

Entwicklung eines Gerätes zur Erfassung von Metainformationen über Signale innerhalb der Dezimeterwelle

Studienarbeit

für die Prüfung zum
Bachelor of Engineering

des Studiengangs Informationstechnik
an der Dualen Hochschule Baden-Württemberg Karlsruhe

von
Tobias Lamm und Sascha Hug

September 2018

Bearbeitungszeitraum
Kurs
Betreuer
Gutachter

5. und 6. Semester
TINF15B3
Stefan Lehmann

Sperrvermerk

Die vorliegende Studienarbeit mit dem Titel *Entwicklung eines Gerätes zur Erfassung von Metainformationen über Signale innerhalb der Dezimeterwelle* enthält unternehmensinterne bzw. vertrauliche Informationen der , ist deshalb mit einem Sperrvermerk versehen und wird ausschließlich zu Prüfungszwecken am Studiengang Informationstechnik der Dualen Hochschule Baden-Württemberg Karlsruhe vorgelegt. Sie ist ausschließlich zur Einsicht durch den zugeteilten Gutachter, die Leitung des Studiengangs und ggf. den Prüfungsausschuss des Studiengangs bestimmt. Es ist untersagt,

- den Inhalt dieser Arbeit (einschließlich Daten, Abbildungen, Tabellen, Zeichnungen usw.) als Ganzes oder auszugsweise weiterzugeben,
- Kopien oder Abschriften dieser Arbeit (einschließlich Daten, Abbildungen, Tabellen, Zeichnungen usw.) als Ganzes oder in Auszügen anzufertigen,
- diese Arbeit zu veröffentlichen bzw. digital, elektronisch oder virtuell zur Verfügung zu stellen.

Jede anderweitige Einsichtnahme und Veröffentlichung – auch von Teilen der Arbeit – bedarf der vorherigen Zustimmung durch den Verfasser und .

Erklärung

gemäß §5 (3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 29. September 2015.

Ich erkläre hiermit ehrenwörtlich:

1. dass ich meine Studienarbeit mit dem Thema *Entwicklung eines Gerätes zur Erfassung von Metainformationen über Signale innerhalb der Dezimeterwelle* ohne fremde Hilfe angefertigt habe;
2. dass ich die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autoren an den entsprechenden Stellen innerhalb der Arbeit gekennzeichnet habe;
3. dass ich meine Studienarbeit bei keiner anderen Prüfung vorgelegt habe;
4. dass die eingereichte elektronische Fassung exakt mit der eingereichten schriftlichen Fassung übereinstimmt.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Karlsruhe, September 2018

Tobias Lamm und Sascha Hug

Abstract

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue dui dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse

Inhaltsverzeichnis

Abkürzungsverzeichnis	VI
Abbildungsverzeichnis	VII
Tabellenverzeichnis	VIII
Quellcodeverzeichnis	IX
1 Einleitung	1
1.1 Problemstellung	1
1.2 Zielsetzung	1
1.3 Abgrenzung	1
1.4 Vorgehensweise	1
2 Theoretische Grundlagen	2
2.1 Elektromagnetische Wellen	2
2.2 Maxwell'sche Gleichungen	3
2.2.1 Eigenschaften einer elektromagnetischen Welle	4
2.2.2 Elektronisches Rauschen	4
2.3 Nachrichten- und Übertragungstechnik	5
2.4 Signale und Spektren	6
2.4.1 Kontinuierliche und diskrete Signale	6
2.4.2 Nyquist-Shannon-Abtasttheorem	7
2.4.3 Spektrum eines Signals	7
2.4.4 Fourier-Transformation	7
2.5 Basisbandübertragung und Trägersignale	9
2.5.1 Modulationsverfahren	10
2.6 Frequenzbereiche	11
2.6.1 Rechtliche Grundlagen	11
2.7 Anwendungen im Bereich der Dezimeterwelle	12
2.7.1 Bluetooth	12
2.7.2 Wireless Local Area Network	13
2.8 Software Defined Radio Systeme	13
3 Praxis Kapitel	15
3.1 Aufbau/Entwurf	15
3.2 SDR Sharp	15
3.3 GNU Radio	15
3.3.1 Funktionsweise	15

3.4	Hardware	16
3.4.1	Antenne	16
3.4.2	SDR-Gerät	17
4	Praxis Kapitel	19
4.1	Einrichten der Entwicklungsumgebung	19
4.2	Grundbausteine in GNU Radio Companion	19
5	Fazit	21
5.1	Zusammenfassung	21
5.2	Ausblick	21
	Literatur	22
	Anhang	24

Abkürzungsverzeichnis

ITU	International Telecommunications Union
UHF	Ultra-High-Frequency
FFT	Fast Fourier Transform
DFT	Discrete Fourier Transform
SDR	Software Defined Radio
CRC	Cyclic Redundancy Check
osmocom	Open Source Mobile Communications

Abbildungsverzeichnis

2.1	Elektromagnetische Welle mit senkrecht aufeinander stehendem elektrischem und magnetischem Feld	2
2.2	Kommunikationsmodell nach Shannon	5
2.3	Sinus-Signal als kontinuierliches und als diskretes Signal	6
2.4	Aliasing Effekt. Abtastung zweier Sinussignale verschiedener Frequenzen .	7
2.5	Zeitsignal, gefensterter Zeitsignal und Spektrum eines diskreten Sinus-Signals	9
2.6	Spektrum elektromagnetischer Wellen und gebräuchliche Bandbezeichnungen	11
2.7	Eintrag: 2,4 GHz WLAN im Frequenzplan	12
2.8	Blockschaltbild eines SDR Systems	13
2.9	Nachrichtentechnisches Blockschaltbild eines digitalen Übertragungssystems	14
3.1	Sirio SD 3000N stationäre Funkantenne	17
3.2	Hack RF ONE Platine	18
4.1	Implementation eines FM-Radioempfängers in GNU Radio Companion . .	20

Tabellenverzeichnis

Quellcodeverzeichnis

4.1	Erstellen einer udev-Regel	19
4.2	Das Kommando "hackrf_info" wird zum Test auf dem System ausgeführt .	19

1 Einleitung

1.1 Problemstellung

Warum ist das Thema relevant? In welchem Kontext?

1.2 Zielsetzung

Welche Fragen soll die Arbeit beantworten?

Welchem Zweck dient die Arbeit?

1.3 Abgrenzung

1.4 Vorgehensweise

Zu Beginn werden in Abschnitt 2 die theoretischen Grundlagen geschaffen, die für das Verständnis dieser Projektarbeit nötig sind. Dann wird in Kapitel 3 die praktische Ausarbeitung und Umsetzung thematisiert. Abschließend folgt eine Zusammenfassung mit Fazit und Ausblick.

Welche Vorgehensweise wird hierzu gewählt?

2 Theoretische Grundlagen

2.1 Elektromagnetische Wellen

Als elektromagnetische Welle werden räumlich ausbreitende Wellen bezeichnet, die aus elektrischen und magnetischen Feldern besteht. Die laufende Welle breitet sich entlang der Ausbreitungsgeschwindigkeit mit einer Geschwindigkeit von

$$c = 3 * 10^8 m/s$$

aus. Die elektrischen und magnetischen Feldvektoren der Welle stehen orthogonal zueinander, wie in der Abbildung 2.1 gut zu erkennen.

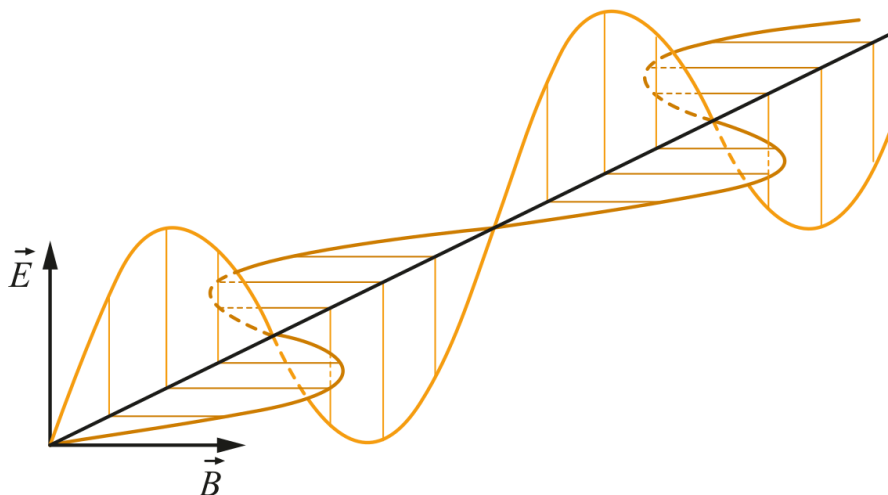


Abbildung 2.1: Elektromagnetische Welle mit senkrecht zueinander stehendem elektrischem und magnetischem Feld. Quelle: [1, Harten, S. 130]

Der Frequenzbereich, auch Spektrum einer solchen elektromagnetischen Welle reicht von langsamen Radiowellen, Infrarotwellen über den Bereich des sichtbaren Lichts bis hin zur Röntgenstrahlung und der extrem kurzwelligigen Gammastrahlung. In der Abbildung 2.6 werden die Frequenzbereiche detaillierter dargestellt.

Die elektromagnetischen Wellen, die auf unsere Erde einwirken werden auch natürliche Strahlung genannt. Sie ermöglicht das Leben auf der Erde, da die Energiezufuhr des Lebens auf der Erde über infrarot Wellen der Sonne gegeben ist. Elektromagnetische Wellen benötigen kein Medium, um sich auszubreiten. Sie können sich daher auch über

weiteste Entfernungen ausbreiten. Sie bewegen sich im Vakuum unabhängig von ihrer Frequenz mit Lichtgeschwindigkeit fort. Elektromagnetische Wellen können sich aber auch in Materie ausbreiten wie etwa Gas oder Flüssigkeit, jedoch verringert sich dabei ihre Geschwindigkeit.

Die Existenz der elektromagnetischen Wellen folgt aus den Maxwell-Gleichungen. Sie wurden 1886 von H.Hertz erstmals durch den elektrischen Schwingkreis erzeugt. Diese werden im folgenden Kapitel genauer erklärt.

2.2 Maxwellsche Gleichungen

Die Maxwell-Gleichungen sind grundlegende Gleichungen der Elektrodynamik. Sie dienen zur Beschreibung der Phänomene des Elektromagnetismus und sie sind damit ein wichtiger Teil der Elektrodynamik. Mit Hilfe der Gleichungen können alle elektrischen und magnetischen Effekte beschrieben werden, wie den Zusammenhang elektrischer und magnetischer Felder untereinander. Außerdem die Korrelation von elektrischer Ladungen und elektrischen Strom durch definierte Randbedingungen. Clerk Maxwell beschrieb wie groß die elektrischen und magnetischen Felder sind und damit die wirkenden Kräfte.

Maxwell-Gleichungen:

Gaußscher Satz für Elektrizität

$$\operatorname{div} \vec{E} = \frac{\rho}{\epsilon}$$

Gaußscher Satz für Magnetismus

$$\operatorname{div} \vec{B} = 0$$

Faradaysches Gesetz

$$\operatorname{rot} \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

Ampere-Maxwellsches Gesetz

$$\operatorname{rot} \vec{B} = \mu \vec{j} + \epsilon \mu \frac{\partial \vec{E}}{\partial t}$$

[2]

Die dabei auftretenden Konstanten ϵ (elektrische Feldkonstante) und μ (magnetische Feldkonstante) sind im SI-Einheitensystem definiert. Die Abkürzungen div und rot stehen für Divergenz und Rotation.

2.2.1 Eigenschaften einer elektromagnetischen Welle

2.2.2 Elektronisches Rauschen

Rauschen im Allgemeinen ist der Oberbegriff für Störspannungen, die ein Nutzsignal überlagern. Es wird als unerwünschtes Signal bezeichnet, das in Kommunikationssystem leider allgegenwärtig ist. Das Rauschen behindert den Empfang von Nachrichten bei der Übertragung, deshalb ist es erforderlich diesen Nebeneffekt zu begrenzen. Rauschen kann mehrere Ursachen haben, die alle durch physikalische Gesetzmäßigkeiten begründet werden können. Üblicherweise sind Rauschen zufällig auftretende Störspannungen, die keine Phasen oder Frequenzbeziehung zueinander haben.

2.3 Nachrichten- und Übertragungstechnik

Die Nachrichten- und Übertragungstechnik beschäftigt sich mit dem Übertragen elektronischer Nachrichten. Als Nachricht wird in diesem Kontext ein vom Sender gezielt erzeugtes Signal verstanden, welches mit Informationen behaftet und für den Empfänger der Nachricht bestimmt ist [3, vgl. Werner, S. 3].

Das in Abb. 2.2 dargestellte Kommunikationsmodell nach Shannon beschreibt den grundlegenden Aufbau eines Nachrichtenaustausches zweier Systeme. Im Folgenden werden die zum weiteren Verständnis notwendigen Begriffe eingeführt:

Die Informationsquelle („Information Source“) übergibt die Nachricht dem Sender („Transmitter“), der diese mit einem Signal als physikalischem Träger der Nachricht über einen Kanal („Channel“) sendet.

Als Kanal bezeichnet man in der Nachrichtentechnik sämtliche technische Komponenten, welche eine Information vom Sender zum Empfänger transportiert. [4, vgl. Dankmeier, S. 13].

Die im Kanal auftretenden Störsignale, hier durch die Störsignalquelle („Noise Source“) dargestellt, überlagern sich mit dem ursprünglichen Signal.

Aus dem für den Empfänger („Receiver“) bestimmten Empfangssignal („Received Signal“) wird anschließend wieder eine Nachricht generiert, die im letzten Schritt der Informationssinke („Destination“) übergeben wird.

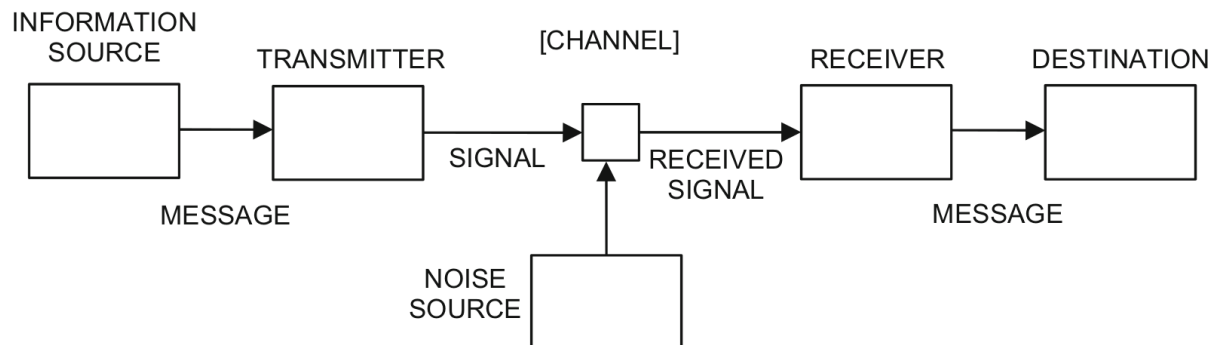


Abbildung 2.2: Kommunikationsmodell nach Shannon. Quelle: [5, Werner, S. 11f]

Die von der Informationsquelle zu übertragenden Daten werden, je nach Datenquelle, durch eine Quellcodierung komprimiert und beim Empfänger dann durch die entsprechende Umkehroperation die ursprünglichen Daten wiederhergestellt.

2.4 Signale und Spektren

Signale werden üblicherweise auf 2 Arten dargestellt:

1. Als *Signal* im Zeitbereich
2. Als *Spektrum* im Frequenzbereich

2.4.1 Kontinuierliche und diskrete Signale

Als Signal gilt eine Funktion mit mindestens einer unabhängigen Variablen, beispielsweise der Zeit t . Ist die Zeitvariable nur für diskrete Werte definiert, so spricht man von einem zeitdiskreten Signal. Man schreibt auch $x[n]$, wobei n die normierte Laufvariable genannt wird [5, vgl. Werner, S. 24].

In Abb. 2.3 wird das kontinuierliche Signal

$$x(t) = \sin \omega t = \sin 2\pi f t$$

mit $f = 50$ Hz dargestellt und mit dem diskreten Signal

$$x[n] = x(nT_a) = \sin 2\pi f T_a n$$

überlagert, welches mit einer Abtastrate von $f_a = 1$ kHz oder anders ausgedrückt: einem Abtastintervall von $T_a = 1/f_a = 1$ ms abgetastet wird [6, vgl. Heuberger, e. a., S. 11f].

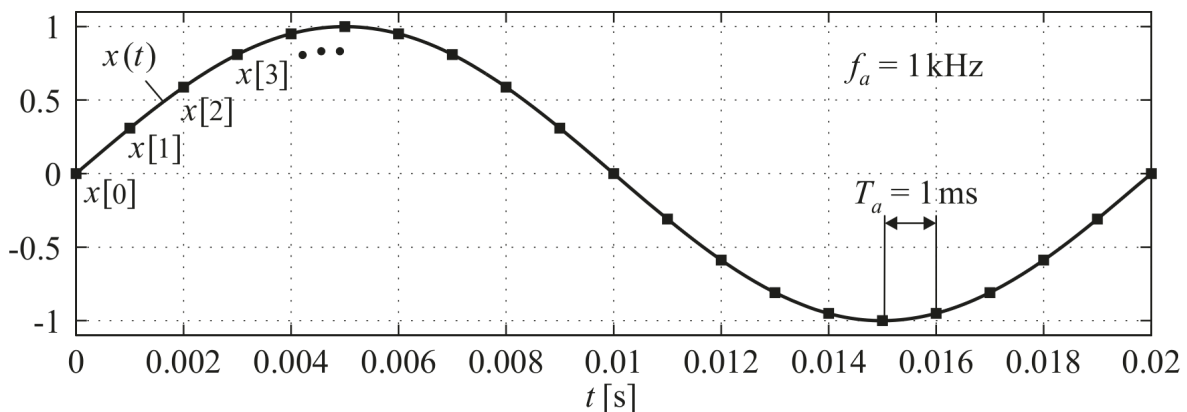


Abbildung 2.3: Sinus-Signal als kontinuierliches und als diskretes Signal.

Quelle: [6, Heuberger, e. a., S. 12]

2.4.2 Nyquist-Shannon-Abtasttheorem

Das Abtasttheorem nach Nyquist und Shannon besagt, dass ein Signal der Funktion $x(t)$ welches die Frequenz f besitzt, mindestens mit der Abtastrate f_a abgetastet werden muss, wobei gilt: $f_a \geq 2f$, damit aus dem abgetasteten Signal das Original durch eine Interpolation ausreichend genau beschrieben werden kann [3, vgl. Werner, S. 30]. Ist dies nicht der Fall, kann beim Abtasten zweier Signale unterschiedlicher Frequenzen dazu kommen, dass die resultierenden diskreten Signale identisch sind. Dieser Effekt wird als „Aliasing“ bezeichnet:

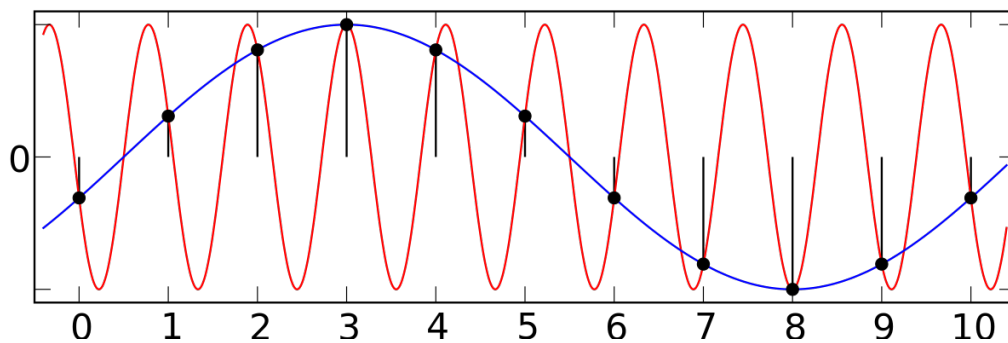


Abbildung 2.4: Aliasing Effekt. Abtastung zweier Sinussignale verschiedener Frequenzen.
Quelle: [7, Moxfyre]

In der Praxis wird daher meist eine Abtastrate verwendet, die ausreichend größer ist, als der doppelte Betrag der höchsten Frequenz im gegebenen Signal.

2.4.3 Spektrum eines Signals

Eine alternative Darstellung von Signalen kann im Frequenzbereich erfolgen. Dort wird ein Signal mit einzelnen Sinus-Schwingungen beschrieben, aus denen es sich zusammensetzen lässt [8, vgl. Karrenberg, S. 42].

2.4.4 Fourier-Transformation

Um ein Signal aus dem Zeitbereich in den Frequenzbereich zu überführen wird die sogenannte Fourier-Transformation verwendet.

Im wesentlichen wird ein Signal bzw. eine Funktion mittels Fourier-Transformation als Summe mehrerer Sinus-Schwingungen unterschiedlicher Frequenzen und Amplituden dargestellt.

Signale können also entweder aus Sinusschwingungen konstruiert, oder in solche zerlegt werden. Nach der Zerlegung ergeben sich einige Möglichkeiten mit den einzelnen Frequenzen zu arbeiten:

- Aus einem Signal können einzelne Frequenzen hervorgehoben werden
- Bei Audiosignalen beispielsweise können ungewollte Frequenzen ausgeblendet werden (etwa Hintergrundrauschen)

Um von dem resultierenden Spektrum wieder zu einer Darstellung im Zeitbereich zu gelangen, kann die Umkehroperation, die inverse Fourier-Transformation angewandt werden.

In der Praxis wird für die Überführung in den Frequenzbereich meist die Fast Fourier Transform (FFT) genutzt [6, vgl. Heuberger, e. a., S. 14]. Die FFT ist allerdings nur eine effizientere Berechnungsart der Discrete Fourier Transform (DFT), welche die Fouriertransformation auch mit diskreten Werten ermöglicht [9, vgl. Meyer, S. 175].

Um ein Signal mittels FFT in den Frequenzraum überführen zu können, muss es die Länge der Form $N = 2^L$ aufweisen. N muss also eine 2er-Potenz sein [6, vgl. Heuberger, e. a., S. 15]. Für das zu überführende Signal gilt also:

$$\underline{x} = \begin{bmatrix} x[0] & x[1] & x[2] & \dots & x[N-2] & x[N-1] \end{bmatrix}$$

Fensterfunktionen

In der Praxis, so auch bei Software Defined Radio (SDR)-Systemen, handelt es sich in der Regel um Ausschnitte eines Signales. Bei der FFT wird mit periodischen Signalen gearbeitet, ein Signalausschnitt ist aber nur quasiperiodisch. Denn an den Rändern gibt es bei der periodischen Fortsetzung des Signals Sprungstellen [9, vgl. Meyer, S. 187].

Wird also ein Signal, dessen Länge kein vielfaches einer ganzen Periode ist, aufgezeichnet, entsteht durch die Unstetigkeiten am Rand eine spektrale Streuung durch die Umwandlung mit der FFT.

Der Signalausschnitt wird deshalb mit einer sogenannten Fensterfunktion gewichtet:

$$\underline{w} = \begin{bmatrix} w[0] & w[1] & w[2] & \dots & w[N-2] & w[N-1] \end{bmatrix}$$

Die gefensterte FFT Funktion:

$$\text{FFT}_w \underline{x}[n] = \sum_{n=0}^{N-1} w[n] \underline{x}[n] e^{-j2\pi nm/N} \text{ mit } m = 0, \dots, N-1$$

Das Spektrum dieser Funktion lässt sich als den gewichteten Betrag des resultierenden Ergebnisses ausdrücken [6, vgl. Heuberger, e. a., S. 14]:

$$s_x[m] = \frac{1}{c_w^2} \left| \underline{X}[m] \right|^2 \text{ mit } c_w = \sum_{n=0}^{N-1} w[n]$$

In Abbildung 2.5 wird das diskrete Zeitsignal $x[n]$ dem gefensterten Zeitsignal $w[n]x[n]$ und dem aus der FFT resultierenden Spektrum $S_x[m]$ gegenübergestellt:

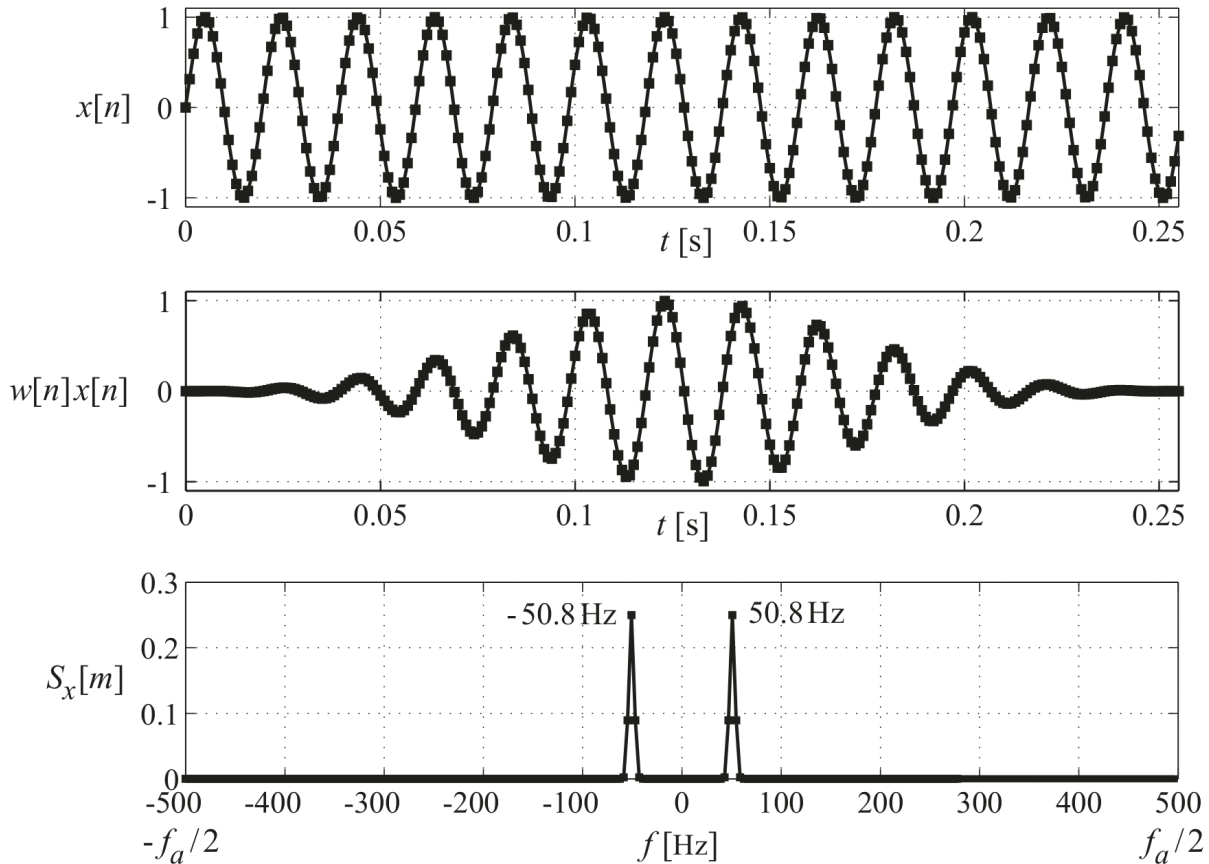


Abbildung 2.5: Zeitsignal, gefenstertes Zeitsignal und Spektrum eines diskreten Sinus-Signals.
Quelle: [6, Heuberger, e. a., S. 16]

2.5 Basisbandübertragung und Trägersignale

Die Übertragung von Signalen kann über verschiedene Medien erfolgen, etwa metallische- und Lichtwellenleiter oder über Funk. Eine Übertragung im sogenannten Basisband ist jedoch nur mit metallischen Leitern möglich [10, vgl. Read, S. 149]. Diese haben den Vorteil, dass ein Signal zur Übertragung den gesamten Frequenzbereich uneingeschränkt nutzen kann. Dies bedeutet, dass das volle Spektrum des Signals in den Übertragungskanal

(z. B. Telefonleitung, LAN Kabel) eingespeist werden kann. Eine Verschiebung von den Frequenzen informationstragender Signale ist also nicht notwendig [3, vgl. Werner, S. 158]. Ist das der Fall, so spricht man von einer Basisbandübertragung.

2.5.1 Modulationsverfahren

Signale, die mit einer Funkübertragungstechnik gesendet werden, müssen vor der Übertragung jedoch an Frequenz und Bandbreite des entsprechenden Kanals angepasst werden [10, vgl. Read, S. 24]. Das hat unter anderem damit zu tun, dass für verschiedene Anwendungen spezielle Bereiche im Frequenzspektrum reserviert sind, siehe Abschnitt 2.6. Des weiteren ist es zum Senden und Empfangen von Signalen vorteilhaft, wenn die Größe der Antenne in etwa der halben Wellenlänge des Signals entspricht [11, vgl. Kark, S. 4]. Bei der Übertragung von Sprachsignalen, welche (bei Männern) durchschnittlich bei etwa 120 Hz liegen, wäre zum Senden eine Antenne der Größe 1.250 km ideal:

$$\frac{\lambda}{2} = \frac{c}{2f} = \frac{3 * 10^8 \text{ m/s}}{2 * 120 \text{ Hz}} = 1.250.000 \text{ m}$$

Da eine Antenne dieser Größe utopisch ist, können die zu übertragenden Informationen einfach auf höhere Frequenzen (mit entsprechend kleineren Wellenlängen) verschoben werden. Hierbei spricht man von *Modulation*. Die informationstragenden Signale werden dann bevorzugt einer elektromagnetischen, sinusförmigen Welle über die Amplitude, der Phase und/oder der Frequenz aufgeprägt [5, vgl. Werner, S. 242f].

Bei der Modulation wird der Frequenzbereich des Basisbandes, also des zu modulierenden Signals, in einen anderen Frequenzbereich transformiert [12, vgl. Plaßmann, S. 1204].

I/Q-Modulation

2.6 Frequenzbereiche

Zur Orientierung im Spektrum elektromagnetischer Wellen haben sich international verschiedene Systeme zur Klassifikation sogenannter Frequenzbänder gebildet. Die International Telecommunications Union (ITU) empfiehlt eine Einteilung des Spektrums von 3 kHz bis 300 GHz in acht Frequenzbereiche, auch Frequenzdekaden genannt. [13, vgl. ITU-R v.431-8]

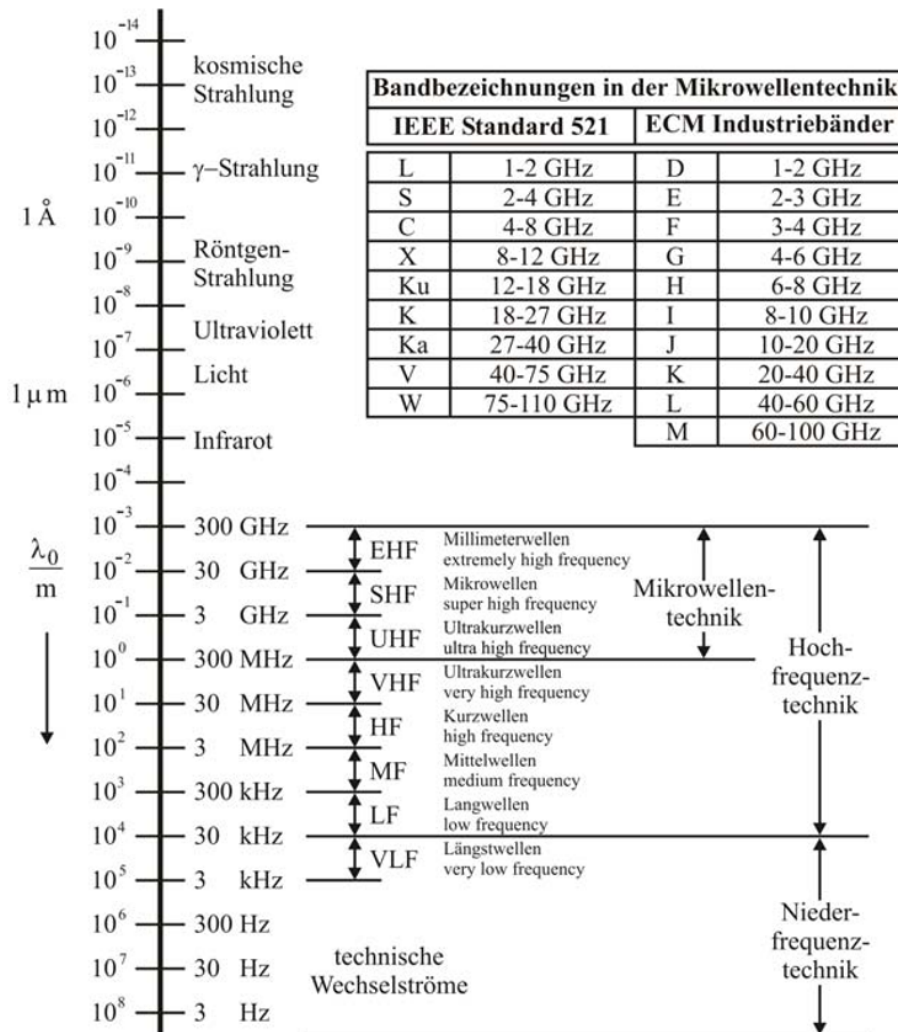


Abbildung 2.6: Spektrum elektromagnetischer Wellen und gebräuchliche Bandbezeichnungen.
Quelle: [11, Kark, S. 1]

2.6.1 Rechtliche Grundlagen

In Deutschland gilt rechtlich zudem die Aufteilung des Frequenzbereiches von 9 kHz bis 3000 GHz, welche von der Bundesnetzagentur im sogenannten Frequenzplan [14, Bundesnetzagentur, 2016] gemäß § 54 TKG festgehalten wird. Dort werden die Frequenzbereiche

nach Frequenznutzung (Amateurfunk, Seefunk, WLAN, etc.) eingeteilt und entsprechende Nutzungsbestimmungen spezifiziert:

Frequenzteilplan:	302	Eintrag:	302003	Stand:	APRIL 2016
Frequenzbereich:	2400 - 2450 MHz				
Nutzungsbestimmung(en):	D150 D282 10 26 31				
Funkdienst:					
Nutzung:	ziv, mil				
Frequenznutzung:	26: WLAN				
Frequenzteilbereich(e):	2400 - 2450 MHz				
Frequenznutzungsbedingungen:	Breitbandige Datenübertragung Maximal zulässige äquivalente Strahlungsleistung: 100 mW EIRP Der Grenzwert der Strahlungsleistung bezieht sich - unabhängig vom Modulationsverfahren - auf die Summenleistung mit Bezug auf das Frequenzband 2400 - 2483,5 MHz.				

Abbildung 2.7: Eintrag: 2,4 GHz WLAN im Frequenzplan. Quelle: [14, Bundesnetzagentur, 2016]

2.7 Anwendungen im Bereich der Dezimeterwelle

Das Frequenzband von 300 MHz bis 3 GHz, auch Ultra-High-Frequency (UHF)-Band genannt, ist ein Frequenzbereich in dem die Wellen eine Länge von zehn Dezimeter bis einem Dezimeter besitzen: $\lambda = \frac{c}{f} = \frac{3 \cdot 10^8 \text{ m/s}}{300 \text{ MHz}} = 1 \text{ m}$ und $\frac{3 \cdot 10^8 \text{ m/s}}{3000 \text{ MHz}} = 0.1 \text{ m}$

2.7.1 Bluetooth

Bluetooth ist eine Übertragungstechnik für kabellose Kommunikation über kurze Distanzen. Es wird im Frequenzbereich von 2,4 bis 2,4835 GHz betrieben [15, Bundesamt für Strahlenschutz, S. 1]. Insgesamt gibt es unter Bluetoothgeräten drei verschiedene Sendeleistungsklassen:

Klasse 1: bis 1,0 mW Reichweite: bis 10m

Klasse 2: bis 2,5 mW Reichweite: 10m und mehr

Klasse 3: bis 100 mW Reichweite: 100m und mehr

Die Aufteilung des Frequenzbereiches von 0 kHz bis 3000 GHz wird von der Bundesnetzagentur im sogenannten Frequenzplan [14, Bundesnetzagentur] gemäß § 54 TKG festgehalten.

2.7.2 Wireless Local Area Network

Unter dem Begriff Wireless Local Network (WLAN) versteht man ein kabelloses lokales Netzwerk, welches meist an Orten eingesetzt wird, bei der kabelgebundene Datenübertragung zu teuer, umständlich oder unkomfortabel wäre.

2.8 Software Defined Radio Systeme

SDR Systeme sind digitale Datenübertragungssysteme, bei denen der Großteil der Signal- und Datenverarbeitung mittels Softwarekomponenten erfolgt [6, Heuberger, e. a., S. 1]. Besonders hervorzuheben ist bei SDR Systemen, dass ihre Hardware größtenteils unabhängig nachrichtentechnischer Eigenschaften wie der Symbolrate und Modulationsart sind. SDR Systeme können verschiedene Standards verwenden um entsprechende Übertragungsarten zu implementieren, da die Funktionalität durch Software, also Hardware-unabhängig, realisiert wird [6, Heuberger, e. a., S. 36].

Abbildung 2.8 zeigt den Aufbau eines SDR Systems als Blockschaltbild, in dem sowohl Sender und Empfänger als SDR realisiert sind. Für jedes Element im Sender gibt es ein entsprechendes Element im Empfänger, welches die Senderoperationen rückgängig macht, um die ursprünglichen Daten rekonstruieren zu können.

Da sich diese Studienarbeit mit dem Empfangen und Auswerten von Signalen, aber nicht dem Senden befasst, wird im weiteren Verlauf des Dokumentes hauptsächlich die Seite des Empfängersystems und der Übertragungsstrecke betrachtet.

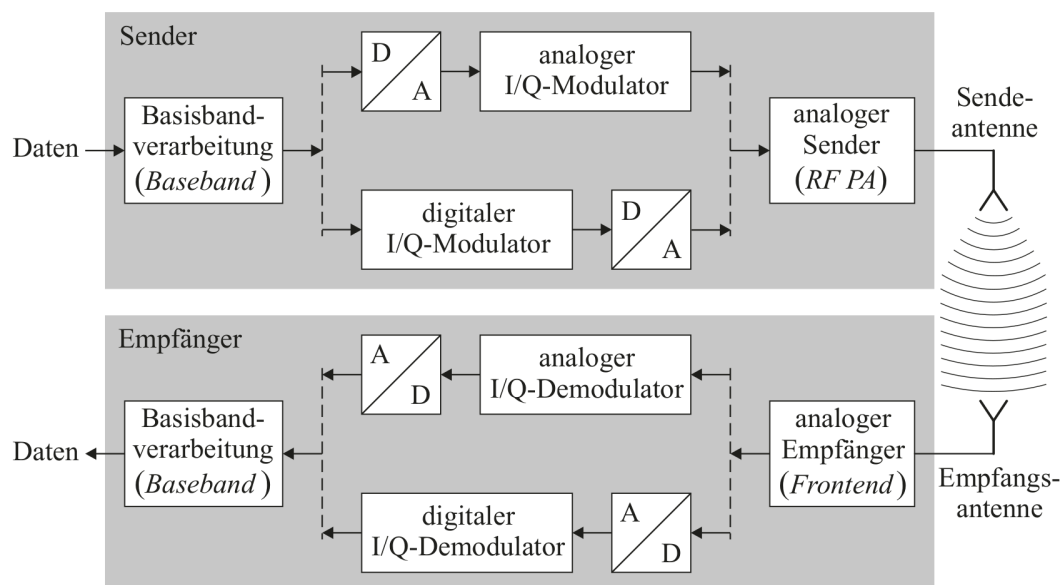


Abbildung 2.8: Blockschaltbild eines SDR Systems. Quelle: [6, Heuberger, e. a., S. 37]

Abbildung 2.9 zeigt den Aufbau eines klassischen digitalen Übertragungssystems. Die Funktionsweise lässt sich wie folgt zusammenfassen:

1. Um später die Integrität der digitalen Daten verifizieren zu können, werden sie mit einer Cyclic Redundancy Check (CRC)-Kodierung versehen.
2. Kanalcodierung
3. Scrambler
4. Symbol-Mapper
5. Das Signal wird einem Trägersignal aufgeprägt, damit es übertragen werden kann.

Anschließend erfolgen auf der Empfängerseite die entsprechenden inversen Operationen zu den aufgeführten Schritten. In einem Software Defined Radio System werden *alle* diese Vorgänge durch Software in der Basisbandverarbeitung abgebildet [6, vgl. Heuberger, e. a., S. 38]

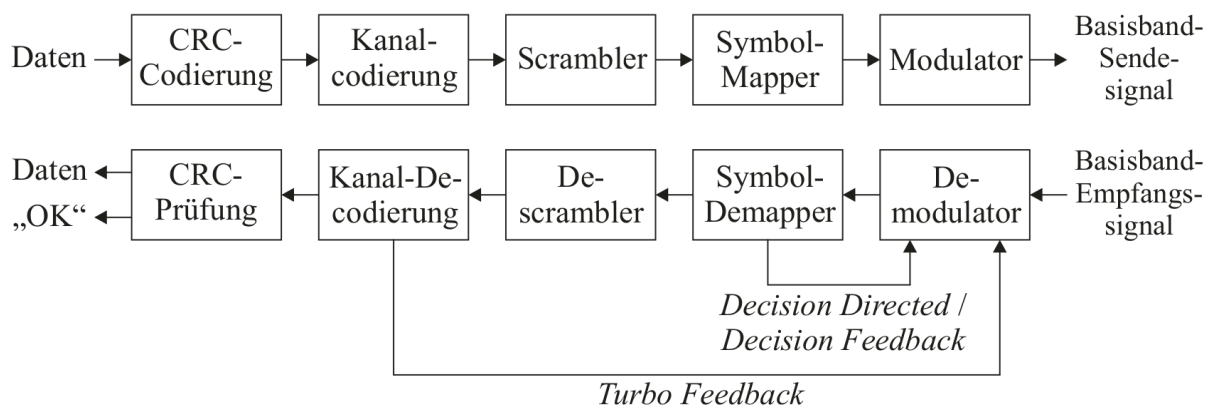


Abbildung 2.9: Nachrichtentechnisches Blockschaltbild eines digitalen Übertragungssystems.
Quelle: [6, Heuberger, e. a., S. 38]

3 Praxis Kapitel

3.1 Aufbau/Entwurf

3.2 SDR Sharp

SDR Sharp ist eine kostenlose Software von AIRSPY die ausschließlich für Windows erhältlich ist. Mit dieser Anwendung kann man die empfangenen Rohdaten von USB Geräten auslesen, jedoch kann sie nur mit externer Hardware betrieben werden.

3.3 GNU Radio

GNU Radio ist ein freies Open Source Entwicklerwerkzeug zur Implementierung von Software Defined Radio (SDR) mittels Signalverarbeitungsblöcken. Es kann mit externer Funkhardware oder als Simulation ohne Hardware genutzt werden. GNU Radio ist im Hobbybereich weit verbreitet, wird aber auch in der Wissenschaft und im kommerziellen Bereich genutzt. GNU Radio Programme kann zusätzlich durch selbst programmierte Ergänzungsblöcke optimiert werden. Welche hauptsächlich in der Programmiersprache Python geschrieben, wobei echtzeitkritische Signalverarbeitungen auch in C++ implementiert werden kann.

3.3.1 Funktionsweise

GNU Radio verarbeitet den Datenstrom, der vom Empfänger kommt, und bereitet Daten vor, um diese zu senden. Dabei ist die gesamte Datenverarbeitung in Blöcke eingeteilt, die beliebig zusammengestellt werden können. GNU Radio liefert eine Vielzahl von Filtern, Kanal-Codes, Synchronisationselementen, Equalizern, Demodulatoren, und vieles mehr. Diese Blöcke stellen die Hardwarekomponenten klassischer Funkhardware dar. Falls nötig können auch selbst Blöcke hinzugefügt werden. Dabei sollte darauf geachtet werden, dass ein Block genau eine Aufgabe erledigt, damit er so vielseitig wie möglich eingesetzt werden kann. GNU Radio bietet die Möglichkeit, diese Blöcke miteinander zu verbinden und regelt dadurch den Datenfluss dazwischen. Für die digitale Verarbeitung von Daten kommen

in GNU Radio verschiedene Datentypen zum Einsatz: Der Datenstrom des Empfängers besteht in den meisten Fällen aus komplexen Zahlen, also einem Datentyp, bei dem jedes Datum aus zwei Float-Werten, dem Imaginärteil und dem Realteil, besteht. Zwischen Blöcken können jedoch beliebige Datentypen zum Einsatz kommen, üblicherweise Short, Byte, Integer und Float. Der Datentyp am Eingang und Ausgang eines Blockes muss dabei nicht gleich sein. Um mit GNU Radio eine SDR-Anwendung zu bauen, muss man Blöcke, die die einzelnen Funktionseinheiten darstellen, miteinander zu einem Graphen kombinieren. Sollte ein benötigter Block nicht verfügbar sein, kann man diesen mittels einem Tool selbst hinzufügen. Beim Starten des Graphen ruft GNU Radio nun jeden Block nacheinander auf und stellt sicher, dass Daten von einem Block zum Nächsten weitergereicht werden. Ergebnisse können durch Graphical User Interface (GUI)-Blöcke dargestellt werden. Diese nutzen die freien und plattformübergreifenden GUI-Toolkits.

3.4 Hardware

3.4.1 Antenne

Eine Antenne die aus der Aufgabenstellung hervorgeht, muss dementsprechend auch den Frequenzbereich der Dezimeterwelle abdeckt. Zu erst war die Überlegung eine mobile Antenne zu benutzen, somit könnte man die Analysefunktion des Gerätes auch unterwegs nutzen. Aus Gründen wie Flexibilität und Mobilität entschieden wir uns jedoch dagegen. Eine mobile Antenne, die den Frequenzbereich der Dezimeterwelle abdecken, würde relativ groß und ziemlich teuer sein. Deshalb haben wir uns auf eine stationäre Antenne geeinigt, da diese preislich als auch dem Verwendungszweck dennoch am Nächsten kommt. Wir haben uns für die Sirio SD 3000N entschieden, ihr preis liegt bei 90 Euro und deckt den kompletten Frquenzbereich der Dezimeterwelle ab.



Abbildung 3.1: Sirio SD 3000N stationäre Funkantenne. Quelle: [16]

Auf Grund analytischen Zwecken haben werden zwei Antennen für die Aufgabe erworben, somit können wir an zwei unterschiedlichen Standorten eine Analyse der Metainformationen betrachten. Präsentation vom Hochfrequenztechnik aus Mechatronik siehe WhatsApp

3.4.2 SDR-Gerät

Ein Software Defined Radio Gerät, das man experimentell betreiben kann, reicht von mehreren tausend Euro teuren Entwicklergeräten bis zu kostenlosen Geräten, da selbst mittels einem Mikrofoneingang der Soundkarte am Computers, derartige Signale empfangen werden können. Die Geräte unterscheiden sich hauptsächlich im Frequenzbereich, der maximalen Bandbreite und der Abtastrate. Beim Computer kommen häufig Universal Serial Bus (USB), Ethernet als Schnittstelle zum Einsatz. Da theoretisch nur Signale empfangen werden sollen, würde ein DVB-T-Stick eine günstige Option darstellen. Mithilfe

eines veränderten Treibers könnte der Stick mit GNU Radio genutzt werden, jedoch deckt sich der Frequenzbereich des Gerätes nicht, mit dem innerhalb der Aufgabenstellung der Dezimeterwelle. Das SDR-Gerät muss in Kombination mit der Funkantenne den kompletten Funkbereich der Dezimeterwelle erstrecken, um die Metainformationen in diesem Bereich zu analysieren. Aus diesem Grund kann ein solches Gerät für diese Arbeit nicht verwendet werden. Eine mögliche Lösung ist das HackRF One Board. Die HackRF One Platine ist ein flexibles Testmodul für die Funkmesstechnik, das wie ein Software Defined Radio (SDR) arbeitet. Sie ist ein Open Source Hardware Transceiver, der hauptsächlich zu eigenen Versuchen und Messungen für SDRs eignet, außerdem ist dieses Gerät für die HF-Technik und messtechnischen Versuchsaufbauten im Amateurfunk vergleichsweise geringen Preises von rund 300 Euro sehr beliebt. Der Hack RF One deckt einen weiten Frequenzbereich von 1 bis 6000 MHz (6 GHz) ab, und erfasst damit sehr viele Frequenzbänder für kommerzielle, experimentelle und Amateurfunk-Anwendungen. Die Hardware bietet eine maximale Abtastrate des Signales von 20MS/s, dadurch werden Messungen und Experimente auch mit breitbandigen Signalen wie DECT, WFM oder WLAN möglich, jedoch nur halbduplex. Der AD-Wandler arbeitet mit 8 Bit Datenbreite und erreicht somit einen theoretischen Dynamikbereich von 48dB. Die digitalisierten I/Q Daten werden auf einem nachgeschalteten CPLD weiterverarbeitet und über den integrierten ARM-Prozessor per USB ausgegeben. Die gesamte Schaltung des HackRF Boards ist sehr stromsparend ausgelegt, sie wird komplett über USB versorgt. Die Platine hat eine Mikro-B USB Buchse. Abschließend lässt sich sagen, dass die oben genannten Gründe für eine Nutzung dieses Gerätes sprechen.[17]

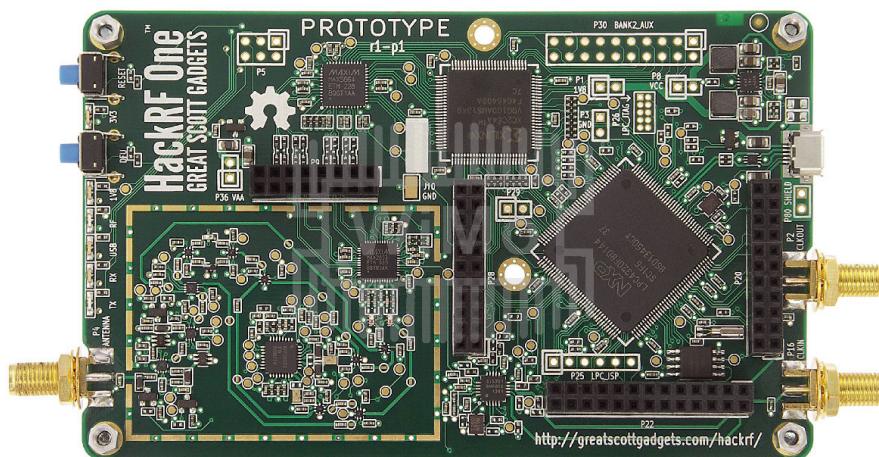


Abbildung 3.2: Hack RF ONE Platine. Quelle: [18]

4 Praxis Kapitel

4.1 Einrichten der Entwicklungsumgebung

Für den täglichen Gebrauch ist es nicht empfehlenswert Binaries als Root-User auszuführen. Um das HackRF One mit einem regulären Nutzer auf einem Linux System nutzen zu können, ist es notwendig eine entsprechende udev-Regel für das Gerät zu schreiben:

```
1 ATTR{idVendor}=="1d50", ATTR{idProduct}=="6089", SYMLINK+="hackrf-one-%k  
  ", MODE="660", GROUP="plugdev"
```

Quellcode 4.1: Erstellen einer udev-Regel

Die Datei mit der Regel wird unter `/etc/udev/rules.d/` abgelegt. Verbindet man das Gerät nun mit dem Computer, wird ein Symlink unter `/dev/` angelegt und Mitglieder der Gruppe *plugdev* haben Zugriff darauf. Die erfolgreiche Installation kann durch das Ausführen des Kommandos **hackrf_info** als User ohne root-Berechtigung überprüft werden:

```
1 hackrf_info version: git-a4c57ef  
2 libhackrf version: git-a4c57ef (0.5)  
3 Found HackRF  
4 Index: 0  
5 Serial number: 0000000000000000a06063c824237d5f  
6 Board ID Number: 2 (HackRF One)  
7 Firmware Version: 2017.02.1 (API:1.02)  
8 Part ID Number: 0xa000cb3c 0x00544765
```

Quellcode 4.2: Das Kommando "hackrf_info" wird zum Test auf dem System ausgeführt

4.2 Grundbausteine in GNU Radio Companion

Um das HackRF One als Signalquelle zu verwenden, wird der quelloffene, von Open Source Mobile Communications ([osmocom](#)) [19] entwickelte GNU Radio Block *gr-osmosdr* [20] benutzt. Dieser unterstützt das HackRF durch die zuvor installierte Bibliothek *libhackrf*.

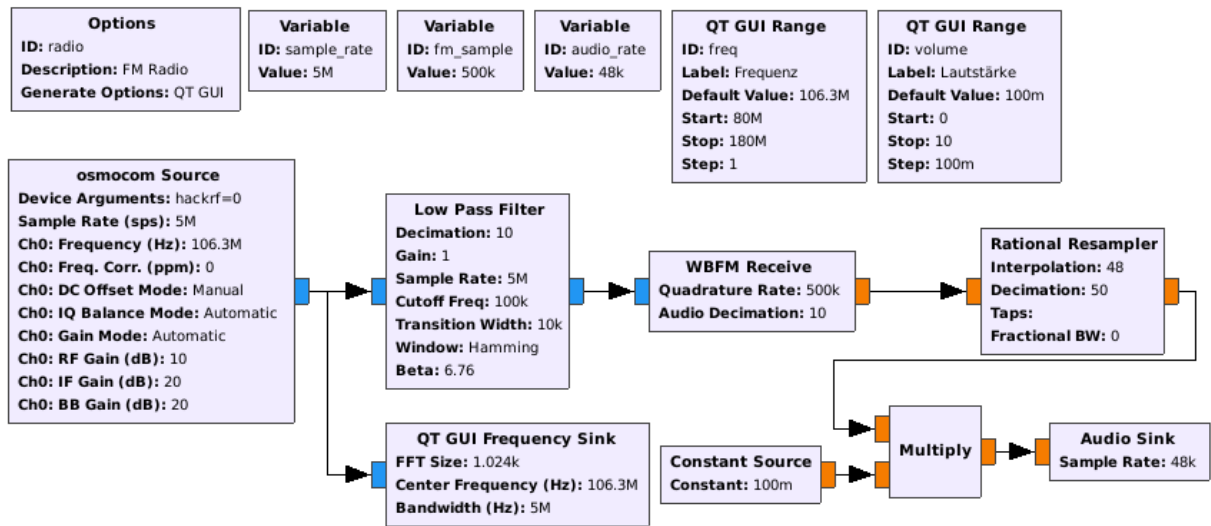


Abbildung 4.1: Implementation eines FM-Radioempfängers in GNU Radio Companion. Quelle: Eigene Darstellung

5 Fazit

Hilfreiche Fragestellungen

Was sind die wichtigsten Ergebnisse?

Was kann evtl. nicht beantwortet werden?

Welchen Zweck haben die Ergebnisse (sowohl für die Arbeit an sich als auch für die Praxis / Wissenschaft)?

Ergebnis der wissenschaftlichen Arbeit Nach dem Hauptteil schreiben! Rückschluss von den Ergebnissen auf die Einleitung (Rückblick zur Einleitung herstellen) Keine Wiederholung aller Inhalte! Nur wichtigste Aspekte aufgreifen Wertvoll, wenn Hauptteil um neue Gedankengänge / Aspekte erweitert wird Unerwartete Ergebnisse bedeuten nicht, dass die Thesis gescheitert ist; sie müssen kritisch diskutiert werden

5.1 Zusammenfassung

5.2 Ausblick

Literatur

- [1] Ulrich Harten. *Physik. Eine Einführung für Ingenieure und Naturwissenschaftler*. Berlin: Springer Vieweg, 2017. ISBN: 978-3-662-49753-1. DOI: [10.1007/978-3-662-49754-8](https://doi.org/10.1007/978-3-662-49754-8). URL: <https://doi.org/10.1007/978-3-662-49754-8>.
- [2] D. Halliday u. a. *Halliday Physik*. Wiley, 2017. ISBN: 9783527812608. URL: <https://books.google.de/books?id=ldM3DwAAQBAJ>.
- [3] Martin Werner. *Nachrichten-Übertragungstechnik. Analoge und digitale Verfahren mit modernen Anwendungen*. Wiesbaden: Vieweg & Teubner, 2006. ISBN: 978-3-528-04126-7.
- [4] Wilfried Dankmeier. *Grundkurs Codierung. Verschlüsselung, Kompression und Fehlerbeseitigung*. Wiesbaden: Springer Vieweg, 2017. ISBN: 978-3-8348-1674-0. DOI: [10.1007/978-3-8348-2154-6](https://doi.org/10.1007/978-3-8348-2154-6). URL: <https://doi.org/10.1007/978-3-8348-2154-6>.
- [5] Martin Werner. *Nachrichtentechnik. Eine Einführung für alle Studiengänge*. Wiesbaden: Springer Vieweg, 2017. ISBN: 978-3-8348-2580-3. DOI: [10.1007/978-3-8348-2581-0](https://doi.org/10.1007/978-3-8348-2581-0). URL: <https://doi.org/10.1007/978-3-8348-2581-0>.
- [6] Albert Heuberger und Eberhard Gamm. *Software Defined Radio-Systeme für die Telemetrie*. Berlin, Heidelberg: Springer Vieweg, 2017. ISBN: 978-3-662-53233-1. DOI: [10.1007/978-3-662-53234-8](https://doi.org/10.1007/978-3-662-53234-8). URL: <https://doi.org/10.1007/978-3-662-53234-8>.
- [7] Wikimedia User: Moxfyre. *Two different sinusoids that fit the same set of samples*. 2009. URL: <https://en.wikipedia.org/wiki/File:AliasingSines.svg>.
- [8] Ulrich Karrenberg. *Signale - Prozesse - Systeme. Eine multimediale und interaktive Einführung in die Signalverarbeitung*. Berlin: Springer Vieweg, 2017. ISBN: 978-3-662-52658-3. DOI: [10.1007/978-3-662-52659-0](https://doi.org/10.1007/978-3-662-52659-0). URL: <https://doi.org/10.1007/978-3-662-52659-0>.
- [9] Martin Meyer. *Signalverarbeitung. Analoge und digitale Signale, Systeme und Filter*. Wiesbaden: Springer Vieweg, 2017. ISBN: 978-3-658-18320-2. DOI: [10.1007/978-3-658-18321-9](https://doi.org/10.1007/978-3-658-18321-9). URL: <https://doi.org/10.1007/978-3-658-18321-9>.
- [10] Richard Read. *Nachrichten- und Informationstechnik. Im Klartext*. München: Pearson Education Deutschland, 2004. ISBN: 3-8273-7100-7.

- [11] Klaus W. Kark. *Antennen und Strahlungsfelder: Elektromagnetische Wellen auf Leitungen, im Freiraum und ihre Abstrahlung*. Wiesbaden: Vieweg, 2017. ISBN: 978-3-658-13964-3. DOI: [10.1007/978-3-658-13965-0](https://doi.org/10.1007/978-3-658-13965-0). URL: <https://doi.org/10.1007/978-3-658-13965-0>.
- [12] Wilfried Pläßmann. „Modulation“. In: *Handbuch Elektrotechnik: Grundlagen und Anwendungen für Elektrotechniker*. Hrsg. von Wilfried Pläßmann und Detlef Schulz. Wiesbaden: Springer Fachmedien Wiesbaden, 2016, S. 1203–1228. ISBN: 978-3-658-07049-6. DOI: [10.1007/978-3-658-07049-6_96](https://doi.org/10.1007/978-3-658-07049-6_96). URL: https://doi.org/10.1007/978-3-658-07049-6_96.
- [13] International Telecommunications Union - Radiocommunication Sector. *Recommendation ITU-R V.431-8. Nomenclature of the frequency and wavelength bands used in telecommunications*. 2015. URL: <https://www.itu.int/rec/R-REC-V.431-8-201508-I/en> (besucht am 10.02.2018).
- [14] Bundesnetzagentur. *Frequenzplan*. 2016. URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Grundlagen/Frequenzplan/frequenzplan-node.html.
- [15] Bundesamt für Strahlungsschutz. *Sprach- und Datenübertragung per Funk: Bluetooth und WLAN*. 2012. URL: https://www.bfs.de/SharedDocs/Downloads/BfS/DE/broschueren/emf/info-bluetooth-und-wlan.pdf?__blob=publicationFile&v=4.
- [16] Funktechnik Bielefeld. *Sirio SD 3000N*. 2018. URL: <https://www.funktechnik-bielefeld.de/sirio-sd-3000n-discone-stationsantenne-fuer-300-3000-mhz>.
- [17] Wimo. *Hack RF One*. 2018. URL: http://www.wimo.com/hackrf-sdr_d.html.
- [18] Wimo. *Hack RF One*. 2018. URL: https://www.google.de/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiT_P_Qs7faAhWiMewKHUSCDLEQjRx6BAGAEAU&url=http%3A%2F%2Fwww.wimo.com%2Fhackrf-sdr_d.html&psig=A0vVaw3F2NrypAJSJgEbVIZ-9Jpz&ust=1523714136900811.
- [19] *Open Source Mobile Communications*. 2018. URL: <https://osmocom.org/>.
- [20] *gr-osmosdr*. 2018. URL: <https://github.com/osmocom/gr-osmosdr>.

Anhang

(Beispielhafter Anhang)