Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorthesis

Tobias Jähnichen

Entwicklung eines Telemetriesystems für flugfähige eingebettete Systeme

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Tobias Jähnichen

Entwicklung eines Telemetriesystems für flugfähige eingebettete Systeme

Bachelorthesis eingereicht im Rahmen der Bachelorprüfung
im Studiengang Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. rer. nat. Dipl.Ing. Thomas Lehmann
Zweitgutachter : Prof. Dr.Ing. Franz Korf

Abgegeben am 18. März 2015

Tobias Jähnichen

Thema der Bachelorthesis

Entwicklung eines Telemetriesystems für flugfähige eingebettete Systeme

Stichworte

Telemetrie, Funkkommunikation, GCS, IEEE802.15.4, PAN, ZigBee, WLAN, UAV, UAS, eingebettetes System

Kurzzusammenfassung

Ziel dieser Arbeit war es ein Telemetriesystem für ein flugfähiges eingebettetes System zu entwerfen und zu implementieren. Dieses System sollte sich in ein im Aufbau befindliches System zur Flugsteuerung integrieren und eine transparente Kommunikation zwischen eingebetteten System in der Luft und einer Bodenstation ermöglichen. Darüberhinaus sollte mehr als nur ein Funkstandard zeitgleich genutzt werden

Tobias Jähnichen

Title of the paper

Development of a Telemetrysystem for airborne embedded Systems

Keywords

Telemetry, Radiocommunication, GCS, IEEE802.15.4, PAN, ZigBee, WLAN, UAV, UAS, embedded System

Abstract

The aim of this work is to design and implement a telemetry system for an airborne embedded system. This system should be integrated into a flight control system which is still under construction. It should enable transparent communication between the airborne embedded system and an groundstation. In addidition, more than just one radio standart has to be supported and used simultaneously.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Randbedingungen

1.1.1 Organisatorisches Umfeld

Bereits seit 2001 existiert an der HAW-Hamburg im Department Fahrzeugtechnik und Flugzeugbau das studentische „Projekt BWB AC20.30“[1]. Dieses Projekt beschäftigt sich seit seiner Gründung mit Konzepten für das Flugzeug und das Fliegen der Zukunft. Dabei steht die Untersuchung von Blended Wing Body (BWB) Flugzeugkonfigurationen im Vordergrund. Zur Erprobung dieser Flugzeugkonfiguration wurde 2003 eine erste Version als Versuchsträger im Maßstab 1:30 mit dem Namen AC2030 umgesetzt. 2008 wurde eine zweite Version gebaut, für die ein Messsystem, der Flugdatenlogger (FDL), angeschafft wurde. Dieses System hat jedoch noch keine Komponente, um den Versuchsträger autonom fliegen zu können. Die Versuche müssen bisher stets von einem erfahren Modellbaupiloten über eine 2,4-GHz-Fernsteuerung geflogen werden. [vgl. CCNF, 2012]

Die Erfahrungen mit den ersten beiden Versionen, sowie neue gewünschte Einsatzzwecke des AC2030 über die Funktion eines reinen Versuchsträgers für die Flugerprobung hinaus, z.B. im Katastrophenschutz, sorgten dafür, dass an einer dritten Version des AC2030 gearbeitet wird. Diese soll auch autonome Flugmanöver bis hin zu kompletten (teil-) autonomen Missionen fliegen können.

Um die, für den Betrieb als autonomes Flugzeug, benötigten Systeme zu entwickeln wurde am Department Informatik im Sommersemester 2013 das Projekt „Airborne Embedded Systems“ (AES) gegründet. Dieses soll sich um den Entwurf und die Entwicklung eines Flugcomputers, der FCU, sowie der Auswahl und Entwicklung der dazu benötigten Hardware und Software kümmern. Dazu wurde in den Sommersemestern 2013 und 2014 sowie im Wintersemester 2013/14 jeweils eine Wahlpflichteinheit angeboten, in der Studierende des Departments Informatik sich mit dem vorhanden System und den Anforderungen an ein neues System auseinander gesetzt haben. Darüber hinaus sind bereits mehrere Bachelorarbeiten in diesem Projektumfeld entstanden. So gab es Untersuchungen zur Sicherheit von Mikrocontroller-basierten

[1] http://ac2030.de/

Unmanned Aerial Vehicles (UAVs) [Richter, 2013], den Entwurf einer Safety-Architektur [Büscher, 2014] , den Entwurf einer ersten Softwarearchitektur der FCU [Rohrer, 2014] und ein Testkonzept für Flugregler [Hasberg, 2014].

Aktuell ist das Projekt im Projekt *FAUST - Fahrerassistenz und Autonome Systeme* eingebunden.

1.1.2 Systemumfeld

Basierend auf den Ergebnissen der Projekte und Bachelorarbeiten der vergangenen Semester existiert zur Zeit eine Systemarchitektur die in Abbildung 1.1 dargestellt ist. Es ist dabei zu beachten, dass sich dieses System noch im Konzeptstadium befindet. Die hier dargestellte Architektur gibt den aktuellen Projektstatus wieder. Die Anforderungen und Spezifikationen der einzelnen Komponenten sind sehr unterschiedlich ausführlich dokumentiert. Zum Teil fehlen diese Spezifikationen noch komplett, was auch der Tatsache geschuldet ist, dass es derzeit kein flugfähiges Modell gibt und die Neuentwicklung nur schleppend beginnt.

Für diese Arbeit ist die dargestellte Architektur zugrunde gelegt worden, jedoch mit dem Wissen, dass sich zum Teil auch noch größere Änderungen ergeben können.

Herzstück der Systeme, die im Flugzeug eingesetzt werden sollen, bildet die FCU. Diese ist für das Sammeln aller Daten der Sensoren und die Ermittlung des Systemzustands aus diesen verantwortlich. Darüber hinaus sollen diese Daten auf eine SD-Karte gespeichert werden.

Die Sensorik besteht derzeit aus einem Air Data Sensor (ADS), einem Global Positioning System (GPS)-Modul und einem Attitude Heading Reference System (AHRS). Der ADS misst Windgeschwindigkeiten und -richtungen sowie den barometrischen Druck. Mit dem AHRS werden Beschleunigungen sowie die Änderung der Roll-, Nick-, und Gierwinkel gemessen. Das GPS ist zur Bestimmung der Position, Geschwindigkeit und Höhe geeignet.

Der Radio Control Receiver (RCR) ist ein handelsüblicher Funkempfänger für den Modellbau, der im 2,4Ghz Band empfängt. Er gibt die empfangenen Steuersignale als Puls-Weiten-Modulation (PWM) Signale aus. Diese Signale werden durch den PWM zu Serial Peripheral Interface (SPI)-Wandler (P2S) in SPI Signale umgewandelt.

Das Safe-Live-Board (SLB) wurde im Rahmen der Arbeit [Büscher, 2014] konzipiert und ist derzeit noch nicht für den (Test-) Einsatz vorhanden. An das SLB soll ein Rettungssystem angeschlossen werden, sodass bei kritischem Systemzustand ein unkontrolliertes Abstürzen verhindert werden kann. Das SLB routet die Steuersignale vom Piloten zur FCU und die von dieser verarbeiteten Signale weiter an den Control Surface Allocator (CSA).

Der CSA ist eine Art Servomischer, der aus den Steuersignalen die an das konkrete Flugzeugmuster angepassten Stellwerte für Servos und Motoren generiert. Die hier generierten

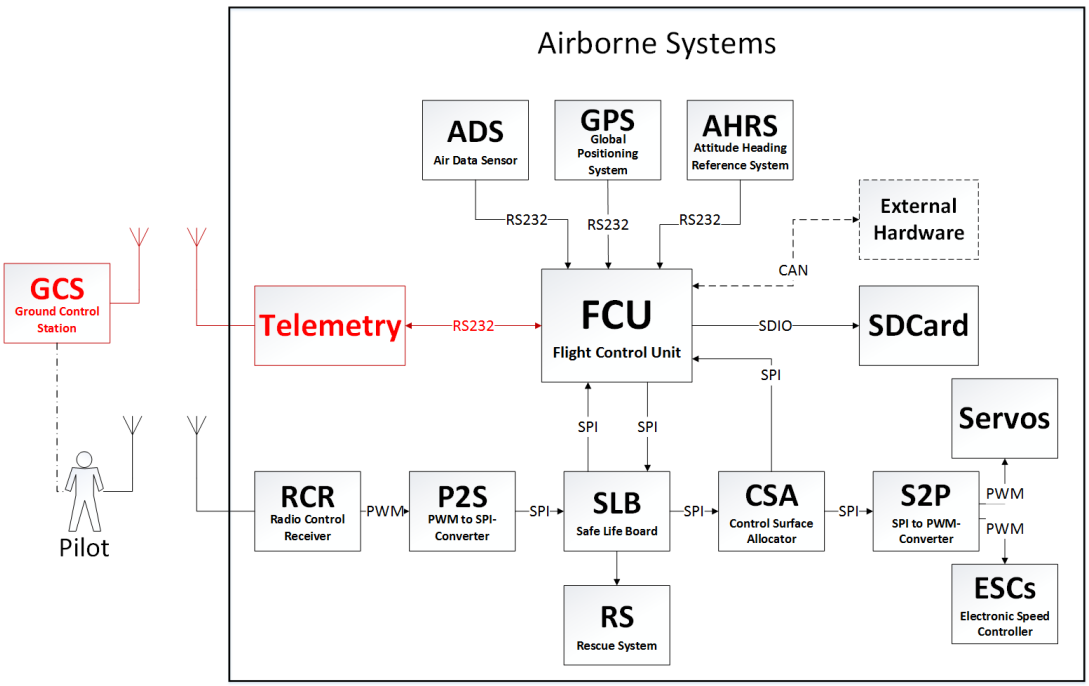


Abbildung 1.1: Aktuelle Systemarchitektur der FCU und ihrer Komponenten. Die rot markierten Teile sind Gegenstand dieser Arbeit und existierten bisher nur teilweise.

Signale werden zum Speichern an die FCU weitergeleitet und zur Wandlung für die Servos und Electronic Speed Controllers (ESCs) in PWM-Signale an den SPI zu PWM-Wandler (S2P) weitergegeben.

Über einen Bus, z. B. Controller Area Network (CAN), soll es möglich sein weitere Hardware, wie z. B. ein Kamerasystem an die FCU anzuschließen. Dies ist momentan noch nicht möglich.

In dieser Architektur nicht betrachtet ist die Stromversorgung und dessen Monitoring, da diese Komponente noch nicht vorhanden ist und das System in seiner jetzigen Form ein reines Laborsystem ist, welches sich noch nicht für den Einsatz im Flugzeug eignet.

Durch die Arbeit [Hasberg, 2014] und ein Projekt von Mechatronik-Studenten wurde ein Hardware-In-the-Loop (HIL) Testsystem gebaut, sodass aktuell die Software der FCU entwickelt und diese direkt im HIL System getestet werden kann. Es existiert bisher jedoch keine „fertige“ FCU-Software.

Als Hardwareplattform für die FCU wird in der HIL-Umgebung ein *stm32f4 Discovery Board* der

Firma STMicroelectronics eingesetzt. Der auf diesem Board eingesetzte Chip soll in Zukunft auf einer eigens entwickelten Platine eingesetzt werden.

Für den HIL-Teststand und ein ebenfalls in [Hasberg, 2014] entwickeltes Software-In-the-Loop (SIL) Testsystem wurde in der Arbeit von Herrn Hasberg ein Software-Bus definiert, der *AES-Link*.

Bis zu dieser Arbeit gab es bereits zwei Funkmodule der Firma Amber Wireless mit denen eine serielle Kommunikation per Funk möglich ist. Diese stammen aus dem alten AC2030, wurden jedoch noch nicht mit der neuen FCU eingesetzt.

1.2 Motivation und Zielsetzung

Gerade im Hinblick auf einen möglichen Einsatz eines UAVs mit dem vom Projekt AES entwickelten System ist es dringend notwendig, dass das Flugzeug mit einer Bodenstation kommunizieren kann. Um so z. B. neue Missionsziele zu erhalten oder den Erfolg eines Auftrags (z. B. Orten einer verletzten Person) an die Bodenstation melden zu können.

Aber auch im Einsatz als reines Messsystem zur Erforschung neuer Flugzeugmuster ist es hilfreich schon während des Fluges den Systemzustand und Messwerte analysieren zu können und Parameter an einem Autopiloten für vorgesehene Testmanöver zu ändern.

Je nach Einsatzzweck und Einsatzbedingungen entstehen dadurch unterschiedliche Anforderungen an Reichweite, Bandbreite und Zuverlässigkeit. Darum ist der Einsatz unterschiedlicher Kanäle, die entweder als Redundanzen zum Sichern der Verbindung eingesetzt werden können oder durch Aufteilen der zu übertragenden Daten auf mehrere Kanäle die Bandbreite erhöhen, sinnvoll. Bisherige Systeme nutzen meistens nur einen Kanal bzw. auf ein System.

Ziel dieser Arbeit ist die Entwicklung einer Basisplattform, eines Telemetriemoduls, das dem eingebetteten System einen transparenten Kanal zu einer Bodenstation bereitstellt. Die Basisplattform soll dabei alle Aufgaben übernehmen, die mit der Abwicklung des Funkverkehrs zusammenhängen. So muss von ihr das Routing auf die einzelnen genutzten Kanäle übernommen werden. Dadurch soll die FCU nicht mit dieser Aufgabe belastet werden, sodass bei Verbindungsproblemen das autonome oder stabilisierende Fliegen durch diese nicht gefährdet ist.

Als Kommunikationstechnologien sollen Systeme wie WLAN, LTE, UMTS, Narrow Band Funkmodule (869MHz) oder ZigBee untersucht und eingesetzt werden. Für alle Systeme ist auch eine entsprechende Gegenstelle am Boden bereitzustellen.

Dazu ist zunächst eine allgemeine Recherche zu Telemetrie und Funkmodulen mit den gedachten Technologien durchzuführen. Bei allen Systemen soll die Eignung und der Energieverbrauch, sowie die Kosten mit betrachtet werden.

In einer Analyse soll die Eignung bezüglich der Ansteuerung und der notwendigen Ressourcen im Routing-Knoten evaluiert werden. Hieraus soll sich dann die erforderliche Rechnerplattform und die Notwendigkeit eines Betriebssystems ableiten. Passende Gegenstellen in der Ground Control Station sind in der Analyse miteinzubeziehen.

Auf Basis dieser Analyse soll eine Plattform als Laborprototyp entworfen und, nach Auswahl einer geeigneten Konfiguration, realisiert werden. Neben der Inbetriebnahme sollen auch Tests im Feld durchgeführt werden. Neben der erzielten Reichweite sind auch der Datendurchsatz und die Latenz zu bestimmen. Der Einfluss von Bewegung soll berücksichtigt werden.

Bei dem System sollen die Funkstandards nicht verändert werden, sondern es soll nach Möglichkeit auf bestehende Module und Protokolle/Software-Stacks aufgesetzt werden.

Im letzten Schritt sind die Ergebnisse der Recherche, die entwickelten Konzepte, die Umsetzung und die durchgeführten Tests adäquat zu dokumentieren.

2 Grundlagen

2.1 Telemetrie

Das Wort Telemetrie stammt von den altgriechischen Wörtern *tēle* „fern“ und *métron* „Maßstab“ ab. Die moderne Definition des Begriffs hat sich nicht sehr weit von diesem Ursprung entfernt: „Der Zweck eines Telemetrie Systems ist es Daten von einem Ort zu erfassen, der entfernt gelegen oder schwer zugänglich ist, und sie an einen Punkt weiterzuleiten, wo die Daten ausgewertet werden könnten.“[Carden u. a., 2002] Es handelt sich demnach um ein System das Daten von einem oder mehreren Sensoren an eine räumlich getrennte Stellung unidirektional überträgt.

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA), die in Deutschland als Bundesbehörde u. a. für die Regulierungen im Bereich der Nutzung von Funkfrequenzen verantwortlich ist, definiert Telemetrie als „Fernmess-Anwendungen (Telemetrie) dienen dem Fernmessen mit Hilfe von Funkwellen. Es handelt sich um Funkanlagen in Luftfahrzeugen oder um terrestrische Funkanlagen, sowohl für zivile als auch militärische Anwendungen.“[Frequenzplan, 2014]

Im Rahmen dieser Arbeit schließt Telemetrie jedoch auch einen Rückpfad ein, sodass auch (Steuerungs-)Daten an das entfernte System übertragen werden können.

2.2 Ground Control Station

Unter dem Begriff Ground Control Station(GCS) werden alle Komponenten zusammengefasst, die für die (Live-)Datenauswertung und Steuerung sowie Missionsplanung eines UAV am Boden eingesetzt werden. Eine GCS besteht somit u. a. aus den Komponenten, die für die Kommunikation mit dem UAV zuständig sind, Komponenten der Steuerung, wie z. B. Funkfernbedienungen, sowie Interfaces zur Datenvisualisierung.

2.3 Funkübertragung

Bei Funkübertragungen handelt es sich um die drahtlose Übertragung von Signalen durch Modulation von elektromagnetischen Wellen, insbesondere im Bereich der sogenannten Radio- und Mikrowellen. Im folgenden sollen die physikalischen, technischen und rechtlichen Grundlagen kurz erläutert werden.

2.3.1 Physikalische Grundlagen

Elektromagnetische Wellen

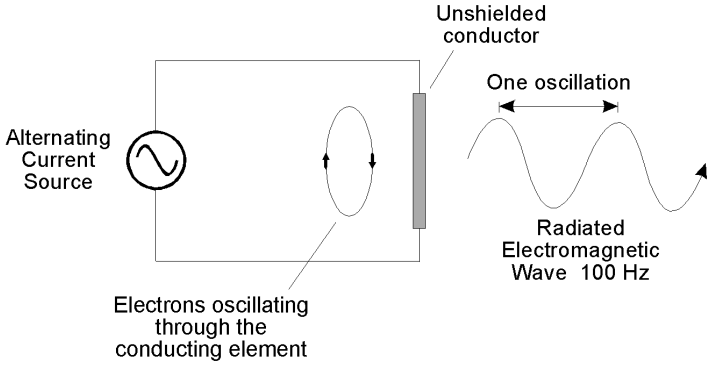


Abbildung 2.1: Erzeugung elektromagnetischer Wellen[Bailey, 2003]

Durch eine sinusförmige variierende Oszillation von Ladung in einem ungeschirmten Leiter ändert sich das umgebende elektrische und magnetische Feld ebenfalls sinusförmig die Richtung und Stärke. Diese Änderungen treten räumlich nicht überall gleichzeitig auf, sondern breiten sich mit der Lichtgeschwindigkeit c aus. Die beiden Felder bilden so eine elektromagnetische Welle, deren Frequenz f gleich der Frequenz der Oszillation der erzeugenden Ladung ist.

Folgende Eigenschaften treffen immer auf elektromagnetische Wellen zu:

1. Elektrisches und magnetisches Feld $\vec{E}$ und $\vec{B}$ stehen stets senkrecht aufeinander.
2. Elektrisches und magnetisches Feld stehen stets senkrecht zur Ausbreitungsrichtung. Es handelt sich damit um transversale Wellen.
3. Die Felder schwingen stets sinusförmig.
4. Beide Felder sind in Phase und Frequenz gleich.

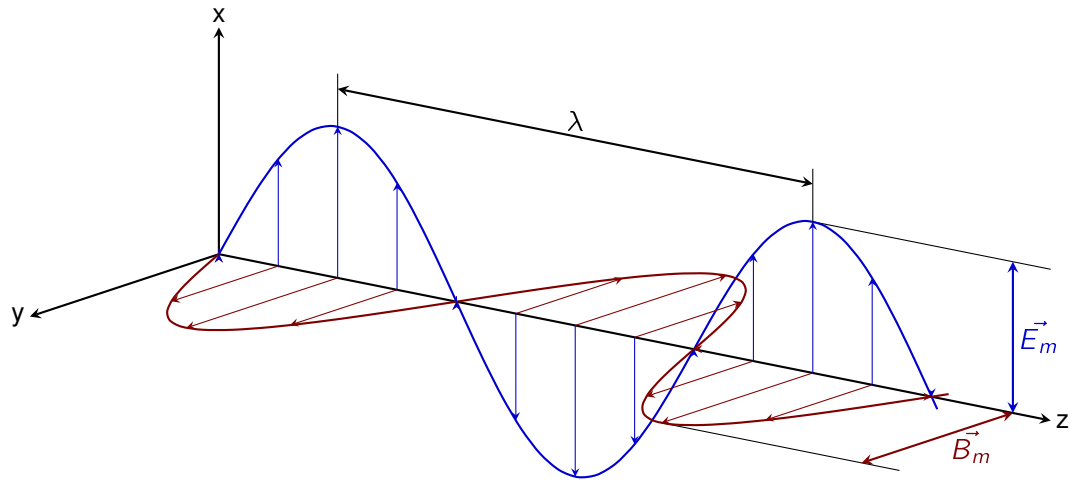


Abbildung 2.2: Ortsdarstellung der magnetischen Feldstärke $\vec{B}$ und der elektrischen Feldstärke $\vec{E}$ zu einem festen Zeitpunkt. Die Welle bewegt sich in positiver z-Richtung fort. Das elektrische Feld (blau) schwingt parallel zur x-Achse und das magnetische (rot) zur y-Achse. $\vec{E_m}$ und $\vec{B_m}$ bezeichnen die Amplituden. λ ist die Wellenlänge

Elektromagnetische Wellen benötigen für ihre Ausdehnung kein Medium und können sich somit auch im Vakuum ausbreiten. Die Lichtgeschwindigkeit für Vakuum beträgt $c = 299792459 ms^{-1}$.

Zwischen Frequenz und Lichtgeschwindigkeit gilt folgender Zusammenhang:

$$c = \lambda f \tag{2.1}$$

Energietransport und Intensität

Elektromagnetische Wellen können Energie transportieren. Die Rate des Energietransports pro Flächeneinheit wird durch den Poynting-Vektor $\vec{S}$ beschrieben:

$$\vec{S} = \frac{1}{\mu_0} \vec{E} \times \vec{B} \tag{2.2}$$

μ_0 ist die magnetische Feldkonstante[1].

Die Richtung des Poynting-Vektors gibt in jedem beliebigen Punkt einer elektromagnetischen Welle deren Ausbreitungsrichtung und die Richtung des Energietransports an. Der Betrag des

[1] $\mu_0 \equiv 4\pi \cdot 10^7 \frac{N}{A^2}$

Poytingvektors ist die momentane Leistung pro Flächeneinheit und ist gegeben durch:

$$S = \frac{1}{\mu_0} EB = \frac{1}{c\mu_0} E^2 \tag{2.3}$$

Für die Praxis deutlich relevanter ist jedoch der Energietransport pro Zeiteinheit. Es wird daher der zeitliche Mittelwert, auch Intensität oder Bestrahlungsstärke I genannt, benötigt:

$$I = \frac{E_0}{\sqrt{2} \cdot c\mu_0} = \frac{1}{c\mu_0} E_{rms}^2 \tag{2.4}$$

Geht man von einem idealen Kugelstrahler (**isotroper Strahler**) aus, so wird die Strahlung homogen zu allen Richtungen in Form einer Kugel abgegeben. Vernachlässigt man zusätzlich noch Dämpfungseffekte oder sonstige Verluste, so muss sämtliche Energie der Punktquelle die gesamte Kugel durchlaufen. Bei einer Leistung der Quelle P_Q so ist die Intensität auf der Kugeloberfläche gegeben durch:

$$I = \frac{P_Q}{4\pi r^2} \tag{2.5}$$

Dies zeigt, dass die Intensität der abgegebenen Strahlung mit dem Quadrat des Abstandes r abnimmt.

Aus der Quantenphysik ist heute bekannt, dass elektromagnetische Wellen auch Teilchencharakter haben können. Daher kann man eine elektromagnetische Welle auch als Strom von Teilchen (Photonen) betrachten. Diese Sichtweise ist notwendig, um bestimmte Effekte zu erklären. So lässt sich mit Hilfe der Quantenphysik auch der Zusammenhang zwischen der Energie einer Welle, bzw. des Photons, und ihrer Frequenz herstellen:

$$E = hf \tag{2.6}$$

Dabei ist h das Plancksche Wirkungsquantum mit einem Wert von $h = 6,63 \cdot 10^{-34} J \cdot s$.

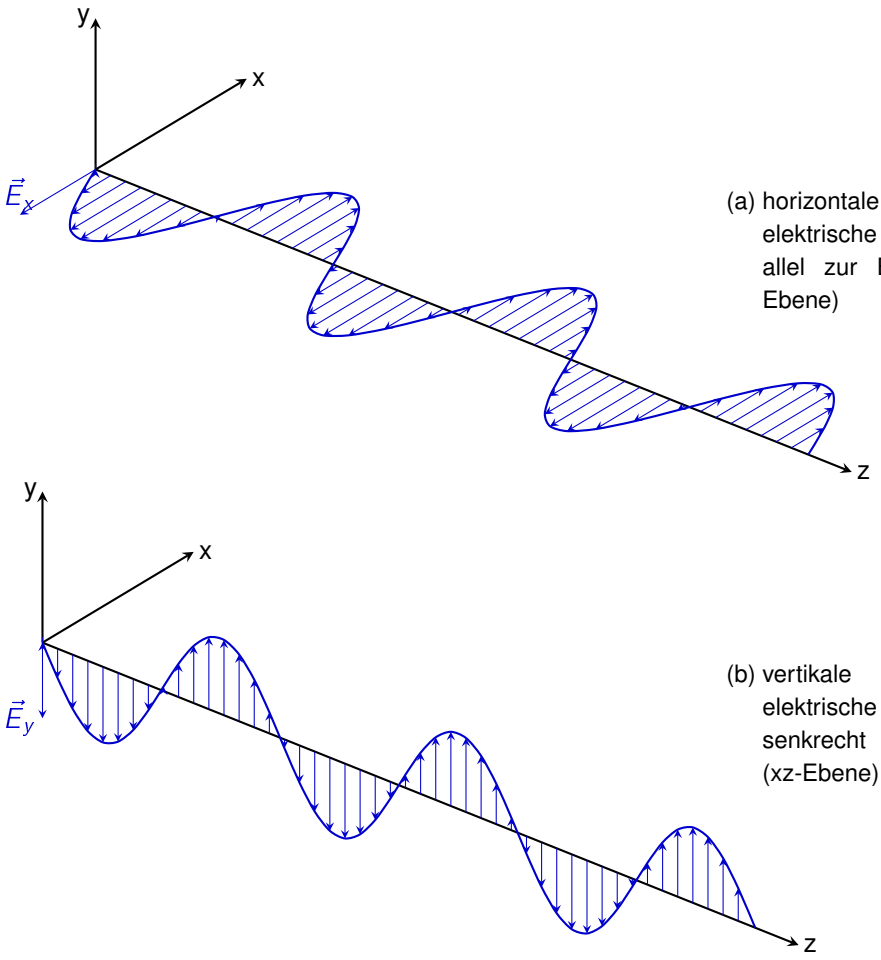
Aus Gleichung 2.6 ist zu erkennen, dass die Energie einer elektromagnetischen Welle proportional zu ihrer Frequenz ist, sodass für eine Welle mit höherer Frequenz mehr Energie aufgewendet werden muss, um die gleiche Intensität wie eine Welle mit kleinerer Frequenz zu erhalten. [Halliday u. a., 2005]

Polarisation

Neben Frequenz und Amplitude ist die Polarisation eine weitere Kenngröße der elektromagnetischen Wellen. Sie wird bestimmt durch die Orientierung des elektrischen Feldvektors an

einem festen Punkt im Raum während der Dauer einer Schwingungsperiode.[Kark, 2014] Es gibt folgende Polarisationen:

linear Befinden sich alle elektrischen Feldvektoren während fortschreitender Zeit innerhalb einer Geraden, so spricht man von **linearer Polarisation**. Liegt diese Gerade parallel zur Erdoberfläche handelt es sich um **horizontale Polarisation**(vgl. Abb. 2.3a). Steht jene senkrecht zu dieser, so spricht man von **vertikaler Polarisation**(vgl.. Abb. 2.3b). Es sind jedoch auch alle anderen Orientierungen möglich.



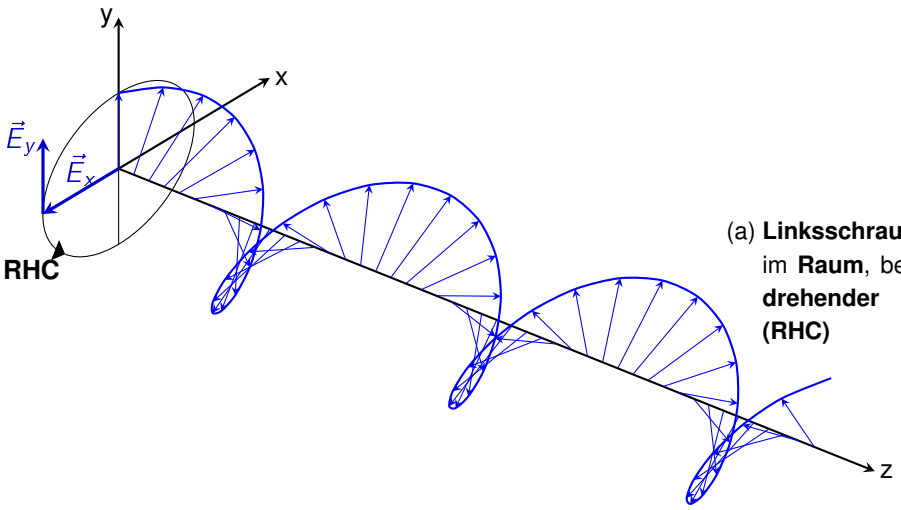
(a) horizontale Polarisation, das elektrische Feld schwingt parallel zur Erdoberfläche (xz-Ebene)

(b) vertikale Polarisation, das elektrische Feld schwingt senkrecht zur Erdoberfläche (xz-Ebene)

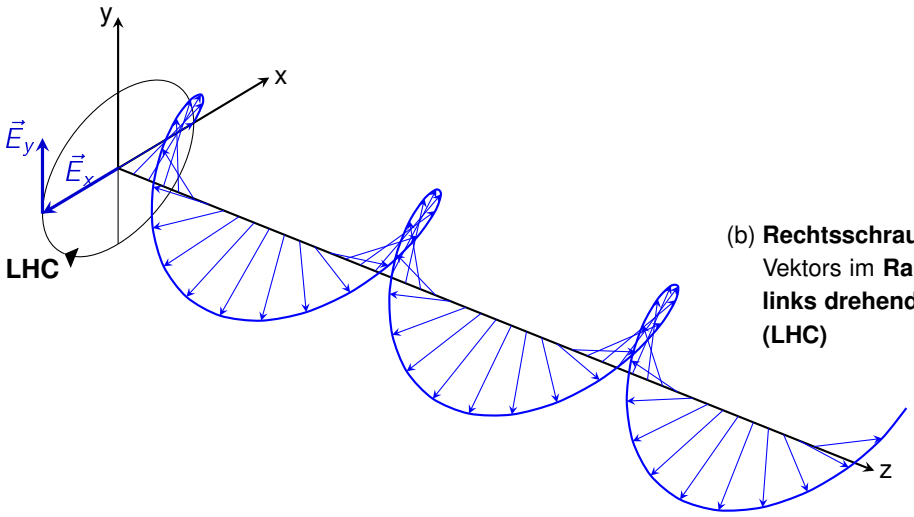
Abbildung 2.3: Räumliche Lage des E-Vektors einer linear polarisierten elektromagnetischen Welle zu einem festen Zeitpunkt

elliptisch Setzt sich der elektrische Feldvektor aus zwei Anteilen zusammen, die eine Phasenverschiebung gegeneinander haben, so handelt es sich um **elliptische Polarisation**

zirkular Eine Form der elliptischen Polarisation ist die **zirkulare Polarisation**. Bei dieser stehen die Feldvektoren des elektrischen Feldes senkrecht aufeinander und der Phasenunterschied beträgt $\pm\frac{\pi}{2}$. Die Amplituden sind gleich. Dadurch geht die Ellipse in einen Kreis über.



(a) **Linksschraube** des E-Vektors im **Raum**, bei **zeitlich rechts drehender Polarisation (RHC)**



(b) **Rechtsschraube** des E-Vektors im **Raum**, bei **zeitlich links drehender Polarisation (LHC)**

Abbildung 2.4: Räumliche Lage des E-Vektors zirkular polarisierter elektromagnetischer Wellen zu einem festen Zeitpunkt

Betrachtet man an einem festen Ort die zeitliche Änderung der Vektororientierung des elektrischen Feldes und diese bildet mit der Ausbreitungsrichtung ein Rechtssystem, so

handelt es sich um **rechtsdrehende Polarisation (RHC - right hand circular)**(vgl. Abb. 2.4a). Andernfalls handelt es sich um **linksdrehende Polarisation (LHC - left hand circulation)**(vgl.. Abb. 2.4b). Zu beachten ist dabei, dass eine **räumliche** Rechtsschraube zu einer **zeitlich** linksdrehenden Polarisation zugehörig ist.

2.3.2 Technische Grundlagen

Bandbreite

Bei dem Begriff Bandbreite kann es leicht zu Verwirrungen kommen, da er im Bereich der Elektro-/Signaltechnik etwas anderes als im Informatikkontext bedeutet. In der ersteren bezeichnet die (analoge) Bandbreite einen Frequenzbereich eines physikalischen Kanals in dem ein Signal übertragen wird. Ihre Einheit ist Herz (Hz). Im Kontext der Informatik ist die (digitale) Bandbreite die maximale Datenrate eines Kanals, gemessen in Bits pro Sekunde. Die Datenrate ist ein Resultat der Bandbreite des genutzten physikalischen Kanal.[Tanenbaum, 2011]

Ist die untere Grenzfrequenz eines Kanals $f_{\text{min}} = 0\text{Hz}$ so spricht man von **Basisbandlage** (engl. baseband). Liegt die untere Grenzfrequenz oberhalb 0Hz so spricht man von einer **Bandpasslage** (engl. passband). Bei Funkübertragungen handelt es sich typischerweise um Bandpassübertragungen, bei denen das Signal einen Frequenzbereich um das Trägersignal belegt.

Ein idealer Kanal mit der Bandbreite B hat eine maximale Datenrate C in Bits pro Sekunde von:

$$C = 2B \log_2 V \tag{2.7}$$

Dabei bezeichnet V die Anzahl an diskreten Signalzuständen, für die binäre Übertragung ist $V = 2$. Die theoretisch maximal mögliche Datenrate eines Kanals ist demnach doppelt so groß wie dessen Bandbreite.

Da jeder physikalische Kanal jedoch ein Grundrauschen beinhaltet, kann diese Rate nie erreicht werden. Das Verhältnis von Signal S zu Rauschen N wird bezeichnet als **SNR (Signal-to-Noise Ratio)**. Üblicherweise wird dabei das Verhältnis in einer logarithmischen Skala ausgedrückt:

$$SNR = 10 \log_{10} \frac{S}{N} \tag{2.8}$$

Die Einheit dieser Skala ist **dB** (decibel).

Für einen verrauschten Kanal ist die maximale Datenrate gegeben durch:

$$C = B \log_2(1 + \frac{S}{N}) \tag{2.9}$$

Dies zeigt, dass für die Datenrate eines realen Kanals die Anzahl der Signalzustände keine Rolle spielt.

Modulationsverfahren und Multiplexing

Bei der Funkübertragung handelt es sich um analoge Übertragungskanäle. Soll nun ein digitales Signal übertragen werden, so müssen die analogen Signale so modifiziert werden, dass sie die digitalen Bits repräsentieren. Die Umwandlung von Bits in die sie repräsentierenden analogen Signale wird **digitale Modulation** genannt.[Tanenbaum, 2011]

Durch direkte Modulationsverfahren erhält man ein Signal in Basisbandlage, dessen obere Grenzfrequenz von der Übertragungsrate abhängt.

Beispiele für direkte Modulationsverfahren sind:

NRZ (Non-Return-to-Zero) Dies ist die einfachste Form der Modulation. Das analoge Signal folgt direkt den Bits. So repräsentiert ein positiver Pegel eine 1 und ein negativer Pegel eine 0. (siehe Abbildung 2.5(b))

NRZI (Non-Return-to-Zero Inverted) Bei dieser Modulationsart wird für eine 1 eine Transition definiert und eine 0 wird durch keine Änderung des Signals repräsentiert.(siehe Abbildung 2.5(c))

Manchester Bei dieser Modulationsart wird ein Taktsignal mit den Bits zusammengelegt. Dazu läuft der Takt mit der doppelten Bitrate. Dadurch gibt es in jedem Bit eine Transition. Die beiden Signale werden mittels XOR logisch verknüpft. Dadurch repräsentiert eine Transition von Low-Pegel zu High-Pegel eine 0 und die Transition von High zu Low eine 1. Dies erleichtert auf der Empfängerseite die Taktrückgewinnung.(siehe Abbildung 2.5(d))

AMI (Alternate Mark Inversion) Bei der Signalübertragung wird angestrebt, im Mittel ausgeglichene Signale zu haben, sodass kein Zustand überwiegt. Dies wird u. a. durch die AMI-Modulation erreicht. Hierbei gibt es drei Zustände: Einen High-Zustand (+), einen Low-Zustand (-) und einen Mittelwert. Der Mittelwert repräsentiert die 0. Die beiden anderen die 1. Dabei treten sie stets im Wechsel auf.(siehe Abbildung 2.5(e))

Da bei Funkübertragungen die untere Grenzfrequenz bei mindestens einigen tausend Herz liegt, muss für die Übertragung das Signal in Bandpasslage gebracht werden. Dies wird durch

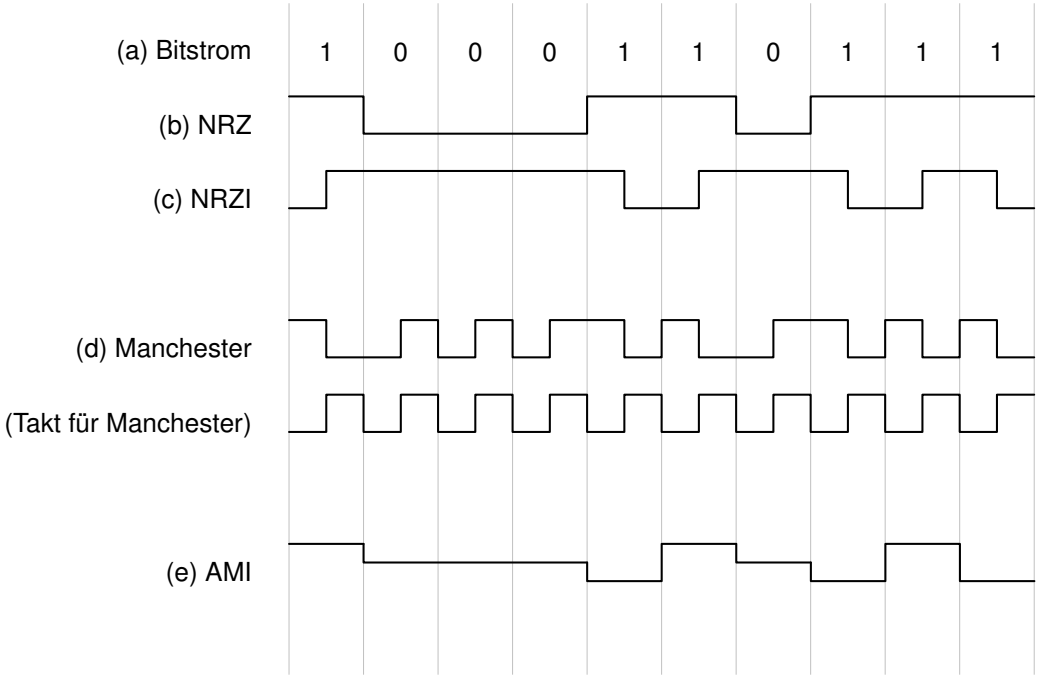


Abbildung 2.5: Direkte Modulationsverfahren

Änderung der Phase, Amplitude oder Frequenz des Trägersignals erreicht. Ein Signal in Basisbandlage mit der Bandbreite 0Hz bis BHz kann in ein Signal in Bandpasslage mit der Bandbreite SHz to $S + B$Hz geschoben werden.

Beispiele für diese Modulationsverfahren sind:

Amplitudenumtastung (ASK) (engl. Amplitude Shift Keying) Bei diesem Verfahren werden für die unterschiedlichen Symbole unterschiedliche Werte der Amplitude verwendet. (siehe Abbildung 2.6(b))

Frequenzumtastung (FSK) (engl. Frequency Shift Keying) Dieses Verfahren setzt für jedes Symbol unterschiedliche Frequenzen ein. (siehe Abbildung 2.6(c))

Phasenumtastung (PSK) (engl. Phase Shift Keying) Bei diesem Verfahren wird für jedes Symbol eine feste Phasenverschiebung angewendet. (siehe Abbildung 2.6(d))

Neben der in Abbildung 2.6 verwendeten 2 Symbole (0 und 1) ist es auch möglich mehrere Symbole zu nutzen. Bei der **Quadraturphasenumtastung (QPSK)** z. B. existieren 4 Symbole (00, 01, 10, 11). Es können damit 2 Bits pro Symbol übertragen werden.

Darüber hinaus kann durch Kombination zweier Methoden (Amplitude und Frequenz oder Amplitude und Phase) ebenfalls eine höhere Anzahl an Bits pro Symbol erreicht werden. Eines

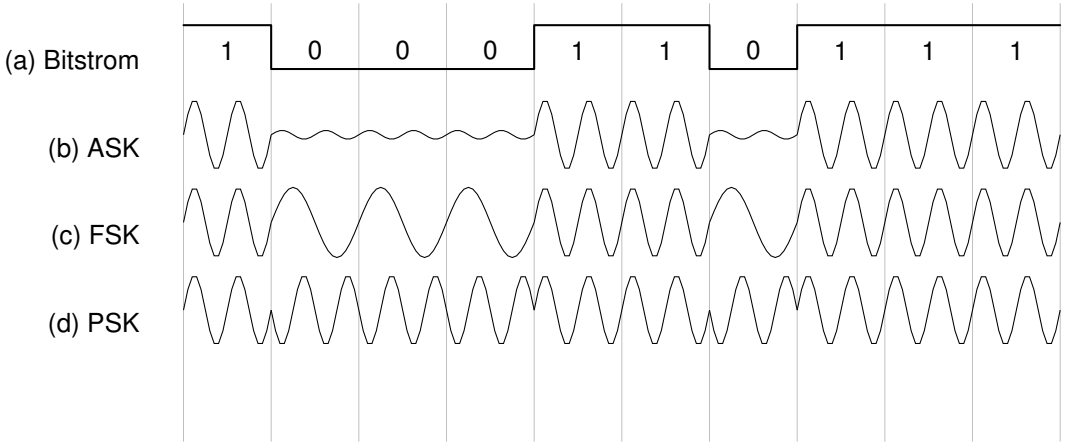


Abbildung 2.6: Digitale Modulatonsverfahren

dieser Verfahren ist die **Quadraturamplitudenmodulation (QAM)**. Hierbei werden ASK und PSK miteinander kombiniert. So lassen sich mit 4096-QAM[2] 12 Bit pro Signal übertragen

Teilen sich mehrere Signale einen Kanal, so kommen Verfahren des **Multiplexing** zum Einsatz, damit sich die Signale nicht gegenseitig blockieren. Grundlegende Verfahren sind:

Zeitmultiplexverfahren (TDM) (engl. Time Division Multiplexing) Bei diesem Verfahren werden Zeitschlitze definiert. Pro Zeitschlitz hat ein Sender die Bandbreite des Kanals alleine zur Verfügung. Außerhalb seines Zeitschlitzes muss der Sender warten. Bei diesem Verfahren ist eine Koordination der Zeitschlitze notwendig. Außerdem müssen Sicherheitsabstände zwischen den Zeitschlitzen vorhanden sein.

Frequenzmultiplexverfahren (FDM) (engl. Frequency Division Multiplexing) Bei diesem Verfahren wird ein Kanal in mehrere Unterkanäle aufgeteilt. Jeder Sender sendet in seinem eigenen Unterkanal. Dabei ist auf genügend Abstand zwischen den Frequenzbändern zu achten.

Codemultiplexverfahren (CDM) (engl. Code Devision Multiplexing) Bei diesem Verfahren ist es jedem Sender möglich über die komplette Bandbreite und Zeit zu senden. Zur Unterscheidung der Signale werden diese speziell codiert. Dazu ist es notwendig den genutzten Frequenzbereich, im Vergleich zu der Bandbreite, die für die eigentlichen Nutzdaten notwendig wäre, deutlich auszudehnen.

Für das Ausdehnen des Frequenzbereichs beim CDM gibt es verschiedene **Frequenzspreizungsverfahren**. Zwei dieser Verfahren sind:

[2] 4096 Symbole, im Rahmen von DVB-C2 angedacht, mindest SNR 36dB

FHSS Beim Frequency Hopping Spread Spectrum (Frequenzsprungverfahren) werden nacheinander verschiedene Kanäle benutzt und die zu übertragenden Daten auf diese Aufgeteilt. Dadurch steht eine höhere Bandbreite zur Verfügung. Der Empfänger muss synchron die selben Kanäle nutzen.

DSSS Das Direct Sequence Spread Spectrum Verfahren verknüpft die Nutzdaten in direkter Folge mit einem Spreizcode (ähnlich dem CDM). Dadurch wird jedes Nutzdatenbit auf die Größe des Spreizcode ausgedehnt. Dadurch verringert sich die Energiedichte im Spektrum. Das Sender stört dadurch andere Funkübertragungen weniger. Der Empfänger muss den Spreizcode kennen, um das Signal rekonstruieren zu können.

Frequenzzugriffsverfahren

Wenn sich mehrere Anwendungen einen Frequenzbereich teilen, so können sie die oben beschriebenen Multiplexverfahren verwenden. Ist dies technisch nicht möglich, so gibt es noch andere Verfahren, wie eine Kollision von Signalen verhindert werden kann, bzw. ein fairer Zugang zu dem Kanal hergestellt werden kann. Diese Verfahren werden u. a. in der Euronorm EN300220-1[3] beschrieben und definiert.

Eines dieser Verfahren ist **Listen Before Talk (LBT)**. Dabei muss jeder Sender eine bestimmte Zeit in den Kanal hineinhören, ob dort gerade ein anderer Sender sendet. Ist der Kanal belegt, muss er mit dem Beginn des eigenen Sendens warten. Darüber hinaus darf der Sender nach dem Senden mindestens eine bestimmte Zeit lang nicht senden. Außerdem muss der Kanal nach einer bestimmten Zeit wieder frei gegeben werden.

Es gibt die Möglichkeit dieses Verfahren mit der **Adaptive Frequency Agility (AFA)** zu verbinden. Dies bedeutet, dass der Sender die Möglichkeit unterstützt dynamisch seinen sende Kanal innerhalb seiner Bandbreite zu wechseln, wenn ein Kanal z. B. belegt ist.

Wenn Sender diese beiden Verfahren nicht unterstützen, so müssen sie sich an einen Bestimmten **Duty Cycle (DC)** halten. Dies bedeutet, dass sie nur eine bestimmte Dauer senden dürfen. Dabei bezieht sich der Wert auf eine Stunde. Ein DC von 10% bedeutet demnach, dass innerhalb einer Stunde maximal 6 Minuten gesendet werden können. Die restliche Zeit muss der Sender aus sein.

2.3.3 Antennen

Eine Antenne dient dem Abstrahlen und Empfangen von elektromagnetischen Wellen.

[3] Version 2.4.1 (http://www.etsi.org/deliver/etsi_en/300200_300299/30022001/02.04.01_40/en_30022001v020401o.pdf)

Richtfaktor und Antennengewinn

Da ein Kugelstrahler nur theoretisch möglich ist, hat jede reale Antenne eine unterschiedliche Strahlungsintensität abhängig von der Raumrichtung. Als Maß dieser Richtwirkung wird der **Richtfaktor** D genutzt. Er gibt das Verhältnis von maximaler zu mittlerer Strahlungsdichte an. Dabei entspricht die mittlere Strahlungsdichte der Strahlungsdichte eines Kugelstrahlers (isotroper Strahler) mit gleicher Strahlungsleistung P_S.

Da jede Antenne die eingespeiste Leistung P_Q nicht komplett in abgestrahlte Leistung P_S umwandeln kann muss bei jeder Antenne auch der **Wirkungsgrad** betrachtet werden. Dieser ist das Verhältnis aus abgegebener Leistung P_S zu eingespeister Leistung P_Q.

Aus Wirkungsgrad und Richtfaktor erhält man den **Antennengewinn (Gain)** G Dieser ist ein Vergleich der maximalen Strahlungsdichte einer Antenne mit der Strahlungsdichte des verlustfreien Kugelstrahlers bei gleicher Generatorleistung P_Q. Der Antennengewinn wird üblicherweise im logarithmischen Maßstab angegeben.

$$g = 10 \log_{10} G \mathrm{dBi} \tag{2.10}$$

Das an das Dezibel angehängte i soll verdeutlichen, dass sich auf eine isotrope Strahlungsquelle bezogen wird. Wird ein Halbwellendipol als Bezugsantenne verwendet, hängt man ein d an, erhält somit: dBd.

Betrachtet man das Produkt aus eingespeister Leistung mit dem Antennengewinn verglichen zum Halbwellendipol, so spricht man von der **Effektiven Strahlungsleistung (ERP)**. Wird dabei keine Abstrahlungsrichtung angegeben, so gilt der größte Antennengewinn, der in Hauptstrahlrichtung gilt.

Benutzt man als Bezugsgröße den isotropen Strahler, erhält man die **Äquivalente isotrope Strahlungsleistung (EIRP)**. Die EIRP gibt die äquivalente Leistung eines isotropen Strahlers an, der überall die gleiche Leistungsdichte erzeugt, wie sie die verglichene Antenne nur in ihrer Hauptstrahlungsrichtung erreichen kann. [Kark, 2014]

Der Antennengewinn und die Richtcharakteristik die für das Senden ermittelt wird, gilt gleichermaßen für das Empfangen mit dieser Antenne.

Für die **Empfangsleistung** einer Funkübertragung gilt, bei Ausbreitung im freien Raum mit zwei Antennen die sich jeweils in der Hauptstrahlrichtung der anderen befinden und einen Gewinn von G_{rx} der Sendeantenne und G_{rx} der Empfangsantenne haben. Dann gilt:

$$P_{\mathrm{rx}} = P_{\mathrm{tx}} G_{\mathrm{tx}} G_{\mathrm{rx}} \left(\frac{4\pi r}{\lambda_0} \right) \tag{2.11}$$

Debei bezeichnet r den Abstand zwischen den Antennen und P_{tx} die Sendeleistung. Die empfangene Leistung nimmt proportional zum Quadrat der Entfernung ab.[Gustrau, 2013]

Antennentypen

Es gibt eine Vielzahl an verschiedenen Bauformen von Antennen. Denn für jede technische Anforderung lassen sich unterschiedliche Antennen nutzen, die Vor- und Nachteile haben. Wichtige Kriterien für die eingesetzte Antenne sind u. a. der Frequenzbereich, der Gewinn, das Abstrahlverhalten (Richtcharakteristik), Baugrößen und Produktionskosten.

Wichtig ist bei der Wahl und Installation der Antenne auch die Polarisation zu beachten. Bei ungünstiger Kombination z. B. horizontale Polarisation des ausgesendeten Feldes und vertikaler Polarisation der Empfangsantenne wird das Signal unendlich gedämpft.

Einige häufig eingesetzte Antennentypen sind:

Dipolantenne Die Dipolantennen gehören zu den linearen Antennen. Sie ist die einfachste und daher am weitesten eingesetzte Bauart. Sie besteht im einfachsten Fall aus einem geraden zylindrischen Leiter, der an einer Bestimmten Stelle, meist symmetrisch in der Mitte unterbrochen und an die Speisung angeschlossen ist. Ist die Länge des Dipols $\frac{\lambda}{2}$ so spricht man vom Halbwellendipol. Er ist ein guter Rundstrahler, der keine besondere Richtcharakteristik hat.

Parabolantennen Parabolantennen bestehen aus einem Reflektor mit einer paraboloidförmigen Fläche. Die Reflektorfläche ist im Allgemeinen deutlich größer als die Betriebswellenlänge, so dass näherungsweise von einer strahlförmigen Ausbreitung elektromagnetischer Wellen ausgegangen werden kann. Befindet sich im Brennpunkt eine Antenne, so kann mit einer solchen Antenne ein hoher Gewinn realisiert werden. [Gustrau, 2013]

Yagi-Uda-Antenne Diese Antennenform gehört zu den Gruppen- und Richtantennen und wird für einen Frequenzbereich von ca. 10MHz bis ca. 2500MHz eingesetzt. Sie besteht meist aus einem aktiven Dipol und mehreren Direktor- und Reflektordipolen. Diese sind passive Dipole, die durch den aktiven Dipol angeregt werden. Dadurch senden die passiven Dipole in der Phase verschobene Wellen aus. Durch geschickte Wahl der Abstände zwischen den Elementen erhält man eine vorwärts gerichtete konstruktive Überlagerung und rückwärtig eine Auslöschung. Dadurch erhält man eine stark gerichtete Antenne. (Siehe Abbildung 2.7)

Wendelantennen (auch Helixantenne) Diese dienen dem Senden und Empfangen zirkular polarisierter Wellen. Dazu bestehen sie aus schraubenförmig gewundenen Leitern. Der Drehsinn von sendender und empfangender Antenne muss übereinstimmen, da es sonst zu einer unendlich großen Dämpfung des Signals beim Empfänger kommt. Es können

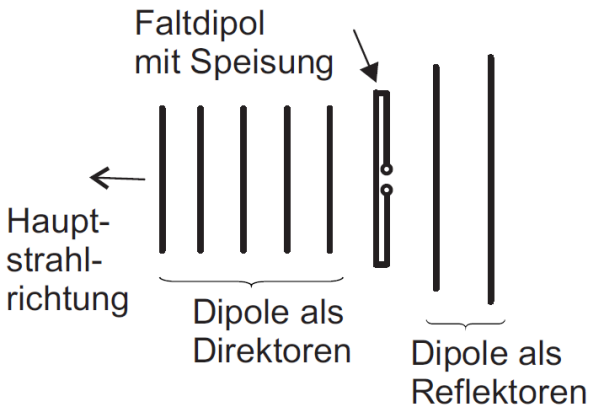


Abbildung 2.7: Aufbau einer Yagi-Uda-Antenne aus aktivem Faltdipol und passiven Dipolen als Direktoren und Reflektoren [aus Gustrau, 2013]

jedoch beliebig orientierte linear polarisierte Wellen empfangen werden. Die Dämpfung beträgt dabei 3dB.[Kark, 2014]

Phased-Array-Antennen Bei den phasengesteuerten Gruppenantennen werden mehrere Antennen mit unterschiedlicher Phase angesteuert. Dadurch lässt sich die Richtcharakteristik variieren. Es ist dadurch z. B. möglich ein bewegtes Ziel zu verfolgen, ohne die Antenne mechanisch bewegen zu müssen.

2.3.4 Rechtliche Grundlagen

Auf europäischer Ebene wird seit 2002 eine Vereinheitlichung der Nutzung und Zuteilung von Frequenzbereichen angestrebt. Dazu wird von dem *Electronic Communications Commitee (ECC)* der *European Conference of Postal and Telecommunications Administrations (CEPT)*, dem 48 europäische Länder angehören, die *European Table of Frequency Allocations and Aplications in the Frequency Range 8.3kHz to 3000 GHz (ECA Table)*[siehe ECA-Table, 2014] herausgegeben. Für die rechtlichen Regelungen und Frequenzzuteilungen ist in der Bundesrepublik Deutschland die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (kurz Bundesnetzagentur (BNetzA)) zuständig. Sie erstellt auf Basis des Telekommunikationsgesetzes (TKG), insbesondere der §§52 bis 65, den *Frequenzbereichszuweisungsplan (FreqBZP)* und den ausführlicheren *Frequenznutzungsplan (FreqNP)*. In der,

dem *FreqBZP* zugrundeliegenden, Frequenzverordnung[4] sind im §4 verschiedene Funkdienste definiert. Für den Bereich dieser Arbeit sind dabei die Dienste

7. Flugnavigationsfunkdienst: Navigationsfunkdienst zum Zwecke des sicheren Führens von Luftfahrzeugen.

9. Funkdienst : Gesamtheit der Funknutzungen, deren Verwendungszweck ein wesentliches gemeinsames Merkmal besitzt.

12. Mobiler Flugfunkdienst : Mobilfunkdienst zwischen Bodenfunkstellen und Luftfunkstellen oder zwischen Luftfunkstellen, an dem auch Rettungsgerätfunkstellen teilnehmen dürfen; Funkbaken zur Kennzeichnung der Notposition dürfen auf festgelegten Notfrequenzen ebenfalls an diesem Funkdienst teilnehmen.

22. Mobilfunkdienst: Funkdienst zwischen mobilen und ortsfesten Funkstellen oder zwischen mobilen Funkstellen.

von Interesse. Da UAVs in Deutschland sich noch in einer rechtlich nicht eindeutig geklärten Lage befinden, kommt zunächst jedoch nur der Bereich 22: Mobilfunkdienst in Betracht.

Im *FreqBZP* sind für einzelne Frequenzbereiche die zugewiesenen Dienste und ihre Nutzung - zivil und/oder militärisch - aufgelistet. Die Zuweisungen reichen von 8kHz bis 3000GHz. Im *FreqNP* sind für die im *FreqBZP* festgelegten Bereiche jeweils sogenannte Frequenznutzungsteilpläne aufgeführt. In diesen ist der genaue (unter) Frequenzbereich sowie die Nutzungsbestimmungen festgelegt. Außerdem sind die zulässige Frequenznutzung und deren Bedingungen. Dies sind regulatorische, technische und betriebliche Bestimmungen, die bei der Frequenznutzung einzuhalten sind.

Im *FreqNP* sind für den Bereich dieser Arbeit folgende Frequenznutzungen von Bedeutung:

Datenfunk Der Datenfunk dient der paketorientierten Übertragung von Datensignalen (z. B. Messwerten, Schaltbefehlen, Alarmsignalen) zwischen Funkstellen, die ortsfest oder mobil betrieben werden.

Fernmessen (Telemetrie) Fernmess-Anwendungen (Telemetrie) dienen dem Fernmessen mit Hilfe von Funkwellen. Es handelt sich um Funkanlagen in Luftfahrzeugen oder um terrestrische Funkanlagen, sowohl für zivile als auch für militärische Anwendungen.

Fernsteuerung von Flugmodellen Die Fernsteuerung von Flugmodellen dient der Übertragung von Fernwirksignalen zur Fernsteuerung von Flugmodellen.

WLAN WLANs sind breitbandige Funkanwendungen zur Datenübertragung. (...)

[4] Frequenzverordnung vom 27. August 2013 (BGBl. I S. 3326), http://www.gesetze-im-internet.de/freqv/

[vgl. Frequenzplan, 2014]

Ebenso könnten in Zukunft die Bereiche Flugfunk und Flugnavigation eine Rolle spielen, wenn UAVs als Flugzeuge zugelassen sind und die Kriterien für die Nutzung der Flugfunkdienste erfüllt sind.

Grundsätzlich bedarf es für jede Frequenznutzung in der Bundesrepublik Deutschland einer vorherigen Frequenzzuteilung durch die BNetzA. Eine Zuteilung erfolgt auf Antrag an eine natürliche oder juristische Person oder an eine Personenvereinigung. Dabei ist zu beachten, dass die Zuteilung nur erfolgt, wenn u. a. die beantragte Frequenz für die beantragte Nutzung im *FreqNP* vorgesehen ist, sie verfügbar ist und die Verträglichkeit mit anderen Frequenznutzungen gegeben ist.

Darüber hinaus werden von der BNetzA sogenannte Allgemeinzuteilungen für Frequenzen ausgestellt. Diese sind zur Nutzung durch die Allgemeinheit oder einem in der Zuteilung bestimmten Personenkreis freigegeben. Es müssen dabei allerdings die Bedingungen der Zuteilung und des *FreqNP* eingehalten werden. Eine gleichzeitige Nutzung durch mehrere Funkstellen kann nicht ausgeschlossen werden. Die Allgemeinzuteilungen veröffentlicht die BNetzA u. a. auf ihrer Homepage [5].

Neben der Frequenzzuteilung ist es außerdem erforderlich, dass die genutzten Funkanlagen für den Betrieb in der Bundesrepublik Deutschland vorgesehen, bzw. gekennzeichnet sind.

Im Bereich von UAVs sind folgende Allgemeinzuteilungen von Interesse:

Fernsteuerung von Modellen[6] Für die Fernsteuerung von Modellen sind die Frequenzen 26,995-27,145 MHz, 27,195 MHz, 27,255 MHz sowie der ausschließlich für Flugmodelle reservierte Bereich von 35,010-25,200MHz und 35,820-35,910MHz. Dabei ist eine maximale Strahlungsleistung von 100 mW (ERP) erlaubt. Die Kanalbreite Beträgt 10kHz. Diese Allgemeinzuteilung ist bis zum 31.12.2022 befristet.

Neuere Fernbedienungen nutzen bereits den Bereich bei 2,4 GHz. So z. B. auch die Fernbedienung der Firma Spektrum die im Projekt AES verwendet wird.

Funkanwendungen mit geringer Reichweite für nicht näher spezifizierte Anwendungen[7] Nach einer Entscheidung der Europäischen Kommission zur Harmonisierung der Frequenznutzung durch Geräte mit geringer Reichweite (2006/771/EG) sind „Short-Range Devices“ (SRD) Funksender mit uni- oder bidirektionaler Kommunikation, die über kurze Distanz und mit niedriger Leistung senden. Dabei ist kurze Distanz nicht näher definiert.

[5] https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Allgemeinzuteilungen/allgemeinzuteilungen-node.html

[6] Allgemeinzuteilung von Frequenzen zur Fernsteuerung von Modellen

[7] Allgemeinzuteilung von Frequenzen zur Nutzung durch Funkanwendungen mit geringer Reichweite für nicht näher spezifizierte Anwendungen; Non-specific Short Range Devices (SRD)

Die entsprechende Allgemeinzuteilung umfasst insgesamt 28 Frequenzbänder in den Bereichen von 6,765Mhz bis hin zu Bereichen um 246GHz. Für den Bereich der UAVs, insbesondere in dieser Arbeit sind die Bereiche um 433MHz, um 868MHz sowie 2,4GHz und 5,7 GHz. Die genauen Aufteilungen dieser Bereiche sowie Nutzungseinschränkungen können den Tabellen 2.1 und 2.2 entnommen werden. Diese Allgemeinzuteilung ist bis 31.12.2024 befristet.

WLAN-Funkanwendungen[8] Für die Frequenznutzung für WLAN sind zwei Bereiche vorgesehen. Zum einen der Bereich von 2400,0-2483,5MHz mit einer maximalen zulässigen Strahlungsleistung von 0,1W (EIRP). Weiter gelten maximale spektrale Leistungsdichten je nach Zugriffsverfahren.

Außerdem sind im 5GHz Bereich 3 Abschnitte für die Nutzung für WLAN vorgesehen.

Alle WLAN Frequenzen und ihre Nutzungsbegrenzungen sind in Tabelle 2.3 aufgeführt.

[8] Allgemeinzuteilung von Frequenzen für die Nutzung in lokalen Netzwerken; Wireless Local Area Networks (WLAN- Funkanwendungen) und Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN (?Wireless Access Systems including Wireless Local Area Networks?

Tabelle 2.1: Übersicht der Frequenzen und ihrer Nutzungsbedingungen für SRDs bis 1GHz (aus der Allgemeinzuteilung für SDR[7])

Frequenzbereich in MHz	**Maximale äquivalente Strahlungsleistung (ERP)**	**Zusätzliche Parameter/Frequenzzugangs- und Störungsminderungstechniken**	**Sonstige Nutzungsbeschränkungen**
433,050-434,790	10mW		
863-865	25mW	DC von 0,1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Audioanwendungen außer Sprachanwendungen. Keine analogen Videoanwendungen
865,0-868	25mW	DC von 1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Audioanwendungen außer Sprachanwendungen. Keine analogen Videoanwendungen
868,0-868,6	25mW	DC von 1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Videoanwendungen
868,7-869,2	25mW	DC von 0,1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Videoanwendungen
869,3-869,4	10mW	Zur effizienten Nutzung ist ein Zugangsprotokoll (wie z. B. ETSI EN 301 391) erforderlich.	Kanalbandbreite 25kHz
869,40-869,65	500mW	DC von10% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Videoanwendungen
	25mW	DC von 0,1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Audioanwendungen außer Sprachanwendungen. Keine analogen Videoanwendungen
869,7-870,0	5mW		Keine Audio- und Videoanwendungen
	25mW	DC von 1% alternativ Frequenzzugangs-/Störungsminderungstechniken	Keine analogen Audioanwendungen außer Sprachanwendungen. Keine analogen Videoanwendungen

Tabelle 2.2: Übersicht der Frequenzen und ihrer Nutzungsbedingungen für SRDs ab 1GHz (aus der Allgemeinzuteilung für SDR[7])

Frequenzbereich in GHz	**Maximale äquivalente Strahlungsleistung (ERP)**
2,400-2,4835	10mW
5,725-5,875	25mW

Tabelle 2.3: Übersicht der Frequenzen und ihrer Nutzungsbedingungen für WLAN (aus den Allgemeinzuteilungen für WLAN[8]). Es darf keiner der beiden Grenzwerte (Strahlungsleistung und Strahlungsdichte) überschritten werden.

Frequenz-bereich in MHz	**Maximale zulässige mittlere äquivalente isotrope Strahlungsleistung (EIRP)**	**Maximal zulässige mittlere spektrale Strahlungsleistungsdichte (EIRP)**	**Weitere Bestimmungen**
2400,0 - 2483,5	0,1 W	0,1W/100kHz	bei Frequenzsprung-Spektrumspreiz-verfahren(FHSS)
	0,01W	0,01W/1MHz	bei Direktsequnz Spektrumspreizverfahren (DSSS) und anderen Zugrissverfahren
5150-5250	0,2W	10mW/MHz	Nutzung ausschließlich innerhalb geschlossener Räume
5250-5350	0,2W	10mW/MHz	Nutzung ausschließlich innerhalb geschlossener Räume, Leistungsregelung, Minderungstechniken
5470-5725	1,0W	50mW/MHz	Nutzung innerhalb und außerhalb geschlossener Räume, Leistungsregelung, Minderungstechniken

3 Recherche

3.1 Funksysteme

3.1.1 WLAN

Wireless LAN (Local Area Network) basiert im Grunde auf den Institute of Electrical and Electronics Engineers (IEEE) Standrads 802.X, den „Ethernet-Standards“, dies sind Standards für die drahtgebundene Vernetzung von Computern. Das WLAN selbst ist in den IEEE Standards 802.11 spezifiziert.

In diesem Standard sind der Mediumszugriff auf Layer 2 des OSI-Referenzmodell und die physikalische Schicht definiert. Dabei wurde beim Medienzugriff weitestgehend auf die Verfahren aus dem Ethernet-Standard zurückgegriffen.

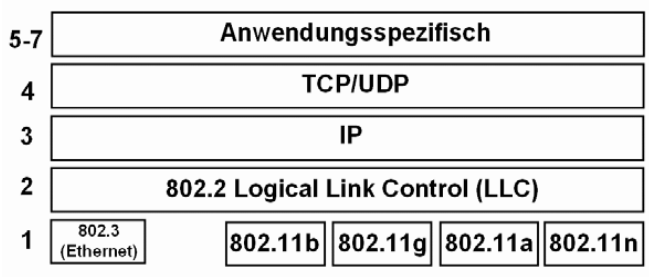


Abbildung 3.1: WLAN Protokollstack [Sauter, 2013]

Funkstandards

Seit der Entwicklung des Standards 802.11 gibt es diverse Weiterentwicklungen, die sich insbesondere in der Art der Funkübertragung unterscheiden. Die gebräuchlichsten Standards sind in Tabelle 3.1 aufgelistet.

Da je nach Qualität der Verbindung (Abhängig von Hindernissen und Entfernung zwischen Sender und Empfänger) die Redundanzen in den Datenpaketen angepasst werden, verringert sich die Übertragungsgeschwindigkeit bei schlechten Verbindungen stark. Die von vielen

Tabelle 3.1: WLAN Standards und ihre Frequenzbänder[Sauter, 2013]

Standard	Frequenzband	Theoretische Maximalgeschwindigkeit
802.11b	2,4GHz(2,401-2,483 GHz)	1-11 Mbit/s
802.11g	2,4GHz(wie oben)	6-54 Mbit/s
802.11a	5GHz(5,150-5,350 GHz und 5,470-5,725GHz)	6-54 Mbit/s
802.11n	2,4GHz (wie oben) 5GHz (wie oben)	6-600 Mbit/s
802.11ac	5GHz	bis zu 6,93 GBit/s

Herstellern angepriesene Reichweite von bis zu 300 m wird bestenfalls bei 1 Mbit/s nur im Freien erreicht, wenn keine Hindernisse zwischen Sender und Empfänger die Übertragung stören.[Sauter, 2013] In Deutschland gelten die in Kapitel 2.3.4 beschriebenen Regelungen für den Betrieb von WLAN-Funkknoten.

Im IEEE 802.11b wird das in Kapitel 2.3.2 beschriebene DSSS Verfahren genutzt. Hierfür steht eine Kanalbandbreite von 22MHz zur Verfügung. Jedoch wurde das Kodierungsverfahren optimiert, sodass höhere Datenraten erzielt werden können.

IEEE 802.11g nutzt ein Frequency Division Multiplexing (FDM) mit dem Namen Orthogonal Frequency-Division Multiplexing (OFDM). Dieses ermöglicht das Nutzen eines 20MHz Kanalrasters, wodurch in Europa der Betrieb von vier überlappungsfreien Kanälen möglich ist.

IEEE 802.11a nutzt ebenfalls das OFDM mit 20MHz Kanalbandbreite jedoch im 5GHz Band.

IEEE 802.11n nutzt ebenfalls das OFDM jedoch sind hier Kanalbandbreiten von 40MHz möglich. Zusätzlich sind in diesem Standard mehrere Multiple Input Multiple Output (MIMO)-Verfahren spezifiziert. Dabei werden verschiedene Datenströme zeitgleich auf der gleichen Frequenz über räumlich getrennte Sendeantennen ausgestrahlt. Auf der Empfängerseite sind die gleiche Anzahl an Antennen notwendig um die einzelnen Ströme wieder zu zerlegen. Es sind bis zu 4 MIMO-Kanäle vorgesehen.

IEEE 802.11ac basiert auf IEEE 802.11n, nutzt jedoch nur das 5GHz Band. Dort sind Kanalbandbreiten bis 160MHz möglich. Außerdem sind bis zu 8 MIMO-Kanäle vorgesehen.

Betriebsmodi

Es gibt verschiedene Betriebsmodi für WLAN. Diese sind:

Ad-hoc Im Ad-hoc Modus kommunizieren alle WLAN-Geräte gleichberechtigt miteinander. Alle Teilnehmer müssen die gleiche Service Set Identifier (SSID), die gleiche Kanalnummern und bei Nutzung von Verschlüsselung den gleichen Verschlüsselungskey benutzten. Außerdem müssen die genutzten IP-Adressen abgestimmt werden. Da alle Teilnehmer gleichberechtigt sind, wird dies nicht von einer Instanz übernommen. Es ist daher ein gewisser Konfigurationsaufwand notwendig.

Infrastruktur-Modus Beim Infrastruktur-Modus gibt es einen zentralen Access-Point (AP), der gewisse Koordinierungsfunktionen übernimmt. So sendet der AP regelmäßig Informationen über die genutzte SSID, unterstützte Datenraten und die genutzte Verschlüsselungstechnik aus.

Darüber hinaus läuft die komplette Kommunikation über den AP. Die Geräte senden ihre Daten an diesen und der AP sendet die Daten an den Empfänger weiter. Dies bedeutet, dass die Luftschnittstelle zweimal mit den gleichen Daten belegt wird, was zu einer Reduzierung der Nutzdatenrate führt. Jedoch können so auch zwei Geräte kommunizieren, die gegenseitig keine direkte Funkverbindung haben.

Da WLAN die gleiche Adressierung wie Ethernet nutzt, können über eine Ethernetverbindung des APs auch kabelgebundene Geräte mit den Geräten im WLAN kommunizieren. Es ist dabei für die Geräte nicht erkennbar, ob sich der Kommunikationspartner im WLAN oder im Ethernet befindet.

Extended Service Set Wenn ein größerer Bereich mit WLAN abgedeckt werden soll, besteht die Möglichkeit mehrere APs einzusetzen. Diese werden dabei über ein Distribution System (meist Ethernet) miteinander verbunden. Ändert ein Gerät seinen Standort und hat über einen anderen AP nun eine bessere Verbindung, kann das Gerät sich zu diesem AP verbinden. Der neue AP und der alte AP tauschen die Teilnehmerinformationen über das Distribution System aus. Kommt nun ein neues Paket für das Gerät an, so wird dieses über den aktuell genutzten AP an das Gerät gesendet.

Damit dies funktioniert, müssen alle AP im gleichen IP-Subnetz sein. Sie müssen die gleiche SSID nutzen. Es müssen unterschiedliche Kanäle genutzt werden, die nicht mit von den benachbarten APs genutzten Kanälen überlappen. Die Sendebereiche müssen sich jedoch überlappen, damit ein kontinuierlicher WLAN-Empfang möglich ist.

Da die Entscheidung für das Wechseln des AP vom Gerät und nicht vom Netzwerk getroffen wird, kann es jedoch dazu kommen, dass ein neuer AP erst gesucht wird, wenn der Kontakt zum alten bereits verloren ist. Ein vom Netzwerk ausgelöster Wechsel ist nicht vorgesehen. An diesem Punkt wird bereits gearbeitet, um auch in WLAN-Netzen unterbrechungsfreie Handoffs zu ermöglichen.

Verschlüsselung

Es ist offensichtlich, dass sich ohne Einsatz von Verschlüsselungstechniken ein drahtloses Netzwerk besonders einfach abhören oder attackieren lässt. Aus diesem Grund unterstützt WLAN mehrere Verschlüsselungsverfahren. Das erste dieser Art war **Wired Equivalent Privacy (WEP)**. Dieses gilt mittlerweile als nicht mehr sicher.

Der Nachfolger von WEP ist **Wi-Fi Protected Access (WPA)**. Dieser Standard setzte auf WEP auf und hatte zum Ziel auf älteren Geräten, die WEP unterstützten, lauffähig zu sein. Es wird für WPA unter anderem das Temporal Key Integrity Protocol (TKIP) zur Generierung dynamischer Schlüssel genutzt. Wie unter anderem von [Tews und Beck, 2009] gezeigt, bietet auch WPA die Möglichkeit von erfolgreichen Angriffen.

Aktuell wird **Wi-Fi Protected Access 2 (WPA2)** als sichere Verschlüsselungsmöglichkeit angesehen.

Beide WPA Standards bieten die Möglichkeit, dass alle Geräte den gleichen Schlüssel verwenden den sogenannten pre-shared key (PSK). Es ist jedoch auch möglich, dass durch Hilfe von einem Authentifizierungsserver die Zugangspasswörter zentral verwaltet werden. Dies ermöglicht u. a. mehrere AP zu betreiben, ohne dazu die Zugangspasswörter in jedem AP zu hinterlegen.

3.1.2 ZigBee

ZigBee ist eine Spezifikation von Kommunikationsprotokollen der höheren Layer des OSI-Referenzmodell, um insbesondere Personal Area Network (PAN) mit kleinen, stromsparenden Funkmodulen zu realisieren. ZigBee baut dabei auf dem IEEE-Standard 802.15.4 auf.

Dieser definiert die ersten beiden Layer für ein konzeptionell sehr einfaches drahtloses Netzwerk. Der Fokus lag bei seiner Entwicklung auf sehr geringer Komplexität, sehr geringen Implementationskosten und sehr geringem Stromverbrauch sowie dadurch bedingte niedrige Datenraten um 250kb/s [IEEE802.15.4, 2011]

Funkstandards

Es werden dabei u. a. das 868MHz-Frequenzband für Europa und weltweit das 2,4GHz-Frequenzband unterstützt. Wobei diese Frequenzbänder physikalisch nicht mit einer Empfangs-/Sendeeinheit genutzt werden können, sondern für jedes Band spezialisierte Hardware benötigt wird.

Tabelle 3.2: Einige Frequenzbänder, ihre Modulationsart und Datenraten aus [IEEE802.15.4, 2011]

Frequnzband (MHz)	Kanal-bandbreite	Modulation	Bit-Rate (kb/s)
868-868,6	300kHz	BPSK	20
		ASK	250
		O-QPSK	100
2400-2483,5	2MHz	O-QPSK	250

Betriebsarten

Der IEEE-Standard sieht zwei unterschiedliche Gerätetypen vor. Zum einen das sogenannte **Full Funktion Device (FFD)**, welches in der Lage ist als Koordinator für das Personal Area Network (PAN) zu fungieren. Der Koordinator legt u. a. den Identifier des Netzes fest, um es gegenüber anderen IEEE-802.15.4-Netzen abzugrenzen. Zum anderen das **Reduced Funktion Device (RFD)**. Diese Art von Geräten hat nur einen sehr eingeschränkten Funktionsumfang und kann daher keine Koordinierungsaufgaben übernehmen. RFDs sind insbesondere für den Einsatz bei besonders einfachen Aufgaben gedacht, bei denen jeweils nur der Kontakt zu einem anderen Knoten aufgebaut werden muss. Dadurch kann diese Art von Knoten sehr einfach implementiert werden.

Im ZigBee-Standard findet sich diese Einteilung wieder. Hier gibt es drei Typen[vgl. ZigBee-Spec, 2007]:

ZigBee Coordinator Ein FFD, das die Rolle des PAN-Koordinators übernimmt.

ZigBee Router Ein FFD das in einem ZigBee Netzwerk teilnimmt, jedoch nicht der Koordinator ist, aber Koordinatoraufgaben im eigenen Umfeld übernehmen kann.

ZigBee End Device Ist ein FFD oder RFD, welches an einem ZigBee-Netz teilnimmt, jedoch weder Router noch Koordinator ist

Die IEEE-802.15.4 sieht unterschiedliche Netzwerktopologien vor:

Stern In dieser Konfiguration ist ein FFD der Koordinator. Alle anderen Teilnehmer müssen sich bei diesem melden und die Kommunikation läuft ausschließlich über diesen Koordinator. Stern-Netzwerke arbeiten komplett unabhängig von allen anderen Netzwerken in Reichweite. Dies wird durch die Wahl einer nicht von anderen Netzen genutzte ID durch den Koordinator sichergestellt. Sobald diese ID gewählt ist, kann der Koordinator anderen Geräten (unabhängig ob FFD oder RFD) den Zutritt zum Netzwerk erlauben. (Beispiel siehe Abbildung 3.2)

Peer-To-Peer in einem Peer-to-Peer (P2P)-Netzwerk ist jeder Teilnehmer prinzipiell in der Lage mit allen anderen Teilnehmern in Reichweite zu kommunizieren. Ein Knoten wird dabei als Koordinator benannt. (Beispiel siehe Abbildung 3.2)

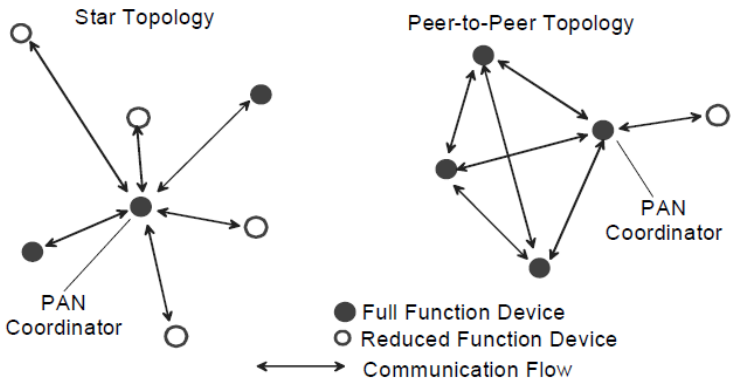


Abbildung 3.2: Beispiel für Stern- und Peer-To-Peer-Netzwerk [IEEE802.15.4, 2011]

Baum Auch Cluster-Tree, ist eine spezielle Art des P2P-Netzwerks. Dabei bilden die RFDs die Blätter, da diese nur eine Verbindung zu einem Koordinator besitzen können. Jedes FFD kann in diesem Netz als Koordinator agieren und Synchronisationsdaten für andere Knoten oder auch andere Koordinatoren zur Verfügung stellen. Es ist jedoch immer nur ein Koordinator der Hauptkoordinator des gesamten PAN. Dieser Koordinator erzeugt das erste Cluster durch Finden und Bekanntgeben einer PAN-ID und sendet Beacon-Frames an die benachbarten Geräte. Empfangen diese dieses, so können sie beim Koordinator um Zutritt zum Netz bitten. Nimmt dieser den anfragenden Knoten auf, so merkt der Koordinator sich diesen Knoten als Kind-Knoten und der aufgenommene Knoten merkt sich den Koordinator als Eltern-Knoten. Danach sendet der neu Aufgenommene selbst Beacon-Frames, sodass sich wiederum an diesem neue Knoten anmelden können. Ein Beispiel für diese Struktur ist in Abbildung 3.3 zu sehen.

Der ZigBee-Standard unterstützt diese Topologie komplett, nennt jedoch das P2P-Netzwerk **Mesh-Netzwerk**. Außerdem trägt nur der PAN-Koordinator auch den Namen *ZigBee Koordinator*. Alle anderen Koordinatoren werden zur besseren Unterscheidung *ZigBee Router* genannt.

Jeder Knoten in einem ZigBee-Netzwerk kann über seine unique 64-bit Adresse adressiert werden. Um jedoch diesen Overhead zu vermeiden, bekommt jeder Knoten beim Zutritt in ein Netzwerk eine 16 Bit lange Adresse zugewiesen, über die der Knoten ebenfalls erreichbar ist.

Darüber hinaus besteht auch die Möglichkeit Gruppen festzulegen und Nachrichten an diese Gruppen zu adressieren.

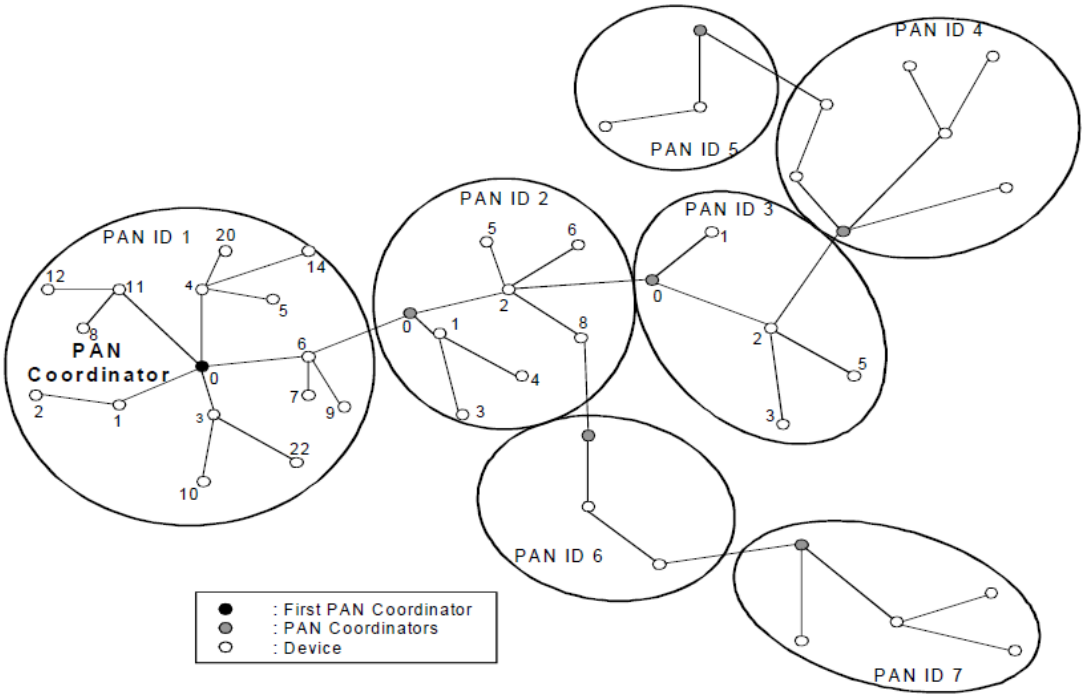


Abbildung 3.3: Beispiel eines Cluster-Tree-Netzwerk nach [IEEE802.15.4, 2011]

Die Reichweite ist bei ZigBee ist auf Grund des eigentlichen Einsatzes als PAN auf wenige Meter bis 100 Meter begrenzt. Es gibt jedoch auch Geräte die speziell für den Einsatz überlängere Distanzen konzipiert sind.

Sicherheit

Der ZigBee-Standard setzt auch bei der Verschlüsselung sehr stark auf dem IEEE-802.15.4-Standard auf. Es wird eine erweiterte Version des CCM-Mode Verfahren (CCM*) eingesetzt. Dieses stellt sowohl Verschlüsselung als auch Authentifizierung zur Verfügung. Dabei wird das Blockchiffreverfahren AES-128 eingesetzt. Es besteht die Möglichkeit Pakete in der Netzwerkschicht zu verschlüsseln. Dies setzt jedoch voraus, dass alle beteiligten Knoten den Netzwerkschlüssel kennen. Es ist jedoch auch möglich auf der Anwendungsebene zu verschlüsseln. Dann reicht es aus, wenn nur die beiden Endpunkte der Kommunikation den Schlüssel kennen.

Ein Problem stellt dabei die Verteilung der Schlüssel dar. Ein Ansatz ist die Schlüssel, insbesondere den Netzwerkschlüssel, bei der Herstellung in dem Knoten zu installieren. Dies hat jedoch den Nachteil, dass der Nutzer dies nicht beeinflussen kann und alle Knoten mit dem

gleichen Schlüssel Zugriff auf das Netzwerk haben. Ein anderer Ansatz ist es den Schlüssel bei Eintritt eines Knotens in das Netzwerk unverschlüsselt zu übertragen. Um dieses Verfahren gegen Abhören oder Manipulation zu sichern, soll z. B. ein anderer Kanal genutzt werden.[ZigBeeSpec, 2007] Bei dem so übertragenen Schlüssel soll es sich nur um einen Initialisierungsschlüssel handeln, an der Sicherheit eines solchen Verfahrens bleiben jedoch Zweifel. Eine weitere Möglichkeit bildet der Einsatz von Trust Centern. Auch eine manuelle Konfiguration der Knoten ist möglich.

3.1.3 Mobilfunk

Im Bereich des Mobilfunk gibt es mehrere Protokolle zur Datenübermittlung. Insbesondere in den letzten Jahren hat hier ein rasanter Ausbau stattgefunden. Mittlerweile wird die sogenannte 4. Generation dieser Standards eingesetzt. Es werden jedoch auch noch alle älteren Systeme eingesetzt und unterstützt. Diese alle zu beschreiben würde den Rahmen dieser Arbeit sprengen, sodass sich auf den grundsätzlichen Aufbau von Mobilfunknetzen und einer Leitungsübersicht der einzelnen Systeme beschränkt wird.

In allen Mobilfunksystemen wird die abzudeckende Fläche in mehrere **Zellen** unterteilt. Darum wird im Englischen auch von *cell phones* gesprochen. Diese Zellen haben einen Radius, von wenigen 100m an stark besuchten Orten, bis zu etwa 15km in dünnbesiedelten Gebieten. Jede dieser Zelle hat eine Basisstation, die mit in der Regel 3 Antennen die Zelle abdeckt. Je nach Mobilfunkstandard dürfen zwei benachbarte Zellen nicht die gleiche Frequenz haben. Bei anderen Standards ist dies nicht der Fall, dort nutzen alle Stationen die gleichen Frequenzen.

Mehrere dieser Basisstation werden an einem Controller zusammengeschlossen. Dieser stellt wiederum die Verbindung in das Core Network her, welches die Vermittlung von Verbindungen, deren Aufbau und deren Kontrolle übernimmt. Zusätzlich werden hier die Verbindungen zu anderen Netzen hergestellt. Alle Verbindungen, auch zu Endgeräten in der gleichen Zelle werden über das Core Network geführt. Jeder Teilnehmer muss sich dazu im Netz registrieren, damit das Netzwerk weiß wo sich das Gerät befindet. Anders als beim WLAN werden Wechsel der genutzten Basisstation vom Netz aus gesteuert, sodass ein Wechsel der Zelle ohne Verbindungsunterbrechung möglich ist.

Die wichtigsten Standards im Mobilfunk für Daten sind General Packet Radio Service (GPRS), das dem Global System for Mobile Communications (GSM)-Netz einen paketorientierten Dienst zur Datenübertragung zur Verfügung stellt. Enhanced Data Rates for GSM Evolution (EDGE) führte für GSM-Netze ein neues Modulationsverfahren ein, womit höhere Datenraten bei gleicher Bandbreite möglich sind. Universal Mobile Telecommunications System (UMTS) wird auch als Standard der 3. Generation bezeichnet. Es ist eine komplette Weiterentwicklung des GSM-Netz. Durch Integration von - seit der Entwicklung von GSM - deutlich schnelleren

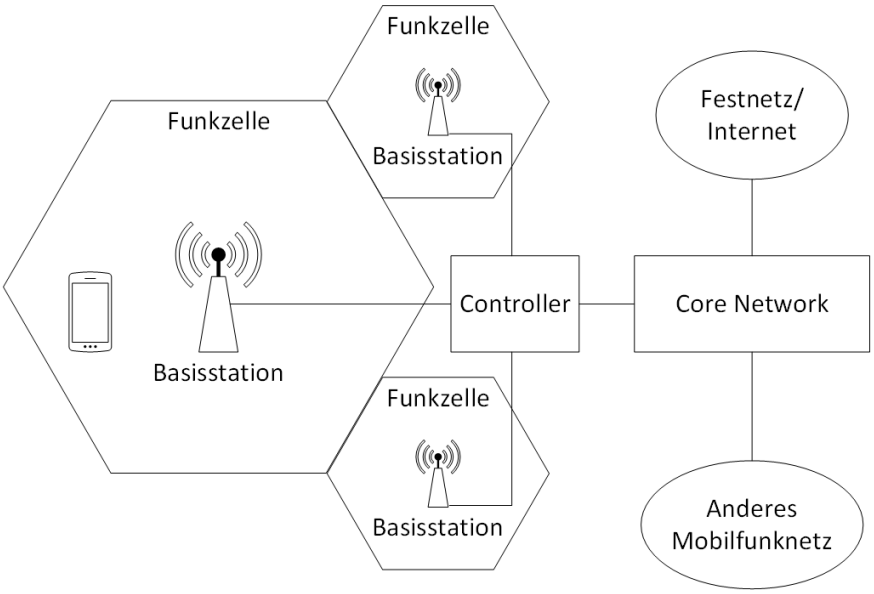


Abbildung 3.4: Grundsätzlicher Aufbei von Mobilfunknetzen

Komponenten, können komplizierte Verfahren beim Zugriff auf die Luftschnittstelle genutzt werden, die wiederum einen deutlichen Zuwachs in der Übertragungsgeschwindigkeit erzeugen. High Speed Packet Access (HSPA) ist eine Erweiterung des UMTS, die wiederum eine Steigerung der Datenrate zur Folge hatte. So sind u. a. hier MIMO-Verfahren vorgesehen. Long Term Evolution (LTE) setzt wiederum auf dem UMTS-Standard auf. Im Gegensatz zu diesem werden jedoch keine festen Kanalbreiten mehr genutzt, sondern es gibt Bandbreiten von 1,25 MHz bis 20 MHz. Zusätzlich wird der Datenstrom in mehrere langsamere Datenströme aufgeteilt, die jedoch parallel übertragen werden. Hierdurch werden negative Einflüsse von sehr schnellen Übertragungen minimiert. Die aktuellste Erweiterung ist das LTE-Advanced, welches als Standard der 4. Generation gilt.

Tabelle 3.3: Theoretische Datenraten einiger Mobilfunkstandards

Technology	Download Rate	Upload Rate
GPRS (2.5G)	57,6 kbit/s	28.8 kbit/s
EDGE	236,8-1894 kbit/s	236,8-947kbit/s
UMTS (3G)	384 kbit/s	384 kbit/s
HSPA	13,98-42 Mbit/s	5,76-11,5 MBit/s
LTE	173 - 326MBit/s	58 - 86 MBit/s

Sicherheit

Alle Mobilfunkstandards nutzen Verschlüsselung auf der Luftschnittstelle. Zumindest die Verschlüsselung von GSM gilt aber als gebrochen. [Nohl und Paget, 2009] Aber auch für die neueren Standards sind bereits Angriffe bekannt, diese nutzen jedoch nicht direkt eine Schachstelle der Verschlüsselung der Luftschnittstelle aus, sondern nutzen Sicherheitslücken im SS7-Protokoll. Dieses ist für die Verbindungsvermittlung und den Austausch von Daten im Core Network, aber auch mit anderen Mobilfunknetzen verantwortlich. Es sind Angriffe bekannt, bei denen es möglich ist Textnachrichten und Gespräche abzufangen und zu entschlüsseln. Ob dies auch bei Datenverbindungen möglich ist, ist noch nicht nachgewiesen.[Engel, 2014]

3.1.4 Narrow Band-Funkmodems

Narrow Band oder zu deutsch Schmalband bezeichnet (Funk-)Übertragungen die einen Kanal mit 12,5kHz Bandbreite nutzen. Durch diese enge Kanalbandbreite ist es vielen Teilnehmern möglich in einem Frequenzband zu senden und zu empfangen. Dies bringt aber auch die Einschränkungen mit sich die in Kapitel 2.3.2 beschrieben sind.

Es gibt in diesem Bereich keine Standards, die nennenswert verbreitet sind. Jedoch gibt es eine ganze Reihe von proprietären Protokollen und Produkten, die insbesondere der drahtlosen Anbindung der seriellen Schnittstelle dienen.

Im Projekt-AES sind zwei Module der Firma *AMBER wireless GmbH* vom Typ *AMB8350* vorhanden. Diese stammen aus der letzten Version des AC20.30. Bei diesen Modulen handelt es sich jedoch strenggenommen nicht um Narrow Band-Module nach der obigen Definition, denn die Kanalbreite kann je nach Betriebsmodus zwischen 10kHz und 200kHz liegen. Die Module können im Frequenzband zwischen 868,059MHz und 869,621MHz senden. Dabei unterstützen sie die Manchester- oder NRZ-Codierung. Je nach Betriebsmodus und Funkqualität lassen sich nach dem Datenblatt 4-30kbit/s realisieren. Als Schnittstellen stehen UART/RS232-Schnittstellen zur Verfügung.

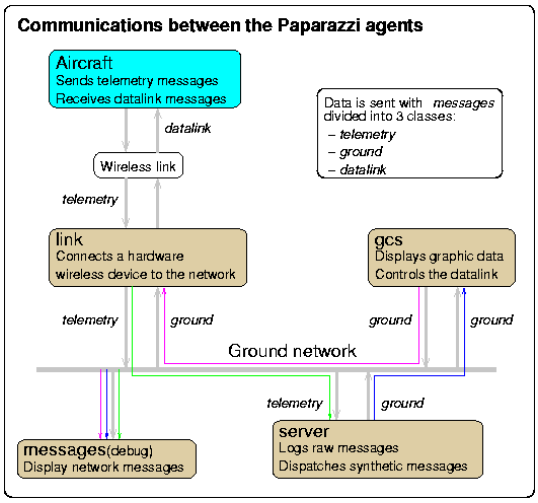
3.2 Telemetrie Systeme in (Open Source) UAV-Projekten

Es gibt mittlerweile eine Vielzahl an Open-Source-Projekten die sich mit UAVs bzw. Modellflugzeugen und Multicoptern beschäftigen. Bei diesen gibt es teilweise schon komplexe Konzepte für eine Kommunikation zwischen Flugzeug und Ground Control Station (GCS), bei anderen ist zumindest eine Schnittstelle zum Anschließen einer Datenübertragung vorgesehen. Wieder andere Projekte haben kein nennenswertes Konzept.

3.2.1 Paparazzi

Paparazzi ist ein Open Source Autopilotsystem. Das Projekt wurde 2003 begonnen und hatte als Ziel einen kostengünstige autonome Flugzeuge zu ermöglichen. Dabei ist das Projekt nicht auf einen bestimmten Typ von Flugzeugen festgelegt. Neben der Software beinhaltet das Projekt auch die Entwicklung eigener Hardware.

(a) Die Systemteile von *Paparazzi*



(b) Architektur des Telemetriesystems von *Paparazzi*

Abbildung 3.5: Das *Paparazzi*-System[Hattenberger u. a., 2014]

Bei der Kommunikation trennt *Paparazzi* zwischen dem **communication segment** und dem **safety link**. Ersterer fast alle (Daten-)Kommunikationsprotokolle zwischen Luft- und Bodensegmenten des Systems zusammen. Letzterer ist eine normale RC-Funkverbindung um unabhängig von einer GCS das Unmanned Aerial Vehicle (UAV) steuern zu können.

Bei der Softwarearchitektur der Bodenkomponente gibt es verschiedene Agenten, die über einen Softwarebus miteinander kommunizieren. Dabei hat jeder Agent eine klar begrenzte Aufgabe. Es können mehrere UAVs gleichzeitig mit einer Bodenstation verbunden werden. Genutzte Technologien können RF-Modems oder WLAN-Verbindungen sein.

Der **link-Agent** koordiniert die Bodenseite der Funkverbindung und verteilt die Telemetriedaten in das Netzwerk. Dieses kann ein einzelner Computer, ein lokales Netzwerk oder das Internet sein. Verschiedene weitere Agenten können die Nachrichten von diesem Netzwerk empfangen und verarbeiten oder ihrerseits Nachrichten an den link-Agenten schicken.

Mit GCS bezeichnet das Projekt den Agenten, der ein grafisches User Interface zur Verfügung stellt.

Die gesamte Bodenkomponente kann auf normalen Laptops mit Linux eingesetzt werden. Es wird außerdem MacOSX und das RaspberryPi unterstützt. Eine GCS-App für Android ist auch vorhanden.

Mittlerweile stößt das verwendete Nachrichtenprotokoll an seine Grenzen. Insbesondere die verfügbare Anzahl an Slots für Nachrichten an die Bodenkomponente ist mittlerweile zu klein. Es wird bereits daran gearbeitet die Nachrichten besser zu organisieren und die Kapselung der Nachrichten zu ändern. Ein anderer Ansatz ist es das *Mavlink*-Protokoll (siehe 3.2.3) zu unterstützen.[Hattenberger u. a., 2014]

3.2.2 OpenPilot - UAVTalk

Das 2009 gegründete Projekt *OpenPilot* hat das Ziel der Gemeinschaft leistungsfähige und dennoch günstige Stabilisierungs- und Autopilotenplattformen zur Verfügung zu stellen. Dabei reichen die selbst definierten Anwendungen vom Search-And-Rescue-Szenario bis zum einfachen Hobby-Modellflieger. Auch hier wird neben der Software eigene Hardware erstellt.

Derzeit existieren zwei Plattformen von *OpenPilot*. Zum einen das **CopterControl** und zum anderen das **Revolution**. Ersteres ist eine Stabilisierungsplattform, letzteres eine Autopilotenplattform.

Zur Kommunikation der Komponenten - innerhalb des Unmanned Aerial System (UAS) und zwischen UAS und GCS - wurde das Protokoll **UAVTalk** entwickelt. Das Protokoll nutzt dabei sogenannte „Telemetrie Objekte“. Durch diesen objektorientierten Ansatz ist es extrem flexibel, auch für langsame Verbindungen. Das Protokoll ist nicht an eine bestimmte Art der Übertragungsstrecke gebunden. Es ist bereits für den Einsatz auf verschiedenen Funkplattformen, wie z. B. ZigBee, entworfen worden. Um eine Vielzahl an Datenobjekten zu unterstützen, ist der Aufbau des Objekts für die unterste Protokollschicht nicht von Belang. Die Interpretation der Daten wird in höheren Schichten geregelt.[UAVTalk]

Die unterste Protokollebene ist nur für das Übertragen von Byte-Arrays zuständig , sowie das Weiterreichen von empfangenen Daten an das richtige Objekt der höheren Schicht.

Der Aufbau dieser Byte-Pakete ist in Tabelle 3.4 dargestellt.

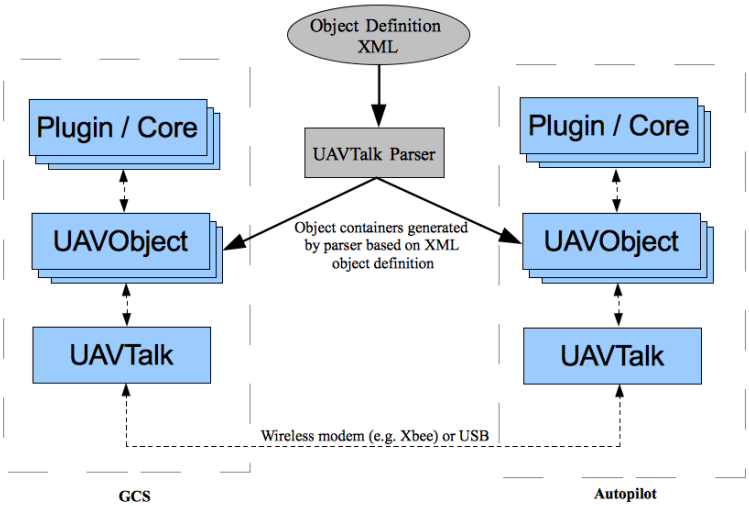


Abbildung 3.6: Aufbau des UAVTalk-Protokolls[UAVTalk]

Tabelle 3.4: Aufbau der UAVTalk-Pakete nach [UAVTalk]

Nachrichten Teil	**Feld**	**Länge (Bytes)**	**Werte**
Header	Sync Val	1	0x3C
	Message type	1	Die niedrigsten 4 Bit geben den NachrichtenTyp an Die höherwertigen 4 Bits geben die Protokollversion oder eine Timestamp-Nachricht an
	Length	2	Wird nicht mehr benötigt, seit Einführung der ObjectID, Bezeichent Länge des Headers und der Daten
	ObjectID	4	Unique ObjektID die vom Parser erzeugt wurde
	InstanceID	2	Unique Objekt InstanzID
	Timestamp	2	Zeitstempel (nur wenn Message type 0x80)
Data	Data	2	Serialisierte Objekte
Checksumme	Checksum	1	CRC-8 checksum

3.2.3 QGroundControl - MAVLink

QGroundControl ist ein Open-Source-Projekt, welches sich nicht mit der Entwicklung einer Autopilotenplattform beschäftigt, sondern sich auf die Entwicklung einer umfangreichen GCS konzentriert. Die GCS unterstützt dabei die Betriebssysteme Windows, Linux und MacOS. Als Kommunikationsprotokoll wird dazu *MAVLink* genutzt.

MAVLink ist eine „header-only“ Marshalling-Library. Sie ist dafür ausgelegt Objekte mit hoher Effizienz in Pakete zu verpacken und über serielle Kanäle zu verschicken. *MAVLink* wird in zahlreichen Autopilot-Plattformen eingesetzt. Die erste Version wurde 2009 veröffentlicht. *MAVLink* kann mit vielen verschiedenen Übertragungsarten genutzt werden.

Ähnlich wie beim *UAVTalk* werden die einzelnen Nachrichten mit Hilfe von xml-Dateien definiert. So ist es möglich beliebige Nachrichten für die Anforderungen des eigenen Systems zu definieren. Auf der Übertragungsebene spielt der konkrete Aufbau der Nachricht keine Rolle. Der Aufbau der MAVLink Pakete ist in Tabelle 3.5 dargestellt.

Tabelle 3.5: Aufbau eines MAVLink Pakets nach [MAVLink]

Byte Index	**Inhalt**	**Werte**	**Erkläru**ng
0	Paket Start Signal	v1.0: 0xFE	Signalisiert den Start eines Pakets
1	Länge der Payload	0-255	Gibt die Länge der Payload an
2	Paketsequenz	0-255	Jede Komponente inkrementiert ihren Sequenzzähler, so können Paketverluste bemerkt werden
3	SystemID	1-255	ID des **sendenden** Systems
4	ComponentID	0-255	ID der **sendenden** Komponente (z. B. Autopilot)
5	MessageID	0-255	ID der Nachricht, gibt an, was die Payload enthält und wie dieses zu dekodieren ist
6 bis (n+6)	Payload	(0-255) Bytes	Daten der Nachricht
(n+7) (n+8)	Checksumme	ITU X.25/SAE AS-4 Hash (CRC-16-CCITT) über die Bytes 1 bis n+6	

3.2.4 AESLink

Bei *AESLink* handelt es sich um einen Software-Bus der in [Hasberg, 2014] zum Zwecke des Testens einzelner Komponenten des AES Projekts in Hardware-In-the-Loop (HIL)- und Software-In-the-Loop (SIL)-Umgebungen entwickelt wurde. Es wurde ausdrücklich nicht im Hinblick auf die Übertragung mittels Telemetrie entworfen.

Im Rahmen der oben genannten Arbeit wurden von Herrn Hasberg neben dem *AESLink* weitere Programme entwickelt, die *AESLink* zur Kommunikation nutzen. So gibt es einen Logger und einen Replayer für *AESLink*-Nachrichten. Außerdem Test-Autopiloten und eine Anzeige des Flugzeugzustandes mittels typischer Instrumente aus einem Cockpit. Darüber hinaus wurden Plugins für Flugsimulatoren entwickelt, sodass diese zur Visualisierung eines Fluges und zum Generieren physikalischer Flugdaten eingesetzt werden können.

Der Bus basiert auf PC-Ebene auf User Datagramm Protocol (UDP) Multicast Verbindungen. Zur Kommunikation mit der Flight Control Unit (FCU) wird ein *HIL-IO-Board* benötigt, welches die physikalischen Schnittstellen der FCU zur Verfügung stellt. Dieses Board wird mittels Universal Asynchronous Receiver Transmitter (UART) mit dem PC verbunden und über den sogenannten *HIL Proxy* mit dem Bus verbunden.

Zur Kommunikation der Komponenten werden Nachrichtentypen definiert. Beim Senden werden diesen Nachrichten Header vorangestellt. Der Header ist dabei 16 Byte groß. Der Aufbau ist in Abbildung 3.7 dargestellt.

Abbildung 3.7: Aufbau des *AESLink*-Headers aus [Hasberg, 2014]

Die einzelnen Felder sind 32 Bit breit. Die *MagicNumber* dient der Erkennung des Starts einer Nachricht im Datenstrom. Es werden keine Prüfsummen verwendet.

4 Entwurf

4.1 Anforderungen

Die folgenden Anforderungen sind beim Entwurf des Systems zu beachten:

1: Transparenz Das zu entwerfende Telemetriesystem soll den im AES-Projekt entwickelten Systemen eine Kommunikation zwischen Airborne- und Bodenstation ermöglichen. Dies soll in der Form geschehen, dass für die Systeme kein Overhead entsteht. Dies bedeutet, dass alle Aufgaben die mit der (Funk-)Übertragung der Daten zusammenhängen, von den Komponenten des Telemetriesystems zu erledigen sind. Die FCU Beispielsweise soll lediglich Daten, die übermittelt werden sollen, an das Telemetriesystem übergeben und danach sich nicht mehr um diesen Vorgang kümmern müssen, sodass ein Problem beim Senden oder Empfangen nicht zu einem zeitlichen Verzug in der Abarbeitung der wichtigeren Aufgaben, wie dem autonomen Flug, führt. Das Telemetriesystem soll demnach transparent sein, sodass Änderungen an dem System keine Auswirkungen auf die Schnittstellen und Protokolle des übrigen Systems haben.

2: Reichweite Das System soll mindestens die Reichweite der RC-Fernbedienung des Piloten erreichen. Idealerweise sollten jedoch auch Verbindungen über größere Entfernungen möglich sein.

3: mehrere Funksysteme Darüber hinaus sollen mehrere Funkmodule mit unterschiedlichen Standards gleichzeitig genutzt werden können, um einerseits eine Redundanz in der Übertragung zu erhalten, andererseits um die Bandbreite zu vergrößern. Außerdem ist so der direkte Vergleich mehrerer Funksysteme unter identischen Einsatzbedingungen möglich.

4: Datenrate Die Datenrate des Systems soll groß genug sein, um den Systemzustand angemessen aktuell am Boden auswerten zu können. Es soll mindestens ein aktueller Systemzustand pro halber Sekunde empfangen werden können.

5: Integration in bestehendes System Das System soll in die aktuelle Systemarchitektur (vgl. Kapitel 1.1.2) passen. Dies bedeutet, dass es mittels UART an die FCU angeschlossen werden kann.

6: Anpassbarkeit Für spätere Entwicklungsstufen der FCU soll jedoch auch ein Anschluss über andere Systeme (z. B. CAN) möglich sein. Der Anschluss von externer Hardware, die nicht an die FCU angeschlossen ist, wäre wünschenswert.

7: Platz- und Energiesparend Da das System in (Modell-)Flugzeugen eingesetzt werden soll, kann das System nicht beliebig groß werden. Es muss versucht werden, auch beim ersten Laborprototypen schon Gine große zu erzielen, die im Flugzeug eingesetzt werden kann, bzw. deren Komponenten so verkleinert werden können (z. B. andere Platinen), dass dies möglich wird. Da auch Energie ein knappes Gut während des Fluges ist muss auch auf diesen Punkt Rücksicht genommen werden.

8: Funkverträglichkeit Da das UAV auch aus rechtlichen Gründern in Deutschland jederzeit von einem Piloten per Fernbedienung gesteuert werden können muss, darf das Telemetriesystem mit den eingesetzten Funksystemen diesen Steuerkanal nie blockieren. Außerdem sind die geltenden Regelungen für die Nutzung von Funksystemen einzuhalten (vgl. Kapitel 2.3.4).

9: Security Auch ist auf ein gewisses Level an Security zu achten. So sollte es nach Möglichkeit für Dritte nicht möglich sein Nachrichten zu verändern oder Befehle an die FCU zu senden.

4.1.1 Komponenten

Das Telemetrisystem muss aus zwei Komponenten bestehen, die jeweils für das Ansteuern der Funkmodule und das Weiterleiten der empfangenen Daten zuständig sind. Dies ist zum einen die **Bodenstation**, sowie die **Airbornestation** die im UAS eingesetzt wird. Dabei sollte es möglich sein, dass auch mehrere Airbornestation mit einer Bodenstation kommunizieren.

Hierzu gibt es zwei Ansätze: Der erste ist, dass beide Komponenten exakt gleich sind. Sie beruhen auf den gleichen Plattformen, auf ihnen läuft die gleiche Software und sie bieten die gleichen Schnittstellen an.

Der andere Ansatz ist, dass jede Komponente genau an die Bedingungen, in denen sie eingesetzt wird, angepasst ist. So muss bei der Bodenstation nicht so viel Wert auf Sparsamkeit bei Größe und Stromverbrauch gelegt werden.

Eine Kombination der beiden Ansätze ist auch möglich.

4.1.2 Schnittstellen

Hardwareschnittstellen

Aus der Anforderung 5 ergibt sich, dass der Teil der im UAS eingesetzt wird, mindestens eine UART-Schnittstelle bieten muss.

Aus der Anforderung 6 leitet sich ab, dass möglichst auch andere Schnittstellen vorhanden sein sollen.

Für den Teil der Bodenstation ist keine Schnittstelle vorgegeben. Diese kann frei gewählt werden. Es sollte nur auf eine möglichst weite Verbreitung der genutzten Schnittstellen geachtet werden, sodass das System vielseitig eingesetzt werden kann und nicht auf eine Plattform festgelegt ist.

Softwareschnittstellen

Das System soll eine möglichst einfache Softwareschnittstelle zur Verfügung stellen, sodass für das Übertragen von Daten aus der FCU heraus oder in sie hinein kein großer Aufwand getrieben werden muss.

Da bisher keine Telemetrie genutzt wurde, ist in der FCU noch keine Softwarekomponente vorhanden, auf die zurückgegriffen werden kann. Es muss daher ein eigenes Protokoll definiert werden.

Da das System transparent arbeiten soll (Anforderung 1) sollten sich die Schnittstelle in der Airborne- und der Bodenstation gleichen.

4.1.3 Protokoll

Für die Übertragung der Daten muss ein Protokoll ausgewählt werden. Dazu könnte auf eines der Protokolle, die in Kapitel 3.2 beschrieben wurden, zurückgegriffen werden oder ein eigenes System entwickelt werden.

Dabei ist zu beachten, dass für die Kommunikation mit der FCU ein anderes Protokoll verwendet werden kann als das, welches zum Übertragen der Daten innerhalb des Telemetriesystems genutzt wird. Hier könnten auch die jeweiligen Protokolle der eingesetzten Funkmodule genutzt werden. Auch in der Bodenstation könnte ein anderes Protokoll verwendet werden.

4.2 Systementwurf

Nachdem die Rahmenbedingungen und die Anforderungen an das Telemetriesystem dargestellt wurden, wird nun der Entwurf des Systems und die ausgewählten Komponenten Erläutert.

4.2.1 Funkmodule

Es wurden diverse Funkmodule zu den in Kapitel 3.1 Beschriebenen Standards betrachtet. Dabei war ein einschränkender Faktor die finanzielle Ausstattung des Projektes.

Amber Wireless

Da es bereits die zwei Module der Firma *Amber Wireless* im Projekt gab, stand ohne Bedingungen fest, dass diese auch genutzt werden sollen. Die Module arbeiten mit einem proprietären Standard im 868MHz-Band mit einer maximalen Sendeleistung von ca. 25mW. Als Schnittstelle steht UART zur Verfügung, entweder mit Pegeln nach RS232-Spezifikation oder mit TTL (3,3V). Die Betriebsspannung muss zwischen +4,0 und +10,0 VDC liegen.

Mobilfunk-Modul

Weiter in die Auswahl kamen Mobilfunkmodule der Firma uBlox, da diese die größte Frequenzabdeckung haben. Da eine Kommunikation über Mobilfunk jedoch keine direkte Kommunikation zwischen zwei Teilnehmern ist, sondern immer das Netz des Mobilfunkanbieters beteiligt ist, wurde entschieden vorläufig kein Mobilfunkmodul zu nutzen, beim Systementwurf aber darauf zu achten, dass ein Modul einfach hinzugefügt werden kann.

WLAN-Modul

Betrachtet wurden auch einige WLAN-Module für eingebettete Systeme, die mittels Serial Peripheral Interface (SPI) und/oder UART angesteuert werden können. Hier wurde ein Modul der Firma *Texas Instruments* aus der *CC3100*-Familie ausgewählt. Dieses unterstützt die Standards IEEE802.11b/g/n und wird mittels SPI und UART angesteuert. Das WLAN-Modul wurde jedoch nicht als Funkmodul im Laborprototyp installiert. Es wurde jedoch beim Entwurf noch berücksichtigt.

ZigBee-Modul

Im Bereich der ZigBee Module wurde ein Modul der Firma *Digi International* mit der Bezeichnung *XBee Pro 868* ausgewählt. Diese implementieren eine proprietären Abwandlung des ZigBee-Standards, bauen jedoch auch auf dem IEEE802.15.4 Standard auf. Der größte Unterschied zum ZigBee-Standard ist, dass die Module nur Point-to-Multipoint-Verbindungen unterstützen und kein richtiges Mesh-Netzwerk, bei dem die Daten über mehrere Knoten weiter gereicht werden. Die Module senden um eine Frequenz von 869.525 MHz. Die Sendeleistung kann bis zu 315mW betragen und es sollen Reichweiten von bis zu 40 km bei direkter Sichtverbindung möglich sein. Für die Nutzung in Gebäuden oder im urbanen Umfeld sollen noch 550m erreicht werden können. Die Datenrate soll 24kbp/s betragen. Wichtig ist bei diesen Modulen, dass sie einen 10%-DC einhalten. Dazu läuft bei jedem Sendevorgang ein interner Timer mit. Wenn dieser Timer 6 Minuten erreicht, wird für den Rest einer Stund keine Paket mehr versendet. Empfangen ist weiterhin möglich. Die *XBee*-Module werden per UART mit 3,3 Volt TTL angesteuert. Als Stromversorgung benötigen sie 3,0 bis 3,6 Volt Gleichspannung. Im Sendezustand wird ein maximaler Strom von 800mA benötigt. [XBEEPRO868]

4.2.2 Airbornestation

Nach Auswahl der Funkkomponenten steht fest, welche Hardwareschnittstellen die Airbornkomponente erfüllen muss:

UART mindestens 4 UART-Anschlüsse müssen vorhanden sein. (Für *AMB8350*, *XBee Pro 868*, FCU)

SPI mindestens 1 SPI-Anschluss muss vorhanden sein. (Für *CC3100*)

Darüber hinaus sollte die Komponente genügend Ressourcen haben, diese Schnittstellen gleichzeitig zu koordinieren und für Erweiterungen noch Platz bieten. Da für einige dieser Erweiterungen, z. B. ein Mobilfunkmodul, zwingend bestimmte Softwarestacks notwendig sind, sollte auf der Komponente ein Betriebssystem laufen können.

Zur Auswahl standen das *STM32f4-Discovery Board*[1] der Firma *STMicroelectronics*, wie es auch für die FCU eingesetzt wird. Der *Raspberry Pi B+*[2] sowie das *BeagleBone Black*[3].

Es wurde das *BeagleBone Black (BBB)* ausgewählt, da die anderen Boards zu wenig Anschlussmöglichkeiten boten. Das *BBB* ist ein etwa Kreditkarten großer Einplatinen-Computer mit einem *ARM Cortex-A8* Prozessor von *Texas Instruments* (AM335x-Serie). Es besitzt 4GB

[1] http://www.st.com/web/catalog/tools/FM116/SC959/SS1532/PF252419# [Abgerufen am 5.03.2015]
[2] http://www.raspberrypi.org/products/model-b-plus/[Abgerufen am 5.03.2015]
[3] http://beagleboard.org/BLACK[Abgerufen am 5.03.2015]

on-board-flash sowie 512MB DDR3 RAM. Im Prozessor sind zwei 32-bit Hard-Realtime-Units vorhanden, über die bestimmte Funktionen mit harten Echtzeitanforderungen gesteuert werden können.

Das *BBB* bietet u. a. 4 UART-Schnittstellen (+1 Debug-UART-Schnittstelle), eine SPI-Schnittstelle und bis zu 69 GPIO-Ports. Diese Anschlüsse sind über die sogenannten *Expansion Header* erreichbar.

Als Betriebssystem wurde *QNX Neutrino 6.5.0 SP1* gewählt. Hierfür gibt es von *Texas Instruments* und *QNX* ein sogenanntes *Board-Support-Package (BSP)* für das *BBB*, welches die komplette Hardware unterstützt. Hierdurch entfallen aufwändige Anpassungen des Betriebssystems an die Plattform. Darüber hinaus bietet *QNX* die Möglichkeiten eines Echtzeitbetriebssystems, was im Rahmen von Telemetrie nützlich ist.

4.2.3 Bodenstation

Für die Bodenstation wurde sich gegen den Einsatz eines zusätzlichen Boards entschieden. Hier sollen alle Komponenten direkt an den PC angeschlossen werden. Für die Module mit serieller Schnittstelle werden USB-UART-Adapter verwendet. Die Verbindung mit WLAN kann ebenfalls über USB hergestellt werden oder es wird per sich per Ethernet mit einem Router verbunden.

Als Betriebssystem wurde *Microsoft Windows 7* ausgewählt, da hier bereits die in [Hasberg, 2014] entwickelten Programme laufen.

4.2.4 Protokolle und Softwareschnittstellen

Bei den Protokollen wurde sich dafür entschieden für die Kommunikation mit anderen Komponenten (FCU, GCS) den in [Hasberg, 2014] definierten Software-Bus *AESLink* zu nutzen. Dies hat den Vorteil, dass die bereits auf diesem Bus aufsetzende Testinfrastruktur unterstützt wird. Programme wie *AESLink Replay* oder *AESLink Logger* können genutzt werden. Außerdem sind für die Plattform der FCU, dem *STM32f4* bereits Implementierungen von *AESLink* in C++ vorhanden. Darüber hinaus nutzt *AESLink* UDP-Multicast, sodass am Boden mehrere Geräte per Netzwerk zusammengeschlossen werden können und jedes Gerät andere Aufgaben im Rahmen der GCS übernehmen kann.

Dies entspricht grob der Architektur, wie sie *Paparazzi* in ihrem Telemetriesystem einsetzt.(vgl. Abbildung 3.5b)

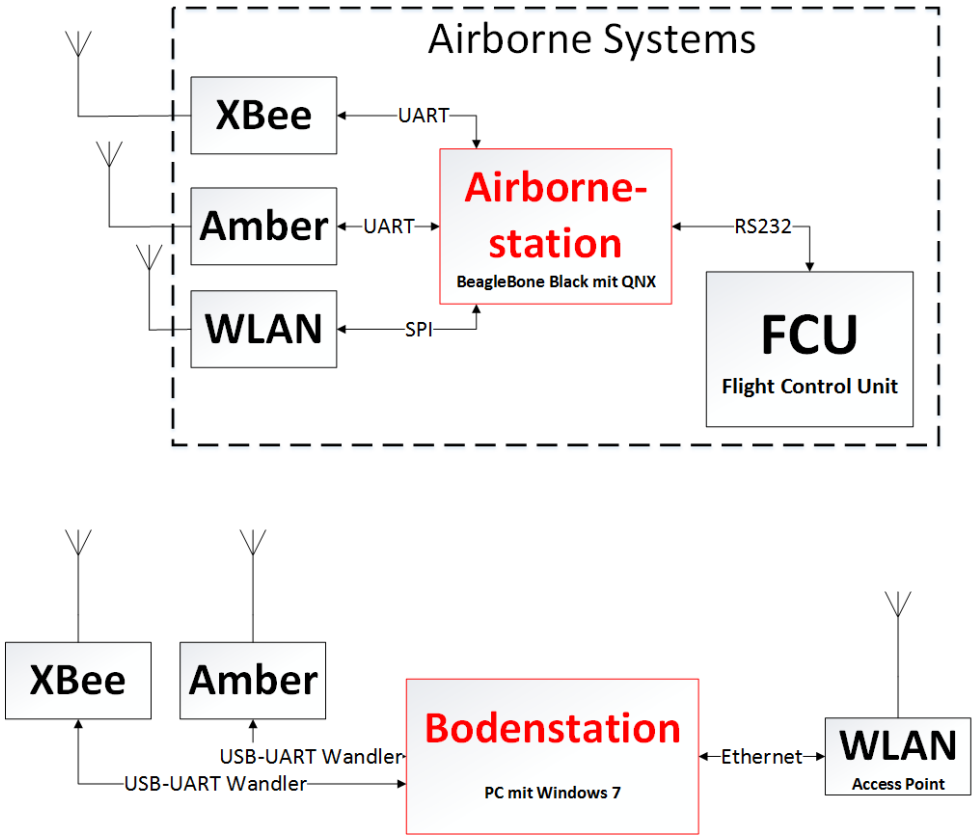


Abbildung 4.1: Systemteile des Telemetriesystems.
(rot: neu zu entwickeln; schwarz: bestehende Hard-/Software)

In späteren Entwicklungsstufen könnten auch andere Protokolle wir *MAVLink* unterstützt werden, um so etwa die *QGroundControll*-GCS zu nutzen. Zwischen FCU und Telemetriesystem könnte weiterhin *AESLink* gesprochen werden.

Da *AESLink* keinerlei Verfahren von Fehlererkennung, wie z. B. Prüfsummen beinhaltet, ist es als Protokoll für die Übertragung per Funk ungeeignet. Auch die Nutzung von 32 Bit großen Variablen für Startsequenz, Protokollnummer, Größe der Nachricht und Nachrichtentyp erzeugen einen Overhead, der bei begrenzter Datenrate im Funk vermieden werden muss.

Darum wird ein neues Verfahren für das Serialisieren genutzt. Das Protokoll wird in Anlehnung an *AESLink WiAESLink* genannt. Die Nachrichten in diesem Protokoll heißen *WiAESLinkMessage*.

Sie bestehen ähnlich wie die Frames in *UAVTalk* oder *MAVLink* aus einem 6 Byte langen Header, den zu übertragenden Daten und einer 16-Bit Checksumme. Die Daten werden dabei

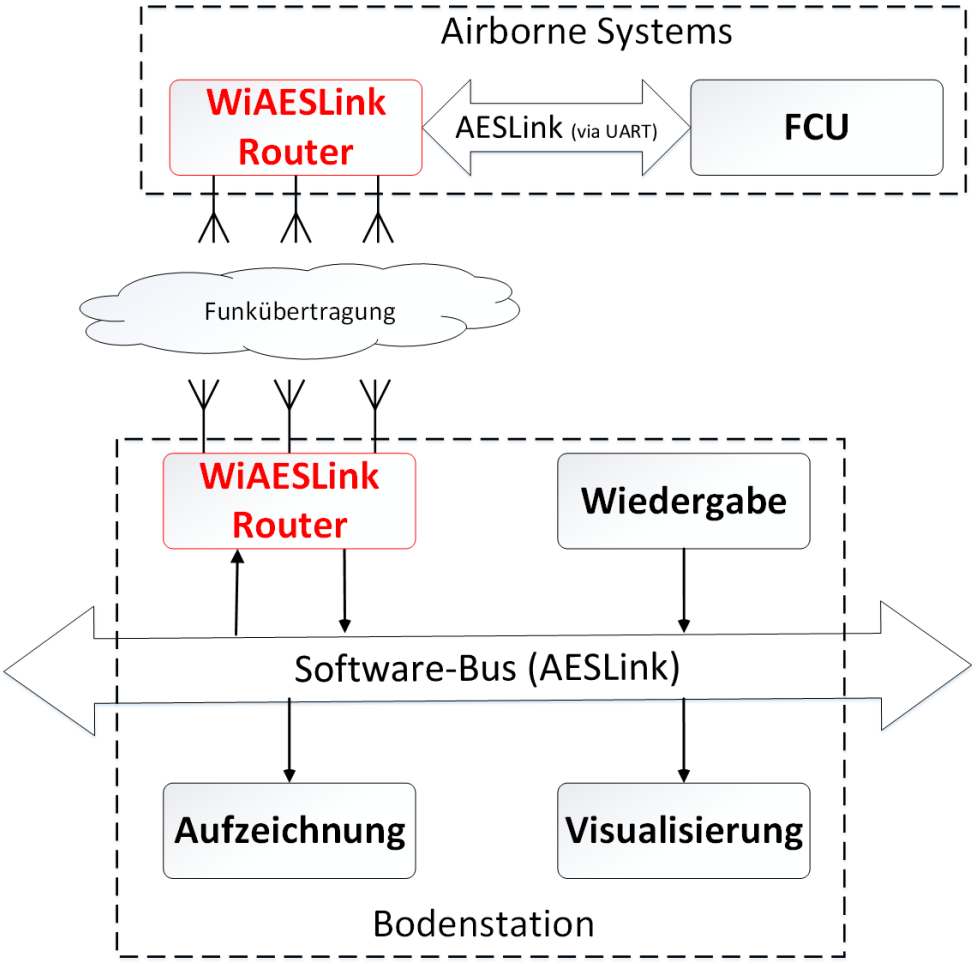


Abbildung 4.2: Systemarchitektur des Telemetriesystem. (rot: nue zu entwickeln ; schwarz: bestehende Hard-/Software)

in 32-Bit große Felder serialisiert. Von diesen können pro *WiAESLinkMessage* maximal 255 übertragen werden. Somit ist die maximale Größe der Payload 1020 Bytes. Dies wurde so gewählt, um in der Größe der Nachrichten flexibel zu sein, ohne unnötig Overhead zu erzeugen. Da die derzeit spezifizierten *AESLinkMessages* alle aus vielfachen von 32-Bit Datenfeldern bestehen, werden keine Bits im Payload der *WiAESLinkMessages* freigelassen. Es reicht für die Kennzeichnung der Länge der Payload jedoch ein 8-Bit-Feld. Würde man ein 16-Bit Feld nutzen, würde in den meisten Fällen das höherwertige Byte unbenutzt bleiben. Der Aufbau ist in Tabelle 4.1 dargestellt.

Innerhalb der *WiAESLinkRouter* genannten Komponenten, die für das Empfangen und Sen-

Tabelle 4.1: Aufbau der *WiAESLinkMessage*

Byte Index	**Name**	**Werte**	**Bedeutung**
0	mark	0xAA	Signalisiert Start einer Nachricht
1	len	0-255	gibt die Länge der Payload an
2	seq	0-255	Für jedes zum Versenden erstelltes Paket inkrementiert ein Router die Sequenz. So kann die Reihen folge der Pakete beim Empfänger eingehalten werden, oder der Verlust eines Pakets festgestellt werden.
3	sysID	0-255	ID des Nachrichtensenders. Sollte unique sein.
4	comID	0-255	ID der genutzten Sendekomponente (z. B. ZigBee)
5	msgID	0-255	Gibt an, was im Payload übertragen wurde, damit dies korrekt dekodiert werden kann
6 bis (n+6)	payload32		Daten der Nachricht in 32 Bit großen Feldern.
(n+7) bis (n+7)	checksum		Es wird CRC-16-CITT genutzt.

Hinweis: n hat den Wert $n = 4 \cdot len$ aufgrund der 32-Bit Größe der Payload

den von Nachrichten über Funk sowie das Weiterleiten und Entgegennehmen über *AESLink* verantwortlich sind, müssen mindestens folgende Komponenten realisiert werden:

- **Eingangspuffer** für eingehende Bitströme
- **Parser** zum erkennen von Nachrichten in einem Bitstrom.
- **(De-)Serialisierung** der Daten zum Versenden über Funk.
- **Routing-Algorithmen** zum Verteilen der Pakete auf die unterschiedlichen Funkdevices.
- **Ansteuerung der Funkdevices**
- ***AESLink*-Anbindung**

5 Realisierung

Die Programmierung der Komponenten erfolgte in C++, um möglichst viele Teile des Sourcecodes sowohl auf dem BeagleBone Black (BBB) als auch unter Windows nutzen zu können.

5.1 Platform unabhängige Komponenten

5.1.1 Interfaces

Es wurden drei Interfaces definiert, die plattformunabhängig Schnittstellen zu den Funkdevices und anderen Geräten herstellen, deren Implementierung jedoch stark plattformabhängig ist:

IRadioDevice RadioDevices sind alle Funkmodule. Jede (platformabhängige) Implementierung eines Funkdevices muss von diesem Interface abgeleitet werden. Es stellt die Schnittstellen zum Empfangen und Versenden von Nachrichten über ein Funkdevice dar.

IAESLinkIO Dieses Interface stellt die Schnittstellen zum AESLink dar.

ILogFile Stellt eine Schnittstelle für das Erstellen von Logfiles dar.

5.1.2 Hal

Die Verwaltung der einzelnen Ein- und Ausgabe-Devices (Funk und *AESLink*) übernimmt die **Hal**. Diese ist ebenfalls plattformunabhängig implementiert. In ihr werden beim Starten des Programms die Devices registriert. Die Hal verwaltet die Devices dazu in einer Liste. Jede Komponente, die Zugriff auf eines dieser Devices benötigt, kann über die Hal so auf diese zugreifen. Die Hal ist dabei nach dem Singletonpattern nach [Alexandrescu, 2001] implementiert. Die Verwaltung der Devices ermöglicht ein einfaches Erweitern der genutzten Devices.

5.1.3 Routing

Für das Routing ist der **WiAESLRouter** zuständig. Dieser ist ebenfalls plattformunabhängig und nach dem Singletonpattern implementiert. Als Routing-Verfahren zum Versenden von Nachrichten ist zur Zeit ein einfaches Round-Robin-Verfahren implementiert, welches abwechselnd neue zu verschickende Nachrichten an die Devices sendet. Allerdings wird beim Verteilen der Nachrichten auch auf den Füllzustand der Sendewarteschlange eines Devices geachtet, sodass bei unterschiedlich schnellen Verbindungen sich am langsameren Device kein Stau bildet.

Neben dem Versenden ist der Router auch für das Puffern der empfangenen Nachrichten verantwortlich. Da mehrere Routen genutzt werden, um die Daten zu übertragen, kann es passieren dass Pakete nicht in der richtigen Reihenfolge ankommen oder Pakete ganz verloren gehen. Damit die an die FCU oder GCS ausgegebenen Nachrichten der realen zeitliche Abfolge ihres Entstehens im aussendenden System entsprechen, werden ankommende Nachrichten nur ausgegeben, wenn ihre Sequenz-Nummer die nächste erwartete Sequenznummer ist. Andernfalls wird die Nachricht gespeichert und auf die korrekte Nachricht gewartet. Trifft diese nach einer bestimmten Zeit nicht ein, gilt diese als verloren und die nächste Nachricht wird ausgegeben. Der implementierte Ablauf dieses Verfahrens ist in Abbildung 5.1 dargestellt.

5.1.4 RadioDevices

Einige Eigenschaften der RadioDevices sind auf beiden Plattformen sehr ähnlich bis gleich implementiert. Lediglich bei der Implementierung der direkten hardwareabhängigen Verfahren gibt es Unterschiede. Diese sind in den Abschnitten 5.2 und 5.3 beschrieben.

Gemeinsam haben die Radiodevices, dass sie einen Empfangs-Buffer haben, indem sie alle empfangenen Bytes speichern. Außerdem gibt es einen Sende-Buffer, indem zu verschickende Nachrichten vom Router abgelegt werden.

Der Empfangs-Buffer ist als Ring-Buffer realisiert. Dieser arbeitet dabei mit Monitoren, um einen überschreibenden Zugriff zu verhindern. Ist der Buffer voll, so werden keine weiteren Daten hineingeschrieben. Der Buffer hat eine Größe von 2048 Byte, sodass fast zwei maximal große Nachrichten gepuffert werden könnten.

Der Sende-Buffer ist ebenfalls als Ring-Buffer realisiert, speichert jedoch keine Bytes sondern mit Hilfe von Smart-Pointern Verweise auf die zu sendenden Nachrichten. Generell werden Nachrichten innerhalb eines Knotens als Referenzen weitergereicht, damit kein ständiges Kopieren der ganzen Nachricht das System bremst. Die Speicherverwaltung der Nachrichten wird dabei insgesamt über Smart-Pointer geregelt. Konkret werden die `std::auto_ptr`

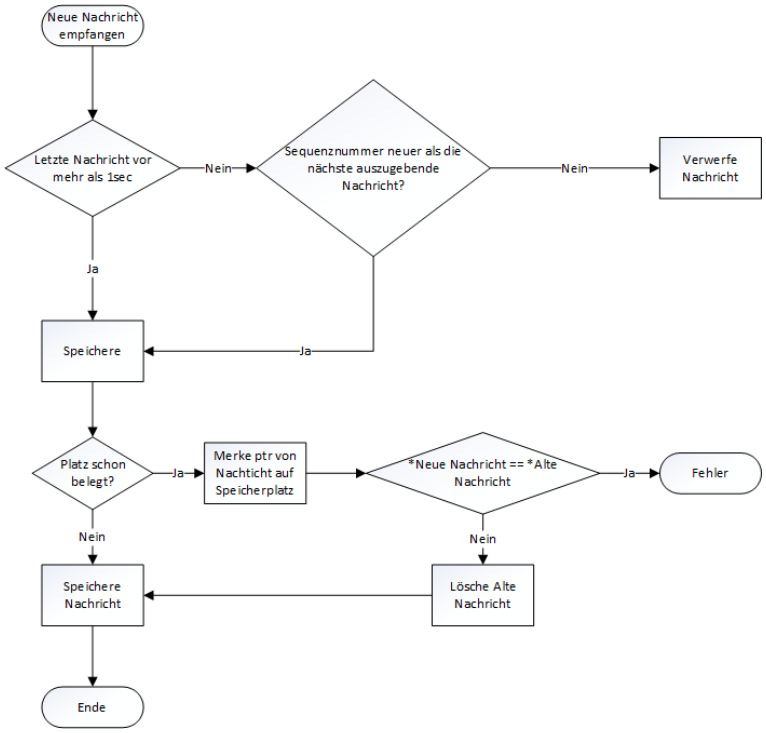


Abbildung 5.1: Verfahren bei eintreffenden Nachrichten zur Einhaltung einer zeitlich korrekten Abfolge

verwendet, da diese sowohl unter vom Windows C++-Compiler als auch vom QNX-Compiler unterstützt werden.

Der Sende-Buffer umfasst nur Platz für wenige Nachrichten, da ein zu langes Zwischenspeichern keinen Mehrwert bietet, sondern eher im Gegenteil ein Problem darstellt, wenn die Daten mit Verzögerung von mehreren Sekunden oder gar Minuten eintreffen, befindet sich das Flugzeug bereits in einem anderen Kontext.

In den Radiodevices sind je ein Receiver und ein Transmitter implementiert. Der Receiver ist für die Entgegennahmen des eintreffenden Bitstrom verantwortlich und leitet diesen in den Empfangs-Buffer weiter und meldet, dass neue Daten eingetroffen sind.

Der Transmitter wird immer aktiv, wenn neue Nachrichten im Sende-Buffer sind. Diese werden vom Transmitter fürs Versenden in ein Byte-Buffer serialisiert und versendet.

5.1.5 Traffic-Shaping

Aus zwei Gründen wurde Traffic-Shaping implementiert.

Zum ersten sind die Sendepuffer in den beiden Funkmodule, *Amber Wireless* und *XBee*, nur etwa 200 Byte groß. Das Beaglebone unterstützt jedoch in der aktuell genutzten Konfiguration kein Hardware-Handshake, sodass ein Überlauf dieses Puffers anders verhindert werden muss.

Zum anderen gilt bei den Modulen im 868MHz Band nur ein begrenzter Duty Cycle (DC) für das Senden. Dies erfordert es den Datenstrom zeitlich aufzuteilen, sodass der Duty-Cycle nicht überschritten wird.

Als Verfahren für das Traffic-Shaping wurde der Token-Bucket Algoritmus [vgl. Tanenbaum, 2011] gewählt. Bei diesem Verfahren gibt es einen sogenannten „Eimer“ mit einer begrenzten Kapazität, in den kontinuierlich eine bestimmte Anzahl an Token „fließt“. Sollen nun Daten verschickt werden, benötigt jedes Byte einen Token. Sind nicht genügen Token vorhanden, muss gewartet werden oder das Paket wird verworfen.

Da es zwei unterschiedliche Limitierungen gibt, werden auch zwei Token-Buckets genutzt. Einer begrenzt die maximale Burst-Größe so, dass der Puffer im Funkmodul nicht überläuft. Der andere sorgt für die Einhaltung des maximalen DC. Der Burst-Bucket ist daher sehr klein und besitzt eine hohe Tokenrate. Der DC-Bucket hingegen hat eine große Kapazität mit kleiner Tokenrate.

Vor dem Senden muss der Transmitter zunächst genug Token aus dem DC-Bucket entnehmen, bevor jedes Bit gesendet wird, das einen Token aus dem Burst-Bucket erhält. Hier kann nicht auf die Anzahl von genügend Tokens gewartet werden, da die Pakete zum Teil die Kapazität des Burst-Bucket überschreiten.

5.1.6 Parser

Der Parser wird indirekt durch den Receiver aktiviert. Sobald neue Daten im Ring-Buffer liegen, sucht der Parser in diesen Daten nach einer Nachricht. Alle Bytes, die nicht zu einer Nachricht gehören werden verworfen, sodass für neu ankommende Daten Platz ist.

Bei der Suche nach den Nachrichten prüft der Parser erst, ob mindestens so viele Bytes im Buffer sind, wie die kürzeste Nachricht lang ist. Ist dies der Fall sucht er nach dem ersten Vorkommen der Startmarkierung einer Nachricht (0xAA). Alle Bytes, die dem nicht entsprechen, werden verworfen.

Ist ein möglicher Nachrichtenbeginn gefunden worden, wird diese Position im Buffer gespeichert. Ab jetzt werden keine Bytes mehr verworfen. Das folgende Byte stellt die Größe der

Nachricht dar. Sind genug Bytes im Buffer, wird über alle Bytes der Nachricht (außer der Startmarke) die Checksumme gebildet. Ist diese 0, so wurde die Nachricht gefunden. Aus den Bytes wird ein *WiAESLinkMessage*-Objekt erzeugt und der Bereich im Buffer verworfen.

Waren nicht genug Bytes im Buffer, wird nach dem nächsten Vorkommen der Startmarke gesucht. So wird verhindert, dass bei fälschlich ermittelten Startmarken und einem sehr großen folgenden Wert für die Nachrichtenlänge gewartet werden muss, bis genug Bytes empfangen wurden.

Wird jetzt keine neue Nachricht ermittelt, gilt die gespeicherte Position als Anfang für den nächsten Suchdurchlauf. Dieser wird erst gestartet, wenn weitere Bytes empfangen wurden. Sollte eine neue Nachricht gefunden werden, werden alle Bytes vor dieser Nachricht verworfen.

Der Parser ist nach dem Factory Method Pattern [Alexandrescu, 2001] implementiert. Denn die Aktion die nach Auffinden einer Nachricht ausgeführt wird, ist von der Plattform abhängig.

5.2 Airborne Komponente

Für die Aiborne Komponente wurde ein eigenes QNX mittels des Board Suport Package erstellt. Zuvor mussten die Einstellungen der Datei `init_pinmux.c`[1] in dem Package angepasst werden, sodass alle benötigten Ports über die Expansion Headers nach außen geführt werden.

Dann mussten im Startup-Script[2], die seriellen Schnittstellentreiber für die UARTs konfiguriert werden. Wichtig ist hierbei, dass alle Schnittstellen im „raw“-Mode betrieben werden müssen, da sie sonst automatisch jedes ankommende Zeichen als Echo aussenden. Außerdem kann hier nicht benötigte Hardware deaktiviert werden.

Nachdem dies konfiguriert ist, kann das BSP kompiliert werden. Das erzeugte Image wird auf eine microSD-Karte geladen.

Da die Schnittstellen beim BeagleBone Black fest konfiguriert sind, muss im Programm keine dynamische Konfiguration vorgenommen werden. Alle Parameter können direkt in den Programmcode geschrieben werden.

Das Router-Programm basiert auf diversen Threads. Jeder Receiver und Transmitter läuft in seinem eigenen Thread. Zur Umsetzung der Threads wurde auf die *HAWThread*-Bibliothek von Prof. Dr. Stephan Pareigis aus dem WP „Effiziente Datenstrukturen in C++ für verteilte Echtzeitprogrammierung“ zurückgegriffen. Neben den Transmittern und Receivern gibt es noch

[1] Die Datei liegt im Unterverzeichnis /src/startup/boards/beaglebone/ der BSP-src
[2] `BeagleBoneBlack.bsh` im Hauptverzeichnis des BSP

einen Dispatcher-Thread, der sich um die Auswertung der von den Prozessen verschickten QNX-Messages kümmert und entsprechende Funktionen aufruft.

5.3 Bodenkomponente

Bei der Bodenkomponente wurde das *Qt*-Bibliothek in der Version 5.4 verwendet. Dies wurde insbesondere zur einfacheren Realisierung der seriellen Schnittstelle genutzt. Darüber hinaus wird in der Bodenkomponente das in [Hasberg, 2014] entwickelte *AESLinkNetwork*-Modul zurück gegriffen. Dieses ist mittels eines eigenen Threads für die Kommunikation mit dem *AESLink*-Netwerk verantwortlich.

In dieser Komponente wurden keine weiteren Threads verwendet, sondern die Qt-Eventloop und Signals und Slots der Qt-Bibliothek. Dies hat zur Folge, dass z. B. die Transmitter und die Receiver nicht Blockieren dürfen, da sonst das gesamte Programm blockiert. Um dies zu Umgehen, wurde das Senden des Transmitters als Statemachine umgesetzt, sodass das Senden verlassen werden kann und beim nächsten Durchlauf an der vorherigen Stelle fortgefahren werden kann.

Da die per USB an den PC angeschlossenen Funkmodule nicht jedes mal dem gleichen COM-Port zugeordnet werden, gibt es die Möglichkeit die Module vom Programm selber suchen zu lassen. Hierzu werden an jedem COM-Port die möglichen Parameter der seriellen Schnittstelle probiert und per AT-Befehlen die ID der Module abgefragt. Erhält das Programm eine erwartete Antwort, so wird die genutzte Konfiguration für das gefundene Modul gespeichert und nach der Initialisierungsphase wird das Modul mit den Einstellungen aktiviert und in der Hal registriert.

5.4 Protokolle

5.4.1 AESLink zu WiAESLink

WiAESLink wurde entworfen, um mit möglichst wenig Overhead Daten zu übertragen. Bei *AESLink* spielte dies noch keine Rolle. Um diesen Overhead beim Senden über Funk abzustellen, gibt es ein spezielles Umsetzungsverfahren von einem Protokoll in das andere.

So wird die `MagicNumber` von *AESLink* nicht mit übertragen. Da es sich bei der Payload um eine *AESLinkMessage* handelt, wird durch die MessageID angezeigt. Ist hier das erste Bit gesetzt, so handelt es sich um eine *AESLinkMessage*. Der `MessageType` von *AESLink* wird dabei direkt in die MessageID mit übernommen. Dies bedeutet, dass die `MessagType` nicht größer als 127 werden darf.

Die Länge der *AESLinkMessage* fließt direkt in die Länge der *WiAESLinkMessage* mit ein. Zusätzlich wird dieser Wert zusammen mit der Protokollversion von *AESLink* in den ersten 32 Bit der Payload gespeichert. Das niederwertigste Byte wir dabei für die Protokollversion genutzt. Diese kann folglich bis 255 hochgezählt werden. Die Protokollversion wird mit verschickt, da so das Telemetrie System unabhängiger von dem *AESLink*-Versionen ist. Solange sich am Aufbau der Nachrichten nichts ändert, können alle Versionen vom Telemetriesystem übertragen werden. Da somit die ersten 32 Bit der Payload genutzt werden und die Protokollversion keine 32 Bit breit ist, kann die originale Länge der *AESLinkMessage* in Byte mitübertragen werden. Dadurch kann am anderen Ende der Übertragung die Nachricht komplett rekonstruiert werden, auch wenn die Daten der *AESLinkMessage* nicht mehr mit einem 4-Byte-Alignment übertragen werden.

5.4.2 AESLink interne Nachrichten

In der Umsetzung sind theoretisch 127 Nachrichten möglich, die zu systeminternen Zwecken wie Konfiguration oder Systemmonitoring eingesetzt werden können. Dazu werden diese Nachrichten, zu erkennen an der 0 im höchsten Bit der MessageID, intern ausgewertet und verarbeitet.

6 Ergebnisse

Insgesamt ist festzuhalten, dass das System noch nicht in einem fertigen Zustand ist. Es wurden bereits einige funktionale Tests durchgeführt, bei denen zum Teil jedoch noch Schwächen in der Umsetzung des Konzepts erkannt wurden. Daher sind bisher erst wenig verwertbare Tests erfolgt.

6.1 Funktionale Verifikation

6.1.1 Fault Injection

Zum Testen der Funktionen der Receiver, dem Ringbuffer und dem Parser wurden verschiedene Fault Injection Tests durchgeführt. Dazu wurden künstlich Byte-Ströme erzeugt, in denen Nachrichten unterschiedlicher Länge enthalten waren. Zusätzlich wurden falsche Nachrichtenanfänge in den Strom eingefügt, sodass geprüft werden konnte ob der Parser blockiert oder die falschen Anfänge korrekt als solche identifiziert.

Das folgende Beispiel zeigt ein paar dieser Testdaten:

```
//Anlegen von Arrays in der Größe einer Nachricht
uint8_t msg[1028];
uint8_t msg2[1028];
uint8_t msg3[1028];

//Anlegen einer korrekten Message
msg[0] = 0xAA; //mark
msg[1] = 255;  //lenght
msg[2] = 0;    //seq
msg[3] = 0;    //sysID
msg[4] = 1;    //comID
msg[5] = 8;    //msgIG

//Befüllen der Payload
```

```
for (int ii = 6; ii < 1026; ii+=4)
{
    msg[ii] = ii-6;
}
//Berechnen der Prüfsumme
uint16_t crc = crc_calculate(msg, 1026);
msg[1026] = (uint8_t)(crc & 0xFF);
msg[1027] = (uint8_t)(crc >> 8);

//Anlegen eienr kaputten Nachricht
 msg2[0] = 0xAA; //mark
 msg2[1] = 255;  //lenght
 msg2[2] = 0;    //seq
 msg2[3] = 0;    //sysID
 msg2[4] = 1;    //comID
 msg2[5] = 8;    //msgIG
 //Befüllen der Payload
 for (int ii = 6; ii < 1026; ii+=4)
 {
     msg2[ii] = ii-6;
 }
 //Keiene Berechnung der Prüfsumme
msg2[1026] = 0;
msg2[1027] = 0;


//Anlegen einer Nachricht, der ein kaputter Header voraus geht
//Pseudeo Nachricht
msg3[0] = 0xAA; //mark
msg3[1] = 255;  //lenght
msg3[2] = 0;    //seq
msg3[3] = 0;    //sysID
msg3[4] = 1;    //comID
msg3[5] = 8;    //msgIG
for (int ii = 6; ii < 40; ii+=4)
{
    msg3[ii] = ii-6;
}

//Korrekte Nachricht
```

```
msg3[40] = 0xAA; //mark
msg3[41] = 2;  //lenght
msg3[42] = 0;    //seq
msg3[43] = 0;    //sysID
msg3[44] = 1;    //comID
msg3[45] = 8;    //msgIG

//Befüllen der Payload
for (int ii = 46; ii < 54; ii+=4)
{
    msg3[ii] = ii-46;
}
//Berechnen der Prüfsumme
uint16_t crc = crc_calculate(&msg[40], 16);
msg3[54] = (uint8_t)(crc & 0xFF);
msg3[55] = (uint8_t)(crc >> 8);
```

Die so generierten Testfälle wurden an die Receiver übergeben, die diese in ihre Buffer schrieben und den Parser aktivierten. Alle generierten Test wurden erfolgreich durchlaufen. Zusätzlich wurden mittels eines Zufallszahlengenerators zufällige Ströme erzeugt und die Leistungsfähigkeit der Parser bei vielen zufälligen Daten überprüft. Es wurde keine Nachricht in den Zufallszahlen gefunden, was erwartet wurde.

6.1.2 Übermittlung von AESLink-Nachrichten

Zum Testen der Übermittlung von AESLink Nachrichten, und somit des ganzen Systems wurden in die Airborne Komponente mittels USB-to-UART-Adapter von einem Laptop aufgezeichnete AESLink-Nachrichten eingespielt. Die Beiden Knoten befanden sich dabei etwa im Abstand von etwa 2m auf einem Tisch im Labor. Diese wurden auf der Bodenseite empfangen und als AESLink-Nachrichten ins Netzwerk eingespielt, wo sie wiederum mit einem Logger gespeichert wurden. Dabei konnte festgestellt werden, dass sich der Paketverlust bei einer Senderate von 10 Nachrichten pro Sekunde bei etwa 10% bewegt. Dieser Wert wurde ohne das beachten der zeitlichen Reihenfolge der Nachrichten ermittelt. An diesem Verfahren muss noch gearbeitet werden, sodass dieser Wert nicht als endgültiger Wert angesehen werden kann.

Wurde jeweils nur ein Modul benutzt und die Last nicht auf beide Module gleichmäßig verteilt, so wurden bei 10 Nachrichten pro Sekunde zum Teil mehr als die Hälfte der Pakete verloren.

6.2 Reichweiten

Es wurde mit dem XBee Modul ein einfacher Reichweitentest durchgeführt. Dazu sendete das XBee Modul alle 10 Sekunden ein 40Byte große Nachricht zur Gegenseite, die die Nachricht direkt zurücksenden sollte. Ein Modul befand sich dabei im Arbeitsraum (Raum 0784) im 7.Stock des Hochhauses Berliner Tor 7. Das andere Modul wurde an einem Laptop betrieben. Dieses Modul wurde bis zu U-Bahnstation Lübeckerstraße bewegt. Dabei war festzustellen, das bei direktem Sichtkontakt zum Gebäude Berliner Tor 7 noch eine Verbindung bestand, obwohl der Arbeitsraum auf der anderen Gebäudeseite liegt. Sobald jedoch ein zweites Gebäude in die Sichtachse kam, war keine Verbindung mehr möglich. Abbildung 6.1 zeigt die maximal gemessene Strecke, bei der noch Funkkontakt bestand.

Abbildung 6.1: Getestete Reichweite des XBee Moduls. Maximal erreicht wurden 470m auf der markierten Strecke.

6.3 Energieverbrauch

Um den Energieverbrauch des Systems (Airborne Komponenten) zu bestimmen wurde diese mittels des USB-to-UART-Adapter an einem Laptop angeschlossen und mittels *AESLink*

Replay mit 50 *AESLink*-Nachrichten pro Sekunde belastet. Auf der Bodenseite wurde das Autopilot-Programm aus[Hasberg, 2014] gestartet, sodass von dort Nachrichten zurück gesendet wurden. Die Stromversorgung des BBB wurde für diesen Test über ein Amperemeter hergestellt. Im nicht sendendem Betrieb wurden vom BBB 0,495A bei 5V verbraucht. Unter Vollast wurden maximal 1,126A bei 5V verbraucht.

7 Ausblick

Diese Arbeit hat einen lauffähigen Laborprotoypen für ein Telemetriesystem mit mehreren Funkmodulen hervorgebracht. Es handelt sich jedoch nur um einen Laborprototypen, der noch kein fertiges Telemetriesystem darstellt. Die entwickelte Software existiert derzeit noch nur als Test-Version, die zumindest auf der BBB-Seite immer noch ein IDE-erfordert. Dies wird in naher Zukunft noch geändert, sodass ein System zur Verfügung steht, welches ohne IDE-Anschluss lauffähig ist, um insbesondere Effekte die durch Bewegung des Systems entstehen besser untersuchen zu können.

Direkte Anknüpfungspunkte an diese Arbeit sind u. a.:

Integration in die FCU Diese Arbeit hat zwar ein Telemetrie-Modul für die FCU entwickelt, jedoch keine Software für die FCU geschrieben. So wäre eine Integration des Senden und Empfangens von AESLinkMessages in die Software der FCU notwendig. Dabei sollte darauf geachtet werden, dass das Telemetriesystem nicht unnötig mit Nachrichten bombardiert wird. Aktuell werden alle ankommenden Pakete einfach verworfen, wenn das System keine freien Slots zum Senden mehr hat.

Verbesserung der Routingalgorithmen Die in dieser Arbeit eingesetzten Routingalgorithmen sind sehr primitiv und können noch stark verbessert werden. Insbesondere das zeitliche sortieren von empfangenen Paketen sollte dringend verbessert werden, um hier bessere Ergebnisse zu erzielen. Auch wäre ein Routing, welches mehr Informationen über die genutzten Routen (z. B. Datendurchsatz und Delays) in seine Entscheidungen einbezieht effektiver.

Weitere Funkstandards Zur Zeit werden zwei Module genutzt, die beide im 868MHz-Band arbeiten. Insbesondere Techniken aus dem 2,4GHz-Band, wie z.B. WLAN wären interessant zu betrachten und könnten zumindest bei geringen Entfernungen deutlich höhere Datenraten ermöglichen. Auch eine Integration eines Mobilfunkmodul bietet einen guten Anknüpfungspunkt. Denn durch die hohe Reichweite, durch das Mobilfunknetz, wäre eine Telemetrie auch dann möglich, wenn man sich nicht in der Nähe des Flugzeugs aufhält. Dies ist insbesondere im Hinblick auf autonome Missionen interessant.

Ground Control Station Die weitere Integration bestehender oder neuer Systeme hin zu einer kompletten Ground Control Station ist ein weiterer Punkt. Hier gäbe es Möglichkei-

ten neue Darstellungsformen des Flugzeugzustand für einen Piloten zu entwickeln. Aber auch die Missionsplanung von einer GCS aus könnte in das System integriert werden.

8 Fazit

Die Entwicklung des Telemetriesystems für das AES-Projekt stellte sich mit dem Verlauf der Arbeit als komplexer heraus als zunächst erwartet. Insbesondere das gleichzeitige nutzen von mehr als einem Übertragungskanal beinhaltet viele nicht triviale Probleme, insbesondere wenn man das eingesetzte Protokoll möglichst simpel halten möchte und Overhaed, z. B. durch das mit Senden von Timestamps in jeder Nachricht vermeiden möchte.

Auch war das Entwickeln für zwei unterschiedliche Plattformen - Windows und QNX - zeitgleich eine Herausforderung, da es immer wieder Momente gab, in denen ein auf einem System entwickeltes Konzepte, so auf dem anderen System nicht umgesetzt werden konnte. So fiel die Entscheidung die Qt-Bibliothek zu nutzen erst relativ spät. Doch die Idee möglichst viel des Entwickelten Source Codes auf beiden Systemen einsetzen zu können machten dies aus meiner Sicht notwendig. Wäre diese Entscheidung früher gefallen, hätte die Entwicklung beider Systeme mit Hilfe von Qt erfolgen können, da Qt auch QNX unterstützt.

Mit dem erreichten System bin ich noch nicht zufrieden. Es gibt noch einige Punkte, die sich erst in der letzten Phase der Arbeit als Problem herausstellten und daher nur sehr oberflächlich betrachtet werden konnten.

Insgesamt denke ich jedoch einen positiven Beitrag zum Vorankommen des AES-Projekts geleistet zu haben. So gibt es mit dieser Arbeit ein Übersicht über einsetzbare Funktechnologien und die rechtliche Lage in Deutschland. Außerdem glaube ich mit dem Konzept, des transparenten Telemetriesystem einen guten Ansatz zu haben und gehe davon aus, dass ich in der nahen Zukunft noch die Arbeiten abschließen kann, sodass das System zur Weiterentwicklung eingesetzt werden kann.

Literaturverzeichnis

[Alexandrescu 2001] ALEXANDRESCU, Andrei: *Modern C++ Design: Generic Programming and Design Patterns Applied*. Boston, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 2001. – ISBN 0-201-70431-5

[Bailey 2003] BAILEY, David: 1 - Radio technology. In: BAILEY, David (Hrsg.): *Practical Radio Engineering and Telemetry for Industry*. Oxford : Newnes, 2003, S. 1 – 103. – URL http://www.sciencedirect.com/science/article/pii/B9780750658034500147. – ISBN 978-0-7506-5803-4

[Büscher 2014] BÜSCHER, René: *Ein Safety-Konzept für Airborne Embedded Systems*, Hochschule für Angewandte Wissenschaften Hamburg, Bachelorthesis, 2014. – URL http://edoc.sub.uni-hamburg.de/haw/volltexte/2014/2628/

[Carden u. a. 2002] CARDEN, Frank ; JEDLICKA, Russell P. ; HENRY, Robert: *Telemetry systems engineering*. Artech House, 2002

[CCNF 2012] ZINGEL, Prof. Dr.-Ing. H. (Hrsg.) ; NETZEL, Prof. Dr.-Ing. T. (Hrsg.): *Competenz Cluster Neues Fliegen 2012 (CCNF)*. 2012. – URL http://www.haw-hamburg.de/fileadmin/user_upload/FakTI/Dokumente/Forschung_neues_Fliegen_CCNF.pdf

[ECA-Table 2014] ELECTRONIC COMMUNICATIONS COMMITTEE (ECC) WITHIN THE EUROPEAN CONFERENCE OF POSTAL AND TELECOMMUNICATIONS ADMINISTRATIONS (CEPT) (Hrsg.): *THE EUROPEAN TABLE OF FREQUECY ALLOCATIONS AND APLICATIONS IN THE FREQUENCY RANGE 8.3 kHz to 3000 GHz (ECA TABLE)*. 2014. – URL http://www.efis.dk/reports/ReportDownloader?reportid=1

[Engel 2014] ENGEL, Tobias: SS7: Locate. Track. Manipulate. In: *31st Chaos communication congress*, URL http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf, 2014

[Frequenzplan 2014] BUNDESNETZAGENTUR FÜR ELEKTRIZITÄT, GAS, TELEKOMMUNIKATION, POST UND EISENBAHNEN (Hrsg.): *FREQUENZPLAN - gemäß 54 TKG über die Aufteilung des Frequenzbereichs von 9 kHz bis 275 GHz auf die Frequenznutzungen sowie über die Festlegungen für diese Frequenznutzungen*. 2014. – URL https://www.bundesnetzagentur.

de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Frequenznutzungsplan.pdf;jsessionid=80FE0A46240DABD63AAE6D6543AB2FCC?__blob=publicationFile&v=4

[Gustrau 2013] GUSTRAU, Frank: *Hochfrequenztechnik: Grundlagen der mobilen Kommunikationstechnik*. 2., überarbeitete und erweiterte Auflage. Carl Hanser Verlag GmbH & Co. KG, 2013. – URL http://www.hanser-elibrary.com/doi/book/10.3139/9783446433991. – ISBN 978-3-446-43399-1

[Halliday u. a. 2005] HALLIDAY, David ; RESNICK, Robert ; WALKER, Jearl ; KOCH, Prof. Dr. Stephan W. (Hrsg.): *Physik*. 1., korrigierter Nachdruck. Wiley-VCH, 2005. – ISBN 978-3-527-40366-0

[Hasberg 2014] HASBERG, Hagen: *Ein Testkonzept für Flugregler*, Hochschule für Angewandte Wissenschaften Hamburg, Bachelorthesis, 2014. – URL http://edoc.sub.uni-hamburg.de/haw/volltexte/2014/2614/

[Hattenberger u. a. 2014] HATTENBERGER, G. ; BRONZ, M. ; GORRAZ, M.: Using the Paparazzi UAV System for Scientific Research. In: *IMAV 2014: International Micro Air Vehicle Conference and Competition 2014*, Delft University of Technology, 2014. – URL http://dx.doi.org/10.4233/uuid:b38fbdb7-e6bd-440d-93be-f7dd1457be60

[IEEE802.15.4 2011] THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*. IEEE Std 802.15.4-2011, 2011

[Kark 2014] KARK, K.W.: *Antennen und Strahlungsfelder: Elektromagnetische Wellen auf Leitungen, im Freiraum und ihre Abstrahlung*. 5., überarb. und erw. Aufl. Springer Fachmedien Wiesbaden, 2014 (Studium Technik). – ISBN 9783658036157

[MAVLink] QGROUNDCONTROL PROJEKT: *MAVLink Micro Air Vehicle Communication Protocol - QGroundControl GCS*. – URL http://qgroundcontrol.org/mavlink/start. – Zugriffsdatum: 17.03.2015

[Nohl und Paget 2009] NOHL, Karsten ; PAGET, Chris: Gsm: Srsly. In: *26C3 in Berlin*, URL http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf, 2009, S. 21–49

[Richter 2013] RICHTER, Arne M.: *Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs*. 2013. – URL http://edoc.sub.uni-hamburg.de/haw/volltexte/2013/2179/

[Rohrer 2014] ROHRER, Alexander: *Softwarearchitektur für Airborne Embedded Systems*, Hochschule für Angewandte Wissenschaften Hamburg, Bachelorthesis, 2014

[Sauter 2013] SAUTER, Martin: *Grundkurs mobile Kommunikationssysteme : UMTS, HSPA und LTE, GSM, GPRS, Wireless LAN und Bluetooth*. 5. überarb. und erw. Aufl. Springer Vieweg, 2013. – ISBN 978-3-658-01460-5

[Tanenbaum 2011] TANENBAUM, Andrew S. ; WETHERALL, David: *Computer Networks*. 5. ed., internat. ed. Pearson, 2011. – ISBN 978-0-13-255317-9

[Tews und Beck 2009] TEWS, Erik ; BECK, Martin: Practical attacks against WEP and WPA. In: *Proceedings of the second ACM conference on Wireless network security* ACM (Veranst.), URL http://dl.aircrack-ng.org/breakingwepandwpa.pdf, 2009, S. 79–86

[UAVTalk] RUSSELL, Jack ; PROJEKT, OpenPilot (Hrsg.): *UAVTalk - OpenPilot Documentation - OpenPilot Documentation*. – URL https://wiki.openpilot.org/display/WIKI/UAVTalk. – Zugriffsdatum: 16.03.2015

[XBEEPRO868] DIGI INTERNATIONAL: *XBee/XBee-PRO 868 RF Modules*

[ZigBeeSpec 2007] ZIGBEE TECHNICAL STEERING COMMITTEE: *ZigBee specification*. Release 17, 2007

Abkürzungsverzeichnis

ADS Air Data Sensor.

AFA Adaptive Frequency Agility.

AHRS Attitude Heading Reference System.

AP Access-Point.

BBB BeagleBone Black.

BWB Blended Wing Body.

CAN Controller Area Network.

CSA Control Surface Allocator.

DC Duty Cycle.

EDGE Enhanced Data Rates for GSM Evolution.

ESC Electronic Speed Controller.

FCU Flight Control Unit.

FDL Flugdatenlogger.

FDM Frequency Division Multiplexing.

FFD Full Funktion Device.

GCS Ground Control Station.

GPRS General Packet Radio Service.

GPS Global Positioning System.

GSM Global System for Mobile Communications.

HIL Hardware-In-the-Loop.

HSPA High Speed Packet Access.

IEEE Institute of Electrical and Electronics Engineers.

ISO International Organization for Standardisation.

LBT Listen Before Talk.

LTE Long Term Evolution.

MIMO Multiple Input Multiple Output.

OFDM Orthogonal Frequency-Division Multiplexing.

OSI Open Systems Interconnect.

P2P Peer-to-Peer.

P2S Puls-Weiten-Modulation (PWM) zu SPI-Wandler.

PAN Personal Area Network. 36–38, *Glossar:* Personal Area Network (PAN)

PSK pre-shared key.

PWM Puls-Weiten-Modulation.

RCR Radio Control Receiver.

RFD Reduced Funktion Device.

S2P SPI zu PWM-Wandler.

SIL Software-In-the-Loop.

SLB Safe-Live-Board.

SPI Serial Peripheral Interface.

SSID Service Set Identifier.

UART Universal Asynchronous Receiver Transmitter. 46, 49–52, 60, *Glossar:* UART

UAS Unmanned Aerial System.

UAV Unmanned Aerial Vehicle. 9, 11, 42, 48, *Glossar:* Unmanned Aerial Vehicle

UDP User Datagramm Protocol.

UMTS Universal Mobile Telecommunications System.

Glossar

B

Beacon

dt. Signalfeuer: dient der Synchronisation in Netzwerken.

M

Marshalling

ist des Umwandeln von strukturierten Daten in eine Form die sich zur Übermittlung an andere Prozesse eignet. Die Rückwandlung in die Objekte bezeichnet man als Unmarshalling..

O

OSI-Referenzmodell

Das Open Systems Interconnect (OSI)-Referenzmodell ist eine von der International Organization for Standardisation (ISO) verabschiedete Designgrundlage für Kommunikationsprotokolle. Es dient der Ermöglichung der Kommunikation zwischen unterschiedlichen technischen Systemen. Dazu definiert das Modell sieben Schichten (Layer), die voneinander getrennte Aufgaben übernehmen. Protokolle der gleichen Schicht können untereinander ausgetauscht werden, ohne das sich dabei die Schnittstellen zu den anderen Schichten ändern.
Das Modell beschreibt dazu den Datenfluss angefangen bei der niedrigsten Schicht, der physikalischen Verbindung bis hin zur Anwendungsschicht. Dabei kommuniziert jede Schicht mit ihren jeweils über- oder untergeordneten Schichten. Bei der Kommunikation zwischen zwei Computern kommunizieren die selben Schichten der Computer untereinander, ohne Kenntnis des Ablaufs der unteren Schichten.
Die sieben Schichten sind:

7. Anwendungsschicht (Application Layer) Datenein- und Ausgabe für Anwendungen.

6. Darstellungsschicht (Presentation Layer) Transformiert die Daten in standardisierte Formate.

5. Sitzungsschicht (Session Layer) Prozesskommunikation zwischen zwei Systemen.

4. Transportschicht (Transport Layer) Segmentierung von Nachrichten und die korrekte Zusammensetzung bem Empfänger. Diese Schciht bietet den anwendungsorientierten Schichten 7-5 einen einheitlichen Zugriff auf die Übertragung, ohne dass diese Kenntnis des konkreten Kommunikationsnetzen benötigen.

3. Vermittlungsschicht (Network Layer) Adressiert Nachrichten mit physikalischen netzwerkübergreifenden Adressen. Sorgt für das Routing der Nachrichten im Netzwerk.

2. Sicherungsschicht (Link Layer) Bildet aus dem Bitdatenstrom Blöcke (Frames) und fügt Prüfsummen zur Fehlererkennung hinzu. Außerdem wird hier der Zugriff auf das physikalische Medium geregelt (MAC-Layer).

1. Bitübertragugnsschicht (Physikal Layer) Stellt die Mittel zur Umwandlung der Bits in physikalisch übertragbare Darstellungsformen (z.B. elektromagnetische Wellen) dar. Hier sind alle nachrichtentechnischen Verfahren zu verorten.

.

P

Personal Area Network (PAN)

Ist ein Netzwerk von Kleingeraten, dessen Fokus auf eine Person ausgelegt ist und weniger auf die Kommunikation mit sehr vielen Teilnehmern.

U

UART

Universal Asynchronous Receiver Transmitter; Serielle Punkt zu Punkt Verbindung..

Unmanned Aerial Vehicle

Ein unbemanntes Luftfahrzeug, welches autark durch einen Computer oder eine Fernsteuerung betrieben werden kann..

Versicherung über die Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §16(5) APSO-TI-BM ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen habe ich unter Angabe der Quellen kenntlich gemacht.

Hamburg, 18. März 2015	
Ort, Datum	Unterschrift