

Friedrich-Alexander-Universität Erlangen-Nürnberg

Lehrstuhl für Technische Elektronik

Prof. Dr.-Ing. Dr.-Ing. habil. Robert Weigel

Förderkennzeichen:13N9770

**ABSCHLUSSBERICHT ZUM FORSCHUNGSPROJEKT
I-LOV**

Dipl.-Ing. Stefan Zorn

Dipl.-Ing. Richard Rose

Dipl.-Ing. Alexander Götz

Projektlaufzeit 01.06.2008 - 30.11.2011

Inhaltsverzeichnis

Abkürzungsverzeichnis	4
1 Aufgabenstellung	9
1.1 Allgemeine Aufgabenstellung	9
1.2 Aufgabenstellung LTE	10
2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde	12
3 Planung und Ablauf des Vorhabens	13
4 Stand der Technik vor Antragstellung	16
4.1 Referenzen	18
5 Zusammenarbeit mit anderen Stellen	19
6 Darstellung der erzielten Ergebnisse - Verwendung der Zuwendung	20
6.1 Das Systemkonzept	20
6.1.1 Schritt 1: Stören aller vorhandener Mobilfunkzellen	20
6.1.2 Schritt 2: Anmeldung der MS am I-LOV GSM-Netzwerk	22
6.1.3 Schritt 3: Identifikation nicht von Opfern stammender MS	22
6.1.4 Schritt 4: Lokalisierung	23
6.2 Die I-LOV BTS	23
6.3 Szenarios der verschiedenen Einsätze	24
6.3.1 Szenario 1	24
6.3.2 Szenario 2	25
6.3.3 Szenario 3	26
6.4 Störsender	26
6.4.1 GSM-Störsender	26
6.4.2 UMTS-Störsender	32
6.5 Das I-LOV GSM-Netzwerk	40
6.5.1 Systemaufbau	40
6.5.2 Hardware	41
6.5.3 Software	42
6.5.4 Einsatz in der Praxis	44
6.6 Die Steuereinheit	45
6.7 Der Feldstärkesensor	49

6.8	Handgerät	57
6.9	Laufzeitbasierte Ortung	58
6.9.1	Grundkonzept und Systemstruktur	60
6.9.2	Algorithmen zur hochgenauen Laufzeitdifferenzmessung	61
6.9.3	Simulation der Leistungsfähigkeit der Algorithmen	66
6.9.4	Entwicklung und Aufbau des Hardwareprototyps	69
6.9.5	Zusammenfassung	76
7	Zahlenmäßiger Nachweis	77
8	Notwendigkeit und Angemessenheit der geleisteten Arbeit	77
9	Verwertung	78
10	Fortschritt bei anderen auf dem Gebiet	79
10.1	STARRS - Sensor for Terrestrial and Airborne Radio transmitter Rescue Search	79
10.2	Rohde&Schwarz	79
11	Veröffentlichungen	80
	Literaturverzeichnis	82

Abkürzungsverzeichnis

ADC	Analog-Digital-Umsetzer, Engl.: Analog to Digital Converter
BCCH	Downlink-Kanal in GSM der dem Endgerät Informationen über die aussendende Zelle liefert, Engl.: Broadcast Control Chanel
BP	Bandpassfilter
BTS	GSM-Mobilfunk-Basisstation , Engl.: Base Transceiver Station
Burst	Eine begrenzte Anzahl von Schwingungen fixer Frequenz
CPICH	Gemeinsamer Pilotkanal einer UMTS-Zelle, Engl.: Common Pilot Indicator Channel
CPWG	Koplanare Wellenleitung mit tieferliegender Masseebene, Engl.: Coplanar Waveguide with Lower Ground Plane
DNG	Digitaler Rauschgenerator, Engl.: Digital Noise Generator
FPGA	Integrierter Schaltkreis der Digitaltechnik, in den eine logische Schaltung programmiert werden kann, Engl.: Field Programmable Gate Array
GERAN	GSM-Netzwerkkern bestehend aus Basisstationen und dazugehörigen Controllern, Engl.: GSM EDGE Radio Access Network
GSM	Globales System für Mobilkommunikation, Engl.: Global System for Mobile Communication
HF	Hochfrequenz

I-LOV	Intelligentes sicherndes Lokalisierungssystem für die Rettung und Bergung von Verschütteten
IC	Integrierte Schaltung
IIP3	Maß für die Nichtlinearität von Übertragungsgliedern, Engl.: Third Order Input Intercept Point
IIR	Filterarchitektur mit unendlicher Impulsantwort, Engl.: Infinit Impulse Response
IMSI	Eindeutige Teilnehmererkennung. Sie besteht aus dem Mobile Country Code (MCC, 3 Ziffern), dem Mobile Network Code (MNC, 2 oder 3 Ziffern) und der Mobile Subscriber Identification Number (MSIN, 1-10 Ziffern), Engl.: International Mobile Subscriber Identity
LCD	Flüssigkristallanzeige, Engl.: Liquid Crystal Display
LNA	Rauscharmer Verstärker, Engl.: Low Noise Amplifier
LO	Lokaloszillator
MMTC	Stiller Verbindungsaufbau zwischen BTS und MS mit maximaler Leistung, Engl.: Modified Mobile Terminated Call
MS	Mobilstation GSM, ugs.: Handy, Engl.: Mobile Station
MSE	Mittlere quadratische Abweichung, Engl.: Mean Square Error
MTC	Klassischer Verbindungsaufbau von BTS zu MS, Engl.: Mobile Terminated Call
NF	Rauschzahl, Engl.: Noise Figure
Node B	UMTS-Mobilfunk-Basisstation, Engl.: Base Transceiver Station
OCXO	beheizter Quarzoszillator mit Temperaturregelung, Engl.: Oven Controlled Crystal Oscillator
PA	Leistungsverstärker, Engl.: Power Amplifier
PCB	Leiterplatte, Engl.: Printed Circuit Board

PCH	Der Paging Channel ist ein Downlink-Kanal im GSM der dazu dient einzelnen Endgeräten einen Verbindungswunsch des Netzes, etwa wegen eines eintreffenden Anrufs oder einer Kurznachricht, zuzustellen; ein so gerufenes Endgerät wird, wenn es diesen Verbindungswunsch empfängt, versuchen, über den RACH oder PRACH eine Verbindung herzustellen; ein Endgerät wird anhand seiner TMSI, in Ausnahmefällen anhand seiner IMSI, gerufen
PLL	Phasenregelschleife, Engl.: Phase-locked loop
RSCP	Leistung eines gespreizten Kanals; auch Nutzleistung, Engl.: Received Signal Code Power
RSSI	Gesamte empfangene Leistung inkl. Rauschen in einem Kanal, Engl.: Received Signal Strength Indicator
SAW	Akustische Oberflächenwelle, Engl.: Surface Accoustic Wave
SDR	Per Software konfigurierbare Sende- und Empfangsschaltung, Engl.: Software Defined Radio
SIM-Karte	Einschubkarte in ein Mobiltelefon, die den Benutzer bei seinem Netzbetreiber identifiziert, Engl.: Subscriber Identity Module
SMS	Kurznachricht mit ursprünglich 256 Zeichen, Engl.: Short Message Service
SNR	Signal- zu Rauschleistungs-Verhältnis, Engl.: Signal to Noise Ratio
TDMA	Zeitmultiplexverfahren, Engl.: Time Division Multiple Access
TDOA	Laufzeitdifferenz, Engl.: Time Difference of Arrival
THW	Bundesanstalt Technisches Hilfswerk
UE	Mobilstation UMTS, ugs.: Handy, Engl.: User Equipment

UMTS	Mobilfunkstandard der dritten Generation, Engl.: Universal Mobile Telecommunications System
USRP	Software Defined Radio Plattform
UTRAN	UMTS-Netzwerkkern bestehend aus Basisstationen und dazugehörigen Controllern, Engl.: Universal Terrestrial Radio Access Network
VCO	Spannungsgesteuerter Oszillator, Engl.: Voltage Controlled Oscillator
VGA	Verstärker mit variabler Verstärkung, Engl.: Variable Gain Amplifier
WCDMA	Breitband-Codemultiplexverfahren, Engl.: Wideband Code Division Multiple Access
ZF	Zwischenfrequenz

1 Aufgabenstellung

In Kapitel 1 sollen sowohl die Gesamtaufgabenstellung des Projektes I-LOV als auch die spezielle Aufgabenstellung des Lehrstuhls für Technische Elektronik (LTE) im Arbeitspaket 4 „Positionsbestimmung und Ortungstechnik“ erläutert werden.

1.1 Allgemeine Aufgabenstellung

Das vorliegende Projekt befasst sich mit technischen rettungs- und bergungsunterstützenden Geräten bei Gebäudeschäden, die Verschüttungen mit sich ziehen. Es setzt sich zum Ziel, Ansatzpunkte für eine Verbesserung der Sicherheit von Helfern und Opfern nach Gebäudeeinstürzen jeglicher Schädigungsart bei natürlichen oder anthropogenen Katastrophen und des Erfolges von Rettungsmaßnahmen zu liefern. Dem Projekt liegt die Thematik in der KatS-LA 261 [KatS-LA 261, 1986] und in Feydt [Feydt, 1971] zu Grunde. Die effektive Ortung bildet dabei die Voraussetzung für Rettungsarbeiten mit großer Leistung und geringer Gefährdung Verschütteter.

Das Projektziel des Projektverbundes der Bundesanstalt Technisches Hilfswerk und ihren Partnern aus Industrie und Forschung ist dem zu Folge die Entwicklung einer neuen Rettungskette unter Berücksichtigung der bereits bestehenden. Schematisch ist dies in Abb. 1 gezeigt. Ein wesentlicher Aspekt ist dabei die begleitende Forschung durch die Technologiepartner der technischen Ausrüstung für Behörden und Organisationen mit Sicherheitsaufgaben, zusammengefasst als intelligentes sicherndes Lokalisierungssystem für die Rettung und Bergung von Verschütteten (I-LOV). Die sozialgesellschaftlichen und einsatzpsychologischen Aspekte von zukünftigen I-LOV unterstützten Einsätzen werden technologiebegleitend zusammen mit der Bundesanstalt Technisches Hilfswerk durchgeführt.

Die neukonzipierte Rettungskette soll primär als nationale Erweiterung und technische Umsetzung des in Zusammenarbeit mit der Bundesanstalt Technisches Hilfswerk entstandenen Band 46 der Zivilschutzforschung "Methoden der Bergung Verschütteter aus zerstörten Gebäuden" gelten. Eine zeitnahe Ortung und Ermittlung der Lageparameter von Opfern würde damit eine schnellere Rettung bzw. Bergung der Verschütteten ermöglichen. Die Einwirkzeiten von Gefahren auf Einsatzkräfte und Opfer könnten hierdurch gering gehalten werden. Zudem könnte einer negativen Berichterstattung entgegengewirkt werden, weil innerhalb kurzer Zeit die Personen geortet und gerettet werden könnten. Die physische und psychische Belastung von Helfern und Verschütteten würden sich damit in vertretbaren Grenzen halten.

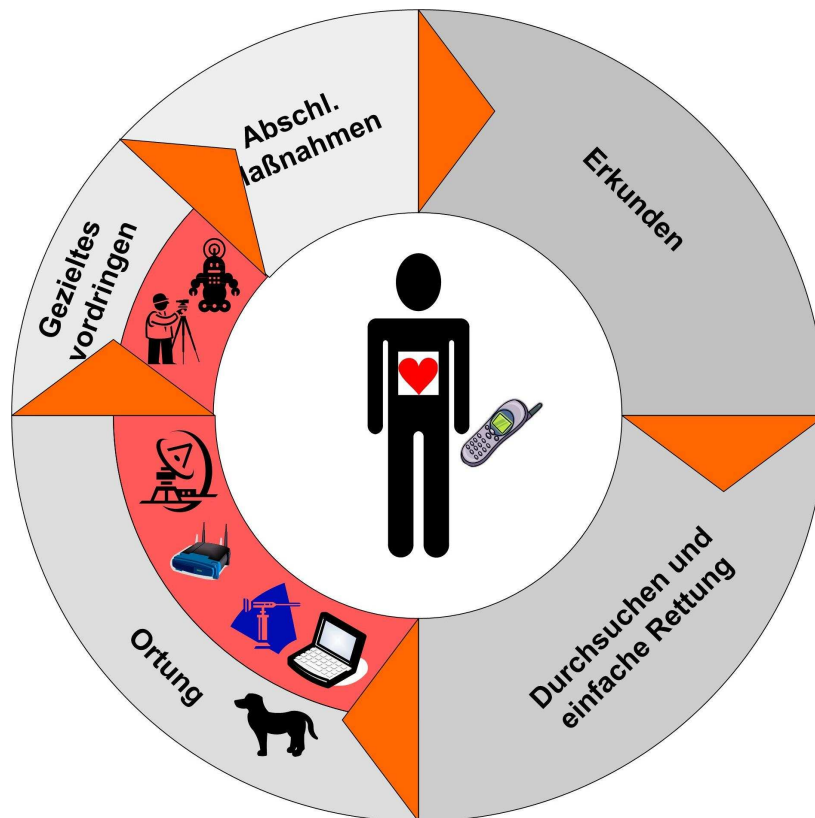


Abbildung 1: Erweiterte Rettungskette

1.2 Aufgabenstellung LTE

In vielen Katastrophenfällen, wie dem Einsturz von Gebäuden nach Erdbeben ist es nötig verschüttete Personen zu lokalisieren und zu bergen. Bislang eignet sich hierfür lediglich der Suchhund als zuverlässigstes Hilfsmittel. Allerdings zeigt die Erfahrung, dass bei einem Katastrophenfall bis zu 80% der Verschütteten ein Mobiltelefon bei sich haben und zum Teil damit selbst die Rettungskräfte kontaktieren. Es ist daher Ziel des hier dargestellten Teilvorhabens innerhalb des Gesamtprojekts I-LOV diesen Umstand zu nutzen und ein neuartiges System zu entwickeln, welches die Ortung von verschütteten Personen mit Hilfe ihrer Mobiltelefone ermöglichen soll. Die Ortung soll dabei anhand von selektiven Feldstärkemessungen von GSM-Mobilfunkgeräten erfolgen. Hierfür müssen zunächst Möglichkeiten der Separation verschiedener Sendesignale von Mobilfunkgeräten untersucht und ein Konzept zur präzisen Feldstärkemessung erarbeitet werden. Im nächsten Schritt muss die gemessene Feldstärke dem korrekten Gerät zugeordnet und im Zeitmultiplex Betrieb verfolgt werden. Hierzu sind Untersuchungen im Bereich der HF-Schaltungstechnik für den Empfang der GSM-Signale und im Bereich der Signalverarbeitung und der Algorithmik

zur selektiven Feldstärkemessung und deren zeitlichen Verlauf (Tracking) durchzuführen. Ziel ist es die prinzipielle Funktionsweise dieses Ansatzes zu untersuchen, die erreichbaren Genauigkeiten und die Ortungstiefe zu evaluieren und schließlich Labormuster für Feldversuche aufzubauen und zu testen. Des Weiteren soll ein neuartiges Konzept für ein raum- und winkelselektives Antennen-Modul für GSM-Signale erarbeitet werden. Mit dessen Hilfe soll einem ausgewählten Empfangssignal eine Richtung zugeordnet werden können, um die Lokalisierung und Ortung des Mobilfunkgerätes anhand der selektiven Feldstärkemessung zu unterstützen. Die daraus gewonnene zusätzliche Information sollte die Genauigkeit des Ortungssystems verbessern. Von zentraler Bedeutung ist dabei auch die Dimensionierung und das Design des Gehäuses, welches die Funktionsweise und Richtcharakteristik der Antennenmodule mitbestimmt und ebenfalls Teil der Untersuchungen sein wird. Neben der reinen Feldstärke soll auch die Laufzeit der Handysignale mit Hilfe der lokalen Stationen bestimmt werden. Dafür werden autonome Referenzstationen verwendet. Diese werden zu Beginn der Suche aufgestellt, vermessen und synchronisieren sich selbstständig. Mit dieser Synchronisation werden die empfangenen Handysignale in jeder Station auf eine einheitliche Uhrzeit gestempelt. Zudem werden Referenzsignale für die mobilen Einheiten bereitgestellt, um die Ortungsfunktion für das räumliche Abtasten der Signalfeldstärke durch die mobilen Einheiten zu ermöglichen. Ein wichtiger Aspekt ist die praktische Anwendbarkeit der Lösung für Helfer vor Ort. Es sollen daher Mittel und Wege zur Integration der mobilen Geräte in eine tragbare Weste untersucht werden. Somit wird der Helfer nicht in seinem Arbeitsraum eingeschränkt. Für diese Anwendung ist insbesondere die Integration der Antennen ein wichtiges Gebiet und wird im Rahmen des Projektes vorangetrieben. Zum Abschluss aller Forschungsarbeiten sollen jeweils Demonstratoren entwickelt werden, welche in Feldversuchen zusammen mit dem Technischen Hilfswerk unter realistischen Einsatzbedingungen getestet werden. Dabei sollen Erkenntnisse über die Lokalisierungsgenauigkeit gewonnen und die Eignung des Systems für den Einsatz in Katastrophengebieten untersucht werden.

Zusammengefasst ergeben sich folgende Aufgaben:

- Teilprojektleitung
- Konzipieren eines GSM-Empfängers zur Separation verschiedener GSM-Geräte
- Auslegung und Erforschung eines Systems zur Ortung von Mobiltelefonen anhand von Feldstärkemessungen mit unterstützender Antennentechnik und zugehörigem Gehäuse
- Tragbare multi-band Antennen für die Rettungsweste

- Untersuchen von Algorithmen zur Positionsberechnung aus Laufzeitsignalen
- Demonstrator-Aufbau und Feldtests

2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Der Lehrstuhl für Technische Elektronik (LTE) der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) kann auf umfangreiche Erfahrungen sowohl im Bereich der hardwareorientierten Elektronik, der Hochfrequenztechnik und Schaltungstechnik als auch in der Nachrichtentechnik verweisen. Dabei hat er vielfältige Expertisen und Kompetenzen im Bereich des Entwurfs von Systemen und integrierten Schaltungen, der Aufbautechnik und der Messtechnik. Im Bereich des Entwurfs von digitalen Schaltungen wurde am LTE die vollständige Protokolllogik eines UHF-RFID-Transponders mit Hilfe eines Industriepartners bis zum fertigen Produktdemonstrator entwickelt. Des Weiteren ist der LTE mit der Erforschung und der Implementierung der Empfängeralgorithmen für Satellitennavigations (Galileo/GPS-) und Nahbereichsortungsanwendungen befasst. Im Mittelpunkt stehen dabei sowohl die Algorithmen- als auch die Schaltungsentwicklung für eine möglichst stromsparende und platzoptimierte Realisierung in CMOS-Technologie. Der LTE arbeitet bereits erfolgreich mit der Firma Symeo als Projektpartner im Bereich Lokalisierung und Positionsbestimmung zusammen: Einem von der Bayerischen Forschungsförderung geförderten Projekt „UPOS - Ultrawide-band (UWB) Positioning in der Produktion“. Ziel dieses Projektes ist die Erforschung einer innovativen Ultrawideband Funkortungstechnik, um Werkzeuge im laufenden Produktionsprozess zu orten. Bei dem geplanten UPOS System handelt es sich um ein klassisches Ortungssystem mit hohen Genauigkeits- und Echtzeit-Anforderungen und nicht um ein Sensornetzwerk. Inhalt des UPOS Projektes ist die Erforschung der UWB-Komponenten, von Verfahren und Algorithmen zur Fusion der Ortungsdaten mit Daten von Beschleunigungssensoren und das Werkzeugortungssystem selbst. Die zentralen Aspekte des Projektes I-LOV, wie die Ortung von Mobiltelefonen basierend auf zeitlich verteilten Messungen, sind nicht Gegenstand des UPOS Projektes, wodurch die Projekte klar gegeneinander abgegrenzt sind. Nach Abschluss beider Projekte ist es sehr gut denkbar, dass Teilergebnisse beider Projekte kombiniert zu interessanten Produktlösungen führen könnten. Hierzu wären dann jedoch weitere Anstrengungen notwendig.

3 Planung und Ablauf des Vorhabens

Das Arbeitspaket „Positionsbestimmung und Ortungstechnik“ umfasst die Entwicklung sowohl eines lokalen positionsbestimmenden Radarsystems zur Überwachung der Einsatzkräfte an der Einsatzstelle als auch eines Ortungssystems für von Verschütteten mitgeführten Mobilfunktelefone. Die Forschung beruht auf der umfangreichen Kompetenz der Partner auf den Gebieten: Hochfrequenztechnik, Systemtechnik und Signalverarbeitung. Auf dem Gebiet der Hochfrequenztechnik liegt dabei Design-Erfahrung bis zu Frequenzen von 77 GHz vor. Auf dem Gebiet der Systemtechnik ist die hochgenaue zeitliche Synchronisation der verteilten Funkstationen der Schlüssel für erfolgreiche Positionsmessung nach dem Laufzeitprinzip. Erfahrungen mit RTOF-Systemen mit FDMA- und TDMA-Separierung sowie Systemkonzepten für Ultra-Wideband Ortung werden hier mit eingebracht. Für die Realisierung der Positionsbestimmung soll zunächst das bestehende Local-Positioning-Radar- (LPR) System von Symeo für das Projekt angepasst werden. Um die große Menge an Einsatzkräften effizienter einsetzen zu können soll zusätzlich eine (Helfer-) Weste entwickelt werden die dann mittels des LPR-Systems die präzise Ortung der Einsatzkraft im Katastrophengebiet erlaubt. Für die Erforschung der Ortungstechnik werden zunächst Kanalmodelle ausgehend von Kanalmessungen in realistischen Katastrophen/Bergungs-Szenarien in den GSM Mobilfunkbändern erstellt. Es folgt die Konzepterarbeitung zur präzisen Feldstärkemessung von einem bzw. mehreren GSM-Mobilfunkgeräten. Basierend auf diesem Schritt soll das Konzept auf den Zeitmultiplex Betrieb erweitert werden, so dass eine Verfolgung (Tracking) mehrerer Mobilfunkgeräte möglich ist. Ausgehend vom detaillierten Hardware-Entwurf des Hochfrequenz- und Basisband-Boards wird ein erster Prototyp aufgebaut. Zeitgleich erfolgt die Spezifikation der Funkanbindung an das SOP-gestützte Informationssystem. Weiterhin ist eine genaue Schnittstellendefinition zum Board der Firma Symeo zu erarbeiten (Basisstationen). Darauf aufbauend erfolgen der Entwurf und die Implementierung der notwendigen Algorithmen zur selektiven Feldstärkemessung von GSM-Mobilfunkgeräten. Es schließen sich die Erprobung der Funktionalität einer reinen Feldstärkemessung (Handgerät) in realistischen Katastrophen/Bergungs-Szenarien und die Bestimmung der entsprechenden Sensitivitäten und Ortsgenauigkeiten an. Diese Tests sollen zusammen mit dem THW durchgeführt werden, um einen möglichst hohen Grad an Übereinstimmung mit späteren realen Einsätzen zur Lebensrettung gewährleisten zu können. Aus den Ergebnissen der vorangegangenen Feldtests erfolgt eine Verbesserung der Hardware und Software und die Konzepterarbeitung für ein raum- und winkelselektives Antennen-Modul. Zusätzlich soll ein erster Entwurf für das Gehäuse des Handgeräts erarbeitet werden. Die Auslegung des Gehäuses umfasst dabei auch die Energieversorgung, die Kommunikation mit weiteren Handgeräten und die Lage-

sensorik. Für einen Prototyp des Antennenmoduls wird zunächst eine 3D-Feldsimulation durchgeführt, das Modul anschließend gefertigt und messtechnisch charakterisiert. Zusammen mit dem detaillierten Entwurf des Gehäuses für das Handgerät soll auch die Möglichkeit einer dielektrischen Linse für das Antennenmodul mit in Betracht gezogen zu werden. Im nächsten Abschnitt erfolgen die messtechnischen Charakterisierungen des Handgeräts inklusive seiner Schnittstellen, sowie die Erprobung auf Praxistauglichkeit im Katastrophengebiet zusammen mit dem THW. Gegebenenfalls sind Anpassungen erforderlich. Zudem soll zeitgleich die Möglichkeit der Ortung von Mobiltelefonen anhand von Laufzeitmessungen der gesendeten Datenpakete untersucht werden. Hier soll nach dem Prinzip des TDOA (Time Difference of Arrival) vorgegangen werden. Als exakte Referenz wird dabei die Synchronisation der Basisstationen von Symeo verwendet. Parallel zu den beschriebenen Arbeitsvorgängen ist für eine genaue Positionsauflösung des Ortungssystems und auch für die Kombination bzw. Fusion der verschiedenen Messwerte eine durchdachte und hocheffiziente Signalverarbeitung zu entwickeln. Dabei sollen mögliche Algorithmen auf ihre Eignung und Realisierbarkeit hin untersucht und optimiert werden. Es ist vorgesehen, sowohl den Einsatz von Kalman-Filtern als auch den Ansatz mit neuronalen Netzen zu untersuchen. Die Ansätze sollen zunächst mit Hilfe von MatLab durchgeführt und anschließend in Hardware umgesetzt werden. Ein wichtiger Punkt ist dabei auch, welche Algorithmen auf welcher Hardware eingesetzt werden können. Denkbar wäre die Verwendung eines digitalen Signalprozessors für die Hauptaufgaben in Kombination mit einem FPGA, der die besonders rechenintensiven und zeitkritischen Algorithmen, wie etwa große Fouriertransformationen, übernimmt. Hierzu sollen Untersuchungen mit Hilfe von Demonstratorboards gemacht und daraus auch eine Spezifikation der digitalen Hardware erarbeitet werden. Abschließend erfolgen dann der vollständige Systemaufbau und dessen Feldtest, bei dem mehrere Handgeräte ohne Basisstationen und der Betrieb von Handgerät mit Basisstation getestet werden. Das vollständige System soll außerdem hinsichtlich seiner Ortsauflösung und Sensitivität charakterisiert werden. Abschließend soll eine simulationsgestützte Verbesserung der Ortungsgenauigkeit erreicht und erarbeitete signalverarbeitende Algorithmen implementiert werden. Abbildung 2 veranschaulicht das geplante Zusammenspiel der verschiedenen Partner in Arbeitspaket 4 und die Aufgaben des LTE. Abbildung 3 zeigt den ursprünglichen Arbeitsplan mit den dazugehörigen Meilensteinen:

- M1: Konzeption und Vorentwicklung abgeschlossen
- M2: Entwicklung und Systemintegration abgeschlossen
- M3: Systemaufbau und abschließende Feldtests

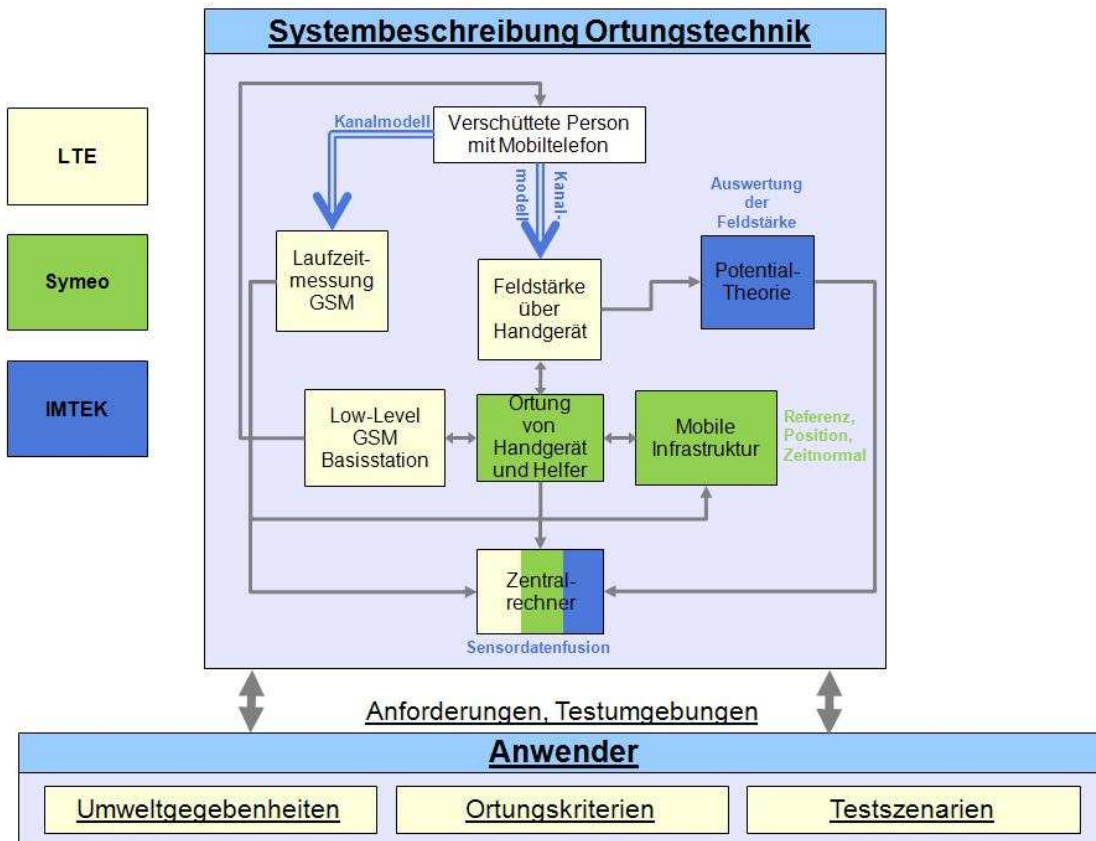


Abbildung 2: Systembeschreibung Arbeitspaket 4

Da unvorhergesehen viel Zeit investiert werden musste, um den Systemansatz (AP4-1) für eine Ortung von Mobiltelefonen und Helfern zu entwickeln und danach zu realisieren (AP4-3) haben sich leider einige Arbeitsschritte entgegen der Planung nach hinten verschoben. Eine große Herausforderung war die erfolgreiche Implementierung der Sendeaufforderung der Mobiltelefone, die für eine Ortung essentiell ist. Vor allem der Aufbau von eigenen Komponenten in AP4-3 hat hier zu Verzögerungen geführt, da wieder erwartete Baugruppen nicht kommerziell verfügbar waren. Erst nachdem diese Aufgabe gelöst war, konnte mit den darauf aufbauenden Arbeiten begonnen werden. Die bis dato durchgeführten Feldtests zeigten, dass das System sehr gut funktioniert und unsere Erwartungen erfüllt hat. Nun galt es das Handgerät für die Ortung fertig zu stellen um den letzten Meilenstein M3 (Test des Gesamtsystems) zu erreichen. Zusätzlich bedurfte der laufzeitbasierte Ortungsansatz aus AP4-5 weiterer Untersuchungen. Durch die Verlängerung der Maßnahme um sechs Monate bot sich die Möglichkeit, auch den Meilenstein M3 zu erreichen und die abschließenden Feldtests mit sehr guten Ergebnissen durchzuführen.

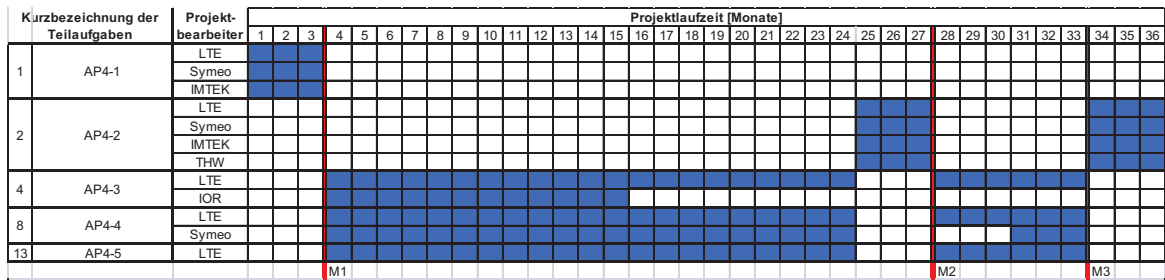


Abbildung 3: Ursprünglicher Arbeitsplan

4 Stand der Technik vor Antragstellung

Es existierte kein System zur aktiven Lokalisierung von Verschütteten mit Hilfe von mitgeführten Mobiltelefonen. Die bislang kommerziell verfügbaren Methoden zur Lokalisierung von GSM-Geräten nutzen die Zelleninfrastruktur der Basisstationen der Netzbetreiber um festzustellen in welcher Zelle sich ein Mobiltelefon befindet. Mit diesem System lassen sich Genauigkeiten in der Größenordnung von mehreren hundert Metern erreichen, was für den Einsatz zur Lokalisierung von Verschütteten völlig ungeeignet ist, zumal diese Art der Ortung ein funktionierendes GSM-Netz voraus setzt, was im Katastrophenfall oftmals nicht gegeben ist. Daneben existierten einige Systeme von Messgeräteherstellern, die dazu dienen ganze Basisstationen nachzubilden, in die sich die Mobiltelefone einbuchen und dadurch eine

völlige Kontrolle des zu ortenden Geräts möglich ist. Solche Systeme wären zwar prinzipiell für die genauere Ortung von GSM-Geräten geeignet, ihr Anschaffungspreis von mehreren hunderttausend Euro pro Gerät ist für das Technische Hilfswerk allerdings nicht finanzierbar. Zudem ergeben sich einige rechtliche Fragestellungen inwieweit man einen völligen Zugriff auf Mobiltelefone nutzen dürfte und wie man die Möglichkeiten des Missbrauchs unterbinden könnte. Der Ansatz der Ortung durch Feldstärkemessung wird in Kombination z.B. mit WLAN-Systemen bereits erfolgreich getestet. Hier kommen bisher eher einfache Verfahren zum Einsatz. Die Verwendung von autonomen, beweglichen, durch ein Referenzsystem georteten Endgeräten ermöglicht erstmals das Abtasten des Feldes an deutlich mehr Stellen. Dadurch wird die räumliche Abtastung des Feldes enorm gesteigert und wesentlich bessere Auswertemethoden z.B. aus der Potentialtheorie können verwendet werden. Die Kombination mit GSM-Geräten stellte zudem einen neuartigen Ansatz dar. Gleiches gilt für die Gewinnung von Richtungsdaten mit Hilfe von gerichteten Antennen und die Ortung über Laufzeitmessung (time difference of arrival). Diese Prinzipien werden in der Forschung z.B. beim KFZ-Radar, der Datenübertragung oder A-GPS untersucht und teilweise kommerziell eingesetzt. Die Nutzung all dieser Methoden für die Lokalisierung von GSM-Geräten stellte daher eine innovative Neuerung dar. Stand der Technik sind heute geschlossene Ortungssysteme, z.B. GPS mit den typischen GPS Signalformen, aber auch Systeme wie LPR (Symeo) oder LPM (Abatec). In allen Systemen wird innerhalb des Systems nur eine Signalform sowohl von den mobilen Einheiten als auch von den Referenzsystemen untereinander verwendet. Sämtliche Systeme beruhen auf fest eingemessener Infrastruktur (Lokalstationen oder Satelliten). Synchronisationssignale werden von diesen Systemen gar nicht oder mit unzureichender Genauigkeit zur Verfügung gestellt. Als Referenzierungssystem für die mobilen Einheiten dient ein hochsynchrones Netzwerk von autonomen Basisstationen. Hierfür sollte die bekannte Lokalisierungstechnologie der Firma Symeo dahingehend erweitert werden, dass eine autonome Selbstreferenzierung von mobilen Referenzeinheiten möglich wird, die Systeme sich also selbst einmessen und anschließend präzise synchronisieren. Auf Grund der hochgenauen Synchronisierung und Selbstreferenzierung der Stationen sind diese zudem in der Lage, den absoluten Eintreffzeitpunkt der ankommenden Handysignale hochgenau zu bestimmen. Ein solches hybrides Ortungssystem, in dem mittels spezieller Signalformen lokal synchronisiert wird, dann aber beliebige Funksignale genau im Eintreffzeitpunkt bestimmt werden können, ist völlig neu gegenüber dem Stand der Technik. Die Referenzstationen stellen zudem die Ortungsreferenzen für die mobilen Geräte dar. Hierfür wurde ein neuartiges Systemkonzept umgesetzt, welches die eigenständige Positionsbestimmung der mobilen Geräte aus den Referenzsignalen ermöglicht. Das System funktioniert nun ähnlich einem lokalen Satellitensystem, welches die Positionsbestimmung von beliebig vielen

Einheiten innerhalb der Zelle ermöglicht. Als weiterer Punkt ist das selbstständige ad-hoc Einbuchen, Kommunizieren und Positionieren der mobilen Systemeinheit zu nennen. Dafür mussten neuartige Ansätze in der Kommunikation entwickelt werden.

4.1 Referenzen

- [1] V. K. Garg, „Principles & Applications Of GSM“, Prentice Hall PTR, 1999, ISBN 0-13-949124-4.
- [2] F. Hillebrand, „GSM and UMTS The Creation of Global Communication“, John Wiley & Sons, 2002, ISBN 0470 84322 5.
- [3] K. Detken, „GSM - Der Mobilfunkstandard“, Mainz, 2007, ISBN 3-89653-221-9.
- [4] S. Redl, M. Weber, „GSM-Technik und Meßpraxis“, Franzis, 1995, ISBN 3-7723-4852-1.
- [5] J. Eberspächer, H.-J. Vögel, C. Bettstetter, „GSM Global System for Mobile Communication“, B.G. Teubner, 2002, ISBN 3-519-26192-8.
- [6] R. Weigel, Z. Zhang, and F. Seifert, „Modellierung und Simulation von Indoor-Mobilfunkfeldern im UHF-Band,“ in ITG-Workshop Antennen für Mobile Systeme, Starnberg, Germany, 1996, pp. 161-164.
- [7] G. Konstanznig, T. Pappenreiter, and R. Weigel, „Design eines vollintegrierten spannungsgesteuerten LC-Oszillators mit 1.65 mW Leistungsaufnahme im Multi-GHz-Bereich für Mobilfunksysteme der 3. Generation unter Verwendung eines 0.12 μm CMOS-Prozesses,“ in Proc. Analog, Bremen, Germany, 2002, pp. 311-316.
- [8] T. Lüftner, G. Märzinger, B. Neuraüter, R. Weigel, M. Scholz, V. Mutlu, and F. Fenk, „Fractional-N Frequenzsynthesizer für den Mobilfunk mit BiCMOS-Technologie“, in Proc. ITG-Workshop Mikroelektronik für die Informationstechnik, Darmstadt, Germany, Nov. 2000, pp. 19-22.
- [9] M. Huemer, A. Pohl, W. Gugler, A. Springer, R. Weigel, and F. Seifert, „Messung und Simulation frequenzselektiver Indoor-Mobilfunkkanäle im 2, 45 GHz ISM-Band“, in Proc. DFG-Workshops ‘Indoor-Mobilkommunikation’, Kassel, Germany, Oct. 1998, p. 117.

-
- [10] B. Sewiolo, M. Hartmann, B. Waldmann, R. Weigel, „An Ultra-Wideband Coupled-Line Balun Using Patterned Ground Shielding Structures“, IEEE Radio and Wireless Symposium, Jan. 2008.
- [11] B. Yang, M. Schoor, R. Weigel, P. Wenig, T. Schöberl, J. Hildebecher, T. Binzer & O. Brüggemann: „Radarsystemtechnik und Radarsignalverarbeitung für Automobilanwendungen“, VDE Kongress, Aachen, Oktober 2006, S. 303-307

5 Zusammenarbeit mit anderen Stellen

Der Lehrstuhl für Technische Elektronik hat im Verlauf des Projektes I-LOV insbesondere mit folgenden Projektpartnern zusammen gearbeitet:

- Symeo GmbH und Institut für Mikrosystemtechnik Freiburg (IMTEK)
Durch die enge Verzahnung der Arbeitspakete war ein Gedankenaustausch bei regelmäßigen Treffen von sehr großem Nutzen. Gemeinsame Schnittstellendefinitionen waren unerlässlich. Auch Feldtests haben LTE, Symeo und IMTEK oft zusammen durchgeführt. Auch diese gute Zusammenarbeit führte zu einem erfolgreichen Abschluss des Projektes.
- Bundesanstalt Technisches Hilfswerk (THW)
Die Zusammenarbeit mit dem THW war ebenfalls sehr fruchtbar. Zum einen half der stetige Input aus Sicht eines Anwenders die Systemkonzepte zu verfeinern und realistische Szenarien zu entwickeln. Zum anderen flossen die Wünsche zur Handhabung der Geräte direkt in den Designprozess mit ein. Desweiteren wäre eine realistische Evaluieren der erreichten Ergebnisse durch Feldtests nicht ohne die seitens des THW eigens für das Projekt angefertigten Trümmerstrukturen und Gelände möglich gewesen.
- Institut für Öffentliches Recht Freiburg (IOR)
Die Begleitforschung durch das IOR brachte sehr wertvolle Beiträge, gerade in der Phase der Systementwicklung. Auf diese Weise waren alle neuen Konzepte auch schnell rechtlich abgeklärt und einer Realisierung stand nichts im Wege.

6 Darstellung der erzielten Ergebnisse - Verwendung der Zuwendung

Im Folgenden sollen die Verwendung der Zuwendung und die erreichten Ergebnisse erläutert werden. Vorangestellt soll das entwickelte Systemkonzept stehen, das die Grundlage für alle Unterarbeitspakete des I-LOV-Gesamtsystems darstellt. Die Arbeitspakete „AP4-1 Systemspezifikation, Schnittstellendefinition“ und „AP4-2 Feldtests“ sind mit den drei Hauptunterarbeitspaketen „AP4-3 Ortung eines GSM Mobiltelefons durch selektive Feldstärkemessung“, „AP4-4 Antennen- und Gehäusekonzept“ und „AP4-5 Ortung durch Laufzeitmessung“ stark verwachsen und fließen dort jeweils mit ein.

6.1 Das Systemkonzept

GSM (Globales System für Mobilkommunikation, Engl.: Global System for Mobile Communication) wurde 1982 entwickelt und wurde zu einem weltweiten Standard. Auch wenn es mittlerweile neuere Standards wie UMTS oder LTE gibt, ist GSM noch immer mit Abstand am verbreitetsten und wird auch von nahezu allen Mobiltelefonen unterstützt. Des Weiteren hat GSM einen weiteren Vorteil gegenüber anderen Mobilfunkstandards. Es bietet ein Uplink-Band von 880 MHz bis 915 MHz, das große Vorteile bei der Durchdringung von Trümmerstrukturen gegenüber neueren, hochfrequenten Standards bietet. Die Dämpfung, die zertrümmerte Wände oder Beton verursachen, ist proportional zur Frequenz des Signals, welches sie durchdringt. Um eine MS (Mobilstation GSM, ugs.: Handy, Engl.: Mobile Station) anhand ihrer abgestrahlten Feldstärke orten zu können, muss sie als aller erstes gezwungen werden ein Signal zu senden. Dieses Signal muss wiederholbar sein, so oft wie es zu einem Ortungserfolg benötigt wird. Da das GSM-Protokoll eigentlich auch unter dem Gesichtspunkt entworfen wurde, nicht einfach ortbar zu sein, stellt dies eines der Hauptprobleme auf dem Weg zum Ortungssystem dar und wurde demnach zuerst untersucht. Abb. 4 zeigt ein Ebenenmodell des Systemansatzes. Dieser soll im Folgenden genauer erläutert werden.

6.1.1 Schritt 1: Stören aller vorhandener Mobilfunkzellen

Da das GSM-Protokoll sehr strikt ist und kaum Ausnahmen und Tricks zulässt, ist die volle Kontrolle über die MS nötig, um sie zum Senden zwingen zu können. Um dies zu erreichen,

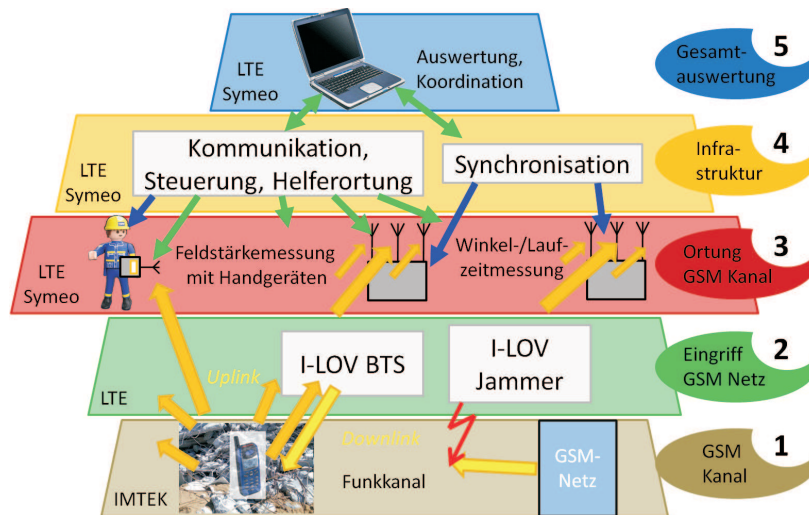


Abbildung 4: Ebenenmodell des Systemansatzes

muss eine eigene GSM-BTS (GSM-Mobilfunk-Basisstation, Engl.: Base Transceiver Station) aufgesetzt werden, in jene sich die MS korrekt einbuchen können. Allerdings buchen sich MS vorrangig in die Netze des eigenen Netzbetreibers ein, also in ein Netz, das den gleichen Network Color Code (Code zur Identifikation eines bestimmten Netzbetreibers) ausstrahlt, der auch auf der SIM-Karte (Einschubkarte in ein Mobiltelefon, die den Benutzer bei seinem Netzbetreiber identifiziert, Engl.: Subscriber Identity Module) in der MS gespeichert ist. Nur falls kein eigenes Netz zur Verfügung steht, bucht sich eine MS in ein fremdes Netz ein, um dem Nur-Notrufe-Protokoll Rechnung zu tragen. Dabei wird sichergestellt, dass im Notfall auch über einen anderen Netzbetreiber ein Notruf abgesetzt werden kann. Zu diesem Zweck kann sich jede MS mit jeder SIM-Karte bei jedem Netzbetreiber einbuchen [1].

Um der MS also den Eindruck zu vermitteln, es wäre kein anderes Netz, außer dem I-LOV Netz verfügbar, werden alle anderen Netze durch passende Jammer (Störsender) gestört. Diese Netze werden im Falle von GSM für alle MS unsichtbar, wenn der von jeder BTS ausgesendete BCCH (Downlink-Kanal in GSM, der dem Endgerät Informationen über die aussendende Zelle liefert, Engl.: Broadcast Control Channel) mit ausreichender Rauschleistung überdeckt wird. Im BCCH ist unter anderem die Information enthalten, um welchen Netzbetreiber es sich handelt und wie sich die MS auf die BTS aufsynchonisieren kann. Fehlt diese Information, ist die Zelle für eine MS nicht vorhanden. Die detaillierte Beschreibung der Störsender wird in den Kapiteln 6.4.1 und 6.4.2 erfolgen.

6.1.2 Schritt 2: Anmeldung der MS am I-LOV GSM-Netzwerk

Nachdem alle sonstigen vorhandenen GSM-Netzwerke gestört wurden, können sich die MS nur noch beim I-LOV-Netzwerk anmelden. Die MS verbinden sich nach einander damit, wo sie gelistet werden und ihnen eine beliebige Telefonnummer zugewiesen werden kann. Jede eingebuchte MS empfängt automatisch eine SMS mit dem Hinweis, dass sich ihr Handy in das Rettungsnetz eingebucht hat und Hilfe unterwegs ist. Eine detaillierte Beschreibung des GSM-Netzwerks erfolgt in Kapitel 6.5.

6.1.3 Schritt 3: Identifikation nicht von Opfern stammender MS

Es ist eine Tatsache, dass heut zu Tage Rettungseinheiten nicht nur ihren analogen und/oder digitalen Funk, wie z.B. TETRA, zur Kommunikation verwenden. Oft kommt es vor, dass solche Verbindungen abbrechen oder durch äußere Einflüsse wie z.B. Abschattung gar nicht erst zu Stande kommen. In solchen Fällen wird dann häufig der private Mobilfunk genutzt. Diese MS müssen von denen potentieller Opfer separiert werden:

- Zu erst sollten alle Personen die nicht zwingend an der Einsatzstelle benötigt werden, diese verlassen. Auch Schaulustige und die Presse sollten einen Mindestabstand von ca. 200 m einhalten. Diese Information kann wiederum über eine SMS an alle eingebuchten MS gesendet werden.
- Es ist weiterhin möglich, im Vorfeld viele der IMSI (Eindeutige Teilnehmerkennung, Engl.: International Mobile Subscriber Identity) der Mobiltelefone der Rettungsorganisationen zu sammeln. Über diese Nummern können MS exakt identifiziert werden und von der Suche bereits zu Beginn ausgeschlossen werden.
- Die dritte und mächtigste Option stellt der Einsatz des TDOA (Laufzeitdifferenz, Engl.: Time Difference of Arrival)-Ansatzes dar. Dieser wurde parallel im Projekt I-LOV (Intelligentes sicherndes Lokalisierungssystem für die Rettung und Bergung von Verschütteten) entwickelt. Hier kann eine Grobortung sehr schnell stattfinden. Darüber hinaus können sich bewegende Ziele identifiziert und damit ausgeschlossen werden können.

6.1.4 Schritt 4: Lokalisierung

Nachdem sich alle erreichbaren MS in die I-LOV BTS eingebucht haben, können diese MS nacheinander gezwungen werden ortbare Signale zu senden. Dazu gibt es mehrere Möglichkeiten die nachfolgend beschrieben werden.

Der klassische Anruf (MTC) Eine mögliche Option wäre es, einen klassischen Anruf aufzubauen. Solche Verbindungen werden MTC (Klassischer Verbindungsaufbau von BTS zu MS, Engl.: Mobile Terminated Call) genannt. Hierbei wird ein PCH (Der "Paging Channel" ist ein Downlink-Kanal in GSM der dazu dient einzelnen Endgeräten einen Verbindungswunsch des Netzes, etwa wegen eines eintreffenden Anrufs oder einer Kurznachricht, zuzustellen) geöffnet und eine messbare Kommunikation zwischen BTS und MS startet. Die MS zeigt den Verbindungsaufbau durch das Klingelzeichen, durch Vibration und/oder durch Leuchteffekte an. Falls der Anruf nicht angenommen wird, wird die Verbindung allerdings nach wenigen Klingelzeichen automatisch getrennt. Dieser Fall der automatischen Trennung wird der wahrscheinlichste sein, da sich Opfer von Hauseinstürzen kaum bewegen können oder bewusstlos sind. Dies würde eine erfolgreiche Rettung stark erschweren. Unter gewissen günstigen Umständen kann dies jedoch zu einem Ortungserfolg führen, da beispielsweise ein Klingelton lokalisiert werden kann. Dies könnte zusätzlich auch durch einen kombinierten Einsatz mit Geophonen verbessert werden.

Der modifizierte MTC (MMTC) Hier wurde die Handhabung eines MTC geändert. Das Paging resultiert nun nicht länger in einem Klingeln der MS, sondern es wird ein stabiler Kanal zwischen BTS und MS aufgebaut. Der Anruf muss nicht entgegengenommen werden, was eine Ortung von in ihrer Bewegungsfreiheit eingeschränkten oder bewusstlosen Verschütteten ermöglicht. Zudem wird die automatische Sendeleistungsregelung der MS außer Kraft gesetzt. Dies erlaubt es, die MS zu zwingen immer mit maximaler Sendeleistung zu senden. Im GSM-Standard beträgt die maximale Sendeleistung 2 W [2].

6.2 Die I-LOV BTS

Die I-LOV-BTS besteht im Wesentlichen aus den in Abbildung 5 gezeigten Komponenten. Dabei wurde der Kern der Anlage, die SDR (Per Software konfigurierbare Send- und Empfangsschaltung, Engl.: Software Defined Radio) basierte GSM-Basisstation bereits in

Kap. 6.1.2 näher erläutert. Weitere wichtige Bestandteile sind die beiden Störsender (Jammer) für GSM900 und DCS1800 einerseits und andererseits für UMTS. Die beiden Module benötigen wiederum jeweils einen Frequenzband-Scanner, der ihnen eine Liste mit vorhandenen Fremdbasisstationen übermittelt. Auf Aufbau und Funktionsweise der Störsender soll noch gesondert eingegangen werden. Zur Steuerung der einzelnen Komponenten und für die Kommunikation untereinander wird ein handelsüblicher PC verwendet. Zur Versorgung der beiden 20 W bzw. 60 W Leistungsverstärker und aller anderen Einzelmodule ist zudem eine herausfordernde Spannungsversorgungsarchitektur notwendig.

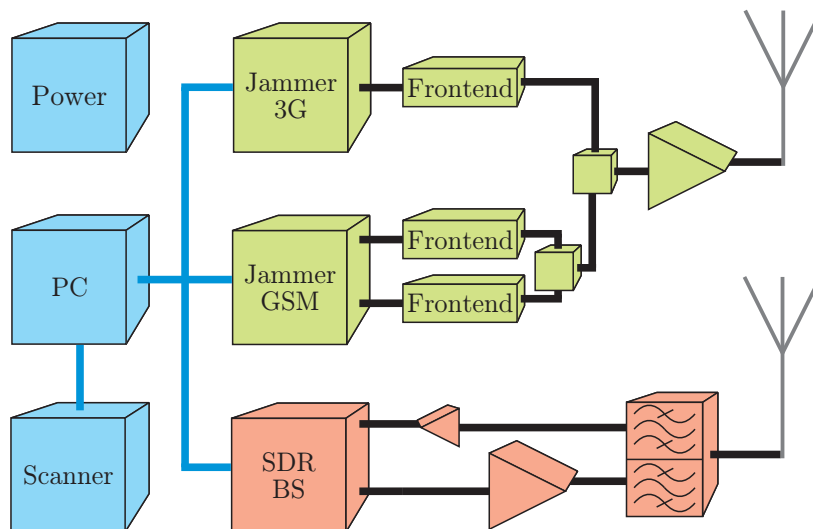


Abbildung 5: Die I-LOV BTS

6.3 Szenarios der verschiedenen Einsätze

Beim Eintreffen am Unglücksort kann das Technische Hilfswerk mit vielen verschiedenen örtlichen Gegebenheiten konfrontiert werden. Dabei sind für das I-LOV-System die drei folgenden Szenarien relevant:

6.3.1 Szenario 1

Das erste Szenario ist auch gleichzeitig das seltenste. Hier ist nach dem Schadensfall die komplette Infrastruktur der Mobilfunkbetreiber intakt. Das bedeutet alle BTS sind sendebereit und die verschütteten MS sind bei ihren jeweiligen Netzbetreibern eingebucht. Ein oder mehrere Verschüttete rufen von sich aus die Notrufnummer und rufen um Hilfe. Dieser

Fall mag selten sein, jedoch gibt es belegte Berichte über solche Meldungen von Opfern. Deshalb muss dieses Szenario selbstverständlich mit berücksichtigt werden. Da die MS in diesem speziellen Fall bereits senden, könnte man davon ausgehen, dass eine Ortung schnell möglich sein sollte. Jedoch ist der Kanal auf dem die MS sendet nicht bekannt und in den meisten Fällen wird von den Netzbetreibern ein Frequenzsprungverfahren verwendet und das Hopping-Schema ist nicht bekannt. Da eine automatische Hopping-Schema-Erkennung nicht implementiert ist (hier wäre zuerst zu klären ob dies überhaupt möglich wäre), kann eine solche sendende MS nicht per Feldstärkemessung oder dem TDOA-Verfahren geortet werden. Es muss also folgendermaßen vorgegangen werden:

- Die Verbindung der MS mit der BTS wird (evtl. nach Absetzen eines Notrufes) mit Hilfe des Störsenders unterbrochen. Falls die verschüttete Person im Vorfeld Hinweise auf ihren Aufenthaltsort geben konnte, können diese für eine grobe Vorortung verwendet werden.
- Anschließend wird die I-LOV-BTS gestartet. Die MS bucht sich ein.
- Nun kann der MMTC (Stiller Verbindungsaufbau zwischen BTS und MS mit maximaler Leistung, Engl.: Modified Mobile Terminated Call) (siehe Kap.:6.1.4) ausgelöst werden und die MS geortet werden.
- Falls ein Opfer versucht einen Notruf abzusetzen, während seine MS in der I-LOV-BTS eingebucht ist, kann der Anruf an eine andere eingebuchte MS weiter geleitet werden; z.B. an einen Vertreter der Rettungskräfte.

6.3.2 Szenario 2

Szenario 2 wird wohl am häufigsten vorgefunden werden. Hier ist die Mobilfunk-Infrastruktur ganz oder teilweise intakt. Es werden keine Notrufe aus den Trümmern abgesetzt. Die MS der Opfer sind entweder bei ihren eigenen Netzbetreibern eingebucht, über das Notrufe-Protokoll bei anderen oder aber bei keiner BTS registriert. Dies stellt den Standardfall dar:

- Die noch vorhandenen Verbindungen der MS mit den intakten BTS werden mit Hilfe des Störsenders unterbrochen.
- Anschließend wird die I-LOV-BTS gestartet. Die MS buchen sich nacheinander ein.
- Nun kann der MMTC (siehe Kap. 6.1.4) ausgelöst werden und die MS geortet werden.

6.3.3 Szenario 3

Das dritte Szenario ist ein Spezialfall von Szenario 2. Falls alle örtlichen BTS auf Grund des Schadenfalls ausgefallen sind, kann auf die Verwendung des Störsenders verzichtet werden. Alle vor Ort liegenden MS suchen eine BTS um Notrufe absetzen zu können.

- Die I-LOV-BTS wird gestartet. Die MS buchen sich nacheinander ein.
- Nun kann der MMTC (siehe Kap. 6.1.4) ausgelöst werden und die MS geortet werden.

6.4 Störsender

6.4.1 GSM-Störsender

Im folgenden soll der GSM-Störsender im Detail beschrieben werden.

Anforderungen an das Störsignal Wie bereits in Kap. 6.1.1 erklärt, ist es möglich den BCCH einer BTS zu verstecken, um eine Verbindung zu verhindern. Dies geschieht indem auf der Grundfrequenz einer BTS, auf dem auch der BCCH ausgestrahlt wird, Rauschen appliziert wird. Dabei muss der Pegel ausreichen, um den BCCH für eine MS im Zielgebiet „unsichtbar“ zu machen. Der BCCH wird auf einem der verfügbaren 200 kHz breiten Kanäle im GSM Downlink-Band (Abwärtsstrecke, von der BTS zur MS) von 925 - 960 MHz für E-GSM900 oder von 1805 - 1880 MHz für DCS1800 gesendet. Folgende Anforderungen an das Störsignal müssen erfüllt sein:

- Der BCCH von allen im Zielgebiet vorhandenen Fremd-BTS muss zuverlässig verdeckt werden.
- Gleichzeitig dürfen aber die Uplink-Frequenzen (Aufwärtsstrecke, von der MS zur BTS) von E-GSM900 keinesfalls gestört werden, da auf diesen Frequenzen später die sendenden MS empfangen und geortet werden sollen. Eine Verschlechterung des SNR (Signal- zu Rauschleistungs-Verhältnis, Engl.: Signal to Noise Ratio) auf diesen Frequenzen würde den Ortungserfolg direkt negativ beeinflussen. Die Frequenzen liegen zwischen 880 MHz und 915 MHz.

- Die Frequenz der eigenen I-LOV-BTS darf nicht gestört werden. Das bedeutet, dass immer ein Kanal für die I-LOV-BTS frei von Störeinflüssen der Jammer bleiben muss, auch wenn in direkter Frequenznachbarschaft (Dies kann bei GSM einen minimalen Abstand von Träger zu Träger von nur 400 kHz bedeuten) eine Fremdbasisstation sendet.
- Der Einzugsbereich der Störungen durch den Jammer sollte möglichst auf das Trümmfeld begrenzt sein.
- Um nicht unnötig Sendeleistung zu verschwenden, was einerseits zu höheren Energiekosten und vor allem zu deutlich höheren Kosten bei der Anschaffung der Leistungsverstärker führen würde, und zum anderen zu höheren Störungen in anderen Bändern, sollen lediglich die Kanäle gestört werden, in denen auch tatsächlich ein BCCH sendet. Dies bedeutet auch, um weiter Energie zu sparen muss jedes Störsignal auf jedem Kanal einzeln in seiner Leistung einstellbar sein.

Diese Anforderungen an das Störsignal führen zu strikten Vorgaben für die Kanalfiltermaske der einzelnen Störsignale (Abb. 6). Die Trägerfrequenz f_0 muss hierbei dem Kanal-Intervall von GSM von 200 kHz folgen können. Zusätzlich kann davon ausgegangen werden, dass zwischen zwei benachbarten BCCH immer ein Kanal frei gelassen wird. Dies ist in der GSM-Spezifikation so geregelt. Weiterhin gibt die Spezifikation eine minimale Dämpfung von 30 dB im Abstand von 200 kHz vom Träger vor. Um Telefongespräche sich in der Nähe befindlicher Personen möglichst wenig zu stören wurde dieser Wert auf 50 dB erhöht. Das stellt einen guten Kompromiss zwischen Dämpfung und Filterordnung des Bandpassfilters dar (Abb. 8).

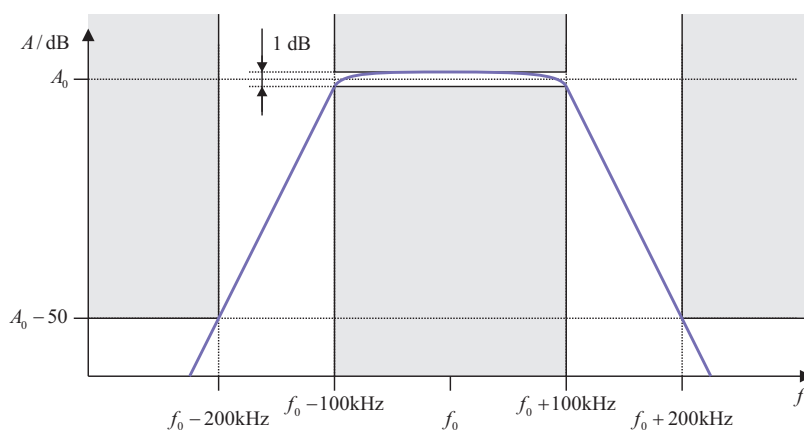


Abbildung 6: Kanalfiltermaske

Architektur des Störsenders. Nachdem verschiedene Ansätze untersucht wurden, wurde der Ansatz aus Abb. 7 gewählt. Abb. 8 zeigt vereinfacht die Signalerzeugung, wie sie auf dem FPGA implementiert wurde. Nachfolgend sollen die einzelnen Elemente aus Abb. 8 vorgestellt werden.

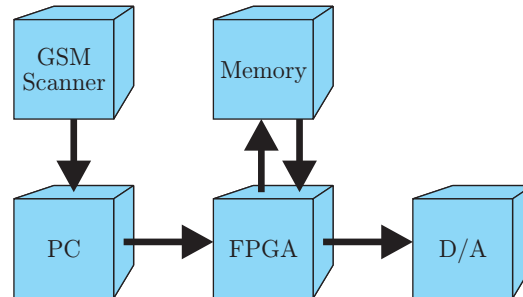


Abbildung 7: Jammer-Architektur

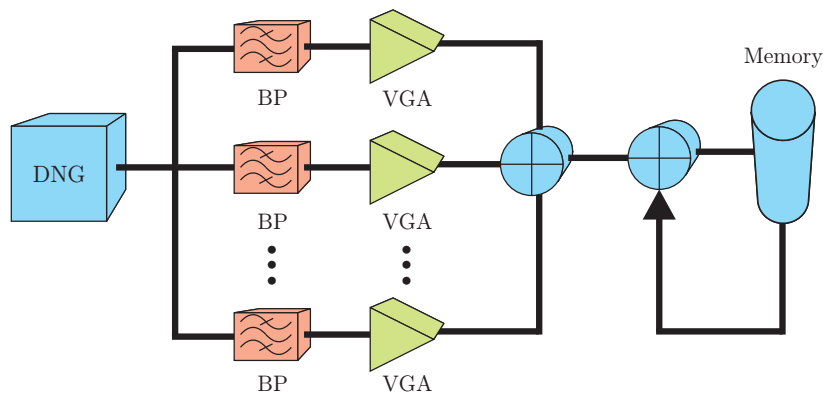


Abbildung 8: Signalerzeugung des Störsignals im FPGA

Erzeugung des Störsignals Als DNG (Digitaler Rauschgenerator, Engl.: Digital Noise Generator) wird ein Pseudo-Zufallszahlengenerator eingesetzt. Als Band-Pass-Filter wurde eine IIR (Filterarchitektur mit unendlicher Impulsantwort, Engl.: Infinite Impulse Response)-Architektur gewählt. Die Charakteristik der Sprungantwort entspricht Tschebyscheff-I Verhalten, da sie nicht unter Stopp-Band-Welligkeit leidet und gleichzeitig eine geringere Filterordnung als z.B. Butterworth-Filter besitzt. Dabei wird die geforderte Filtermaske exakt eingehalten. Abb. 9 zeigt die resultierende Filtercharakteristik aufgenommen vom FPGA (Integrierter Schaltkreis der Digitaltechnik, in den eine logische Schaltung programmiert werden kann, Engl.: Field Programmable Gate Array).

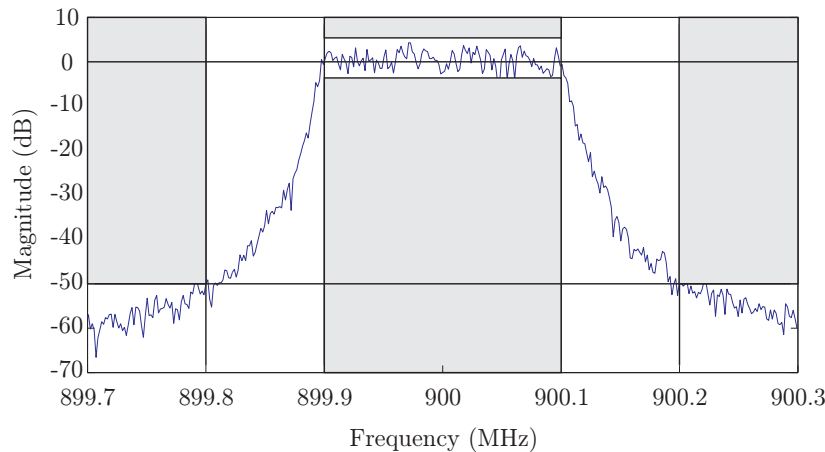


Abbildung 9: Aufgenommene Filterkurve des Bandpasses aus dem FPGA

Der Signalerzeugungsalgorithmus In diesem Kapitel sollen die einzelnen Schritte des Erzeugungsalgorithmus des Störsignals beschrieben werden.

- Zu aller erst sucht der GSM-Scanner das komplette GSM-Downlink-Frequenzspektrum nach vorhandenen sendenden BTS anderer Netzwerke ab. Die spezifische Kanalnummer und ebenfalls die gemessene Leistung des jeweiligen BCCH werden an den Steuer-PC übertragen.
- Der PC bildet die Schnittstelle zwischen dem GSM-Scanner und dem FPGA-Entwicklungsboard. Die gesammelten Daten über vorhandene BTS und Leistungslevel werden an den FPGA übertragen.
- Die Filterkoeffizienten für die einzelnen Kanalnummern sind bereits alle berechnet und im Speicher abgelegt. Das erzeugte weiße Rauschsignal wird nun von den Bandpassfiltern passend geformt, indem jeweils die zugehörigen Filterkoeffizienten geladen werden. Zusätzlich werden die VGAs (Verstärker mit variabler Verstärkung, Engl.: Variable Gain Amplifiers) passend zu den übermittelten Leistungspegeln eingestellt. Da die Anzahl der Hardwaremultiplizierer auf dem Stratix-II-FPGA begrenzt ist, können nur vier Filter gleichzeitig erzeugt werden. Falls mehr Kanäle gestört werden müssen, wird das Signal zuerst im Speicher abgelegt und im nächsten Schritt mit dem nächsten erzeugten Signal akkumuliert. Dadurch entsteht nach einigen Durchgängen das endgültige Störsignal (siehe Abb. 8).
- Nachdem das Störsignal komplett erzeugt wurde, beginnt der Jammer das Signal auszusenden. Nun sucht der GSM-Scanner erneut alle Downlink-Bänder ab. Falls neue

BTS auftauchen oder bereits gescannte BTS noch immer empfangbar sind, startet der Algorithmus von neuem. So lange bis keine BCCH mehr empfangen werden können.

Leistungseinsparung durch diesen Ansatz Verglichen mit einem Standard-Störverfahren bei dem zB. das ganze E-GSM900-Spektrum mit Rauschen überdeckt werden muss, kann der Faktor der Leistungseinsparung P_S folgendermaßen berechnet werden:

$$P_S = \frac{G \cdot \max(K_i)}{\sum_{i=1}^n K_i \cdot \delta} \quad (1)$$

K ist ein Kanal der gestört werden muss, n ist die Gesamtanzahl aller Kanäle in denen ein BCCH messbar ist, G ist die maximale Anzahl an Kanälen in einer bestimmten Bandbreite und δ ist der Kerrekturfaktor zwischen einem rechteckigen BP (Bandpassfilter) und dem real verwendeten. Im Beispiel von Abb. 12 ergibt sich P_S zu 84,29.

Komplette Hardwarerealisierung Abbildung 10 zeigt den Hardwareaufbau der I-LOV-BTS zusammen mit dem GSM-Jammer zur jetzigen Entwicklungsphase. Der GSM-Jammer passt in eine standardmäßige 19“-3HE-Schublade inklusive Spannungsversorgung der FPGA-Boards, HF (Hochfrequenz)-Frontend und der Platine zur Generation der drei benötigten LO (Lokaloszillator)-Signale. Zur Zeit werden der E-GSM900- und der DCS1800-Jammer auf zwei getrennten Boards realisiert. Zukünftig ist es angedacht diese zu einem Board zu kombinieren.

Das entwickelte Front-End ist in Abb. 11 zu sehen. Das Rauschsignal für E-GSM900 wird direkt verarbeitet. Das digital-analog konvertierte Signal wird zweimal tiefpassgefiltert um die spektralen Wiederholungen, die bei der Konvertierung entstehen, um 80 dB zu dämpfen. Das ist wichtig, da diese Spektralanteile das GSM-Uplinkband und andere Kommunikationsbänder stören würden, falls sie in die HF-Lage hoch gemischt würden. Außerdem muss sichergestellt werden, dass so wenig wie möglich zusätzliches Rauschen in die Uplink-Bänder eingefügt werden. Dies würde das SNR verschlechtern und eine Ortung erschweren. Nachdem das Störsignal in die HF-Lage konvertiert wurde, wird das entstandene Spiegel-Signal durch einen BP weitestgehend entfernt. Darauf folgend werden beide Störsignale, also E-GSM900 und DCS1800, kombiniert und einem Leistungsverstärker zugeführt. Eine breitbandige Antenne mit Richtwirkung wird für die Ausstrahlung des Störsignals verwendet.



Abbildung 10: Hardwareaufbau der I-LOV BTS mit dem GSM-Jammer

Die Antenne hat einen Antennengewinn von 7 dBi. Da die das DCS1800 Band eine Bandbreite von 75 MHz auf weist, die ADC (Analog-Digital-Umsetzer, Engl.: Analog to Digital Converter) aber nur eine limitierte Abtastrate von maximal 160 MSpS zur Verfügung stellen, könnten so die spektralen Wiederholungen nur unzureichend gefiltert werden. Ihr Abstand zum Hauptspektrum des Signals wäre zu gering. Deshalb wurde das DCS1800 Band in zwei Teile aufgeteilt, zu jeweils einer Breite von 40 MHz. Das 40 MHz breite Grundsignal muss nun sowohl die Störanteile der unteren als auch der oberen Hälfte des Spektrums enthalten. Danach wird das Signal doppelt in die HF-Lage gemischt, direkt neben einander. Dadurch wird etwas Leistung verschwendet, da jetzt einige Kanäle gestört werden, die nicht gestört werden müssten. Diese Vorgehensweise ist aber trotzdem weit sparsamer als das gesamte Band mit Rauschen zu belegen.

Messungen und Feldtest Verschiedene Messungen der Performanz der Jammer-Module wurden durchgeführt. Abbildung 12 zeigt das Leistungsdichtespektrum eines Beispielstörsignals im E-GSM900-Downlink-Band. Es ist klar erkennbar, dass jeder beliebige Leistungspegel zwischen dem Rauschteppich und ca. -55 dBm (vor den Verstärkern im Frontend) möglich ist. Weiterhin ist ersichtlich, dass die Rauschleistung, wo es möglich ist, um die geforderten 50 dB pro 100 kHz abfällt. Die Anforderungen aus Kapitel 6.4.1 werden also voll erfüllt.

Des Weiteren wurden einige Feldtests durchgeführt. Hierfür wurden auf einem alten Bundeswehr-Trainingsgelände von THW (Bundesanstalt Technisches Hilfswerk)-Helfern Trümmerstruk-

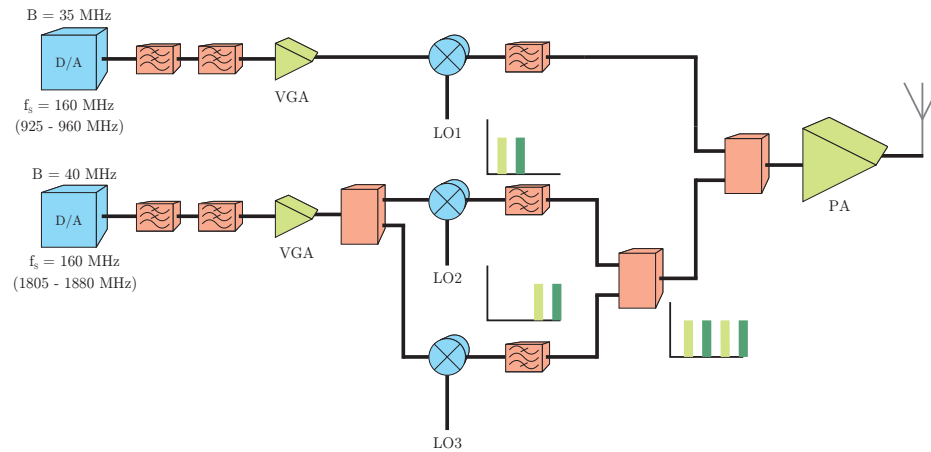


Abbildung 11: Das Frontend des GSM-Jammers.

turen zum Testen aufgebaut. Dabei wurde auch ein Reichweite-Test mit voller Leistung durchgeführt. Mit einem 10 W PA (Leistungsverstärker, Engl.: Power Amplifier) wurde eine etwa kreisförmige Fläche mit einem Radius von 220 m erfolgreich gestört (siehe Abb. 13).

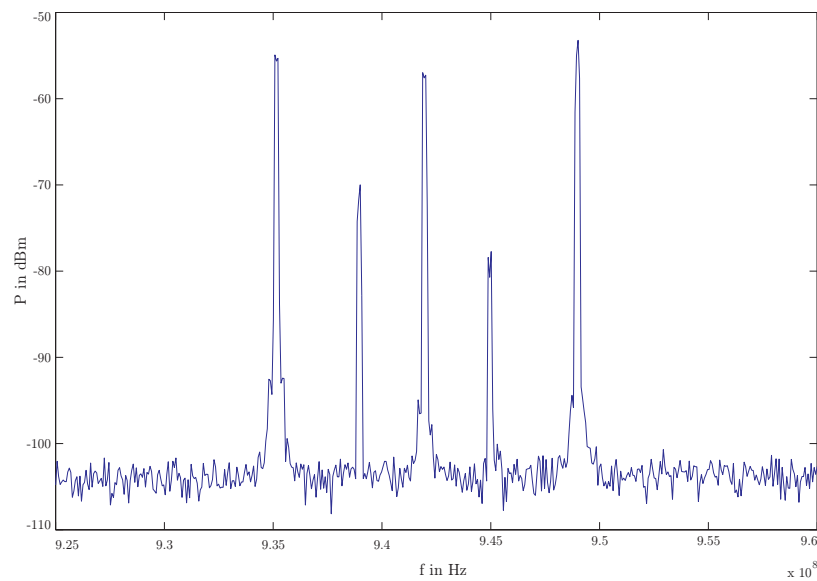


Abbildung 12: Messung eines erzeugten Beispiel-Störsignals im E-GSM900-Band.

6.4.2 UMTS-Störsender

Da fast 100% aller neuen mobilen Endgeräte den UMTS (Mobilfunkstandard der dritten Generation, Engl.: Universal Mobile Telecommunications System)-Standard unterstützen,



Abbildung 13: Extrapolierte gestörte Fläche mit einem 10 W PA.

muss für einen zuverlässigen Betrieb des I-LOV-Systems gewährleistet werden, dass sich trotzdem alle MS an der I-LOV-BTS anmelden. UMTS ist bei neueren Geräten das Standard-System. Sie melden sich nur im GSM-Netz an, wenn kein UMTS-Netz verfügbar ist. Dies bedeutet, es wird ein Jamming-System benötigt das alle MS (bzw. UE (Mobilstation UMTS, ugs.: Handy, Engl.: User Equipment)) zwingt, ihre UMTS-Zelle zu verlassen und GSM zu priorisieren. „Selektive Interferenzeinspeisung“ soll die neu eingeführte Jamming-Strategie für UMTS-Mobilfunk im folgenden genannt werden.

Grundlagen der selektiven Interferenzeinspeisung Der Wechsel einer MS von der UMTS-Netzarchitektur (UTRAN (UMTS-Netzwerkern bestehend aus Basisstationen und dazugehörigen Controllern, Engl.: Universal Terrestrial Radio Access Network)) zur GSM-Netzarchitektur (GERAN (GSM Netzwerkern bestehend aus Basisstationen und dazugehörigen Controllern, Engl.: GSM EDGE Radio Access Network)) wird „Inter-Radio-Access-Technology Handover“ oder kurz „iRATH“ genannt. Ein solcher Wechsel wird ausgelöst, wenn bei einer der regelmäßig ausgeführten Qualitätsmessungen des UE oder bereits beim Versuch des Einbuchens in einer Zelle das Qualitätsmerkmal S_{Qual} wie folgt verletzt wird:

$$S_{Qual} = Q_{Qualmeas} - Q_{Qualmin} \stackrel{!}{>} 0, \quad (2)$$

mit

$$Q_{Qualmeas} = 10 \cdot \log_{10} \left(\text{CPICH} \frac{E_c}{I_0} \right) \quad (3)$$

und

$$-24 \text{ dB} \leq Q_{Qualmin} \leq 0 \text{ dB}. \quad (4)$$

$Q_{Qualmeas}$ stellt also das Verhältnis Chip-Energie E_c im CPICH (Gemeinsamer Pilotkanal einer UMTS-Zelle, Engl.: Common Pilot Indicator Channel) zur gesamten Interferenz der Zelle I_0 dar. I_0 setzt sich aus fremdinduzierter Interferenz I_f erzeugt durch Nachbarzellen, aus eigeninduzierter Interferenz I_e erzeugt durch weitere Kanäle neben dem CPICH und dem Grundrauschen \mathcal{N}_0 zusammen:

$$I_0 = I_f + I_e + \mathcal{N}_0. \quad (5)$$

$Q_{Qualmin}$ kann maximal den Wert des Spreizgewinns $10 \log_{10}(SF) = 10 \log_{10}(256)|_{\text{CPICH}} = 24 \text{ dB}$ auf $Q_{Qualmeas}$ aufaddieren. Dieser Zusammenhang zwischen Spreizgewinn und $Q_{Qualmin}$ legt eine weitere Betrachtungsweise nahe:

Auf Grund der Interferenz die sich die Zellen gegenseitig und selbst einspeisen, wird der Spreizgewinn benötigt, um überhaupt eine stabile Kommunikation in der Zelle zu gewährleisten. Wird $Q_{Qualmin} < 0$ gesetzt, wird ein Teil des Spreizgewinns z.B. für eine höhere Netzabdeckung aufgewendet; also eine größere Interferenz I_0 in Kauf genommen.

Abb. 14 veranschaulicht die Messung der Qualitätsgrößen in einem UMTS-Empfänger.

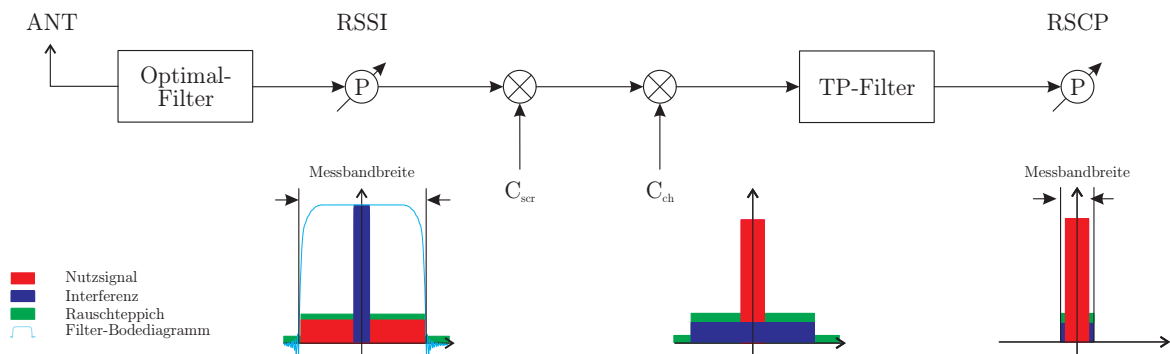


Abbildung 14: Messung der Qualitätsgrößen in einem UMTS-Empfänger

Der RSSI (Gesamte empfangene Leistung inkl. Rauschen in einem Kanal, Engl.: Received Signal Strength Indicator) wird direkt nach dem Empfangsfilter gemessen, während der RSCP (Leistung eines entspreizten Kanals; auch Nutzleistung, Engl.: Received Signal Code Power) nach der Multiplikation mit Spreiz- und Scramble-Code ermittelt wird. Diese

Größen werden laut [3] in Abständen zwischen 5.12 s und 0.64 s zyklisch ermittelt. Eine Veränderung der Qualitätsmerkmale einer Zelle wirkt sich also umgehend aus. Wird keine Empfangs-Antennendiversität eingesetzt, berechnet sich $Q_{Qualmeas}$ zu [3]

$$Q_{Qualmeas} = 10 \cdot \log_{10} \left(\text{CPICH} \frac{E_c}{I_0} \right) = 10 \cdot \log_{10} \left(\frac{\text{CPICH RSCP}}{\text{RSSI}} \right). \quad (6)$$

Aus (6) und Abb. 14 wird klar, an welcher Stelle UMTS angreifbar ist. Wird der RSSI mit zusätzlicher Interferenz innerhalb der Kanalbandbreite angehoben, kann das Verhältnis in (6) so weit verringert werden, dass S_{Qual} aus (2) verletzt wird. Dadurch wird die Zelle vom UE nicht länger als funktional angenommen und ein iRATH wird ausgelöst. Zusätzlich zu betonen ist die Tatsache, dass der UMTS-Standard an diesem Punkt in der Empfangskette keinen weiteren Vorteil aus dem Spreizgewinn ziehen kann, da der RSSI vor der Entspreizung gemessen wird.

Implementierung und Realisierung in Hardware Das System wurde vorrangig für den europäischen Raum entworfen, in dem das WCDMA (Breitband-Codemultiplexverfahren, Engl.: Wideband Code Division Multiple Access)-Band I verwendet wird. Es deckt den Bereich zwischen 2110 MHz und 2170 MHz ab. Eine Anpassung an die Bänder II, IV, V und VI ist mit kleinen Änderungen des HF-Front-Ends problemlos möglich. Diese Bänder sind ebenfalls 60 MHz breit oder schmäler. Nur der LO und die Bandpassfilter müssten angepasst werden. Lediglich Band III ist mit 75 MHz zu breit um ohne Änderungen der Signalerzeugung komplett abgedeckt zu werden. Abb. 16 zeigt die Signalerzeugungshardware bis in die HF-Lage, Abb. 15 den Aufbau im I-LOV-Rack.

Digitale Störsignalerzeugung Im ersten Schritt kann wie bereits in Kap. 6.4.1 für GSM geschildert, auch das UMTS-Spektrum nach vorhandenen Node B (UMTS-Mobilfunk-Basisstation, Engl.: Base Transceiver Station) gescannt werden. Im Gegensatz zum GSM-Jammer wurde jedoch für UMTS eine etwas andere Vorgehensweise zur Störsignalerzeugung gewählt. Die komplexwertigen Rausch-Störsignale werden auf einem PC mit Hilfe einer graphischen Benutzeroberfläche durch digitale Filterung von Zufallszahlenfolgen erzeugt. Dabei entsteht ein Störsignal mit der Bandbreite $-30 \text{ MHz} \leq f_{\text{Basisband}} \leq 30 \text{ MHz}$. Komplexe Signale haben den Vorteil, dass ihr Spektrum nicht symmetrisch sein muss und Information getrennt im Real- und Imaginärteil enthalten sein kann. Daher ist es möglich, die nötige Bandbreite auf 30 MHz zu reduzieren, was wiederum die benötigte Abtastfrequenz der ADCs auf dem FPGA verringert bzw. die Anforderungen an die Anti-Aliasing-Filter des HF-Front-Ends reduziert.



Abbildung 15: Aufbau des UMTS-Jammers im I-LOV-Rack: 1) FPGA-Signalgenerator; 2) Abtastakterzeugung; 3) ADU-Adapterplatine; 4) HF-Frontend.

Grundsätzlich wird immer ein 10 ms langer Frame digitaler Daten wiederholt, denn reale UMTS-Kanäle basieren ebenfalls auf 10 ms-langen Frames. Auf diese Weise ist es mit diesem System auch möglich komplexere Informationen zu generieren, die konform mit dem UMTS-Standard sind. Diese Möglichkeit soll in dieser Arbeit außen vor gelassen werden. Mehr Informationen zu standardkonformen Jammingstrategien kann in [4] gefunden werden.

Da UMTS einen Chiptakt von $R_C = 3.84 \text{ Mcps}$ aufweist, liegt es nahe ein ganzzahliges Vielfaches als Abtastrate zu nutzen:

$$f_s = 16 \cdot 3.84 \cdot 10^6 \frac{1}{s} = 61,44 \text{ MHz}. \quad (7)$$

Um die Anforderungen an die analogen Rekonstruktionsfilter noch weiter zu verringern,

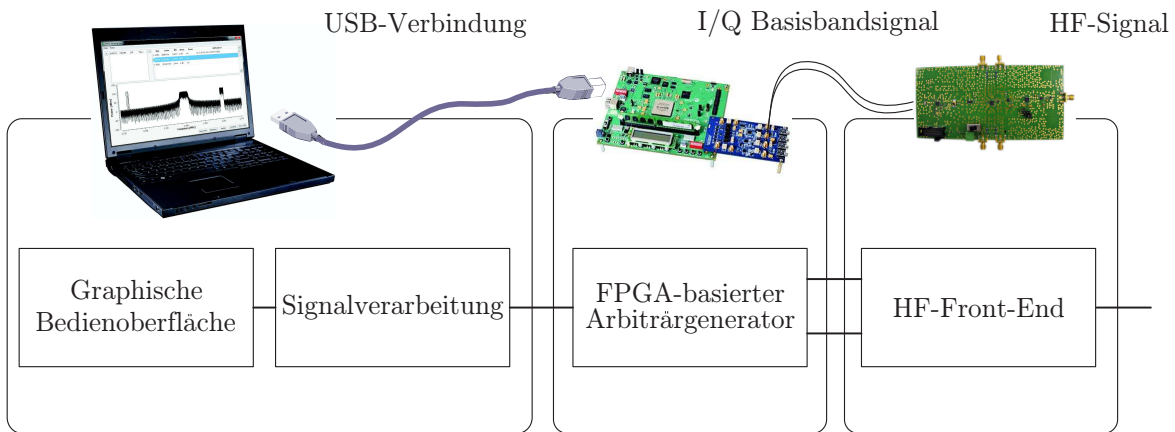


Abbildung 16: Signalerzeugungshardware

wird zusätzlich auf dem FPGA digital die Abtastrate um den Faktor 4 erhöht. Durch diese Maßnahme wird der Abstand der spektralen Wiederholungen auf

$$4 \cdot 61,44 \text{ MHz} - 60 \text{ MHz} = 185,76 \text{ MHz} \quad (8)$$

erhöht und somit die benötigte steilflankigkeit der Filter verringert, bzw. die Dämpfung der spektralen Wiederholungen wird bei konstanter Filtercharakteristik erhöht.

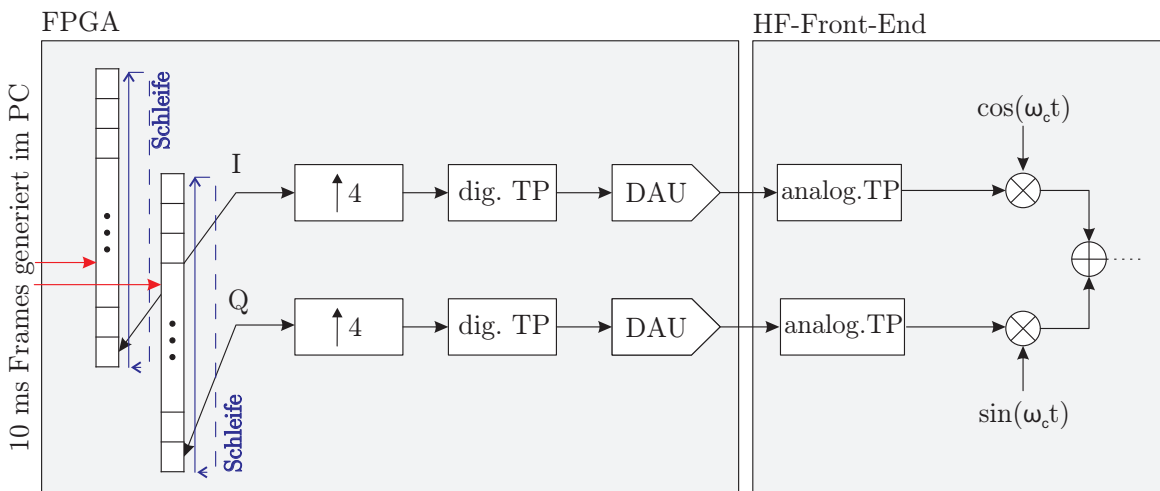


Abbildung 17: Weiterverarbeitung des im PC generierten Störsignals

Das UMTS-HF-Front-End Als Sendearchitektur wurde direkte IQ-Konversion gewählt. Die Vorteile gegenüber einem mehrstufigen Konzept liegen vor allem in den geringeren Anforderungen an die Bandpassfilter (siehe Abb. 18) hinter dem Mischer, da die spektralen

Wiederholungen erst bei der doppelten Lokaloszillatorfrequenz auftauchen, die in diesem Fall deutlich höher liegt. Zusätzlich fällt der Zwischenfrequenzweig weg, was Komplexität, zusätzliche Bauteile und somit Kosten und Energie einspart. Das Blockschaltbild der gewählten Architektur ist in Abb. 18 zu sehen, die Hardwarerealisierung zeigt Abb. 16.

Als Rekonstruktionsfilter für den I - und den Q-Pfad kommt jeweils ein differentielles passives LC-Tiefpassfilter fünfter Ordnung zum Einsatz. Das Filter wurde mit Hilfe der Design-Software „Agilent Advanced-Design-System“ und den S-Parameter-Modellen der Firmen Murata (Kapazitäten) und Würth (Induktivitäten) entworfen. In Abb. 19 ist zum einen ein Vergleich zwischen Simulation und Messung der Filter, und zum anderen die Mischer-Testplatine bestückt mit den Filtern, zu sehen. Die Kombination aus PA_1 , Dämpfungsglied A und PA_2 liefert eine variable Verstärkung zwischen 8 dB und 39 dB. Damit kann der darauf folgende 20 W-Leistungsverstärker optimal angesteuert werden. Auf diese Weise kann die Ausgangsleistung maximiert und gleichzeitig Störungen in anderen Bändern auf Grund von Übersteuerung des PA vermieden werden.

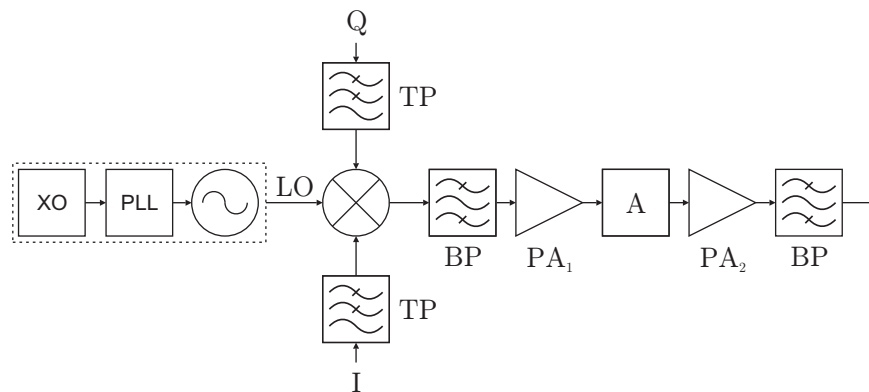


Abbildung 18: Blockschaltbild des UMTS-HF-Front-Ends

Messergebnisse Die Funktionalität wurde sowohl im Labor, als auch im Feldversuch überprüft und bestätigt. Abb. 20 zeigt ein beispielhaftes Störsignal für einen Kanal bei 2120 MHz. Ersichtlich ist zum einen die maximale Ausgangsleistung vor dem PA von -5 dBm und zum anderen eine Unterdrückung von LO und Spiegelfrequenz von 20 dBm bzw. 35 dBm.

Der Messaufbau zur Verifikation der selektiven Interferenzeinspeisung aus Kap. 6.4.2 ist in Abb. 21 zu sehen. Dabei wird ein Rohde&Schwarz CMU200 verwendet um eine Node B möglichst realistisch zu emulieren. Das Störsignal wird über einen Leistungskombinierer zusammen mit den Node B-Signalen über den externen Antennenanschluss an ein UE angeschlossen. Das UE bietet die Möglichkeit auf einem angeschlossenen PC alle Meldungen auf Protokollebene mitzuverfolgen. So kann genau gemessen werden, wann das UE die

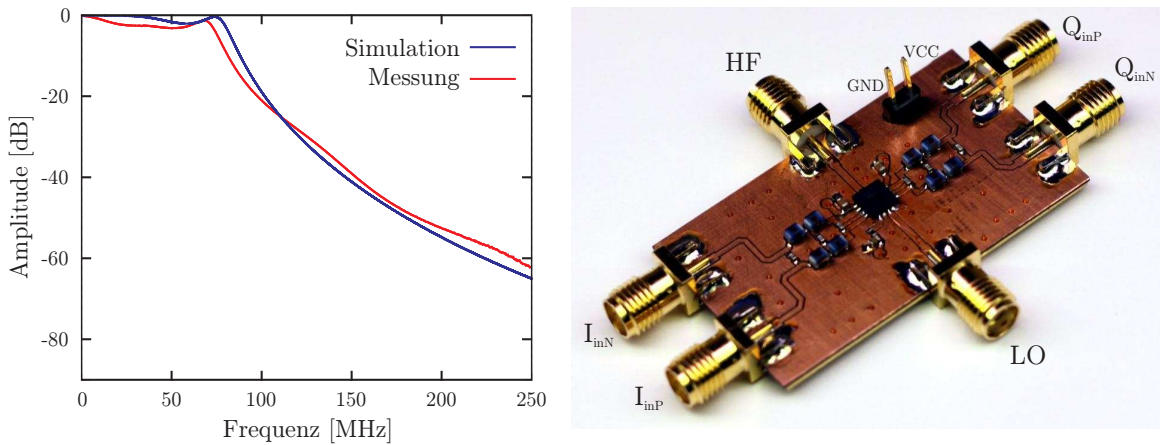


Abbildung 19: Vergleich zwischen Simulation und Messung des Tiefpassfilters (l) und Mischer-Testplatine mit Filtern (r)

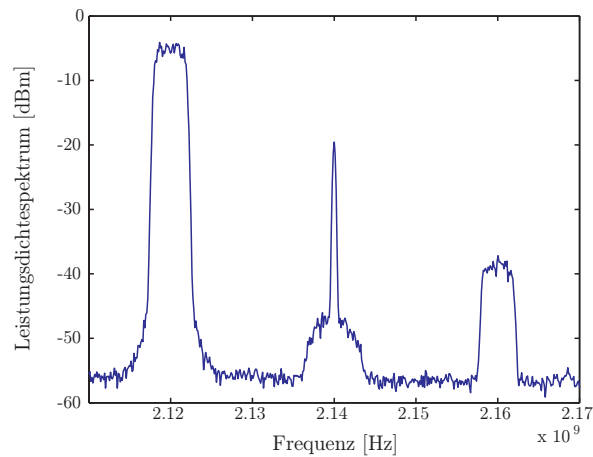


Abbildung 20: HF-Störsignal für einen Kanal bei 2120 MHz

Node B als nicht mehr verfügbar erachtet und versucht einen Handover zu starten. Mehrere Iterationen der Tests wurden durchgeführt. Mit einem $Q_{Qualmin} = -24$ dB war eine mittlere Störsignalleistung von -38 dBm notwendig um eine Zellrelektionsprozedur im UE auszulösen. Wurde $Q_{Qualmin}$ um 9 dB auf $Q_{Qualmin} = -15$ dB erhöht, verringerte sich die mittlere nötige Jammer-Leistung erwartungsgemäß um 9 dB. Die Messung erzeugt also plausible Ergebnisse.

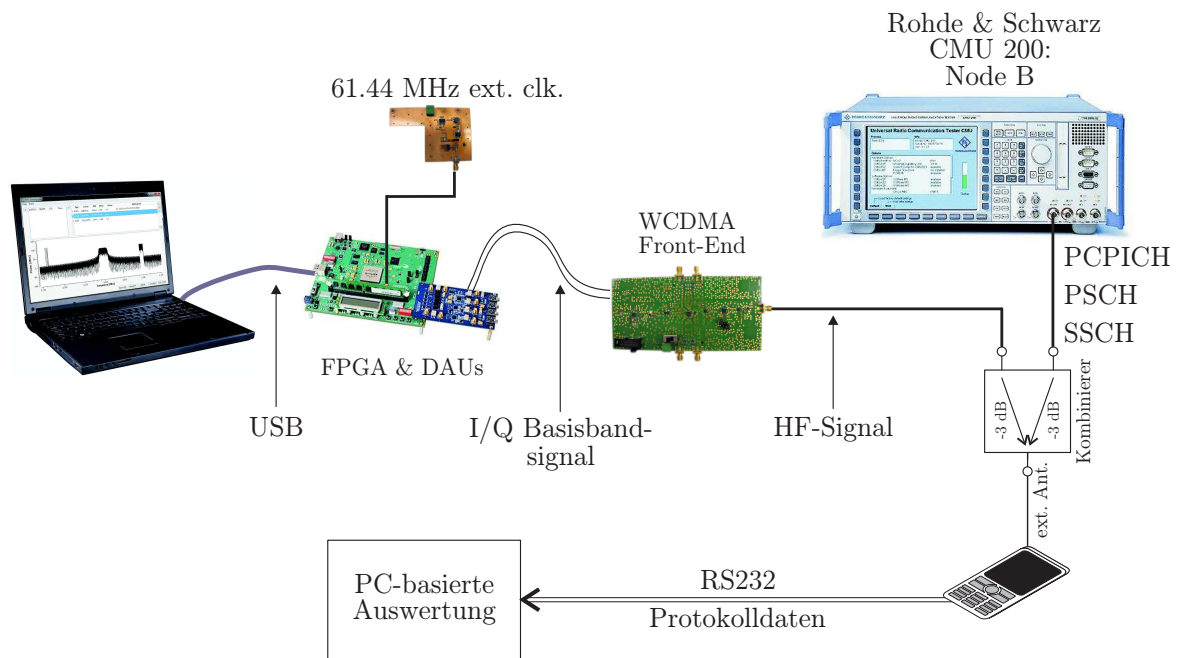


Abbildung 21: Messaufbau zur Verifikation der selektiven Interferenzeinspeisung aus Kap. 6.4.2

6.5 Das I-LOV GSM-Netzwerk

6.5.1 Systemaufbau

Um ein Mobiltelefon gezielt zum Senden aufzufordern, ist es notwendig, Kontrolle über das Telefon zu erlangen. Am besten dafür geeignet ist ein eigenes GSM-Netzwerk welches im Rahmen des Projekts entwickelt wurde. Da alle Mobiltelefone unabhängig vom jeweiligen zugehörigen Netzbetreiber geortet werden sollen, nutzt das Netz nicht die Netzkennung eines existierenden Betreibers, sondern eine neutrale Netzkennung. Das hat jedoch zur Folge, dass sich zunächst kein Telefon registriert.

Der Störsender (Jammer) ist nun dafür zuständig, den Mobiltelefonen im relevanten Bereich den Empfang der kommerziellen Basisstationen zu unterbinden. Sobald ein Telefon keine Basisstation seines Heimnetzes mehr empfangen kann, registriert es sich auch in einem unbekanntem Netz. Dieses Vorgehen ist durch den GSM-Standard festgelegt um jederzeit die Möglichkeit eines Notrufs sicherzustellen.

Für das eigene Mobilfunknetz wurde aus folgenden Gründen GSM900 ausgewählt:

- Jedes zur Zeit erhältliche Mobiltelefon unterstützt den GSM Standard und kann infolge dessen mit dem Netz kommunizieren,
- Das 900 MHz Band hat aus allen Mobilfunk-Frequenzbändern die am wenigsten beeinträchtigtsten Ausbreitungseigenschaften in Trümmerstrukturen und ist damit für die Ortung am besten geeignet,
- GSM ist der einfachste zu emulierende Standard.

6.5.2 Hardware

Im Folgenden werden die Hardwarekomponenten für den Betrieb des GSM-Netzes erläutert. Die einzelnen Komponenten sind in Abbildung 22 in Form eines Blockschaltbilds dargestellt.

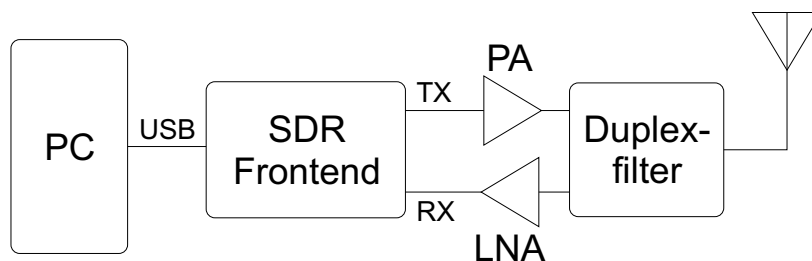


Abbildung 22: Hardwareaufbau als Blockschaltbild

Antenne Das I-LOV GSM-Netzwerk soll wenn möglich nur im Bereich der Unglücksstelle beziehungsweise in einem begrenzten Gebiet zur Verfügung stehen. Um dies zu ermöglichen, kommt hierfür eine Antenne zum Einsatz, deren Abstrahl-/ Empfangscharakteristik sehr stark gerichtet ist. Aufgrund von Reflexionen und stark unterschiedlichen Dämpfungen ist es jedoch unmöglich, einen klar definierten Bereich für das GSM-Netzwerk zu realisieren.

Leistungsverstärker Der maximale Radius der GSM-Zelle wird unter anderem durch die Ausgangsleistung bestimmt. Damit zum einen die Reichweite möglichst flexibel ist und zum anderen auch mit Mobiltelefonen in großer Tiefe kommuniziert werden kann, wird ein Leistungsverstärker (PA) eingesetzt. Die eigentliche Leistungsregelung erfolgt durch die Vorverstärker.

Duplexfilter Für den Betrieb einer GSM-Basisstation ist es notwendig, nahezu gleichzeitig Senden und Empfangen zu können. Für beide Betriebsfälle ist es zusätzlich auch wünschenswert nur eine Antenne einzusetzen.

Die Verbindung der Antenne mit dem Sender und dem Empfänger wurde deshalb mit Hilfe eines Duplexfilters realisiert. Dieses hat die Aufgaben, empfangene Signale aus dem GSM-Uplink-Frequenzbereich an dem Empfänger weiterzuleiten und Signal vom Sender im GSM-Downlink-Frequenzbereich an die Antenne weiterzuleiten. Dadurch wird vermieden, dass der Sender den Empfänger stören kann.

Transceiver Der Transceiver besteht im Wesentlichen aus einer SDR-Plattform (Software Defined Radio) (USRP (Universal Software Radio Peripheral)), die über USB mit einem PC verbunden wird. Vor dem Empfänger wurde zusätzlich ein LNA (Rauscharmer Verstärker, Engl.: Low Noise Amplifier) verbaut. Dieser trägt im Wesentlichen dazu bei, die Reichweite der Basisstation zu erhöhen.

Den Kern des USRP bildet ein FPGA, auf dem Pufferung, Interpolation und Deziemierung realisiert sind. Weiterhin sind zwei Mixed-Signal Front-End ICs (Integrierte Schaltungen, Engl.: Integrated Circuits) verbaut um das HF-Signal zu generieren beziehungsweise zu verarbeiten. Das FPGA und die Front-End ICs sind durch Digital-Analog-/ Analog-Digital-Konverter verbunden.

Als Interface zum Steuerrechner dient eine USB 2.0 - Schnittstelle. Über die Schnittstelle laufen die Basisbanddaten, die im FPGA verarbeitet werden.

Der Aufbau des Transceivers ist in Abbildung 23 zu sehen.

Taktversorgung Der GSM-Standard erfordert eine hochgenaue Taktversorgung. Tests haben gezeigt, dass Mobiltelefone bei einer einfach ausgeführten Taktversorgung sehr schnell die Verbindung zur Basisstation verlieren. Deshalb wurde in der Basisstation ein 52 MHz OCXO (beheizter Quarzoszillator mit Temperaturregelung, Engl.: Oven Controlled Crystal Oscillator) verbaut, wodurch eine stabile Kommunikation sichergestellt ist.

Die Realisierung der Basisstation in einem 19-Zoll-Rack ist in Abbildung 24 zu sehen. Das Duplexfilter befindet sich auf der Rückseite. Der mit „BTS“ bezeichnete Einschub enthält die SDR-Plattform, den Steuerrechner und die Taktversorgung.

6.5.3 Software

Für die Emulation des GSM-Netzes wurde ein Open-Source GSM-Protokoll-Stack als Basis herangezogen. Der verwendete Software Stack ist fähig, alle wichtigen Schritte zur Erzeugung und Prozessierung von GSM-Signalen durchzuführen:

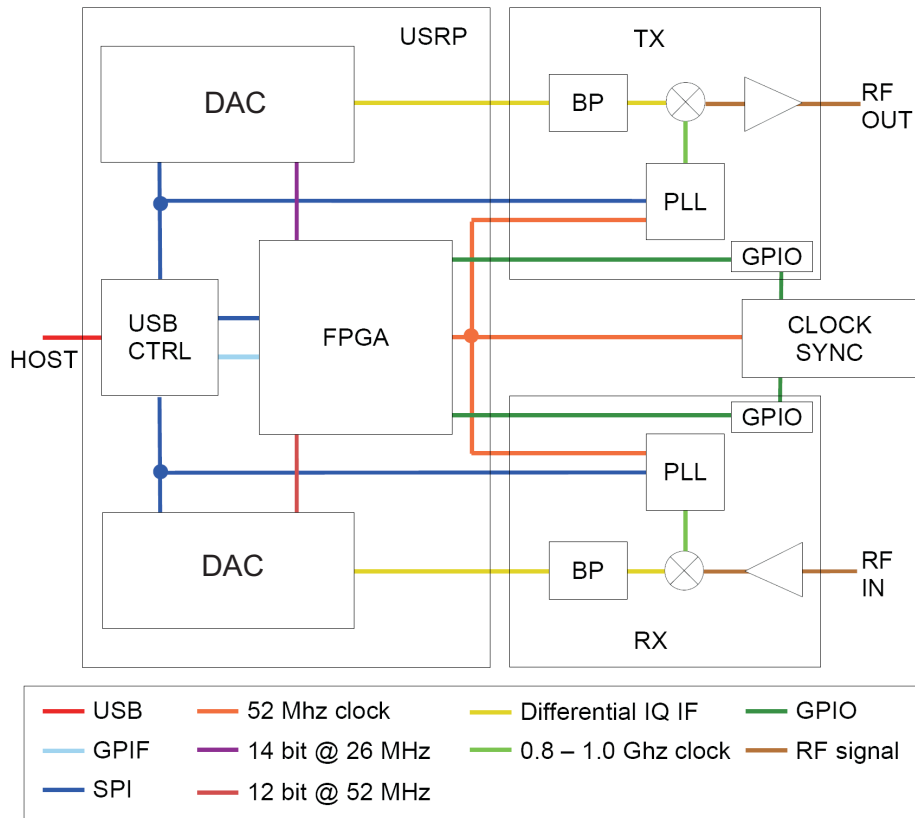


Abbildung 23: Aufbau des SDR Transceivers

- Konvertierung von Signalisierungs- und Sprachdaten zu GSM-Protokoll konformen Bursts (Eine begrenzte Anzahl von Schwingungen fixer Frequenz),
- Modulation und Demodulation dieser Bursts,
- Synchronisierung mit der TDMA (Zeitmultiplexverfahren, Engl.: Time Division Multiple Access)-Rahmenstruktur.

Für den Einsatz des GSM-Stacks für die vorliegende Anwendung, mussten jedoch einige Modifikationen vorgenommen werden. Beispielsweise mussten der modifizierte MTC (aus Kapitel 6.1.4) und die Möglichkeit des „Frequency Hoppings“ (Engl.: Frequenzsprungverfahren) (siehe Kapitel 6.9.2) implementiert werden.

Der wichtigsten Software-Komponenten die zum Einsatz kommen und deren Zusammenhang sind in Abbildung 25 dargestellt. Der Asterisk Server ist für Registrierung und die Verwaltung der angemeldeten Mobiltelefone zuständig. Zusätzlich ermöglicht er es auch,



Abbildung 24: Realisierung der Basisstation

Telefongespräche mit Mobiltelefonen zu führen, war im Katastrophenfall sehr nützlich sein kann. Die Sprachdaten werden hierfür mit Hilfe von Voice-over-IP transportiert.

6.5.4 Einsatz in der Praxis

Das GSM-Netzwerk wurde in einer Reihe von Feldtests im Verlauf des Forschungsprojekts ausgiebig erprobt. Zum einen haben sich dabei sehr viele Hinweise auf Verbesserungsmöglichkeiten ergeben, die jeweils daraufhin noch implementiert wurden. Zum anderen hat sich jedoch deutlich gezeigt, dass mit Hilfe des GSM-Netzwerks die Ortung von Mobiltelefonen ermöglicht wird. Die Ortung funktioniert darüber hinaus unabhängig vom Typ des Mobiltelefons.

Sobald sich ein Mobiltelefon im I-LOV GSM-Netzwerk registriert, bekommt es zur Bestätigung eine SMS (Kurznachricht mit ursprünglich 256 Zeichen, Engl.: Short Message Service) zugeschickt. Ein Beispiel für eine derartige SMS ist in Abbildung 26 zu sehen.

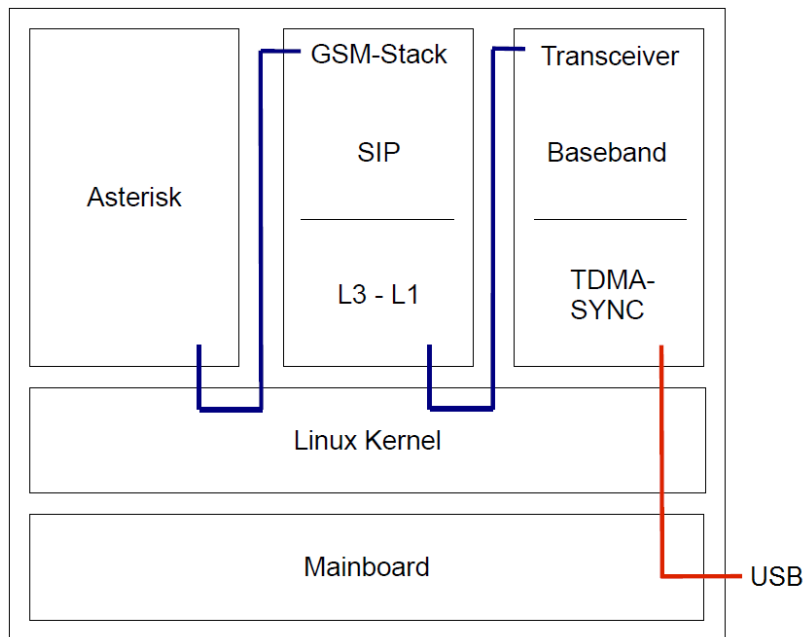


Abbildung 25: Aufbau des SDR Transceivers

6.6 Die Steuereinheit

Sowohl die GSM-Basisstation als auch die Störsender müssen koordiniert und gesteuert werden. Hierfür ist im Rahmen des Projekts eine Software entstanden, die diese Aufgabe übernimmt. Die einzelnen Softwarekomponenten sind in Abbildung 27 zu sehen.

Die Steuersoftware umfasst folgende Aufgaben und Möglichkeiten:

GSM Scanner Der GSM Scanner hat die Aufgabe, die vorhandenen GSM- und UMTS-Netzwerke in der Umgebung zu scannen. Zum einen werden diese Daten an die jeweiligen Störsender weitergeleitet und zum anderen wird die Sendefrequenz der I-LOV Basisstation so gewählt, dass dort die Störungen, sowohl von anderen Basisstationen als auch von den Störsendern, minimal werden.

Die Abfrage der Basisstationsliste kann in der Benutzeroberfläche überwacht werden (Abbildung 28).

Jammer Die Störsender (Jammer) können direkt aus der Benutzeroberfläche gesteuert werden. Dies ist in Abbildung 29 zu sehen. Die Daten werden entweder von Hand eingegeben oder vom GSM-Scanner übernommen. Zusätzlich kann man die Störleistung auf den einzelnen Frequenzen bezüglich der Empfangsleistung an der Messposition

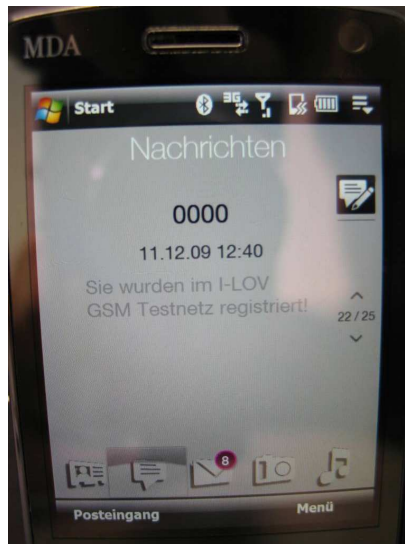


Abbildung 26: Empfang der Willkommens-SMS

bestimmen. Dadurch wird erreicht, dass beispielsweise die Frequenzen von näherliegenden Basisstationen (und mit daraus folgendem höherem Empfangspegel) stärker gestört werden als weiter weg liegende.

GSM-Basisstation Für die Ortung ist es wichtig, die einzelnen Mobiltelefone zu kategorisieren und gezielt zum Senden bringen zu können. Über die Benutzeroberfläche kann man direkt sehen wie viele und welche Mobiltelefone an der Basisstation angemeldet sind (Abbildung 30). Zusätzlich kann die Sendeleistung über einen Drehregler bestimmt werden.

Über die Benutzeroberfläche können je nach Bedarf Telefonnummern vergeben werden, man kann SMS verschicken, man kann die Telefone zum Senden bringen (MMTC) und die gesamte Kommunikation überwacht werden.

D-Bus Die Steuersoftware ist in zwei Teilkomponenten aufgeteilt, der „Daemon“ und der „Controller“. Die Verbindung der beiden Komponenten ist durch das D-Bus Protokoll realisiert. Dadurch wird erreicht, dass beide Teile auf unterschiedlichen PCs betrieben werden. Beispielsweise kann die Steuerung des gesamten Systems auf einem Laptop, der über WLAN verbunden ist, gemacht werden.

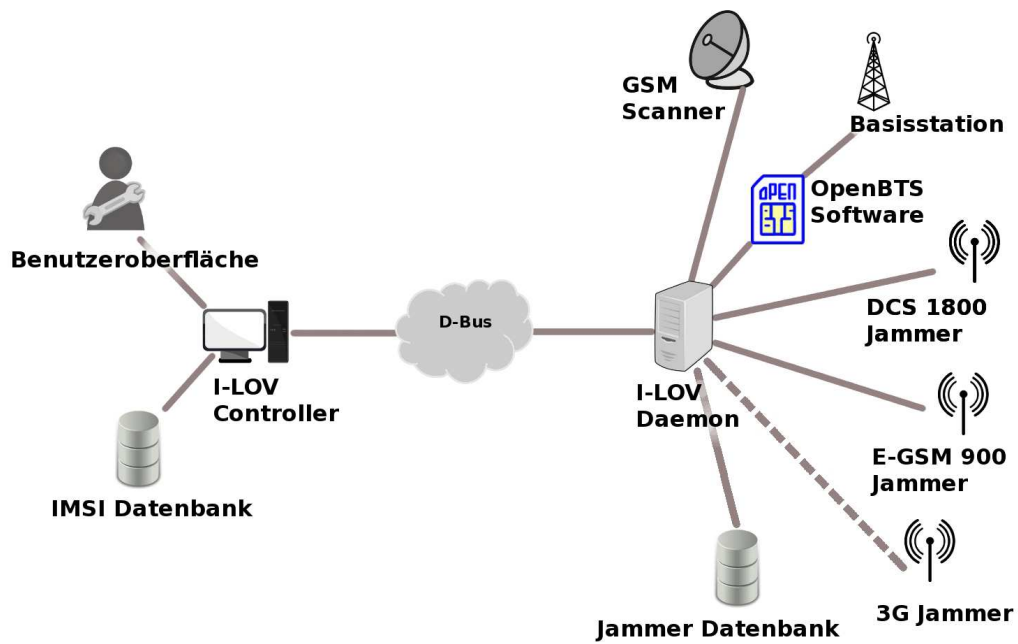


Abbildung 27: Komponenten der Steuereinheit

Das Screenshot zeigt die Benutzeroberfläche des I-LOV Controller. Die Oberfläche ist in mehrere Bereiche unterteilt:

- Reset**: Ein Button zum Zurücksetzen der Anwendung.
- Navigation**: Tabs für Basisstation, Scanner und GSM Jammer.
- Scanner Liste anzeigen**: Ein Button zum Anzeigen der Scanner-Liste.
- Scanner-Liste**: Eine Tabelle mit den folgenden Spalten: arfcn, power (dBm), bs id code, ber, mcc, mnc, lac, cell ID.
- Message Log**: Ein Bereich für Debug- und Warning-Nachrichten.
- Filter**: Checkboxes für Debug, Warning, Critical und Fatal.
- DBus Services**: Ein Textfeld mit dem Wert "controller".
- Beenden**: Ein Button zum Beenden der Anwendung.

arfcn	power (dBm)	bs id code	ber	mcc	mnc	lac	cell ID
997	-86	0	0	262	3 (e-plus)	9127	54847
996	-87	0	0	262	3 (e-plus)	9127	2527
993	-80	0	0	262	3 (e-plus)	9127	0
991	-84	0	0	262	3 (e-plus)	9127	5427
989	-87	0	0	262	3 (e-plus)	9127	54807
988	-83	0	0	262	3 (e-plus)	9127	5437
987	-86	0	0	262	3 (e-plus)	9127	0
984	-81	0	0	262	3 (e-plus)	9127	0
983	-81	0	0	262	3 (e-plus)	9127	0
982	-89	0	0	262	3 (e-plus)	9127	51777
981	-88	0	0	262	3 (e-plus)	9127	21337
95	-85	0	0	262	1 (T-Mobile)	17440	9931
88	-77	0	0	262	1 (T-Mobile)	17440	41247
86	-86	0	0	262	1 (T-Mobile)	17440	4109

Message Log:

```

daemon(debug): gsm::tellit::ScannerDevice: waiting on results.
controller(warning): waiting for scanner result, that could take some time ...
daemon(debug): gsm::tellit::ScannerDevice: Reading results. gsm::tellit::ScannerDeviceThread(0x1061258)
daemon(debug): gsm::tellit::ScannerDevice: Interpreting Results.
daemon(debug): gsm::tellit::ScannerDevice: scanner list updated
controller(debug): starting to update scanner list view

```

no Connection

Abbildung 28: Benutzeroberfläche - GSM-Scanner

6 Darstellung der erzielten Ergebnisse - Verwendung der Zuwendung

Controller About Hilfe

Reset

Basisstation Scanner GSM Jammer

Jammer starten

Liste an Jammer senden

Jammer-Liste von Scanner updaten

Power Offset zu Scanner Liste: 40 dB

	arfcn	power	uplink	downlink
1	1	-26	890,2	935,2
2	6	-7	891,2	936,2
3	8	-25	891,6	936,6
4	12	-11	892,4	937,4
5	15	-27	893	938
6	21	-21	894,2	939,2
7	24	-19	894,8	939,8
8	26	-44	895,2	940,2
9	27	-21	895,4	940,4

Tabelle aktualisieren

Änderungen in Datenbank übernehmen

Änderungen rückgängig machen

Datenbank leeren

Message Log:

```
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: waiting on results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: Reading results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: Interpreting Results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: scanner list updated
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: waiting on results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: Reading results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: Interpreting Results.
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: scanner list updated
I-LOV-Daemon(debug): gsm::telit::ScannerDevice: waiting on results.
```

Debug Warning Critical Fatal

DBus Services: I-LOV-Controller

no Connection

Beenden

Abbildung 29: Benutzeroberfläche - Störsender

Controller About Hilfe

Reset

Basisstation Scanner GSM Jammer

Basisstation beenden

Leistung:

-44 dBm

eingeloggte Telefone:

imsi

262074997313246

262032733222985

001012345678903

001012345678902

Telefon lautlos anrufen SMS senden

Message Log:

```
daemon(debug): gsm::lftte::cm::BTS::onBSProcStdout: "1319034227.0552 NOTICE 139925366126336 MobilityManagement.cpp:449:HandoverController: Handover initiated!"
daemon(debug): gsm::lftte::cm::BTS::onBSProcStdout: "1319034227.5957 WARN 139925364795136 GSML2LAPDm.cpp:579:receiveUFrameSABM: obj: 0x7f42e403bab0 reestablishment not really supported"
daemon(debug): gsm::lftte::cm::BTS::onBSProcStdout: "1319034227.7345 NOTICE 139925366126336 MobilityManagement.cpp:466:HandoverController: Got message: RR 0x28 cause=(0x3)"
daemon(debug): gsm::lftte::cm::BTS::onBSProcStdout: "1319034227.8955 NOTICE 139925366126336 MobilityManagement.cpp:449:HandoverController: Handover initiated!"
daemon(debug): gsm::lftte::cm::BTS::onBSProcStdout: "1319034228.4361 WARN 139925364795136 GSML2LAPDm.cpp:579:receiveUFrameSABM: obj: 0x7f42e403bab0 reestablishment not really supported"
```

Debug Warning Critical Fatal

DBus Services: controller

basestation started

Beenden

Abbildung 30: Benutzeroberfläche - GSM-Netzwerk

6.7 Der Feldstärke­sensor

Im nächsten Abschnitt wird der Entwurf und der Aufbau eines auf die Feldstärkeortung von Mobiltelefonen im 900 MHz - Band optimierten Sensors erläutert werden. Sowohl die Anforderungen an einen solchen Sensor als auch der Entwurf, die Realisierung in Hardware und die Messtechnische Charakterisierung wird dabei genauer betrachtet. Anschließend wird anhand von Erfahrungen im Feldtest die Praxistauglichkeit bewertet.

Anforderungen Um die Anforderungen eines solchen Sensors besonders im Hinblick auf die nötige Mindestdynamik festzulegen, wurde ein Standardszenario entwickelt. Die Schadenslage soll eine Fläche von $100\text{m} \times 100\text{m}$ betragen. Da aber das Rettungspersonal das Trümmerfeld betreten kann (z.B. auch über Seile aus der Luft) wird die maximale Entfernung des Sensors von der MS zu $d = 10\text{m}$ festgelegt. Die Sendeleistung einer MS wird wie bereits in Kap. 6.1.4 erläutert auf die maximale Leistung von $P = 33\text{dBm}$ bzw. 2W eingestellt. Die Standard-Frequenz wird etwa in die Mitte des GSM900 - Uplink - Bandes auf 900MHz gesetzt. Die Wellenlänge λ beträgt dann $0,333\text{m}$. Der Antennengewinn G_S der MS sollte keine große Richtcharakteristik aufweisen. Da zudem nicht auf Herstellerspezifika Rücksicht genommen werden kann wird $G_S = 1$ gesetzt, die Handyantenne also als isotroper Kugelstrahler angesehen. Als Empfangsantenne wird die Richtantenne HE300 der Firma Rohde&Schwarz verwendet. Diese bietet einen Antennengewinn G_E von 17dBi (Faktor $50,1$) und die in Abb. 31 gezeigte Antennencharakteristik.

Mit Hilfe der Friis-Gleichung, die auch Freiraumformel genannt wird, lässt sich nach Gl. 9 die Empfangsleistung P_E in Abhängigkeit von der Entfernung d berechnen [5]:

$$P_E = P_S \left(\frac{\lambda}{4\pi d} \right)^2 G_S G_E \quad (9)$$

P_S stellt dabei die Sendeleistung, λ die Wellenlänge und G_S bzw. G_E jeweils die sender- und empfängerseitigen Antennengewinne dar. Das Übertragungsdämpfungsmaß in dB lässt sich dann anhand folgender Formel errechnen [5]:

$$L[\text{dB}] = -10 \log \left(\frac{P_E}{P_S} \right) \quad (10)$$

Für die empfangene Leistung ergibt sich demnach:

$$P_E = 2\text{W} \left(\frac{0,333\text{m}}{4\pi 10\text{m}} \right)^2 50,1 = 704\mu\text{W} (-1,5\text{dBm}) \quad (11)$$

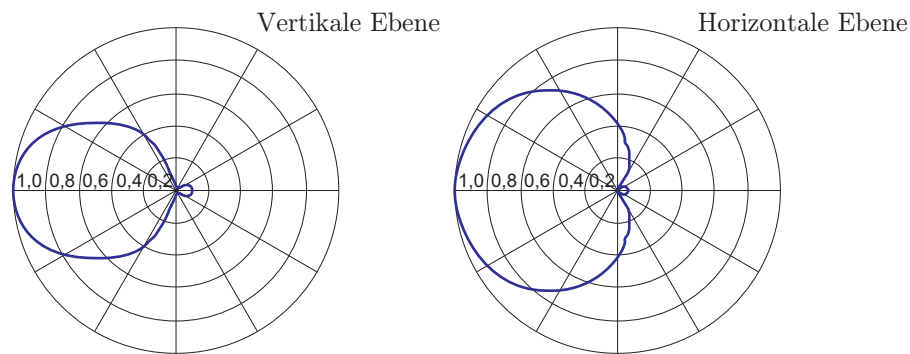


Abbildung 31: Antennencharakteristik R&S HE300 (500-7500 MHz)

und nach Gleichung 10 eine Freiraumdämpfung von 34,5 dB.

Zusätzlich zur Freiraumdämpfung muss eine Abschätzung der Verluste durch die Trümmer entwickelt werden. Natürlich kann kein Modell für jede Schadenslage angegeben werden. Im Folgenden soll als Standardszenario eine Person unter einem zweistöckigen Gebäude eingeschlossen worden sein. In diesem Fall liegen unter anderem Mauerblöcke, Dachziegel, zwei Deckenplatten und die Dachsparren über der Person.

Für die Deckenplatten wird jeweils der Wert des 30,5 cm dicken Betons angenommen. Da die Baumaterialien nach einem Einsturz nicht gestapelt übereinander liegen, gibt es auch Hohlräume und Spalte. Deshalb werden für die Mauern einmalig der Dämpfungswert der 40,6 cm breiten Mauerblöcke, für die Dachziegel 26,7 cm dicke Ziegelsteine und für die Dachsparren zweimal Holz mit 7,6 cm Dicke verwendet [6]. Daraus resultiert für den Bau-schutt alleine eine Dämpfung von

$$2 \cdot 35 \text{ dB} + 17 \text{ dB} + 7 \text{ dB} + 2 \cdot 2,8 \text{ dB} = 99,6 \text{ dB}. \quad (12)$$

Zusammen mit der Freiraumdämpfung ergibt sich das Gesamtübertragungsdämpfungsmaß zu 134,1 dB. Es ist zu beachten, dass dies die Dämpfung bis hinter die Empfangsantenne darstellt bzw. bis zum Eingang der Messschaltung. Berücksichtigt man die Sendeleistung von 33 dBm der MS kann nun eine benötigte Sensitivität des Sensors von -101,1 dBm ermittelt werden. Geht man weiterhin von einer maximalen Empfangsleistung von 5 dBm aus berechnet sich der notwendige Dynamikbereich zu 106,1 dBm. Allerdings sind 5 dBm als maximale Eingangsleistung vorsichtig geschätzt. Nachträgliche Messungen im Labor zeigen eher einen Wert von -5 dBm bis 0 dBm. Und dies auch nur, wenn die MS direkt vor der Antenne liegt. Außer dem großen Dynamikbereich und der hohen Sensitivität gilt es noch folgende Anforderungen zu berücksichtigen:

- Alle 174 200 kHz breiten E-GSM-Uplink-Kanäle zwischen 880 MHz und 915 MHz müssen einzeln gemessen werden können.
- Der Sensor sollte klein, handlich und leicht sein.
- Die Akku-Leistung sollte einen langen Betrieb ermöglichen.
- Das Gehäuse sollte witterungsunempfindlich und stabil sein.

Aufbau Unter Berücksichtigung aller genannten Voraussetzungen, wurde das in Abb. 32 gezeigte System entwickelt. Im folgenden sollen die einzelnen Komponenten vorgestellt werden und ihre Realisierung erläutert werden.

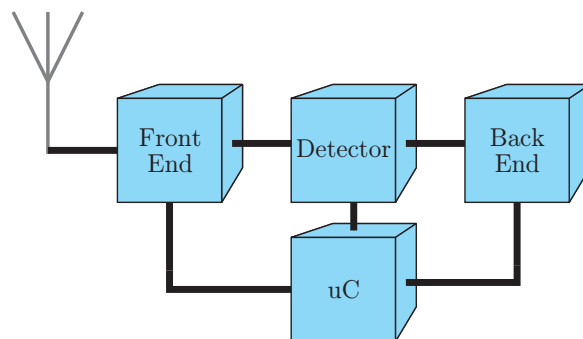


Abbildung 32: Grundlegende Architektur des Feldstärkesensors

Frontend Abbildung 33 zeigt die einzelnen Komponenten des Frontends im Detail. Die Richtantenne ist, wie in Kapitel 6.7 angegeben, die R&S@HE300. Auf Seite 50 ist deren Antennencharakteristik abgebildet.

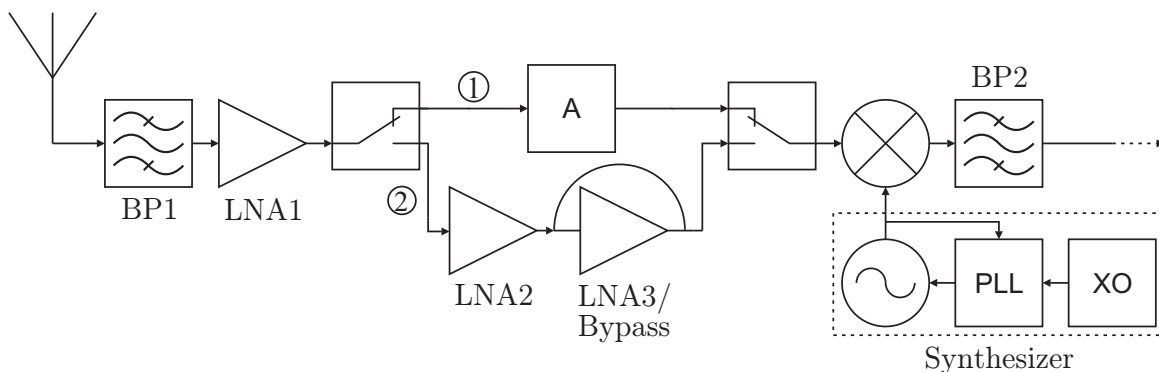


Abbildung 33: Schematische Darstellung des Frontends

Die Signalkette startet nach der Richtantenne mit dem Bandpassfilter BP1. Es besteht aus einer Kaskade aus zwei SAW (Akustische Oberflächenwelle, Engl.: Surface Accoustic Wave) - Filtern mit exakt der Bandbreite des GSM900-uplink-Bandes. Es kann theoretisch passieren, dass auf Kanal 975 (925,2 MHz) eine BTS sendet, die dann gestört werden muss. Um so genanntes Blocking (Desensibilisierung des Systems durch einen starken Störer) zu verhindern wird unter Verwendung der Kaskade immerhin eine Dämpfung von 34 dB in einem Abstand zur Eckfrequenz von 10 MHz erreicht. Das Filter BP1 verursacht eine Einfügedämpfung von 3,8 dB was zwar die Rauschzahl verschlechtert, aber notwendig ist um besagte Blockingszenarios zu vermeiden.

LNA1 liefert eine Verstärkung von 18 dB bei einer Rauschzahl von nur 0.37 dB und einen IIP3 (Maß für die Nichtlinearität von Übertragungsgliedern, Engl.: Third Order Input Intercept Point) von 37 dB bei 900 MHz. Da das Leistungsmessgerät einen sehr großen Dynamikbereich abdecken muss und selbst monolithische Detektoren keinen so großen Leistungsumfang verarbeiten können, muss der Signalpegel des Eingangssignals über einen gewissen Bereich verändert werden können. Ein einziger starker Verstärker kann allerdings nicht verwendet werden, da dies zum einen den Dynamikbereich nicht verändert, sondern ihn nur verschiebt, und zum anderen zu einer Zerstörung der nachfolgenden Bauteile führen kann. Nach LNA1 teilt sich der Signalpfad also in zwei bzw. drei verschiedene Pfade auf. Die Rauschzahl des jeweiligen Pfades kann mit der Friis-Formel abgeschätzt werden [7]:

$$F_{ges} = F_1 + \frac{F_2 - 1}{G_1} + \frac{F_3 - 1}{G_1 G_2} + \dots + \frac{F_N - 1}{G_1 G_2 \dots G_{N-1}} \quad (13)$$

Die Pfadumschaltung ermöglicht eine schrittweise Erhöhung der Verstärkung:

- Pfad ① ist für Signale größer als -30 dBm bestimmt. Hier ist das SNR hoch und es ist wichtig zu verhindern, dass der IIP3 eines nachfolgenden Bauteils (z.B. des Mischers) erreicht wird, oder dass ein Signal den Detektionsbereich verlässt. Deshalb beinhaltet Pfad ① ein zusätzliches Dämpfungsglied. Ein Wert für die Dämpfung von 7 dB hat sich bewährt.
- Pfad ② muss alle Signale zwischen dem Rauschteppich (Dieser liegt bei Raumtemperatur und 200 kHz Bandbreite bei -121 dBm) und -30 dBm verarbeiten. Daher wird ein zweiter LNA in die Signalkette eingefügt, der weitere 18 dB Verstärkung beisteuert. Diese Einstellung wird für Eingangsleistungen zwischen -65 dBm und -30,1 dBm verwendet. Für den letzten Sektor (-121 dBm bis -65.1 dBm) kann ein dritter LNA hinzugeschaltet werden. LNA3 liefert im eingeschalteten Zustand eine Verstärkung

von 19,9 dB bei einer Rauschzahl von 0,7. Im Überbrückungsmodus erzeugt LNA3 eine Dämpfung von 2 dB.

Die Aufgabe des Handgerätes ist es, die empfangene Leistung einer sendenden MS zu messen. Dazu muss aus dem gesamten E-GSM 900 Frequenzbereich der Kanal heraus gefiltert werden, auf dem das Mobiltelefon sendet. Dies erfordert ein sehr steilflankiges und schmalbandiges Filter. Für hohe Frequenzen ist dies nur schwer realisierbar. Deshalb kann kein variables Filter verwendet werden, um den Kanal zu selektieren, da diese bei 900 MHz keine ausreichende Güte aufweisen. Aus diesem Grund werden die E-GSM 900 Frequenzen mittels eines Mischers herabgesetzt und anschließend auf der niedrigeren ZF (Zwischenfrequenz) gefiltert. Es werden 133,2 MHz als ZF gewählt, da hierfür bereits ein GSM-Kanalfilter kommerziell erhältlich ist und die Detektorschleife bei dieser Frequenz einen großen Dynamikbereich und eine hohe Empfindlichkeit aufweist. Mit der Zwischenfrequenz kann nun auch der nötige Lokaloszillator-Frequenzbereich berechnet werden. Es sind 174 Frequenzen erforderlich, da die einzelnen E-GSM 900 Kanäle auf eine feste Frequenz heruntergemischt werden können müssen. Für die beiden äußersten Frequenzen ergibt sich:

$$\begin{aligned} 880,2\text{MHz} - 133,2\text{MHz} &= 747\text{MHz} \\ 914,8\text{MHz} - 133,2\text{MHz} &= 781,6\text{MHz} \end{aligned} \quad (14)$$

Zur Erzeugung der Lokaloszillatorfrequenz für den Mischer wird ein Synthesizer verwendet. Dieser besteht aus einem VCO (Spannungsgesteuerter Oszillator, Engl.: Voltage Controlled Oscillator) und einer PLL (Phasenregelschleife, Engl.: Phase-locked loop). Als äußere Beschaltung müssen lediglich das Schleifenfilter und ein Referenzoszillator angeschlossen werden. Auf diese Weise können die Frequenzen von 746 MHz bis 781,6 MHz variabel erzeugt werden. Dies ist in 200 kHz-Schritten nötig, da das dem Kanalabstand von E-GSM 900 entspricht.

Detektorschleife Die Aufgabe der Detektorschleife ist die Erzeugung einer Gleichspannung, die über einen möglichst großen Dynamikbereich proportional zur Eingangsleistung in dB ist. Jene ist in Abb. 34 dargestellt. Die eigentliche Umsetzung führt der Detektor aus. Der VGA dient zur Erweiterung des Dynamikbereichs. Dazu wird der Verstärker über eine Rückkopplung mit einer Spannung gesteuert, die umgekehrt proportional zu der Ausgangsspannung des Detektors ist. Die nötige Anpassung dieser Spannung übernimmt ein Subtrahierer.

Um eine Messgenauigkeit von ± 1 dB im geforderten Temperaturbereich zu erreichen, müssen die zu messenden Leistungen am Eingang des Detektors zwischen -59 dBm und +4,5 dBm

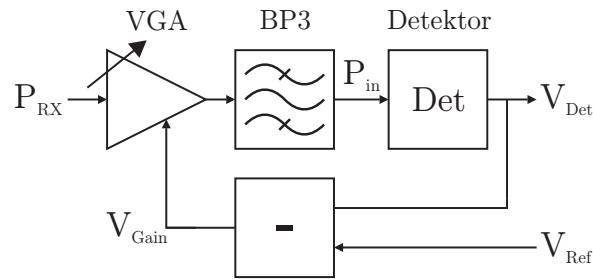


Abbildung 34: Detektorschleife

liegen. Dies ergibt für den Detektor alleine einen linearen Dynamikbereich von 63,5 dB. Der Bandpass BP3 wird zum einen benötigt, um durch Nichtlinearitäten im VGA entstandene Intermodulationsprodukte (z.B. IMD, IP3, HD) wieder zu entfernen. Noch wichtiger ist es aber möglichst viel Rauschleistung um den Nutzkanal herum heraus zu filtern. Der Detektor ist sensitiv für Eingangsfrequenzen von 1 MHz bis 4 GHz und würde die gesamte Rauschleistung in diesem Frequenzbereich auf integrieren. Dies würde zu einer deutlichen Verringerung der Empfindlichkeit des Systems führen. Für BP3 wurde eine π -Struktur sechster Ordnung verwendet. Der gemessene Betragsgang ist in Abb. 35 zu sehen.

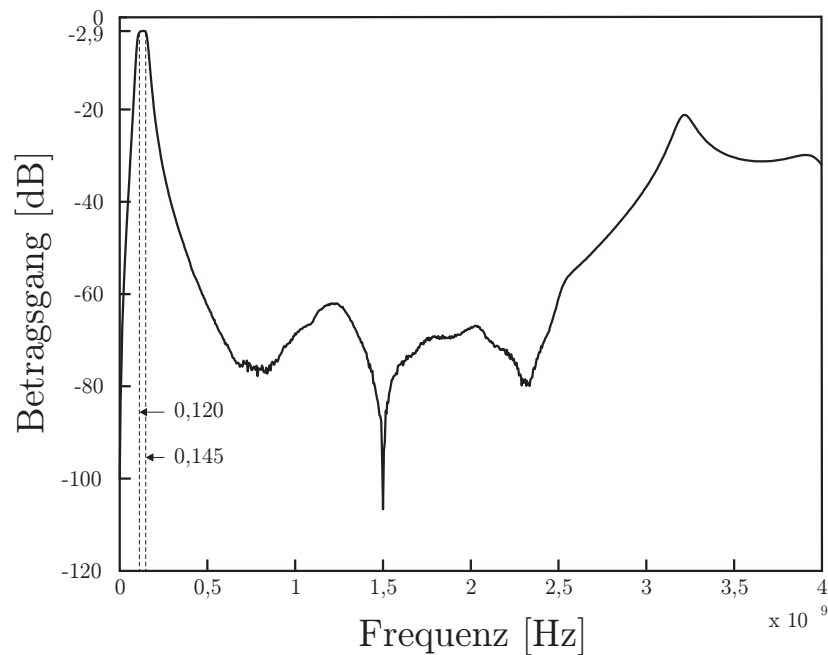


Abbildung 35: Betragsgang von BP3

Backend Die Aufgabe des Backends ist die Verarbeitung und Ausgabe der gemessenen Daten und die Steuerung aller Komponenten. In Abbildung 36 sind dessen Bestandteile und

die Verbindungen dargestellt.

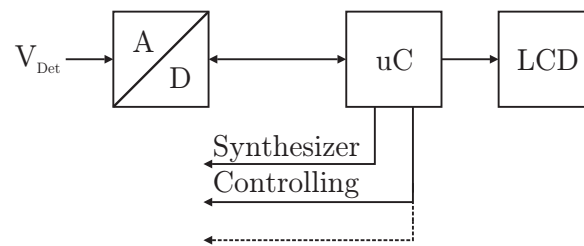


Abbildung 36: Darstellung des Backends

Hardwareimplementierung Der in den vorangegangenen Kapiteln erläuterte Leistungssensor wurde auf einem $15\text{ cm} \times 7\text{ cm}$ kleinen PCB (Leiterplatte, Engl.: Printed Circuit Board) mit vier Lagen realisiert (siehe Abb. 37). Als Substrat wurde FR4 mit einer Dielektrizitätskonstante $\varepsilon = 4,5$ gewählt, was bei ausreichender Linearität die günstigste Variante darstellt. Besonderer Augenmerk beim Layout wurde auf HF-Anforderungen gelegt. Alle HF-Leiterbahnen wurden als CPWG (Koplanare Wellenleitung mit tieferliegender Masseebene, Engl.: Coplanar Waveguide with Lower Ground Plane) ausgelegt. Dies ist eine wirkungsvolle Möglichkeit um die Impedanz der Leitungen auf 50Ω fest zulegen. So werden Fehlanpassungen vermieden und es geht wenig Signalleistung verloren.

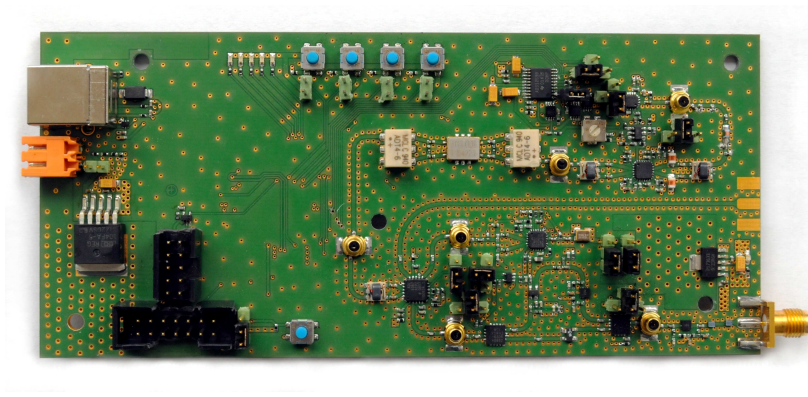


Abbildung 37: PCB des fertigen Sensors (ohne LCD).

Zusammen mit dem LCD (Flüssigkristallanzeige, Engl.: Liquid Crystal Display) wurde die Platine in ein Aluminiumgehäuse verbaut. Abbildung 38 zeigt das eigens angefertigte Gehäuse mit Schaltern um den GSM-Kanal zu wählen, um die Displaybeleuchtung zu triggern, den On/Off - Schalter sowie einen frei belegbaren Schalter für Debug-Zwecke. Das Gehäuse ist sehr stabil und gut geeignet um in schwierigem Trümmergelände verwendet zu werden.

Zusätzlich ist das Gehäuse resistent gegen Feuchtigkeit und Regen. Reflektionen am inneren der Metallbox wurden mit elektromagnetisch dämpfendem Material minimiert.



Abbildung 38: Kompletter Sensor mit Richtantenne.

Messergebnisse Nachdem der Sensor in Hardware aufgebaut wurde, wurden verschiedene Messungen im Labor durchgeführt und die Funktionalität in verschiedenen Feldtests im In- und Ausland bestätigt. Es wurde insgesamt eine Sensitivität von -107 dBm und ein linearer Dynamikbereich von 107 dB erreicht. Die NF (Rauschzahl, Engl.: Noise Figure) des Empfangspfades beträgt $3,8$ dB und der IIP3 19 dBm. Die Stromaufnahme des gesamten Sensors mit Display beläuft sich auf 530 mA. Die wichtigsten Kenngrößen sind in Tab. 2 nochmals aufgelistet. Abbildung 39 zeigt die Übereinstimmung zwischen Eingangsleistung und gemessener Leistung in dBm. Die blaue Linie zeigt die Eingangsleistung, während die rote Linie den gemessenen Wert darstellt. Dabei ergibt sich ein MSE (Mittlere quadratische Abweichung, Engl.: Mean Square Error) von $0,0667$ dB.

Tabelle 2: Verschiedene gemessene Kenngrößen.

Parameter	Value
NF	3.8 dB
IIP3	19 dBm
Sensitivität	-107 dB
Linearer Dynamikbereich	107 dB
MSE	0.07 dB
$I_{\text{inmax}} @7.4\text{V}$	530 mA
$I_{\text{stdby}} @7.4\text{V}$	300 mA

6.8 Handgerät

Das sogenannte Handgerät (Abbildung 40) ist ein Ortungsgerät mit dem Helfer die Mobiltelefone orten können. Als Nachfolger des Feldstärkesensors verfügt das Handgerät über folgende Eigenschaften:

- Robustere Messung des Empfangspegels durch bessere Trennung von verschiedenen Mobilfunksignalen
- Genauere Messung des Empfangspegels durch Polarisationsunabhängige Messung
- Drahtlose Datenverbindung zum Zentralrechner um beispielsweise Messwerte zu übertragen (Zigbee)
- Inertialsensorik und Kompass
- Integration der Local Positioning Module der Firma Symeo
- Display zur Anzeige der Messergebnisse mit der Möglichkeit zur Anzeige von Anweisungen
- Integrierte Antenne
- Trageriemen, damit der Helfer bei Bedarf beide Hände zur Verfügung hat.

Zusätzlich ist das Handgerät so ausgelegt, dass nicht nur Empfangspegel gemessen werden können sondern dass der Benutzer auch den Einfallswinkel des Signals angezeigt bekommt. Daraus ergeben sich folgende Anforderungen an die Antenne:

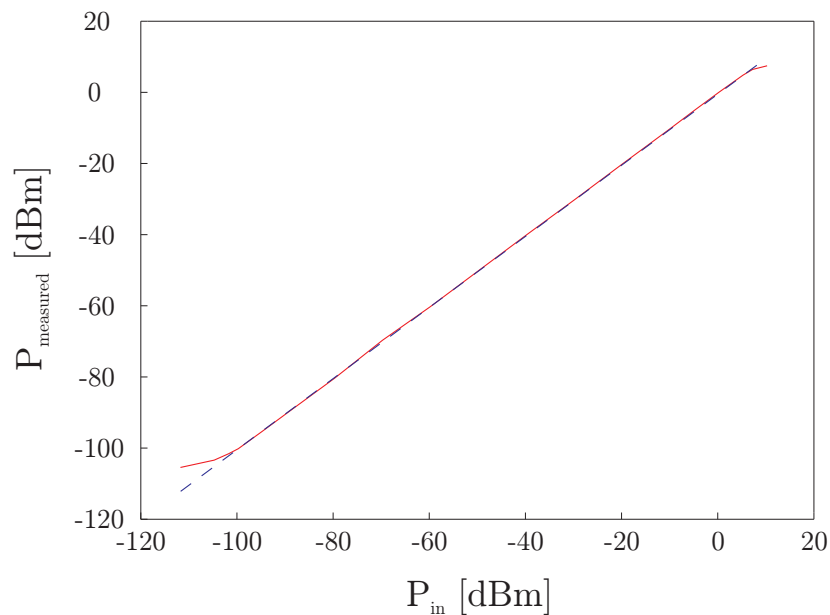


Abbildung 39: Vergleich zwischen idealer Kennlinie und gemessener Kennlinie des Sensors.

- Muss für Richtungsschätzung aus zwei Elementen mit getrennten Speisepunkten bestehen
- Passende Größe für den Anbau an das Handgerät
- Speisepunkte für vertikale und horizontale Polarisationen

Aus diesen Anforderungen ergibt sich als am besten geeigneter Antennentyp eine Patch-Antenne. Diese ist in Abbildung 41 zu sehen. Sie kann auf der Frontseite des Handgeräts angebracht werden.

Für die Ortung der Helfer mit oder ohne Handgerät wurde ebenfalls eine Antenne entworfen. Diese ist in Abbildung 42 zu sehen. Zum einen kann sie an der Helferweste angebracht werden und zum anderen auch in das Handgerät integriert werden.

6.9 Laufzeitbasierte Ortung

Die laufzeitbasierte Ortung stellt ein weiteres Ortungsverfahren dar, das zur Lokalisierung der Mobiltelefone verwendet werden kann. Dieses Ortungsverfahren eignet sich insbesondere für größere Schadenslagen (beispielsweise Erdbeben), bei denen in kurzer Zeit ein Überblick über die Lage aller Mobiltelefone benötigt wird.



Abbildung 40: Handgerät

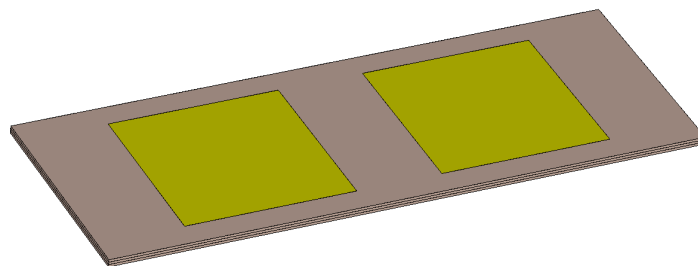


Abbildung 41: Ortungsantenne für Handgerät



Abbildung 42: Antenne für Helferortung

6.9.1 Grundkonzept und Systemstruktur

Das Grundkonzept der Ortung basiert auf dem Time-Difference-Of-Arrival (TDOA) Prinzip. Bei diesem Ansatz werden mehrere zeitsynchrone Funkempfänger in einem Gebiet verteilt und die Laufzeitdifferenz des Funksignals zwischen je zwei Empfängern gemessen. Anhand dieser Informationen kann mittels eines Hyperbelschnittverfahrens die Position der Signalquelle bestimmt werden.

Ein Überblick über das Grundkonzept ist in Abbildung 43 gezeigt.

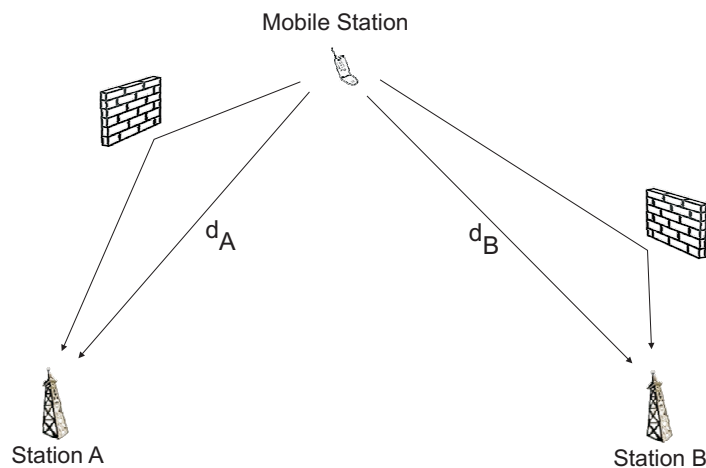


Abbildung 43: Grundkonzept für laufzeitbasierte Ortung

Bei der Ortung anhand des TDOA Prinzips ist es prinzipiell erforderlich, dass alle Empfänger zueinander synchronisiert sind. Insbesondere die Frequenzen und Phasen der Lokaloszillatoren und A/D-Umsetzer sowie die Auslösung der Signalaufzeichnung (Trigger) sind hierbei von Bedeutung.

Die Systemstruktur für das laufzeitbasierte Ortungssystem ist in Abbildung 44 dargestellt. Das System soll den Rettungskräften eine autarke und unabhängige Infrastruktur zur Verfügung stellen.

Die Messstationen werden um das Unglücksgebiet herum verteilt und sind über WLAN an einen Server angebunden. Die Einmessung der Messstationen sowie die Synchronisation der Stationen wird durch das LPR-System der Firma Symeo sichergestellt.

Die Empfangsstationen dienen dem Empfang und Zwischenspeicherung der Empfangssignale und übertragen diese an den Server. Der Server ist für die Berechnung der Laufzeitdifferenzen mittels der vorgestellten Algorithmen zuständig. Auf dem Server ist eine

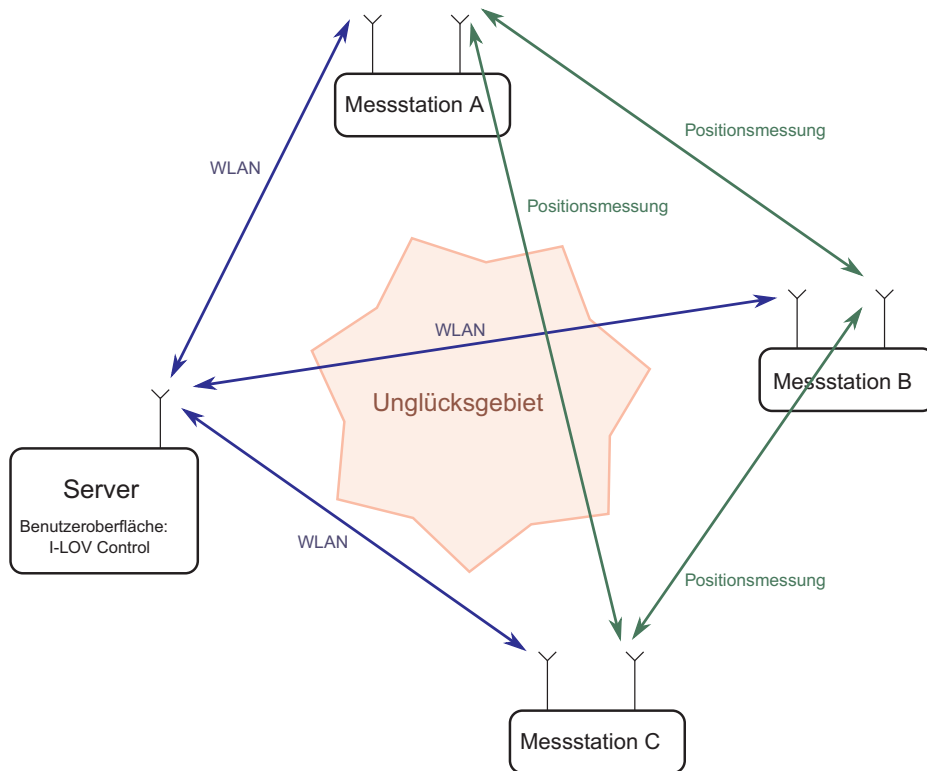


Abbildung 44: Systemstruktur des laufzeitbasierten Ortungssystems

Softwareumgebung implementiert, die eine einfache und direkte Steuerung der Systemkomponenten ermöglicht.

6.9.2 Algorithmen zur hochgenauen Laufzeitdifferenzmessung

Im Laufe des Projektes wurde zwei neuartige Verfahren entwickelt, die eine hochgenaue Laufzeitdifferenzmessung für GSM Mobilfunksignale ermöglichen. Ein wesentliches Merkmal dieser Verfahren ist die Nutzung des Frequenzsprungverfahrens für GSM Signale.

Voraussetzungen für den Signalempfang Für die Anwendbarkeit der neu entwickelten Verfahren zur Laufzeitdifferenzmessung ist es erforderlich, dass die Phaseninformation (d.h. der Startphasenwinkel eines jeden Bursts) beim Empfang der Signale aufrechterhalten bleibt. Zu diesem Zweck sind zwei grundsätzliche Konfigurationen der Empfangshardware möglich:

Breitband-Frontend Die Eingangsbandbreite der Empfänger umfasst mindestens die gesamten 35 MHz. Das Signal wird kontinuierlich (samt der Leerzeitschlitz) empfan-

gen, digitalisiert und weiterverarbeitet. Der Vorteil besteht darin, dass der Lokaloszillator zum Abmischen des Hochfrequenzsignals auf konstanter Frequenz betrieben werden kann. Nachteilig sind die hohe Datenrate und das hohe Datenvolumen - verbunden mit hohem Rechenaufwand.

Schmalband-Frontend Die Eingangsbandbreite der Empfänger umfasst lediglich die erforderliche Bandbreite eines einzelnen Bursts, d.h. etwa 200 kHz. Der Vorteil besteht in der geringeren Datenrate und dem geringeren Datenvolumen. Die Verarbeitung der Signale erfordert daher weniger Rechenaufwand. Für diesen Betrieb ist es jedoch erforderlich, dass die Empfänger zur richtigen Zeit ihre Lokaloszillatoren auf die jeweilige Trägerfrequenz umstellen, d.h. die Empfänger können nicht mehr unabhängig von der Basisstation betrieben werden und es entsteht ein hoher Koordinierungs- bzw. Steuerungsaufwand. Zudem muss der gegenseitige Phasenbezug beim Umstellen der Lokaloszillatoren zwischen allen beteiligten Empfangsstationen aufrechterhalten bleiben.

Frequenzspringende GSM Mobilfunksignale Ein Spektrogramm eines typischen frequenzspringenden GSM Signales ist in Abbildung 45 dargestellt. Das Frequenzsprungverfahren ist dadurch gekennzeichnet, dass die Trägerfrequenz des Signales in aufeinander folgenden TDMA-Rahmen gemäß eines Schemas variiert wird.

Ein frequenzspringendes Signal ist zwingende Voraussetzung für die Anwendbarkeit der neuartigen Algorithmen.

Breitbandige Kreuzkorrelation Bei der breitbandigen Kreuzkorrelation wird auf die klassische Kreuzkorrelation zweier Empfangssignale an Station A und Station B zurückgegriffen.

Die Kreuzkorrelationsfunktion (Cross Correlation Function, CCF) kann mathematisch folgendermaßen formuliert werden:

$$CCF(\Delta\tau) = r_A(t) \star r_B(t) \Big|_{\Delta\tau} = \int_{-\infty}^{\infty} r_A^*(t) \cdot r_B(t + \Delta\tau) dt \quad (15)$$

Die komplexwertigen Empfangssignale werden mit r_A sowie r_B bezeichnet. Üblicherweise wird jenes $\Delta\tau$, das den Betragsgang der CCF maximiert, als Schätzwert für die Laufzeitdifferenzschätzung verwendet:

$$\Delta\hat{\tau}_{BA} = \operatorname{argmax}_{\Delta\tau} |CCF(\Delta\tau)| \quad (16)$$

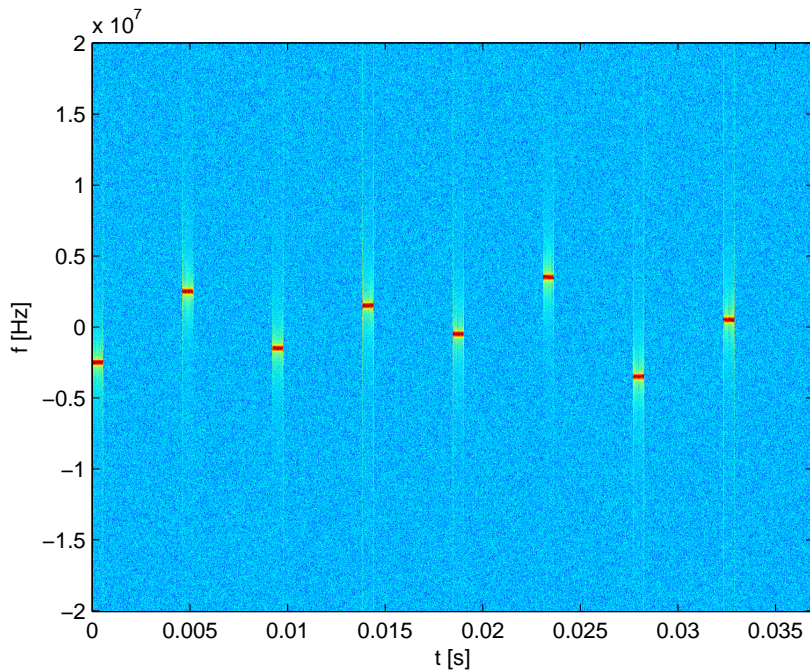


Abbildung 45: Systemstruktur für laufzeitbasierte Ortung

Unser Ansatz besteht nun darin, das gesamte frequenzspringende Signal (in voller Länge inklusive der ungenutzten Zeit- und Frequenzbereiche) als jeweiliges Empfangssignal zu interpretieren und die Kreuzkorrelationsfunktion zu berechnen.

Für eine einfache exemplarische Betrachtung (zwei Signale mit Laufzeitdifferenz gleich Null) ist der Betragsgang für die CCF in Abbildung 46 dargestellt. Eine vergrößerte Darstellung um das Hauptmaximum zeigt Abbildung 47.

Die Breite der Korrelationsfunktion um das Hauptmaximum ist deutlich reduziert und ermöglicht somit eine bessere und genauere Bestimmung der Laufzeitdifferenz.

Burstphasenanalyse Das Burstphasenanalyseverfahren nutzt die Änderung der Phasenwinkel mehrerer Bursts zwischen verschiedenen Empfangsstationen bei unterschiedlichen Trägerfrequenzen und setzt daher ebenfalls ein Frequenzsprungverfahren voraus. Das Konzept soll nun anhand einer einfachen mathematischen Betrachtung verdeutlicht werden.

Wird das Signal an Station A sowie Station B mit jeweiligen Signallaufzeiten τ_A und τ_B

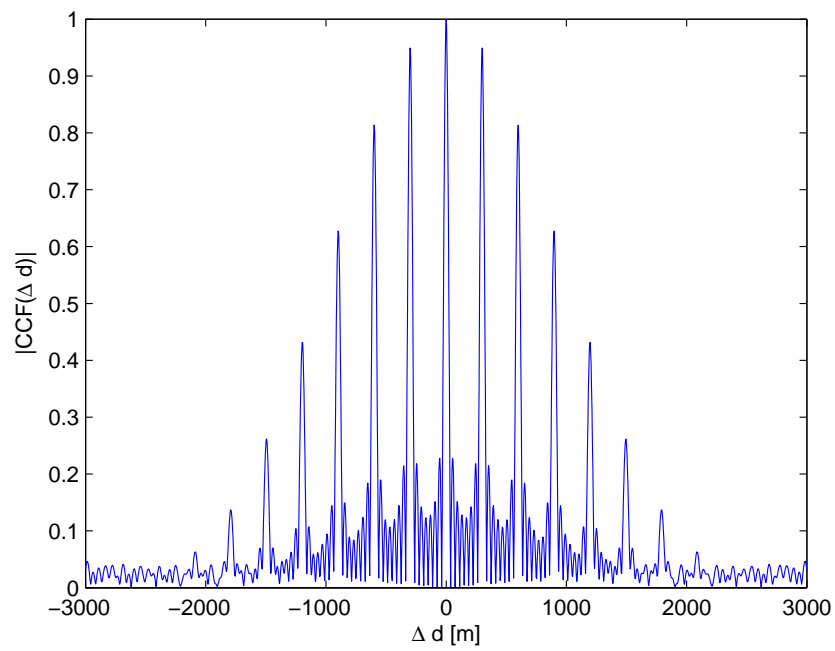


Abbildung 46: Exemplarische breitbandige Kreuzkorrelationsfunktion

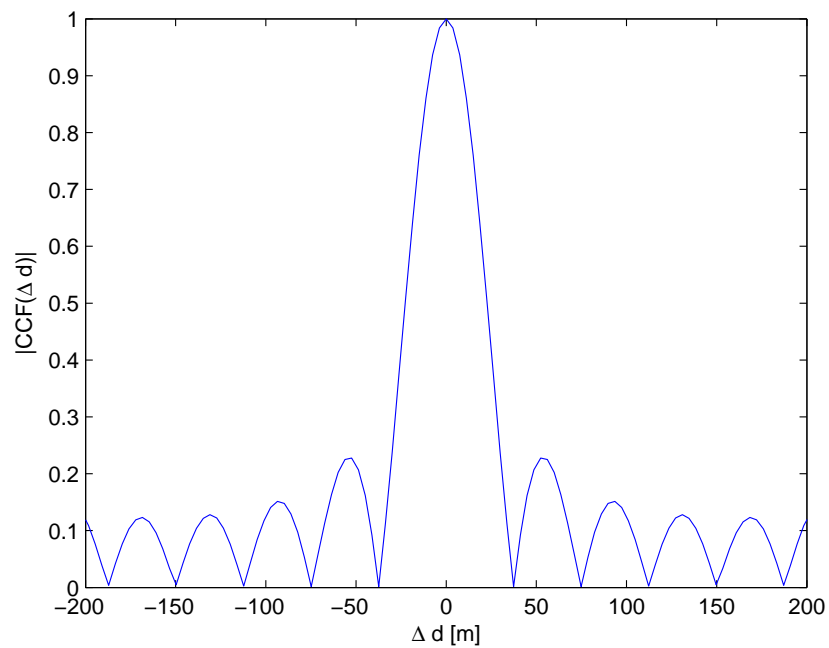


Abbildung 47: Exemplarische breitbandige Kreuzkorrelationsfunktion (vergrößert)

empfangen, so lauten die Empfangssignale:

$$r_{A,n}(t) = s_{Burst}(t - \tau_A, \mathbf{b}_n) \cdot e^{-j2\pi f_{LO,n} \tau_A} \quad (17)$$

$$r_{B,n}(t) = s_{Burst}(t - \tau_B, \mathbf{b}_n) \cdot e^{-j2\pi f_{LO,n} \tau_B} \quad (18)$$

Der Quotient bei Betrachtung von Burst n lässt sich dann mathematisch folgendermaßen darstellen:

$$q_n = \frac{r_{B,n}(t)}{r_{A,n}(t)} = \frac{s_{Burst}(t - \tau_B, \mathbf{b}_n)}{s_{Burst}(t - \tau_A, \mathbf{b}_n)} \cdot e^{-j2\pi f_{LO,n} (\tau_B - \tau_A)} = e^{j \cdot \varphi_{const.}} \cdot e^{-j2\pi f_{LO,n} (\tau_B - \tau_A)} \quad (19)$$

Die Konstante *const.* ist identisch für alle Bursts n , da das Basisbandsignal nur phasenmoduliert ist und der Zeitversatz jeweils konstant ist. Betrachtet man nun mehrere aufeinanderfolgende Bursts mit jeweils identischem Trägerfrequenzabstand Δf , d.h.

$$f_{LO,n+1} = f_{LO,n} + \Delta f_{Step} \quad (20)$$

so ergibt sich für den Quotienten zwischen zwei aufeinanderfolgenden Bursts

$$\frac{q_{n+1}}{q_n} = e^{-j2\pi \Delta f_{Step} \cdot (\tau_B - \tau_A)} \quad (21)$$

Zusammenfassend lässt sich der Zusammenhang folgendermaßen ausdrücken:

$$\Delta \tau_{BA} = \frac{\arg(q_{n+1}) - \arg(q_n)}{-2\pi \Delta f_{Step}} \quad (22)$$

Die gesuchte Laufzeitdifferenz $\Delta \tau_{BA}$ des Sendesignals zwischen zwei Stationen A und B lässt sich also auf die Messung von Phasen der Empfangssignale bei unterschiedlichen Trägerfrequenzen zurückführen.

Für die Auswertung mehrerer Burstsignale, kann der eingeführte Quotient als Rekursionsvorschrift interpretiert werden:

$$q_k = e^{-j2\pi \Delta f_{Step} \cdot k \cdot (\tau_B - \tau_A)} \cdot e^{j \cdot \varphi_0} \quad \text{mit} \quad q_0 = e^{j \cdot \varphi_0} \quad (23)$$

In diesem Falle lässt sich eine Laufzeitdifferenzmessung über eine Least-Squares Approximation (LS) sowie über eine inverse diskrete Fouriertransformation (IDFT) durchführen. Auf diese Weise lässt sich die Genauigkeit des Verfahrens substantiell erhöhen.

Eine exemplarische Least-Squares Approximation sowie der Betragsgang einer beispielhaften IDFT ist in Abbildung 48 gezeigt.

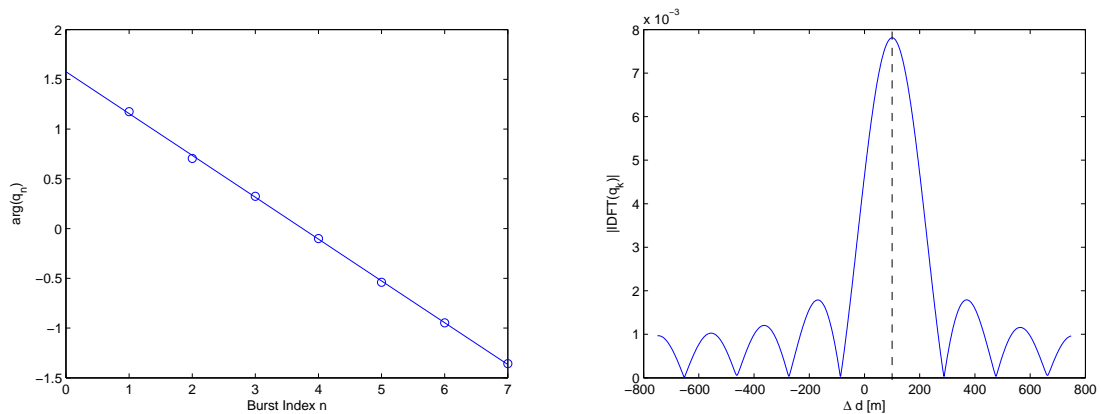


Abbildung 48: Least-Squares Approximation und inverse diskrete Fourier Transformation

6.9.3 Simulation der Leistungsfähigkeit der Algorithmen

Im Folgenden sollen die wesentlichen Simulationsergebnisse für die beiden verwendeten Verfahren dargestellt werden. Die Simulationen dienen der Abschätzung der erwarteten Genauigkeit.

Simulationsumgebung Als Simulationsumgebung wurde das Programm MATLAB der Firma MathWorks verwendet. Es wurde der vollständige Signalfluss mit Signalerzeugung, Funkkanalmodellierung und Empfang der Signale nachgebildet.

Die folgenden Simulationen basieren auf der Anwendung von 8 Burstsignalen mit einem Frequenzabstand von $\Delta f_{Step} = 1$ MHz um vertretbare Simulationszeiten zu ermöglichen. Somit ergibt sich eine Bandbreite in der Simulation von 7 MHz.

In der Realität können bis zu 64 Burstsignale mit Frequenzabständen von $\Delta f_{Step} = 200$ kHz oder Vielfachen davon eingesetzt werden. Für E-GSM 900 lassen sich Bandbreiten bis 35 MHz erzielen. Die Genauigkeit bei voller Ausnutzung dieser Bandbreite ist somit um Faktor 5 besser als in den Simulationen.

Gaußsches Rauschen Beim Gaußschen Rauschen wird die Resistenz der Verfahren gegen Rauschen der Umgebung und der Empfangshardware untersucht. Zu diesem Zweck werden Rauschsignale zufällig erzeugt und eine Laufzeitdifferenzmessung durchgeführt. Die Standardabweichung dieser Messwerte dient als Indikator für die Rauschresistenz und Präzision der Verfahren.

Die Simulationsergebnisse sind in Abbildung 49 dargestellt.

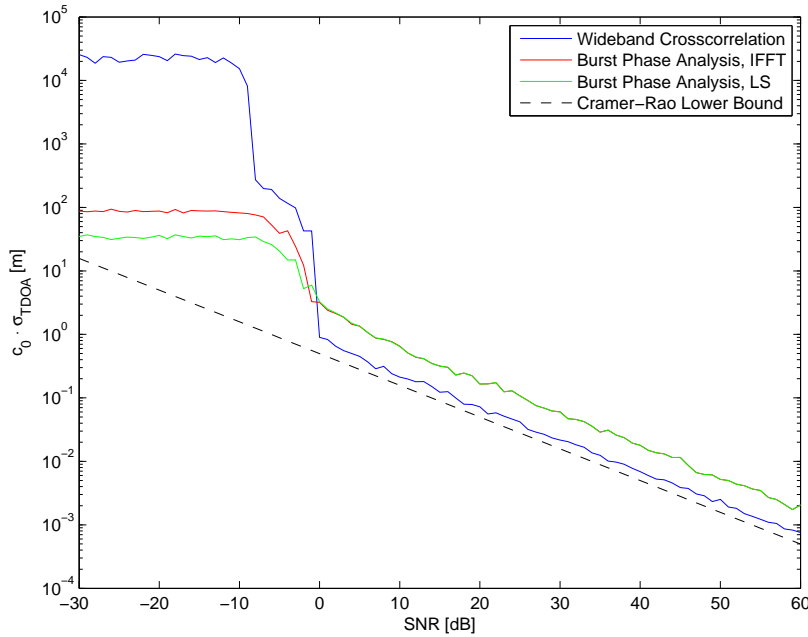


Abbildung 49: Standardabweichung der Messwerte

Als Referenz für die beste erreichbare Präzision ist die sog. Cramér-Rao Grenze (CRLB) eingezeichnet. Es handelt sich hierbei um eine statistische Grenze, die von keinem Verfahren unterboten werden kann und kann folgendermaßen berechnet werden:

$$c_0 \cdot \sigma_{CRLB} = \frac{c_0}{\sqrt{(2 \cdot E_{Total} / \mathcal{N}_0) \cdot \beta}} \quad (24)$$

E_{Total} beschreibt die Energie der Signale und \mathcal{N}_0 die spektrale Rauschleistungsdichte. β bezeichnet die effektive Bandbreite der Signale. Das Signal-Rausch-Verhältnis (SNR) bezieht sich auf die schmalbandigen Burstsignale.

Alle entwickelten Verfahren zeigen für $SNR \geq 0$ dB gute Resultate wobei die breitbandige Kreuzkorrelation die Cramér-Rao Grenze nahezu erreicht. Für $SNR < 0$ dB ist die Leistungsfähigkeit stark eingeschränkt wobei die Burstphasenanalyse bessere Resultate zeigt.

Zusammenfassend liegt die Präzision für typische Signal-Rausch-Verhältnisse im Bereich von unterhalb 1 m.

Zwei-Pfad Szenario Das Zwei-Pfad Szenario beschreibt ein vereinfachtes Mehrwegeszenario und dient der Abschätzung der Genauigkeit der Verfahren. Die Genauigkeit ist ausschließlich von der Signalbandbreite abhängig und ist eng mit dem Auflösungsvermögen verknüpft.

In der folgenden Simulation ist ein weiterer Ausbreitungspfad in einer Signalübertragungsstrecke (beispielsweise zu Station B) angenommen. Die Variablen $\Delta d_{MP} = c_0 \cdot \Delta$ und $\Delta \phi_{MP}$ beschreiben den Zeit- sowie den Phasenversatz zwischen der direkten Komponente und der Mehrwegekomponente.

Die Abweichung des Schätzwertes vom tatsächlichen Wert $\Delta \hat{d}_{BA} - \Delta d_{BA}$ ist in Abbildung 50 dargestellt. Die Resultate sind identisch für alle vorgestellten Verfahren.

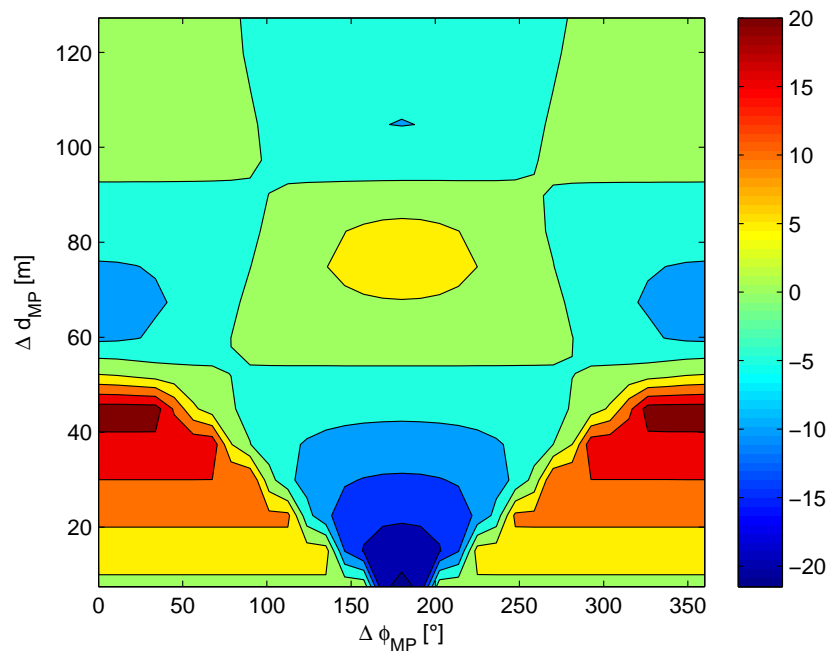


Abbildung 50: Abweichung des Schätzwertes $\Delta \hat{d}_{BA} - \Delta d_{BA}$ in Metern

In diesem Beispiel liegen die Abweichungen im Bereich $[-22\text{ m}, +22\text{ m}]$. Durch Ausnutzung der vollen Bandbreite von 35 MHz lässt sich die Genauigkeit auf $[-4,5\text{ m}, +4,5\text{ m}]$ verbessern.

Mehrwege Szenario Das Mehrwege Szenario soll die Ausbreitungseffekte in realen Funkkanälen möglichst realistisch nachbilden. Die Simulation dient dazu, die Auflösbarkeit von Mehrwegekomponenten zu beurteilen.

Zu diesem Zweck wird der Funkkanal als gewichtete Summe von Delta-Funktionen modelliert:

$$h_A(t) = \sum_i \alpha_{A,i} \cdot \delta(t - \tau_{A,i}) \cdot e^{j \cdot \varphi_{A,i}} \quad (25)$$

$$h_B(t) = \sum_j \alpha_{B,j} \cdot \delta(t - \tau_{B,j}) \cdot e^{j \cdot \varphi_{B,j}} \quad (26)$$

Die Amplituden $\alpha_{A,i}$ und $\alpha_{B,j}$, Verzögerungen $\tau_{A,i}$ und $\tau_{B,j}$ und Phasenwerte $\varphi_{A,i}$ und $\varphi_{B,j}$ hängen von der Ausbreitungsumgebung ab.

Ein beispielhaftes Szenario inklusive der breitbandigen Kreuzkorrelationsfunktion ist in Abbildung 51 dargestellt.

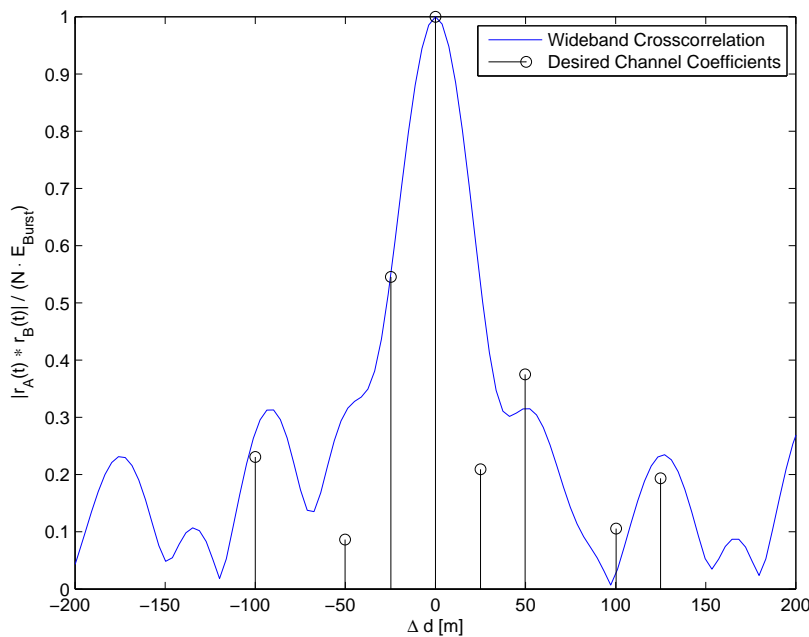


Abbildung 51: Beispielhaftes Mehrwegeszenario mit breitbandiger Kreuzkorrelationsfunktion

In diesem Beispiel ist die gewünschte direkte Komponente $\Delta\tau_{BA}$ bei Null angenommen. Durch Anwendung der breitbandigen Kreuzkorrelationsfunktion können alle relevanten Mehrwegekomponenten identifiziert werden.

6.9.4 Entwicklung und Aufbau des Hardwareprototyps

Zur Evaluierung und zur Demonstration der Anwendbarkeit der neuartigen Verfahren wurde ein Hardwareprototyp aufgebaut. Die Struktur sowie die wesentlichen Komponenten sollen

im Folgenden vorgestellt werden.

Aufbau der Messstationen Die Messstation ist für den Empfang sowie die Zwischenspeicherung der Empfangssignale ausgelegt und überträgt die Daten per WLAN an den Server. Der Aufbau einer einzelnen Messstation ist in Abbildung 52 näher gezeigt.

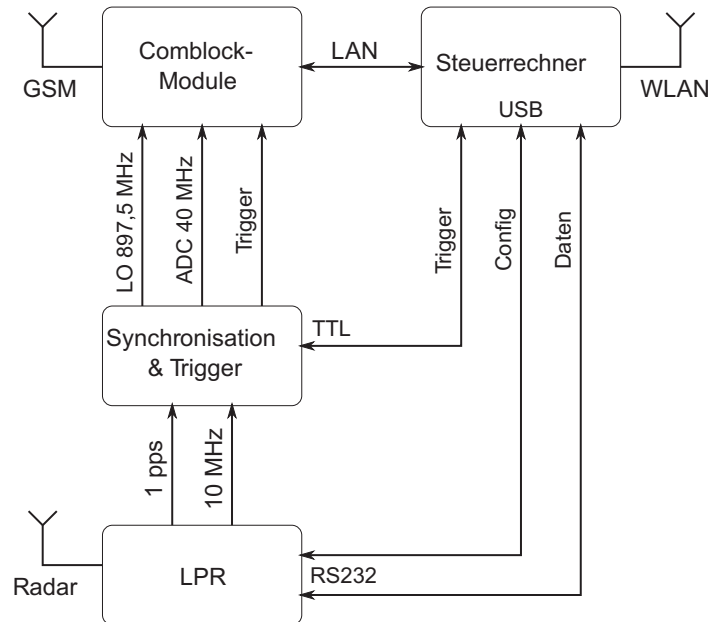


Abbildung 52: Aufbau einer Messstation

Die ComBlock-Module sind für den Empfang der GSM Signale ausgelegt und verfügen über ein breitbandiges Frontend inklusive Lokaloszillator und Analog-Digital-Umsetzer. Zudem ist ein Trigger-Eingang zur Signalaufzeichnung vorhanden. Die Synchronisations- und Triggerplatine generiert aus dem Synchronisationssignal des LPR-Systems geeignete Signale für die Comblock-Module. Das LPR-System dient als Synchronisationsquelle und liefert synchrone Referenzsignale an allen beteiligten Messstationen. Die Steuerung der lokalen Komponenten sowie die WLAN-Anbindung erfolgt über einen Steuerrechner.

Systemkomponenten im Detail Die wesentlichen Systemkomponenten sollen im Folgenden detailliert vorgestellt werden.

Das LPR-System der Firma Symeo dient als Synchronisationsquelle und ist in Abbildung 53 dargestellt. Die LPR-Systeme in unterschiedlichen Stationen messen sich gegenseitig ein und stellen hochsynchronen 1 PPS und 10 MHz Rechtecksignale bereit.

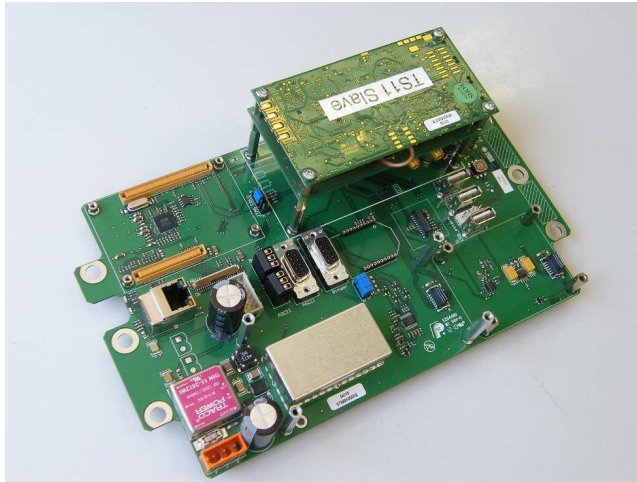


Abbildung 53: LPR-System

Die ComBlock-Module der Firma Mobile Satellite Services Inc. dienen dem Empfang der GSM Signale und sind in Abbildung 54 dargestellt. Sie bestehen aus separaten Teilmodulen für GSM Frontend, Zwischenspeicherung und Netzwerk-Schnittstelle.

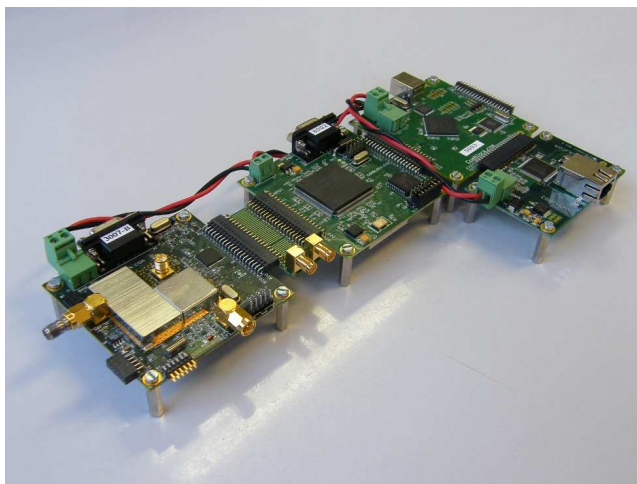


Abbildung 54: Comblock-Module

Die Synchronisations- und Triggerplatine bereitet die Synchronisationssignale des LPR-Systems für den synchronen Betrieb der ComBlock-Module auf und ist in Abbildung 55 dargestellt. Die Platine wurde im Rahmen des Projektes am Lehrstuhl entwickelt und beinhaltet einen Mikrocontroller, ein Field-Programmable-Gate-Array (FPGA) sowie Phasenregelschleifen (PLLs).

Zur Steuerung der Komponenten wird ein Rechner der Firma Kontron verwendet. Der Rechner verfügt über einen Intel Atom-Prozessor sowie volle Computerfunktionalität (USB,

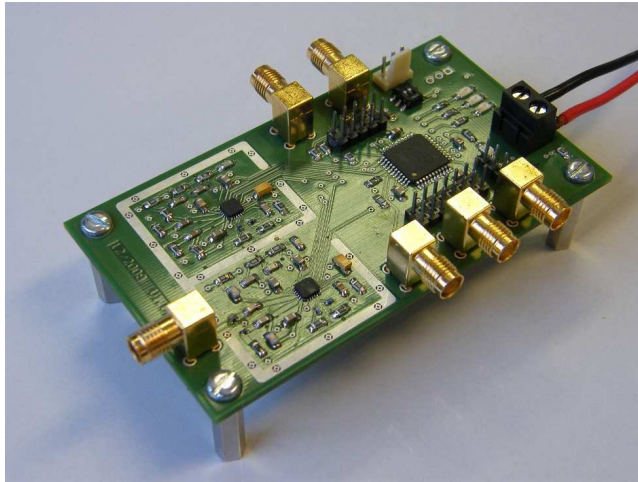


Abbildung 55: Synchronisations- und Triggerplatine

LAN, etc.). Als Betriebssystem wird ein Linux-Derivat eingesetzt. Der Rechner ist in Abbildung 56 dargestellt.

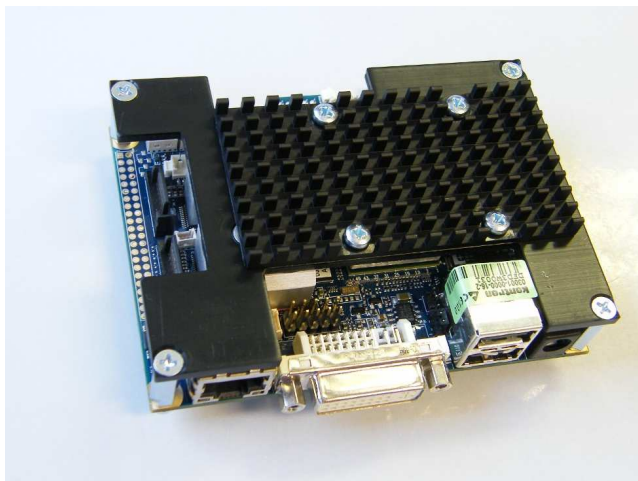


Abbildung 56: Steuerrechner

Integration der Systemkomponenten Die wesentlichen Systemkomponenten wurden in ein Gehäuse der Schutzklasse IP66 eingebaut. Die Energieversorgung wird durch einen Bleiakku sichergestellt, der einen Betrieb der Messstationen von mehreren Stunden erlaubt. Zudem wurde ein DC/DC-Wandler zur Bereitstellung der benötigten Spannungen verwendet.

Eine schematische Zeichnung ist in Abbildung 57 dargestellt. Zwei photographische Aufnahmen sind in Abbildung 58 und 59 gezeigt.

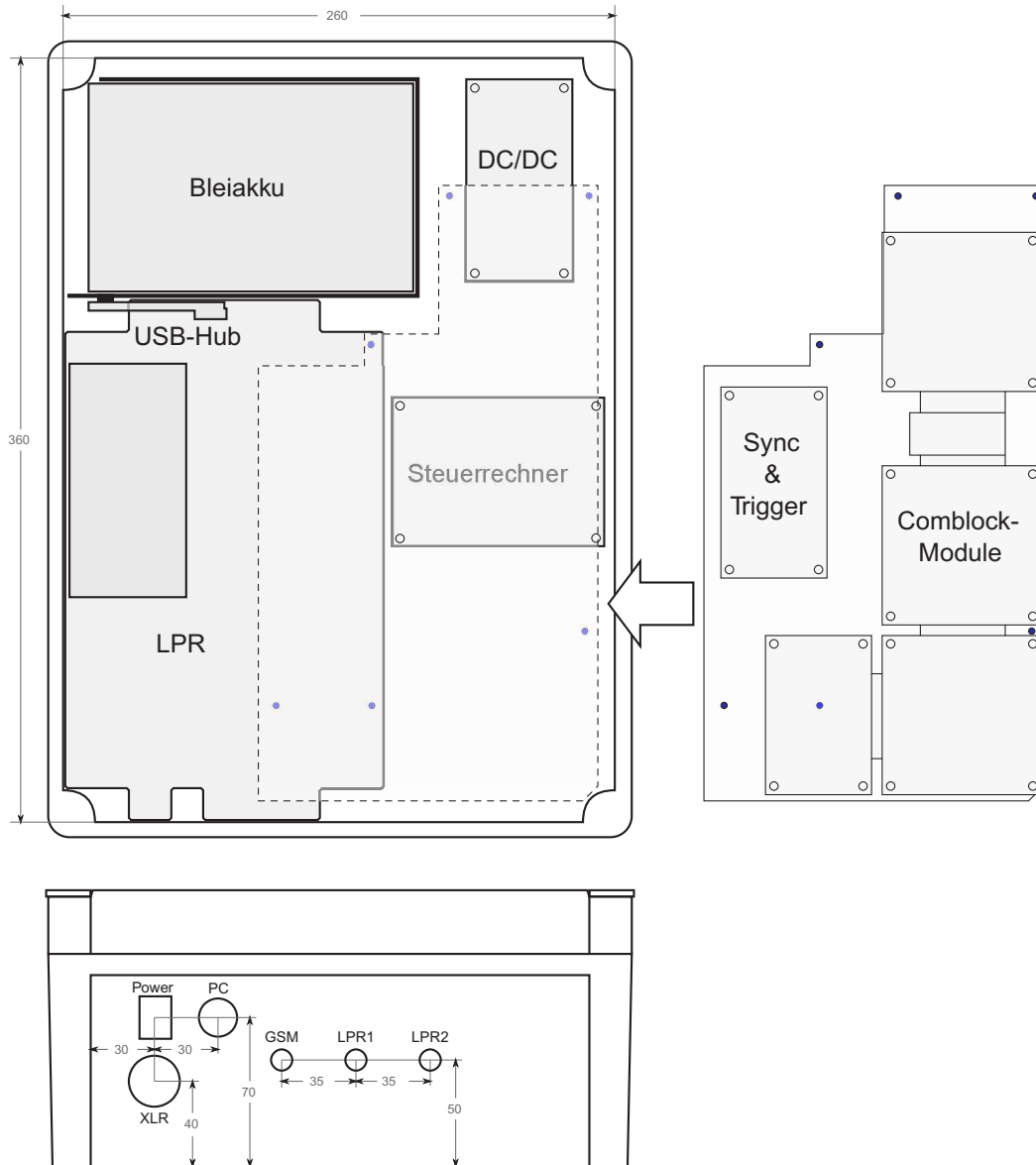


Abbildung 57: Schematischer Aufbau



Abbildung 58: Ansicht von oben



Abbildung 59: Einsatz im Freien

Implementierung der Softwareumgebung Die Netzwerkstruktur des Ortungssystems ist in Abbildung 60 näher dargestellt. Die Messstationen melden sich beim Server nach dem Einschalten automatisch an. Somit ist das System sehr schnell einsatzbereit. Der Messvorgang wird vom Benutzer am Server zentral gesteuert und gesteuert.

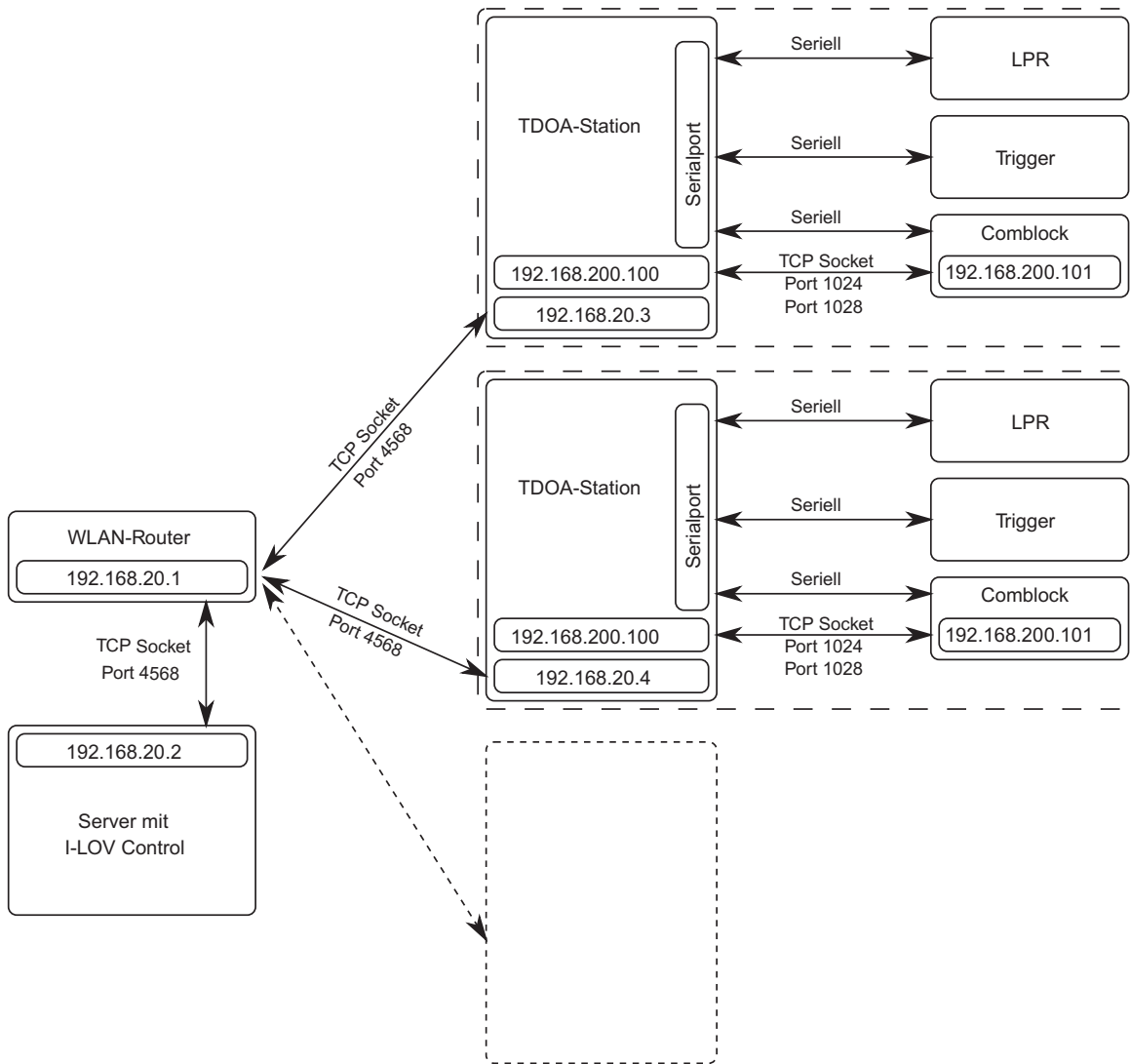


Abbildung 60: Netzwerkstruktur des Ortungssystems

Die Softwareumgebung auf den Messstationen sowie dem Server wurde mit der Programm-bibliothek QT der Firma Nokia implementiert. Es wurde eine graphische Benutzeroberfläche programmiert, die eine einfache Steuerung des Systems ermöglichen soll. Der Startbildschirm für den Benutzer auf dem Server ist in Abbildung 61 dargestellt.



Abbildung 61: Benutzeroberfläche auf dem Server

6.9.5 Zusammenfassung

In diesem Arbeitspaket wurde ein lauffzeitbasiertes Ortungssystem für GSM Mobiltelefone entwickelt.

Das System basiert auf dem Time-Difference-Of-Arrival (TDOA) Prinzip, bei dem synchrone Funkempfänger in einem Gebiet verteilt werden und die Laufzeitdifferenz des Funksignals zwischen je zwei Empfängern gemessen wird. Dadurch kann mittels eines Hyperbelschnittverfahrens die Position der Signalquelle bestimmt werden.

Der Schwerpunkt der Arbeit lag auf der Entwicklung neuartiger Algorithmen zur Laufzeitdifferenzmessung. Die Verfahren wurden analytisch hergeleitet und mittels Computersimulationen verifiziert. Die bestmögliche erwartete Genauigkeit liegt im Bereich von 5-10 Metern und stellt eine substantielle Verbesserung (etwa Faktor 10) gegenüber dem Stand der Technik dar.

Es wurde zudem ein Hardwareprototyp entwickelt und aufgebaut, der die Leistungsfähigkeit der neuartigen Algorithmen demonstrieren soll. Für den Prototyp wurden eigene Komponenten entworfen und mit kommerziellen Komponenten in ein Gehäuse integriert. Für die Steuerung der Komponenten wurde eine Softwareumgebung implementiert, die eine zentrale Auswertung der Messergebnisse ermöglicht.

Erste Messungen und Tests der Algorithmen unter Laborbedingungen waren erfolgreich und bestätigen die Simulationsergebnisse. Ein vollständiger Funktionstest unter realen Bedingungen steht noch aus.

7 Zahlenmäßiger Nachweis

Tabelle 3 zeigt den Gesamtfinanzierungsplan und die Verwendung der Mittel. Insgesamt sind Ausgaben in Höhe von 709.822,47 € entstanden. Die Projektpauschale betrug 15.690,35 €. Der Kassenbestand beläuft sich dato auf -11.716,21 € (vergl. Verwendungsnachweis).

Position	Entstandene Ausgaben	Gesamtfinanzierungsplan
0812	523.764,24	522.888,00
0822	2.584,77	3.165,00
0843	77.340,90	94.273,00
0846	24.482,22	20.000,00
0850	81.650,34	69.394,00
Summe	709.822,47	709.720,00

Tabelle 3: Verwendungsnachweis der Zuwendungen

8 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Das AP4 des Forschungsvorhaben I-LOV stellte einen neuartigen Ansatz zur Ortung von Verschütteten dar. Eine Verbesserung der Ortungsgenauigkeit von Mobiltelefonen von ca. 150 m auf deutlich unter 1 m ist ein gewaltiger Fortschritt auf diesem Gebiet. Sowohl die dafür nötigen theoretischen Grundlagen als auch die technische Infrastruktur musste neu hergeleitet und entwickelt werden. Dabei mussten etwaige Hürden genommen werden. Es musste eine eigene GSM-Basisstation aufgebaut werden, ein neues Verfahren für eine laufzeitbasierte Ortung von Mobiltelefonen entwickelt werden, Standardprotokolle im Mobilfunk angepasst werden, Ortungshardware speziell für die Ansprüche in diesem Projekt entwickelt und aufgebaut werden, um nur einige der vielen nötig gewesenen Innovationen zu nennen.

Diese Leistung wurde von drei Doktoranden und 15 wechselnden Studenten in nur 42 Monaten erbracht. Nach Projektende ist abzusehen, dass die erzielten Ergebnisse die Erwartungen in einigen Bereichen sogar übertroffen haben. Nach der Überführung in ein Produkt wird seitens des THW, aber auch vieler anderer internationaler Katastrophenschutzorganisationen, reges Interesse an der I-LOV Mobilfunkortung bestehen. Wie gefordert, bildet sie eine wertvolle Ergänzung zur bestehenden Rettungskette und kann Ortungserfolge erhöhen und beschleunigen. Damit ist das System in der Lage Menschenleben zu retten.

9 Verwertung

Für den Lehrstuhl für Technische Elektronik der Universität Erlangen-Nürnberg ist zu erwarten, dass die Weiterentwicklung der LTE-eigenen System- und Schaltungssimulationsfähigkeiten und -werkzeuge und die Erarbeitung neuer theoretischer Verfahren dazu beiträgt, seine internationale Reputation in der Forschung im Bereich der Funksystem- und Schaltungstechnik weiter voranzutreiben, so dass der Lehrstuhl für Technische Elektronik noch stärker als bisher als Mitglied eines universitären Center of Excellence (CoE) und universitärer Dienstleister in der Funk- und Ortungstechnik bekannt wird. Eine weitere Motivation für den LTE sich am Förderprojekt zu beteiligen, bestand darin, die Forschungsergebnisse auch in die Lehre (z.B. System- und Schaltungssimulationspraktikumsversuche, Demonstrator für die Lehre) einfließen zu lassen und dadurch seine Attraktivität bei den Studierenden weiter zu erhöhen. Der LTE ist in Deutschland wohl der einzige Lehrstuhl, der die Verknüpfung von System- und Schaltungstechnik in seinem Fokus hat und hohe Anerkennung findet (CoE). Der Lehrstuhl für Technische Elektronik stellt diese Expertise seit dem Jahre 2002 auch regelmäßig im Rahmen jährlicher, nationaler Table-Top-Ausstellungen (EEEfCOM, Ulm; RadCom, Hamburg; RadioTecC, Berlin) durch Messepräsentationen vor (Lehrstuhlmotto: "Making Bits Fly") und plant die Fortführung und Erweiterung dieser Aktivitäten. Die Arbeitspakete des LTE adressieren zum größten Teil sehr grundlegende Fragestellungen der Ortungsmöglichkeiten von GSM-Geräten. Die selektive Lokalisierung von Mobiltelefonen durch Feldstärkemessungen, wie sie innerhalb des Arbeitspaketes AP4-3, und die Ortung durch Laufzeitmessung der Handysignale wie sie in AP4-5 des LTE entwickelt wurde, stellt einen völlig neuen Ansatz der Lokalisierung von Verschütteten dar, von dem man sich signifikante Vorteile bei der Suche von verschütteten Personen versprechen kann. Die im AP4-4 zu untersuchenden Antennenkonzepte zur präziseren Bestimmung der Empfangsrichtung von Signalen von Mobiltelefonen bietet ebenfalls einen neuen Weg der Handylokalisierung, mit der man die Möglichkeit der Positionsbestimmung von Mobiltelefonen

verbessern und beschleunigen kann. Darüber hinaus ist die Verwendung solcher modularer Systeme zur Lokalisierung von GSM-Geräten in einer Vielzahl von weiteren Szenarien im Rettungs- und Sicherheitsbereich denkbar. In einer an das Projekt anschließenden Industrialisierungsphase werden Ergebnisse des Förderprojektes daher in Produkte der Firma Symeo einfließen. Die Verbreitung des erworbenen Know-Hows außerhalb des Projekts soll ferner durch von IEEE, ITG (VDE), GMM (VDE) und der Fa. Gerotron veranstaltete Workshops (sowohl wissenschaftlicher als auch industrienaher Ausrichtung), Special Sessions (auch Panel Sessions) bei Tagungen und Pressemitteilungen erfolgen. Der LTE verfügt hier über sehr gute Kontakte zu diesen Organisationen und arbeitet z.B. mit Gerotron bei deren jährlichen Veranstaltungen EEEfCOM (Ulm), RADCOM (Hamburg) und RadioTeC (Berlin) zusammen. Zusätzlich wird bereits über eine Weiterführung der Arbeiten in einer der Ausgründungen des LTE, der eesy-id GmbH, nachgedacht. Hier könnten die Labormuster bis zur Produktreife geführt werden. Dies wird zur Zeit geprüft.

10 Fortschritt bei anderen auf dem Gebiet

Während der Projektlaufzeit wurden zwei Projekte mit ähnlichem Fokus bekannt.

10.1 STARRS - Sensor for Terrestrial and Airborne Radio transmitter Rescue Search

Das Projekt STARRS wurde von der bekannten Firma Thales Communications geführt. Fokus dieses Projektes war die Flächensuche von GSM-Mobilfunkgeräten mit Hilfe eines Hubschraubers. Es werden ebenfalls Störsender eingesetzt. Dabei wurde eine Ortungsgenauigkeit von 1 m^2 erreicht. Sowohl eine Suche per Hubschrauber als auch eine Auflösung von 1 m^2 sind allerdings für die Erdbebenszenarien im Projekt I-LOV nicht anwendbar bzw. ausreichend.

10.2 Rohde&Schwarz

Die Firma Rohde&Schwarz hat eines ihrer Produkte, einen sog. „IMSI-Catcher“ umgebaut, um damit auch Mobilfunkgeräte in I-LOV-Szenarien orten zu können. Über die Ortungsgenauigkeit ist nichts bekannt.

11 Veröffentlichungen

- Alexander Götz, Richard Rose, Stefan Zorn, Robert Weigel, Ortung von GSM-Mobiltelefonen in Katastrophenszenarien, DGON Navigationskonvent 2009, 9./10.7.2009, Berlin
- Alexander Götz, Stefan Zorn, Richard Rose, Robert Weigel, Ortung von GSM-Mobiltelefonen in Katastrophenszenarien, ION-CH AHORN 2009, 5./6.11. 2009, Zürich
- Alexander Goetz, Stefan Zorn, Richard Rose, Georg Fischer, Robert Weigel, A Time Difference of Arrival System Architecture for GSM Mobile Phone Localization in Search and Rescue Scenarios, Workshop on Positioning, Navigation and Communication (WPNC) 2011, 7./8.4.2011, Dresden
- Alexander Götz, Stefan Zorn, Richard Rose, Georg Fischer, Robert Weigel, Ortung von GSM Mobiltelefonen zur Vermissten- und Verschüttetensuche, Electrical and Electronic Engineering for Communication (EEECOM) 2011, 25./26.5.2011, Ulm
- Alexander Goetz, Richard Rose, Stefan Zorn, Georg Fischer, Robert Weigel, Algorithms for High Resolution Time Difference of Arrival Estimation for GSM Mobile Phones, Kleinheubacher Tagung 2011, 26.-28.9.2011, Miltenberg
- Alexander Goetz, Richard Rose, Stefan Zorn, Georg Fischer, Robert Weigel, A Wideband Crosscorrelation Technique for High Precision Time Delay Estimation of Frequency Hopping GSM Signals, European Microwave Week (EuMW) 2011, 9.-14.10.2011, Manchester, UK
- Alexander Goetz, Richard Rose, Stefan Zorn, Georg Fischer, Robert Weigel, A Burst Phase Analysis Technique for High Precision Time Delay Estimation of Frequency Hopping GSM Signals, Asia-Pacific Microwave Conference (APMC) 2011, 5.-8.12.2011, Melbourne, Australien
- Alexander Goetz, Richard Rose, Stefan Zorn, Georg Fischer, Robert Weigel, Performance of Coherent Time Delay Estimation Techniques for Frequency Hopping GSM Signals, Radio Wireless Week (RWW) / Wireless Sensors and Sensor Networks (WiS-Net) 2012, 15.-18.1.2012, Santa Clara, USA
- Richard Rose, Stefan Zorn, Alexander Götz, Robert Weigel, Ortung verschütteter Personen anhand ihrer GSM-Mobiltelefone, RadioTecC - Transmit&Test Solutions, 2009, Berlin

-
- Richard Rose, Christian Meier, Stefan Zorn, Alexander Götz, Robert Weigel, A GSM-network for mobile phone localization in disaster scenarios, Microwave Conference (GeMIC), , 14-16 March 2011, Darmstadt
 - Richard Rose, Stefan Zorn, Alexander Götz, Georg Fischer, Robert Weigel, A new technique to improve AoA using dual polarization, 41st European Microwave Conference (EuMC), 10-13 Oct. 2011, Manchester
 - Zorn, S.; Maser, M.; Goetz, A.; Rose, R.; Weigel, R.; , „A power saving jamming system for E-GSM900 and DCS1800 cellular phone networks for search and rescue applications“, Wireless Sensors and Sensor Networks (WiSNet), 2011 IEEE Topical Conference on , vol., no., pp.33-36, 16-19 Jan. 2011, doi: 10.1109/WISNET.2011.5725020
 - Zorn, S.; Rose, R.; Goetz, A.; Weigel, R.; , „A novel technique for mobile phone localization for search and rescue applications“, Indoor Positioning and Indoor Navigation (IPIN), 2010 International Conference on , vol., no., pp.1-4, 15-17 Sept. 2010, doi: 10.1109/IPIN.2010.5647107
 - Zorn,S.; Bozsik, G.; Rose, R.; Goetz, A.; Weigel, R.; Koelpin, A., „A power sensor unit for the localization of GSM mobile phones for search and rescue applications,“ Sensors, 2011 IEEE , vol., no., pp.1301-1304, 28-31 Oct. 2011
 - Zorn, S., „A new Approach on Mobile Phone Localization for Search and Rescue Applications“, ITG-Fachausschuss 7.2: Funksysteme, „Funklokalisierung - sicher, schnell und genau“, 4.11.2010, TU Ilmenau
 - Zorn, S.; Rose, R.; Goetz, A.; Weigel, R.; Koelpin, A., „A New System for Mobile Phone Localization for Search and Rescue Applications“, 6th Future Security Research Conference, Berlin, September 5th -7th, 2011, ISBN 978-3-8396-0295-9
 - Zorn,S.; Gardill, M.; Weigel, R.; Koelpin, A., „A Smart Jamming System for UMTS/WCDMA Cellular Phone Networks for Search and Rescue Applications“, International Microwave Symposium, Montreal, Kanada, 2012, to be published

Literatur

- [1] ETSI: Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling). In: *ETSI SR 002 180 V1.1.1* 12 (2003), S. 9ff
- [2] MEIER, Dipl.-Ing. C.: *Aufbau einer GSM-Zelle zur Emulation eines GSM-Netzwerkes*, Friedrich-Alexander-Universität Erlangen-Nürnberg, Diplomarbeit, 2010
- [3] 3RD GENERATION PARTNERSHIP PROJECT (3GPP): Requirements for support of radio resource management(FDD). 2009 (3GPP TS 25.133 V9.0.0 (2009-05)). – Forschungsbericht
- [4] GARDILL, M. ; ZORN, S. ; WEIGEL, R. ; KOELPIN, A.: Triggering UMTS user equipment inter-RAT cell reselection using noise jammers. In: *Proc. German Microwave Conf. (GeMIC)*, 2011, S. 1–4
- [5] WEIGEL, Robert ; REINHARDT, S.: *Systeme und Schaltungen der Übertragungstechnik*. Lehrstuhl für Technische Elektronik, 2005
- [6] MAXSTREAM: *Indoor Path Loss*. <http://digilander.libero.it/windflow/eng/Usage/RFIDSensor/Indoor\discretionary-%20Path%20Loss.pdf>. Version: September 2003
- [7] ESSWEIN, Alexander ; MASER, Matthias ; WEIGEL, Robert: *Analog Electronic Systems*. Lehrstuhl für Technische Elektronik, 2008

Abbildungsverzeichnis

1	Erweiterte Rettungskette	10
2	Systembeschreibung Arbeitspaket 4	15
3	Ursprünglicher Arbeitsplan	16
4	Ebenenmodell des Systemansatzes	21
5	Die I-LOV BTS	24
6	Kanalfiltermaske	27
7	Jammer-Architektur	28
8	Signalerzeugung des Störsignals im FPGA	28
9	Aufgenommene Filterkurve des Bandpasses aus dem FPGA	29
10	Hardwareaufbau der I-LOV BTS mit dem GSM-Jammer	31
11	Das Frontend des GSM-Jammers.	32
12	Messung eines erzeugten Beispiel-Störsignals im E-GSM900-Band.	32
13	Extrapolierte gestörte Fläche mit einem 10 W PA.	33
14	Messung der Qualitätsgrößen in einem UMTS-Empfänger	34
15	Aufbau des UMTS-Jammers im I-LOV-Rack: 1) FPGA-Signalgenerator; 2) Abtastakterzeugung; 3) ADU-Adapterplatine; 4) HF-Frontend.	36
16	Signalerzeugungshardware	37
17	Weiterverarbeitung des im PC generierten Störsignals	37
18	Blockschaltbild des UMTS-HF-Front-Ends	38
19	Vergleich zwischen Simulation und Messung des Tiefpassfilters (l) und Mischer-Testplatine mit Filtern (r)	39
20	HF-Störsignal für einen Kanal bei 2120 MHz	39
21	Messaufbau zur Verifikation der selektiven Interferenzeinspeisung aus Kap. 6.4.2	40
22	Hardwareaufbau als Blockschaltbild	41
23	Aufbau des SDR Transceivers	43
24	Realisierung der Basisstation	44
25	Aufbau ders SDR Transceivers	45
26	Empfang der Willkommens-SMS	46
27	Komponenten der Steuereinheit	47
28	Benutzeroberfläche - GSM-Scanner	47
29	Benutzeroberfläche - Störsender	48
30	Benutzeroberfläche - GSM-Netzwerk	48
31	Antennencharakteristik R&S HE300 (500-7500 MHz)	50
32	Grundlegende Architektur des Feldstärkesensors	51

33	Schematische Darstellung des Frontends	51
34	Detektorschleife	54
35	Betragsgang von BP3	54
36	Darstellung des Backends	55
37	PCB des fertigen Sensors (ohne LCD).	55
38	Kompletter Sensor mit Richtantenne.	56
39	Vergleich zwischen idealer Kennlinie und gemessener Kennlinie des Sensors.	58
40	Handgerät	59
41	Ortungsantenne für Handgerät	59
42	Antenne für Helferortung	59
43	Grundkonzept für laufzeitbasierte Ortung	60
44	Systemstruktur des laufzeitbasierten Ortungssystems	61
45	Systemstruktur für laufzeitbasierte Ortung	63
46	Exemplarische breitbandige Kreuzkorrelationsfunktion	64
47	Exemplarische breitbandige Kreuzkorrelationsfunktion (vergrößert)	64
48	Least-Squares Approximation und inverse diskrete Fourier Transformation	66
49	Standardabweichung der Messwerte	67
50	Abweichung des Schätzwertes $\Delta \hat{d}_{BA} - \Delta d_{BA}$ in Metern	68
51	Beispielhaftes Mehrwegeszenario mit breitbandiger Kreuzkorrelationsfunktion	69
52	Aufbau einer Messstation	70
53	LPR-System	71
54	Comblock-Module	71
55	Synchronisations- und Triggerplatine	72
56	Steuerrechner	72
57	Schematischer Aufbau	73
58	Ansicht von oben	74
59	Einsatz im Freien	74
60	Netzwerkstruktur des Ortungssystems	75
61	Benutzeroberfläche auf dem Server	76

Tabellenverzeichnis

2	Verschiedene gemessene Kenngrößen.	57
3	Verwendungsnachweis der Zuwendungen	77