gateway soll an Orten mit gehäuftem Containervorkommen stationär montiert werden und Containern über Lokalfunk eine globale Kommunikation ermöglichen. Container können durch den Gateway über Lokalfunk GPS-Koordinaten abfragen sowie SMS-Nachrichten versenden und empfangen. Ein eigener Dienst ermöglicht das Versenden und Empfangen von größeren Datenmengen. Darüber hinaus wird durch den EGW eine interaktive Konsolenverbindung zwischen einem Benutzer im Internet und einem Container ermöglicht. Durch die Nutzung der Dienste am EGW können die beschränkten Energieressourcen an den Containern geschont werden. Als Folge kann die Betriebsdauer der Elektronik an den Containern verlängert werden.

Zu Beginn der Arbeit wurde ein Überblick über die Anforderungen und den prinzipiellen Aufbau eines drahtlosen Überwachungssystems für Container gegeben. Danach wurden die Kommunikationstechnologien, die bei der Containerüberwachung eingesetzt werden, betrachtet. Dabei wurde zwischen lokaler und globaler Kommunikation unterschieden. Bei der globalen Kommunikation erfolgte eine Einführung in GSM- und UMTS-Netze. Neben den zellulären Mobilfunknetzen wurde darüber hinaus die globale Positionsbestimmung mit Hilfe von GPS erklärt. Als wichtige Vertreter der lokalen Kommunikation wurden ZigBee und RFID behandelt. Am Beispiel marktreifer Produkte wurde im Anschluss der Stand der Technik auf dem Gebiet der Containerüberwachung erarbeitet, wobei gleichzeitig Anwendungen der, zuvor behandelten, Kommunikationstechnologien gezeigt wurden. Aufbauend auf den gesammelten Informationen wurden die Probleme und das Umfeld beim Einsatz eines Gateways im WCMS analysiert. Dabei wurde der Einsatz von Gateways in Lagerhallen und auf Lagerplätzen betrachtet. Am Beispiel eines Eisenbahntransports wurde die Eignung des Gateways zum Einsatz in einer dynamischen Umgebung analysiert. Es folgten Überlegungen zum erreichbaren Durchsatz und der prinzipiellen Tauglichkeit des Gateways für die geplanten Anwendungen. Aus den Ergebnissen der Analyse wurde die eingesetzte Gateway-Architektur sowie die Definition der Schnittstellen erarbeitet. Es folgte eine detaillierte Beschreibung der einzelnen Kommunikationspakete für die Netzwerk- und Funkanbindung. Darüber hinaus wurden der Anmeldevorgang am Gateway sowie die implementierten Dienste erklärt. Darunter fallen das Location-Service, das SMS-Service und das Stream-Service. Für die Verifikation der Gatewayapplikation am Gatewaycontroller wurde ein eigenes Testsystem entwickelt. Die Testläufe zeigten, dass die Gatewayapplikation am Gatewaycontroller die Testfälle stabil und korrekt bearbeiten konnte. Mit einem erweiterten Testlauf wurde abschließend die gesamte Infrastruktur vom CGW bis zur Schnittstelle zum Funkcontroller erfolgreich überprüft.

6.4 Ausblick

Die Arbeiten am Prototypen des EGW sind bis auf die Funkapplikation abgeschlossen. Sobald eine lauffähige Version der Funkapplikation verfügbar ist, wird ein intensiver Testlauf mit dem EGW-Prototypen im Labor erfolgen. Werden dabei gute Ergebnisse erzielt, ist der nächste Schritt die Montage einiger EGW bei Partnerunternehmen. Die Tests im realen Umfeld dienen dazu, das Verhalten im Feld zu beobachten und Erfahrungen zu sammeln.

Neben der Standardausführung mit einem (W)LAN-Modul sollen in Zukunft auch EGW für Spezialanwendungen entwickelt werden. Diese Ausführungen werden keine externe Versorgung besitzen und an Stelle des (W)LAN-Moduls ein GSM-Modul verwenden. Der Energieverbrauch dieser EGW-Ausführung soll so niedrig sein, dass die Versorgung durch eine Solarzelle erfolgen kann. Der EGW kann dadurch an beliebigen Orten ohne lokale Infrastruktur montiert werden.

Ein weiterer Punkt in der Zukunft des WCMS-Projekts ist die Entwicklung einer tragbaren mobilen Einheit, mit der Container über Lokalfunk elektronisch versiegelt und geöffnet werden können. Darüber hinaus sollen autorisierte Personen über die mobile Einheit Logfiles und den Zustand der Container auslesen können sowie Konfigurationsparameter ändern können. Die tragbare mobile Einheit könnte auf gleiche Weise auch zur Konfiguration des EGW benutzt werden.

Derzeit kommunizieren die einzelnen EGW nur mit Containern oder dem CGW. Zukünftig könnte die Kommunikation zwischen den einzelnen EGW eventuell eine Rolle spielen. Darüber hinaus ist die Montage eines EGW nicht nur auf Lagerplätze, Lagerhallen und dergleichen beschränkt. Auch der Einsatz eines EGW in E-Loks beim Eisenbahntransport ist denkbar. Der EGW kann an die Energieversorgung der E-Lok angeschlossen werden und über GSM/GPRS oder UMTS mit dem CGW kommunizieren. Die Container auf den Waggons können dadurch während des gesamten Eisenbahntransports die Dienste am EGW nutzen.

Die Realisierung des EGW-Prototypen bildet die Basis für den Einsatz eines Gateways zur Anbindung von Containern über Lokalfunk. Aufbauend auf den gewonnenen Erkenntnissen bieten sich für den zukünftigen Betrieb im WCMS viele interessante Optionen.

Wissenschaftliche Literatur

- [Atm05] ATMEL: Datenblatt - SPI Serial Extended Temperature EEPROMs AT25640A, 2005
- [Atm07] ATMEL: Datenblatt - Low Power 2.4 GHz Radio Transceiver for ZigBee and IEEE 802.15.4 Applications AT86RF230, 2007
- [Dem07] DEMBOWSKI, Klaus: *Lokale Netze*. München : Addison-Wesley Verlag, 2007
- [Fas08] FASTRAX: Technical Description - UC322 OEM GPS Receiver Module, 2008
- [FM05] FLEISCH, Elgar ; MATTERN, Friedmann: *Das Internet der Dinge*. Berlin : Springer Verlag, 2005
- [GG04] GLOVER, Ian A. ; GRANT, Peter M.: *Digital Communications*. Harlow : Pearson, 2004
- [Hit08] HITEX: The Insider's Guide To The STM32 ARM Based Microcontroller, 2008
- [KAT06] KOUBAA, Anis ; ALVES, Mário ; TOVAR, Eduardo: A Comprehensive Simulation Study of Slotted CSMA/CA for IEEE 802.15.4 Wireless Sensor Networks. IEEE, 2006
- [Lan09] LANTRONIX: Product Brief - MatchPort AR, 2009
- [LLF07] LIN, Shizhuang ; LIU, Jingyu ; FANG, Yanjun: ZigBee Based Wireless Sensor Networks and Its Applications in Industrial. IEEE, 2007
- [MM07] MAHLKNECHT, Stefan ; MADANI, Sajjad A.: On Architecture of Low Power Wireless Sensor Networks for Container Tracking and Monitoring Applications. IEEE, 2007
- [MS01] MISERRE, Rainer ; SVEN, Montanus: *Mobiler Datenfunk*. Berlin : Verlag Technik, 2001
- [PFGM08] PINEDO-FRAUSTO, E. D. ; GARCIA-MACIAS, J. A.: An Experimental Analysis of Zigbee Networks. IEEE, 2008
- [Sag09] SAGEM: HiLo technical specification URD1-OTL 5635.1-005/70086, 2009
- [Sau08] SAUTER, Martin: *Grundkurs Mobile Kommunikationssysteme*. Wiesbaden : Vieweg Verlag, 2008

- [Sch08] SCHIER, Arkadius: *Drahtlose Sensornetzwerke in der Logistik*. Saarbrücken : VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, 2008
- [Sie03] SIEGMUND, Gerd: *Einführung in die Telekommunikation*. Heidelberg : UTB, 2003
- [SST06] SST: Datenblatt - 8 Mbit SPI Serial Flash SST25VF080B, 2006
- [TVS07] TANENBAUM, Andrew S. ; VAN STEEN, Maarten: *Distributed Systems*. New Jersey : Pearson, 2007
- [YT06] YAMAGUCHI, Seiji ; TOSHIYUKI, Tanaka: GPS Standard Positioning using Kalman filter. IEEE, 2006

Internetreferenzen

- [1] Gesamtverband der Deutschen Versicherungswirtschaft e.V.. *Homepage*, Oktober 2009. www.containerhandbuch.de.
- [2] GSM Association. *Homepage*, September 2009. www.gsmworld.com.
- [3] CEPT. *Homepage*, Oktober 2009. www.cept.org.
- [4] ETSI. *Homepage*, Oktober 2009. www.etsi.org.
- [5] 3GPP. *Homepage*, Oktober 2009. www.3gpp.org.
- [6] Global Positioning System. *Homepage*, Oktober 2009. www.gps.gov.
- [7] ZigBee Alliance. *Homepage*, September 2009. www.zigbee.org.
- [8] CSB Technologies GmbH. *Homepage*, August 2009. www.csb-koch.de.
- [9] AIRSIS Inc. *Homepage*, August 2009. www.airsis.com.
- [10] CommerceGuard AB. *Homepage*, August 2009. www.commerceguard.com.
- [11] Fraunhofer-Institut für Fabrikbetrieb und -automatisierung. *Homepage*, Oktober 2009. www.iff.fraunhofer.de.
- [12] Deutsche Post DHL. *Homepage*, Oktober 2009. www.dhl-innovation.de.
- [13] GlobalTrack. *Homepage*, September 2009. www.globaltrack.com.
- [14] ORBCOMM Inc. *Homepage*, Oktober 2009. www.orbcomm.com.