Christian Fischer

Entwicklung von ZigBee-Modulen für spontane Funknetzwerke

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang Technischer Informatik
am Fachbereich Elektrotechnik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. rer.nat. Gunter Klemke
Zweitgutachter : Prof. Dr. rer.nat. Kai von Luck

Abgegeben am 29. August 2005

Christian Fischer

Thema der Bachelorarbeit

Entwicklung von ZigBee-Modulen für spontane Funknetzwerke

Stichworte

ZigBee, Funknetzwerke, Sensornetzwerke, Verteilte Systeme, Smart Dust, Disappearing Computer, Ubiquitous Computing

Kurzzusammenfassung

Die technologische Entwicklung bringt eine Erleichterung von Arbeit und Aufwand für den Menschen. Technische Geräte werden kompakter und ansehnlicher. Die Zahl der computergestützten Aufgaben im Alltag wächst unaufhaltsam, der Trend geht zu „Ubiquitärem Computing“ – Computer sind überall vorhanden, der Mensch bemerkt sie nicht mehr.

Diese Arbeit hat die Aufgabe, ein spezielles Alltags-Szenario dem heutigen Fortschritt anzupassen und als Resultat die manuelle Arbeit zu verringern. Im Vordergrund steht dabei die hardwaretechnische Entwicklung eines Sensornetzwerkes.

In diesem Zuge wird eine Analyse der aktuell vorhandenen Funkstandards, insbesondere ZigBee durchgeführt. Es folgt der Entwurf eines energieeffizienten, unauffälligen und robusten Systems mit geringer Komplexität. Die Erstellung der Hardware und beispielhafter Software vervollständigt die Arbeit, durch abschließende Tests werden praktische Erfahrungen vermittelt.

Ein Ausblick erläutert das breite Spektrum an Einsatzmöglichkeiten dieses Systems.

Christian Fischer

Title of Paper

Development of devices for spontaneous radio networks based on ZigBee-Technology

Keywords

ZigBee, radio networks, mesh, distributed systems, sensor network, smart dust, ubiquitous computing, disappearing computer

Abstract

Today’s technological development brings an easement of work and expenditure for the people. Technical devices become compact and smart. The number of computer based tasks increases, the future trend is “Ubiquitous Computing“.

The objective of this thesis is to adapt a special everyday life situation to the technical progress whereby the manual part decreases. The gist of this work is the development of an ideal hardware solution for a sensor network.

An analysis will be performed to figure out the best capable radio technology with a special view on ZigBee. It follows the design of a power-efficient, smart and robust system with low complexity. This dissertation will be completed by the development of the hardware device and an exemplary application. Practical experiences are obtained by tests.

A view on possible Applications shows the wide range of use.

Danksagung

Ohne die Unterstützung einiger Personen und Firmen hätte ich die Bachelorarbeit in dieser Art nicht bewerkstelligen können. Somit nutze ich die Möglichkeit denjenigen, die mich fachlich und vor allem moralisch tatkräftig unterstützt haben, einen Dank auszusprechen:

Vielen Dank für die kontinuierliche Unterstützung durch die Professoren und Mitarbeiter der HAW Hamburg, insbesondere sind gemeint:

Prof. Gunter Klemke, für die Anregung, Kritik und Ermunterung und
Prof. Kai von Luck für seine Eigenschaft, ständig die eigene Überzeugung komplett zu verdrehen, so dass man gezwungen ist, sich noch tiefgründigere Gedanken zu machen. Bewundernswert ist bei Euch beiden, dass ihr stets ein offenes Ohr für Fragen habt und euch in den stressigsten Momenten Zeit für die Studenten nehmt.

Die Mitarbeiter aus dem CPT-Labor für die fachliche und materielle Unterstützung.

Einige meiner Kommilitonen, danke Jungs und Mädels, das war ein (mehr oder weniger) spaßiges Studium. Besonderer Dank sei an Olaf Rempel gerichtet!

Materielle Unterstützung erfolgte von den Firmen: ATMEL, MAXIM, Micrel und Samtec. Danke.

Der herzlichste Gruß sei an meine unglaublich tolle Familie gerichtet, besonders:

Ein riesengroßer Dank geht an meine Eltern, ohne euch wäre das Ganze überhaupt nicht möglich gewesen. Danke für die Unterstützung.

Meine Schwester Carla, was hätte ich bloß ohne dich gemacht? Es waren lange Nächte, hat sich aber gelohnt. Keine Ahnung wie ich das wieder gut machen soll.

Mein lieber Engel Nena, dass du mir ständig den Rücken freihältst und stärkst, mich immer wieder auf den Boden der Tatsachen zurückholst.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation

Hinter Forschung und Entwicklung steckt der Drang, Arbeit und Aufwand einfacher und gleichzeitig effektiver werden zu lassen.
Gerade in der Informationstechnologie verläuft der Fortschritt mit einer rasanten Geschwindigkeit. Betrachtet man den Verlauf des letzten halben Jahrhunderts, wird dies nur allzu deutlich.
Vor einiger Zeit noch waren informationstechnische Neuerungen lediglich kleinen Kreisen zugänglich. Zum einen waren sie für den Einzelnen zu teuer, zum anderen waren sie viel zu sperrig. Darüber hinaus war der Nutzen für einen Normalverbraucher eher gering.
Später gelangte ein Großteil der neuen Erfindungen und Entwicklungen ohne große Umwege direkt auf den Markt und wurde für den Normalverbraucher zugänglich. Das hat mehrere Ursachen: Die Geräte der IT-Branche wurden bezahlbar und gleichzeitig relativ handlich. Zudem sahen die Endverbraucher einen Nutzen in den Komponenten.

Diese Entwicklung hat sich bis heute so fortgesetzt, jedoch hat ein Faktor in der Entwicklung immer mehr an Bedeutung gewonnen:
Da die Zielgruppe im Großteil aus Menschen besteht, welche die Technik nutzen möchten, sie aber auf der anderen Seite nicht als lästig oder störend wahrnehmen wollen, muss neben dem technischen Hintergrund auch auf das äußere Erscheinungsbild Wert gelegt werden. Bei Handys beispielsweise wird auf Form, Farbe und Design geachtet, was sie zusätzlich zu ausschmückenden Accessoires macht. Komponenten, mit denen man nicht direkt (physikalisch) in Verbindung treten muss, sollen gar nicht zu sehen sein. Hier fällt der Begriff „Disappearing Computer“ [DC].
Die Initiative „Disappearing Computer“ verfolgt das Ziel, sämtliche Technologien und deren Gerätschaften so in den Alltag zu integrieren, dass sie dem Menschen nicht mehr auffallen. Beispielsweise werden alltägliche Objekte als Container verwendet.

Da ein Anspruch an die Module auch die Kopplung untereinander ist, muss die Möglichkeit der Verbindung gewährleistet sein. Hierbei bietet sich die kabel- bzw. drahtlose Kommunikation an.
Kabellos bedeutet wiederum, dass Module sich selbst mit Strom versorgen müssen. Damit das System effektiv bleibt, muss zudem auf geringen Stromverbrauch geachtet werden.

Im Endeffekt ist bei der Entwicklung neuer bzw. Optimierung alter Technologien auf drei Eigenschaften zu achten:

1. Eine Technologie sollte einem nützlichen Zweck dienen, es soll Arbeit abnehmen oder zumindest erheblich erleichtern.
2. Das technische Gerät sollte nicht mehr als dieses erkennbar sein. Entweder ist es versteckt oder in ein attraktives Design verpackt.
3. Die Kommunikation soll uneingeschränkt möglich sein. Um dem Anspruch von „Disappearing Computer“ gerecht zu werden, geschieht diese vorzugsweise kabellos. Autonome Module werden im Idealfall nicht extern mit Strom ver-

sorgt. Die Versorgung über Batterien oder Akkumulatoren erfordert eine stromeffiziente Technologie.

1.2 Szenario

Im Folgenden wird ein Szenario beschrieben, welches der Arbeit als exemplarischer Bezugspunkt dient:

Im Mittelpunkt steht eine Person, welche im Besitz eines großen Grundstückes ist. Das Stück Land ist abwechslungsreich gestaltet. Es ist in einzelne Parzellen aufgeteilt, welche mit diversen Bodengewächsen und Sträuchern bepflanzt sind. Zudem ist ein relativ kleiner Teich vorhanden, der genutzt wird, um das Land mit Wasser zu versorgen.
Erreichbar sind die verschiedenen Parzellen über sehr lange Trampelpfade, zurückgelegt werden diese per Fahrrad oder zu Fuß.
Die Bewässerung erfolgt über einfach aufgebaute Sprinkleranlagen und Bewässerungsgräben. Als Haupttransportmittel für Betriebsmittel und Werkstoffe dient eine Schubkarre.
In der Nähe der Grundstücksgrenze befindet sich das Haus des Eigentümers. Es ist in zwei Bereiche unterteilt: zum einen als Wohnstätte, zum anderen sind hier sämtliche Maschinen, Werkzeuge und Verbrauchsgüter wie beispielsweise Dünger und Samen für die Arbeit auf dem Stück Land untergebracht.

Um einen Einblick in den Alltag des Eigentümers zu geben, werden exemplarisch ein paar Arbeitsabläufe genauer erläutert:

1. Bewässerung der Felder in Abhängigkeit vom Zustand der Felder

   Grundlage für ein ausgewogenes Wachstum ist die regelmäßige Überprüfung des Zustandes seiner Pflanzen. Es wird jedes Feld abgelaufen bzw. abgefahren und die Beschaffenheit des Bodens in Bezug auf Feuchtigkeit kontrolliert. Mangelt es an Wasser, erfolgt die Aktivierung des Bewässerungssystems, indem die Ventile der Sprinkleranlagen bzw. die Zuleitungen zu den Wassergräben geöffnet werden. Ist der Zustand des Bodens zufrieden stellend, werden die Ventile und Zuleitungen geschlossen. Die *Abbildung 1: Szenario - Zustandsprüfung* verdeutlicht diesen Vorgang mittels eines Flussdiagramms.

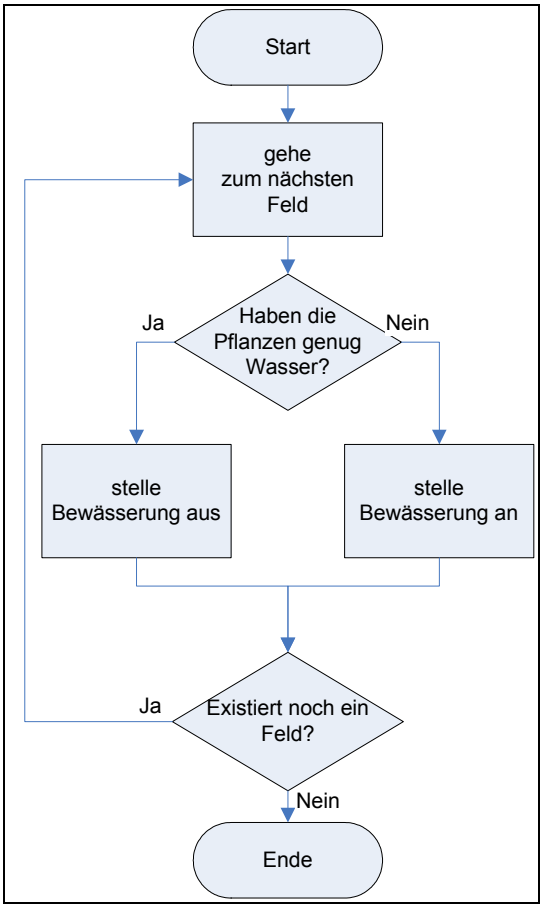

Abbildung 1: Szenario - Zustandsprüfung

2. Bewässerung der Felder in Abhängigkeit vom Wetter

   Aufgrund der geringen Größe des Teiches, welcher als primäre Wasserquelle dient, muss mit dem Wasser sparsam umgegangen werden.
   Sobald es regnet, werden sämtliche Bewässerungssysteme abgestellt. Das Bewässerungssystem eines jeden Feldes wird auf Aktivität hin geprüft und gegebenenfalls abgestellt (*Abbildung 2: Szenario - Regen*).

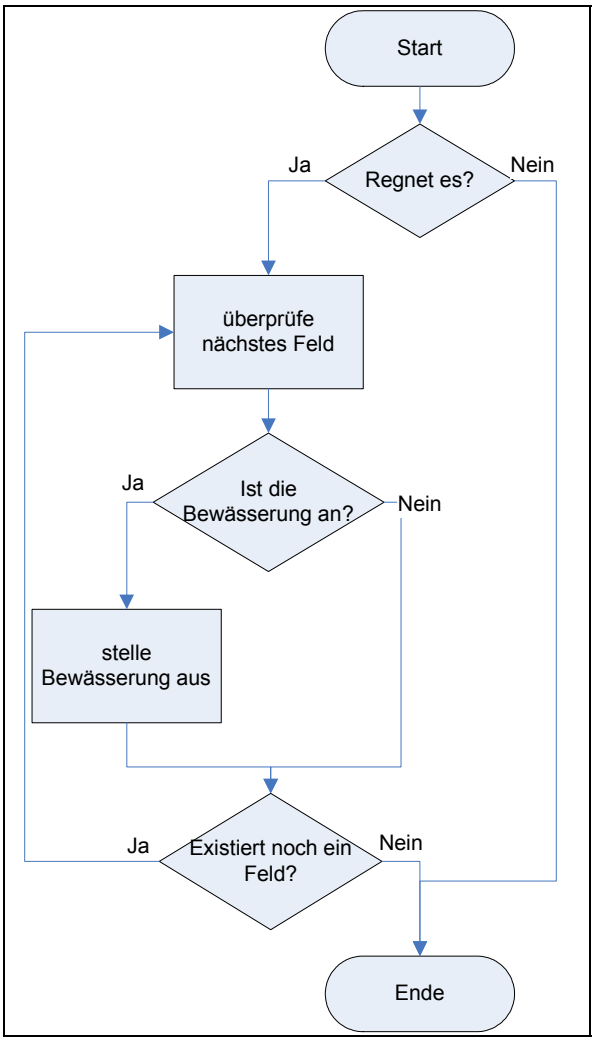

Abbildung 2: Szenario - Regen

3. Die Wasserversorgung des gesamten Grundstückes ist folgendermaßen gewährleistet:
   Die Hauptquelle ist der auf dem Grundstück befindliche Teich. Durch ein Pumpensystem wird bei Bedarf Wasser entnommen und direkt in die Bewässerungsanlage gefördert. Gerade in der Sommerzeit, wo entsprechend viel Wasser benötigt wird, kann es passieren, dass der Wasserspiegel schnell einen niedrigen Pegel erreicht. Der Besitzer vollzieht regelmäßig eine Sichtprüfung durch eine einfache Markierung, welche den Mindeststand im Teich kennzeichnet. Erreicht der Teich diese Mindestmarke, wird das Pumpensystem deaktiviert. Alternativ wird eine Grundwasserpumpe eingesetzt. (*Abbildung 3: Szenario - Versorgung*)

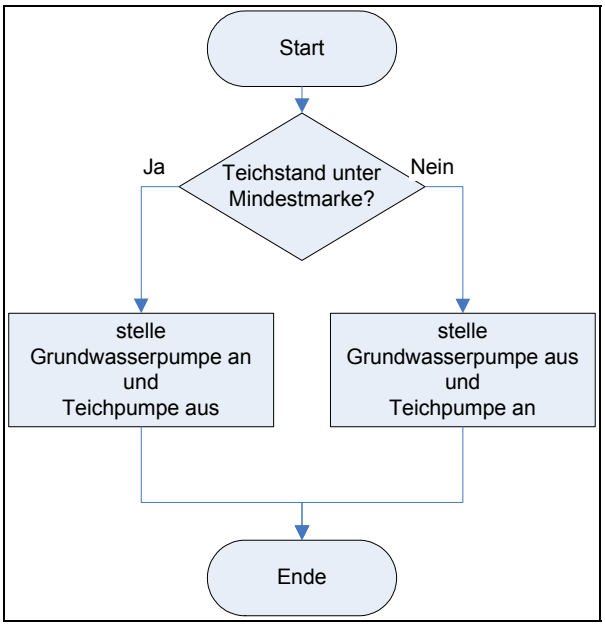

Abbildung 3: Szenario - Versorgung

1.3 Zielsetzung

In Anbetracht des Szenarios mit Rückblick auf die Motivation ergibt sich für diese Arbeit folgendes Ziel:

1. Es ist ein System zu entwickeln, welches die Arbeitsabläufe des Grundstückseigentümers effektiver gestaltet und somit seinen Alltag erleichtert.
2. Das System soll nicht als dieses zu erkennen sein oder zumindest in einem dermaßen dezenten Design entwickelt werden, dass es kaum bemerkbar ist.
3. Die Kommunikation innerhalb des Systems sowie nach außen hin soll hauptsächlich kabellos funktionieren, was wiederum den Einsatz einer leistungseffizienten Technologie voraussetzt.

Schwachstellen des bisherigen Arbeitsablaufes:

Da das Gebiet sehr groß ist, verwendet der Eigentümer einen Großteil seiner Zeit durch das Zurücklegen von Strecken. Vorort werden dann oftmals nur kurzweilige Tätigkeiten durchgeführt, wie die Feuchtigkeitsprüfung des Bodens oder das An- und Abschalten von Bewässerungsanlagen oder Pumpen.

An folgenden Stellen sind die Tätigkeiten zu erleichtern:

- Sämtliche Messungen, wie die Feuchtigkeitsprüfung des Bodens oder die Untersuchung des Wasserstandes des Teiches, werden manuell verrichtet. **An dieser Stelle lassen sich ohne weiteres elektronische Sensoren einsetzen.**

- Abhängig von gemessenen Werten reagiert der Besitzer mit Aktivierung bzw. Deaktivierung von Geräten. Beispiele sind das Ein- und Ausschalten von Bewässerungsanlagen oder das Umschalten von der Teich- auf die Grundwasserpumpe.
  Durch Modifikation der Geräte lassen sich diese leicht elektronisch regeln.

Die Grundidee ist es, ein System zu entwickeln, in dem die Sensorik und die Aktorik über logische Algorithmen miteinander verknüpft werden.

Das bedeutet konkret, einzelne Module zu entwickeln, die auf lokaler Basis Messdaten der Sensoren empfangen, auswerten und direkt Aktoren ansteuern.

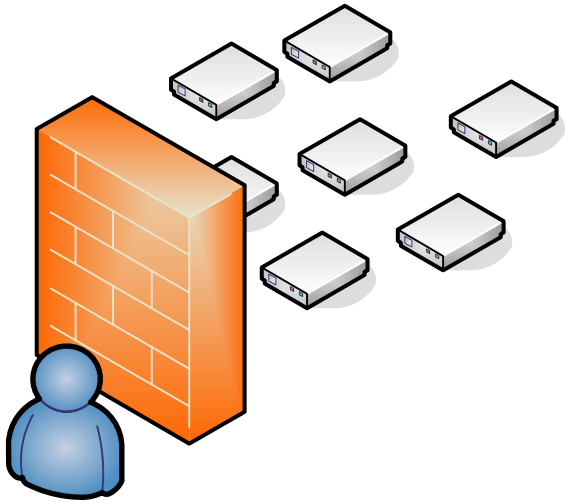

Abbildung 4: Ziel - Modul 1

Mit diesem Konzept hätte der Eigentümer jedoch weder Kontrolle über noch Einfluss auf die Arbeitsabläufe. Es muss in dem Maße erweitert werden, dass der Besitzer zum einen die Möglichkeit erhält, das System nach allen Arten des Monitoring zu nutzen. Zum anderen muss zu jeder Zeit die Option bestehen, in das aktuelle Geschehen eingreifen und die Aktoren manuell regeln zu können.

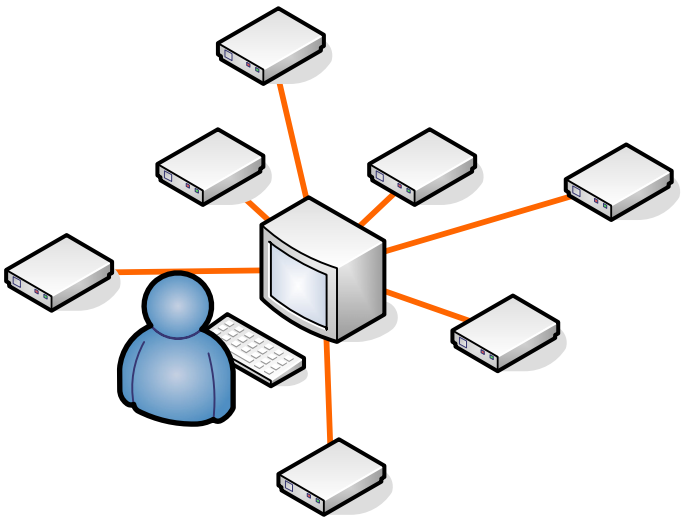

Abbildung 5: Ziel - Modul 2

Somit bildet sich ein sternförmiges Netzwerk. Um den Anforderungen an dieses Konzept gerecht zu werden, müssen kabelgebundene Verbindungen so weit wie möglich durch drahtlose ersetzt werden.

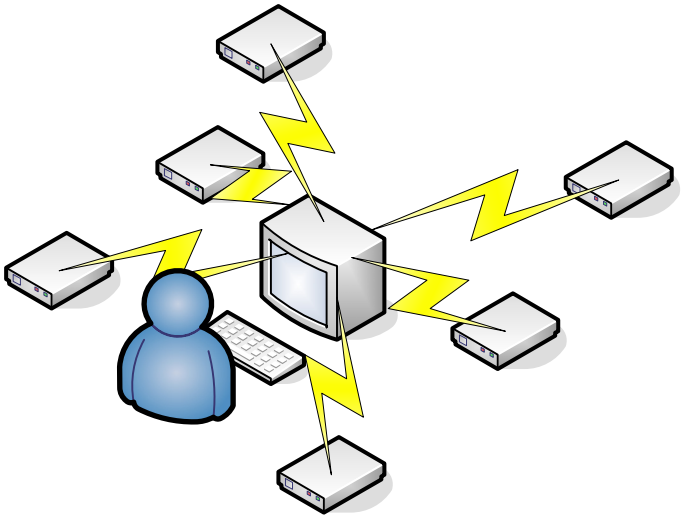

Abbildung 6: Ziel - Modul 3

Eine spätere Erweiterung des Grundstückes und die damit erforderliche Vermehrung der Sensorik und Aktorik sind nicht ausgeschlossen. Es muss stets die Möglichkeit bestehen, das Netzwerk ohne großen Aufwand um Module zu erweitern beziehungsweise zu verringern.
Das System darf nicht nur auf die derzeit angeschlossene Hardware beschränkt sein. Neue Sensorik und Aktorik muss sich ebenfalls ohne großen Aufwand in das System einbinden lassen.
Die Module kommunizieren kabellos. Um sie nicht aufgrund der Stromversorgung wieder ans Kabel zu binden, werden sie per Batterie bzw. Akkumulator betrieben und müssen dementsprechend stromeffizient arbeiten.

Distanzierung:
Um die Entwicklung des Systems mit geringem Aufwand auf andere Problemstellungen übertragen zu können, distanziert sich die Arbeit im Folgenden von dem ursprünglichen Szenario im speziellen Sinn. Die aus dem Szenario gewonnen Kernaussagen bzw. Anforderungen sind Basis für die Entwicklung.

Das System besteht aus einem Netzwerk beliebig vieler Knoten, die sich voneinander nicht unterscheiden. Lediglich die angeschlossene Sensorik und Aktorik sind verschieden oder können es sein. Somit sind im Endeffekt ein Modul, welches einen Knoten bildet, und die Topologie des Netzwerkes zu entwickeln. An diese werden, noch einmal zusammengefasst, folgende Anforderungen gestellt:

- Anforderungen an das Modul:
  - Anschlussmöglichkeit für beliebige Sensoren und Aktoren
  - normierte Schnittstelle (als Anschlussmöglichkeit für z.B. einen Computer)
  - Stromversorgung per Batterie bzw. Akku

- Anforderungen an das Modul-Netzwerk
  - zentralisierte Steuerung und Monitoring der Knoten
  - Netzwerk beliebig erweiterbar und reduzierbar
  - drahtlose Kommunikation

1.4 Gliederung der Arbeit

Die Motivation für diese Arbeit ist im Kapitel 1, Einleitung beschrieben. Zusätzlich wird dort ein spezielles Szenario vorgestellt, welches einen beispielhaften praktischen Bezug vermittelt.

In dem 2. Kapitel, Technologien, werden vorausgehend Technologien erläutert, die einen wesentlichen Kern in dieser Arbeit bilden.

Im 3. Kapitel, Analyse werden aktuelle Funktechnologie-Standards miteinander verglichen und die geeignete bezüglich der Zielsetzung dieser Arbeit ausgewählt.

Die praktische Entwicklung des Moduls wird im Kapitel 4, Design und Realisierung geschildert. Hier werden die schlussendlich verwendeten Komponenten festgelegt, das Design des Moduls erarbeitet und der Entwicklungsablauf beschrieben.

Das 5. Kapitel, Das Modul setzt sich mit dem praktischen Ergebnis, dem entstandenen Modul auseinander. Hier werden wesentliche Funktionsmöglichkeiten aufgezeigt und die grundlegende Handhabung dokumentiert.

Analog zum fünften wird im 6. Kapitel, Applikation eine beispielhafte Implementierung vorgestellt.

Das 7. Kapitel, Validierung und Teste setzt sich mit dem hier entstandenen Modul auseinander. In der praktischen Anwendung wird gestestet, ob die Praxis der Theorie entspricht.

Das 8. Kapitel, Verwendungsmöglichkeiten beschreibt das Anwendungsgebiet des Moduls anhand von exemplarischen Szenarien. Es soll ein Eindruck davon vermittelt werden, wie vielfältig das System einsetzbar ist.

Im 9. Kapitel, Zusammenfassung werden Gedanken bezüglich dieser Arbeit angesprochen. Beispielsweise mit welchen Fragen und an welcher Stelle diese Arbeit fortgeführt bzw. erweitert werden könnte. Zudem werden Verbesserungsmöglichkeiten an der eigenen Arbeit aufgezeigt.

2 Technologien

2.1 IEEE 802.15.4

Quelle: [IEEE 802.15.4], [JGut]

2.1.1 Kurzdarstellung

Das durch die IEEE 802.15.4-Spezifikation definierte Protokoll beschreibt den kompatiblen Verbund von Daten-Kommunikations-Geräten unter Hochfrequenztechnik. Die beteiligten Geräte zeichnen sich in

- geringer Datenübertragungsgeschwindigkeit
- geringem Leistungsverbrauch
- geringer Reichweite und
- geringer Komplexität

aus und bilden ein kabelloses Netzwerk, das LR-WPAN.

Die Haupteigenschaften des Netzwerkes sind:

- Bandbreiten von 250 kb/s, 40 kb/s und 20 kb/s
- Sternen- oder Peer-to-Peer- Struktur
- Verfügbarer Adressraum von 16 Bit oder 64 Bit
- garantiert zugewiesene Zeitscheiben
- Kanalzugriffssteuerung durch CSMA/CA – Algorithmus
- Zuverlässiger Datentransfer durch gesichertes Protokoll
- Anzeige der Verbindungsqualität
- 16 Kanäle bei 2450 MHz, 10 Kanäle bei 915 MHz, 1 Kanal bei 868 MHz

2.1.2 Komponenten des WPAN

Ein System gemäß der IEEE 802.15.4 setzt sich aus mehreren Komponenten zusammen. Es entsteht dann ein WPAN, wenn sich mindestens zwei Geräte in einem definierten Bereich befinden und auf demselben Kanal arbeiten. Jedes Gerät kann entweder eine vollständig funktionsfähige Einheit (FFD) oder eine beschränkt funktionsfähige Einheit (RFD) sein, wobei jedoch ein Gerät als FFD und somit als PAN-Koordinator fungieren muss.

2.1.3 Netzwerktopologien

Die Art der Anwendung entscheidet, welche Netzwerkstruktur in einem LR-WPAN verwendet wird: die Stern- oder die Peer-to-Peer-Topologie (siehe *Abbildung 7: IEEE 802.15.4 - Netzwerktopologie*).

In der Stern-Topologie ist der zentrale Punkt ein PAN-Koordinator, alle weiteren Module sind ausschließlich mit ihm verbunden. Jedes Gerät hat eine bestimmte Aufgabe und ist entweder der Anfangs- oder der Endpunkt einer Kommunikation.
Der PAN-Koordinator erstellt Verbindungen, trennt sie oder leitet den Verkehr innerhalb des Netzwerkes weiter (Routing). Ihm kann zusätzlich eine bestimmte Aufgabe zugeteilt werden.

Die Peer-to-Peer-Topologie hat als zentralen Punkt ebenfalls einen PAN-Koordinator. Alle Geräte sind innerhalb ihrer Reichweiten des PAN miteinander verbunden.
Die somit entstandene Struktur ist sehr komplex, kann sich ad-hoc formen und kann unterbrochene Wege selbständig heilen.

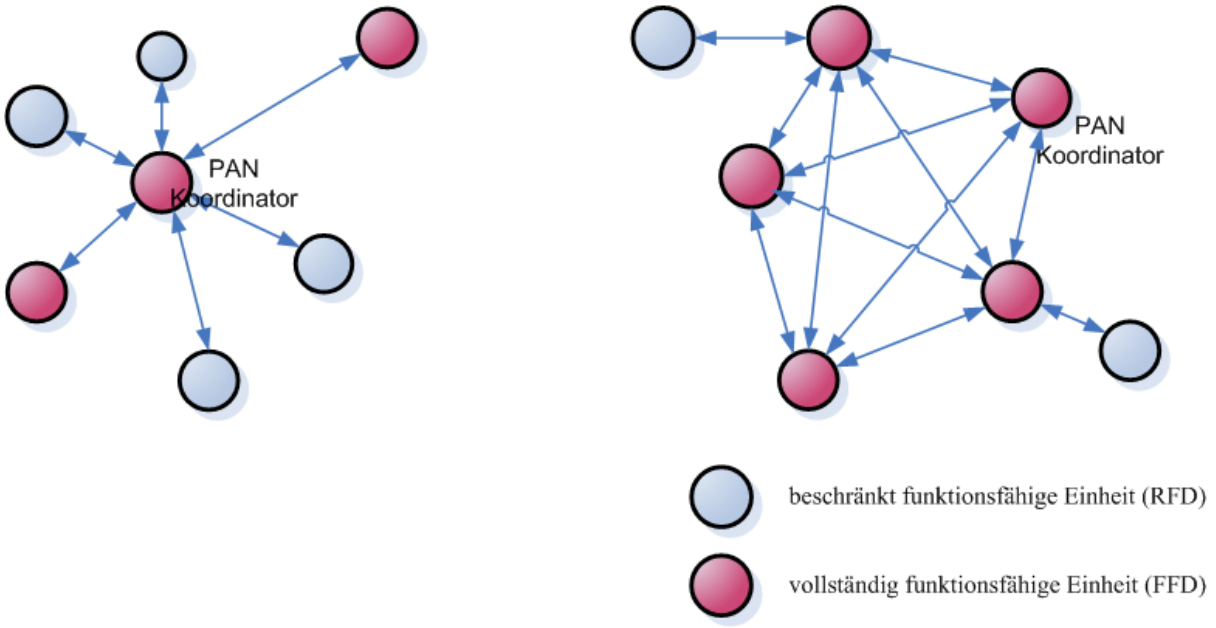

Abbildung 7: IEEE 802.15.4 - Netzwerktopologie

2.1.4 Architektur

Die Architektur des LR-WPAN basiert auf dem Layout des ISO /OSI –Modell. Sie ist in Schichten eingeteilt, jede Schicht stellt Dienste zur Verfügung, welche von der oberen Ebene genutzt werden (*Abbildung 8: IEEE 802.15.4 - Schichtenmodell*).

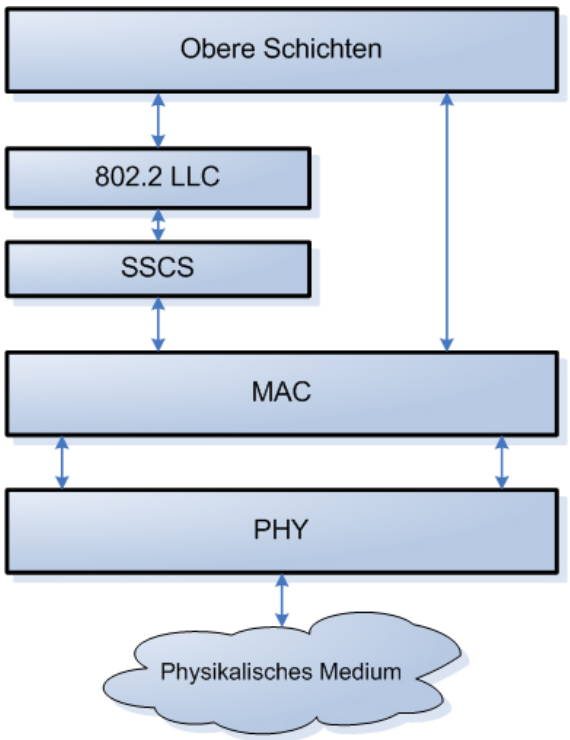

Abbildung 8: IEEE 802.15.4 - Schichtenmodell

2.1.4.1 Die Physikalische (PHY) Schicht

Die PHY-Schicht offeriert zwei Dienstleistungen: der PHY Datendienst und der PHY Managementdienst. Der Datendienst ist für das Senden und Empfangen der PHY-Protokoll Dateneinheiten (PPDU's) auf dem Funkkanal verantwortlich. Die Fähigkeiten der PHY-Schicht sind:

- Ein- bzw. Ausschalten des Funksendeempfängers
- ED innerhalb des aktuellen Kanals
- Angabe der Verbindungsqualität für empfangene Pakete
- CCA für CSMA/CA
- Auswahl der Kanalfrequenz
- Datentransport

Die Funkverbindung muss auf einer der folgenden Frequenzen betrieben werden:

- 868 - 868.6 MHz (z.B. für Europa)
- 902 - 928 MHz (z.B. für Nord-Amerika)
- 2400 - 2483.5 MHz (weltweit)

2.1.4.2 Die MAC-Schicht

Die MAC-Schicht teilt sich in zwei Bereiche, den MAC Datendienst und den MAC Managementdienst. Der Datendienst ist verantwortlich für das Senden und Empfangen der MAC-Protokoll Dateneinheiten (MPDU's) über den PHY Datendienst. Die Fähigkeiten der MAC-Schicht sind:

- Erzeugung von Beacons innerhalb des Netzwerkes, falls das Gerät ein Koordinator ist
- Synchronisation nach den Beacons
- Auf- und Abbau der PAN-Verbindung
- Sicherheit des Gerätes
- Vermeidung von Konkurrenzsituationen beim Senden durch Anwendung des CSMA/CA-Algorithmus
- Anwendung und Aufrechterhaltung des GTS-Mechanismus
- Bereitstellung einer gesicherten Verbindung zwischen zwei MAC-Einheiten

2.1.5 Funktionen

2.1.5.1 Superframe-Struktur

Die Superframe-Struktur bietet dem Koordinator die Möglichkeit, die Geräte in einem Netzwerk zu synchronisieren, das PAN zu identifizieren und die Struktur der Superframes zu beschreiben. Ob es zur Anwendung dieser kommt, wird durch den Koordinator entschieden. Durch den am Anfang einer jeden Superframe-Struktur (Gesamtlänge: 16 Frames) befindlichen Beacon (ein Frame) wird der Zeitraum (CAP) definiert, in dem durch CSMA/CA der Zugriff auf den Kanal erreicht werden kann (siehe *Abbildung 9: IEEE 802.15.4 - Superframestruktur ohne GTS*).

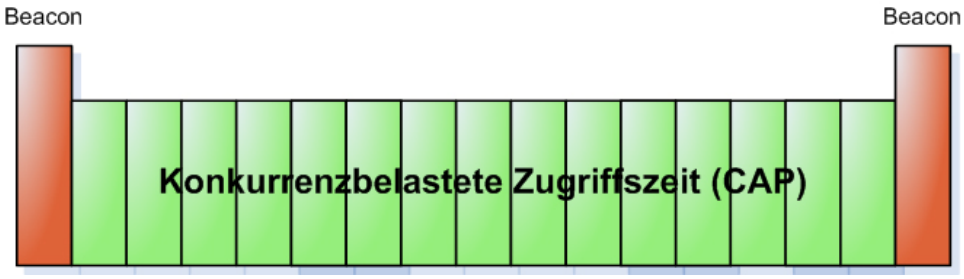

Abbildung 9: IEEE 802.15.4 - Superframestruktur ohne GTS

Für das Senden von Daten innerhalb des CAP können auch Zeitschlitze (GTS) vergeben werden. Dadurch ist eine echtzeitfähige Anwendung gewährleistet. Interessant ist dies beispielsweise bei dem Auslesen von Daten in fest definierten Perioden. Es sollte nicht das komplette Superframe in Zeitschlitze aufgeteilt werden, um anderen Netzteilnehmern die Chance zum Senden zu geben oder den Eintritt neuer Geräte zu ermöglichen(siehe *Abbildung 10: IEEE 802.15.4 - Superframestruktur mit GTS*).

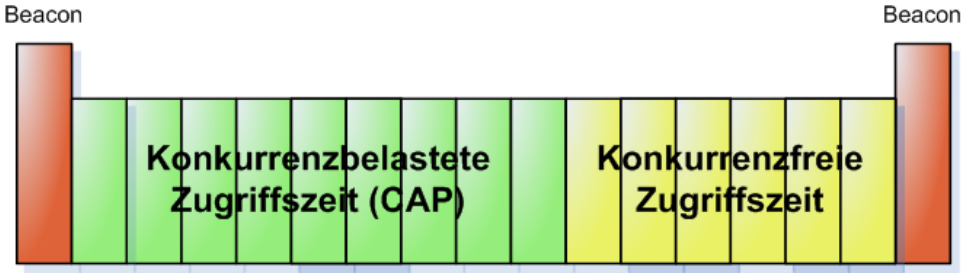

Abbildung 10: IEEE 802.15.4 - Superframestruktur mit GTS

2.1.5.2 Datenübertragung

Drei Arten der Datenübertragung sind definiert:

2.1.5.2.1 Transfer zum Koordinator

In diesem Fall handelt es sich um den Datentransfer von einem Gerät zum Koordinator.
Will ein Gerät in einem Beacon-Netzwerk Daten an den Koordinator übertragen, muss auf das Beacon gewartet werden. Sobald dieser erkannt wurde, erfolgt die Synchronisation zu der Superframe-Struktur. Unter Verwendung von slotted CSMA/CA werden an der entsprechenden Stelle die Daten an den Koordinator übertragen. Optional wird der Empfang dieser vom Koordinator via ACK-Frame bestätigt (siehe *Abbildung 11: IEEE 802.15.4 – Transport zu Koordinator in einem Beacon-Netzwerk*).

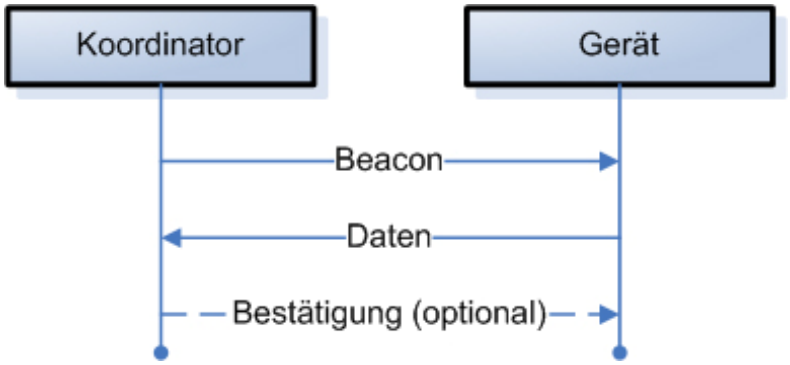

Abbildung 11: IEEE 802.15.4 – Transport zu Koordinator in einem Beacon-Netzwerk

Befindet sich das Gerät in einem Non-Beacon-Netzwerk, erfolgt die Datenübertragung einfacher. Es wird das unslotted CSMA/CA verwendet und die Daten mit einem Mal an den Koordinator gesendet. Der Koordinator hat die Möglichkeit, den Empfang über ein ACK-Frame zu quittieren (siehe *Abbildung 13: IEEE 802.15.4 – Transport zu einem Gerät in einem Beacon-Netzwerk*).

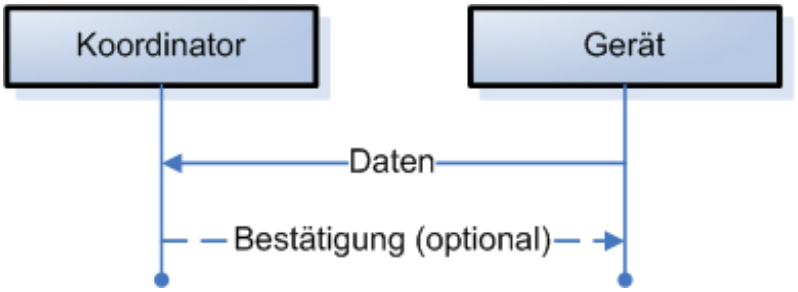

Abbildung 12: IEEE 802.15.4 – Transport zu Koordinator in einem Nicht-Beacon-Netzwerk

2.1.5.2.2 Transfer vom Koordinator

Der Datentransfer vom Koordinator zu einem Gerät:
Wenn der Koordinator in einem Beacon-Netzwerk Daten an ein Gerät übertragen möchte, wird dies in einem Beacon anhand einer Nachricht signalisiert.
Das Gerät horcht in regelmäßigen Abständen auf das Beacon. Liegt eine Nachricht vor, wird unter Verwendung von slotted CSMA/CA eine Datenanforderung gesendet.

Der Koordinator schickt nach einem unverbindlichen ACK-Frame die Daten, ebenfalls unter Verwendung von slotted CSMA/CA. Das Gerät kann den Empfang per ACK-Frame quittieren. Anschließend wird die Nachricht durch den Koordinator aus der Liste im Beacon entfernt (siehe *Abbildung 13: IEEE 802.15.4 – Transport zu einem Gerät in einem Beacon-Netzwerk*).

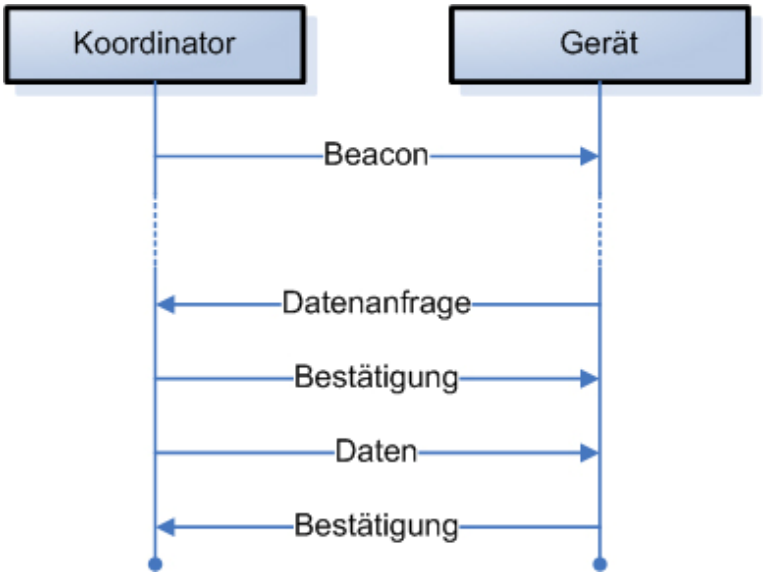

Abbildung 13: IEEE 802.15.4 – Transport zu einem Gerät in einem Beacon-Netzwerk

In einem Non-Beacon-Netzwerk speichert der Koordinator die Daten zwischen und wartet auf eine explizite Anfrage durch das adressierte Gerät:
Unter Verwendung von unslotted CSMA/CA schickt das Gerät in programmspezifischen Abständen Datenanforderungen an den Koordinator. Dieser quittiert mit einem ACK-Frame und sendet bei vorhandenen Daten, ebenfalls unter Verwendung von unslotted CSMA/CA, die Daten an das Gerät.
Sollten keine Daten vorhanden sein, wird ein Datenpaket der Länge null geschickt. Das Gerät bestätigt den Empfang mit einem ACK-Frame (siehe *Abbildung 14: IEEE 802.15.4 – Transport zu einem Gerät in einem Non-Beacon-Netzwerk*).

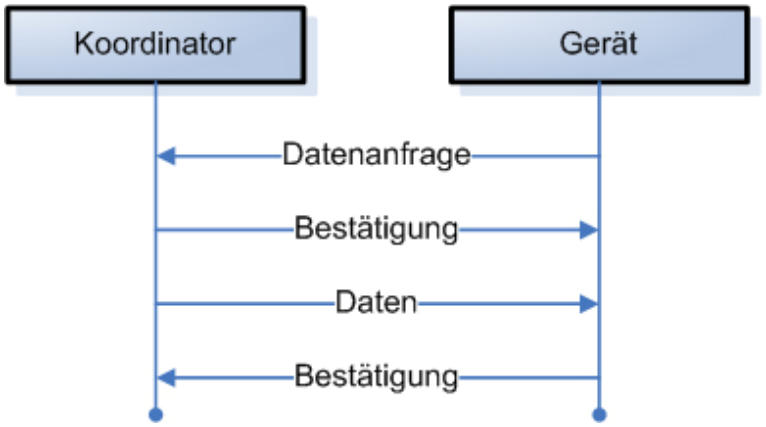

Abbildung 14: IEEE 802.15.4 – Transport zu einem Gerät in einem Non-Beacon-Netzwerk

2.1.5.2.3 Peer-to-Peer-Transfer

In einem Peer-to-Peer-Netzwerk kann jedes Gerät mit jedem anderen innerhalb seiner Reichweite kommunizieren. Um dies effektiv zu tun, kann beispielsweise unslotted CSMA/CA verwendet werden. Eine aufwändige Lösung gehört nicht zu dem Umfang dieses Standards.

2.1.5.3 Frame-Struktur

Das LR-WPAN definiert vier Rahmenstrukturen für Pakete (Frames). Im Hintergrund liegen hierbei die Aspekte, die Komplexität der Struktur niedrig zu halten und sie gleichzeitig ausreichend robust zu gestalten. Somit kann der Verkehr auf einem empfindlichen Kanal gewährleistet werden.
Die einzelnen Pakete setzen sich aus dem Header der PHY-Schicht und der MPDU zusammen, welche durch die MAC-Schicht definiert wird.
Die MPDU besteht aus drei Teilen:

- **der Header (MHR)**
  Das Frame-Control-Field liefert neben einigen Kontroll-Flags Informationen über den Pakettyp. Neben der Paket-Sequenznummer sind im MHR spezielle Adress-Felder reserviert. Anwendungsabhängig können dort diverse Informationen bezüglich Absender, Empfänger und PAN-ID abgelegt werden.

- **die MAC Dateneinheit (MSDU)**
  Die MSDU speichert abhängig vom Pakettyp spezifische Daten wie weiter unten kurz beschrieben.

- **der Footer (MFR)**
  Am Ende des MAC-Frame befindet sich eine Feld für die Checksumme des Paketes, über welches die Vollständigkeit des Paketes geprüft wird.

2.1.5.3.1 Beacon-Frame

Die MSDU des Beacon-Frame beinhaltet Informationen zum Netzaufbau. Enthalten sind beispielsweise Informationen über die Super-Frame-Struktur und der Dateninhalt des Beacon.

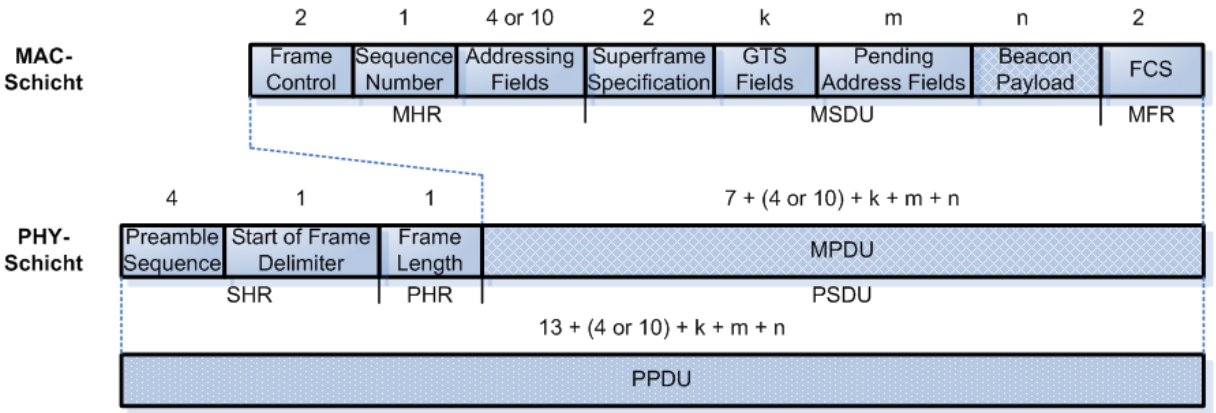

Abbildung 15: IEEE 802.15.4 - Beacon-Frame

2.1.5.3.2 Daten-Frame

Das Daten-Frame führt in der MSDU ein einziges Datenfeld, wo bis zu 116 Byte Daten abgelegt werden können.

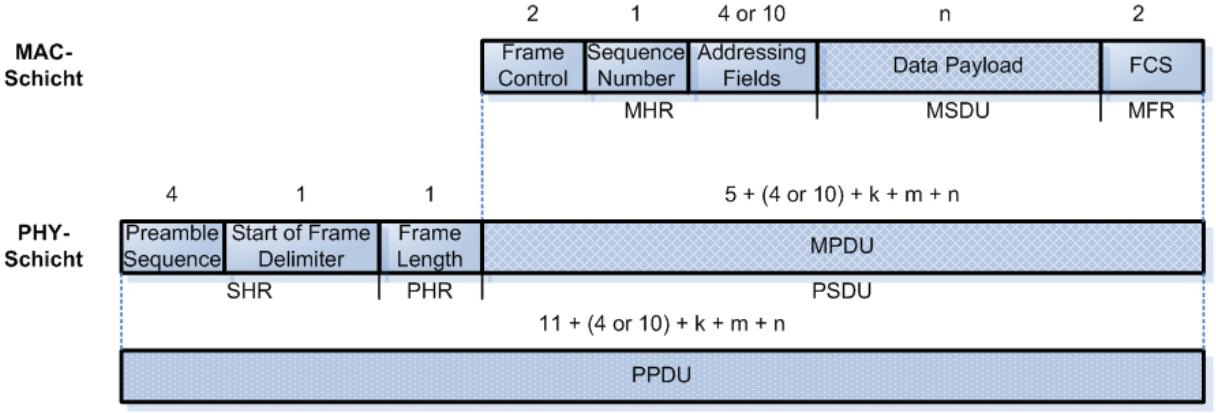

Abbildung 16: IEEE 802.15.4 - Daten-Frame

2.1.5.3.3 Acknowledgement-Frame

Das Acknowledgement-Frame ist das am einfachsten aufgebaute Paket. Die MSDU ist nicht vorhanden, es wird im Header lediglich die Sequenz-Nummer des zu bestätigenden Paketes überragen.

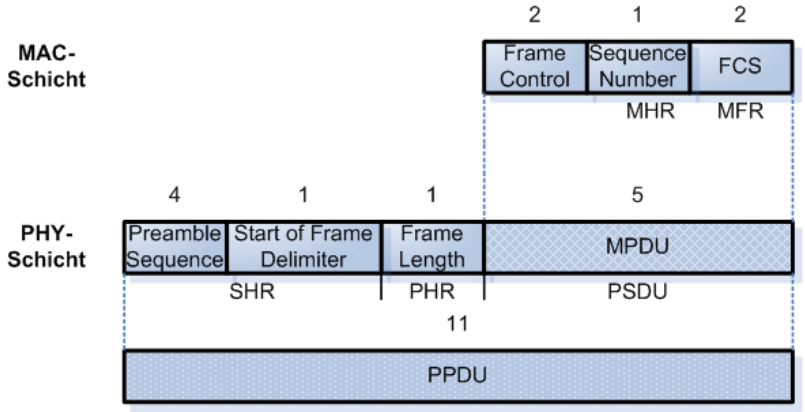

Abbildung 17: IEEE 802.15.4 - Acknowledgement-Frame

2.1.5.3.4 MAC-Command-Frame

Das MAC-Command-Frame trägt in der MSDU Informationen über den Kommandotyp und die Kommando-relevanten Daten.

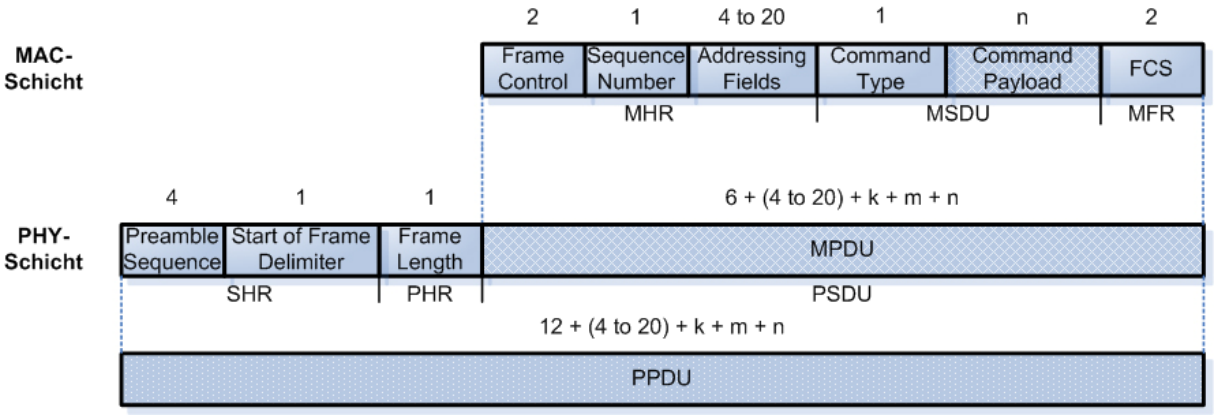

Abbildung 18: IEEE 802.15.4 - MAC-Command-Frame

2.1.5.4 Robustheit

Ausreichende Robustheit erreicht das LR-WPAN mithilfe folgender Mechanismen:

2.1.5.4.1 CSMA/CA Mechanismus

Es werden zwei Mechanismen genutzt um auf einem Kanal zu operieren (siehe *Abbildung 19: IEEE 802.15.4 - CSMA/CA-Mechanismen*). Interessant ist das CSMA/CA-Verfahren für Daten-Frames oder MAC-Kommandos. ACK- und Beacon-Frames werden ohne Verwendung des CSMA/CA-Mechanismus verschickt.

- Non-Beacon-Netzwerke verwenden unslotted CSMA/CA. Will ein Gerät ein Paket senden, wartet es eine unbestimmte Zeitspanne. Nach Beendigung und wenn der Kanal frei ist, beginnt die Übertragung der Datenpakete. Sollte der Kanal belegt sein, wiederholt sich die Prozedur.

- Beacon-Netzwerke verwenden slotted CSMA/CA. Damit ein Gerät Daten senden kann, muss es auf das Ende einer Zeitschlitzperiode warten. Anschließend verharrt es ein zufällig generiertes Vielfaches einer Zeitschlitzperiode. Mit Beendigung der Zeitspanne lauscht das Gerät auf den Kanal. Ist er frei, beginnt die Übertragung, ansonsten startet die Prozedur erneut.

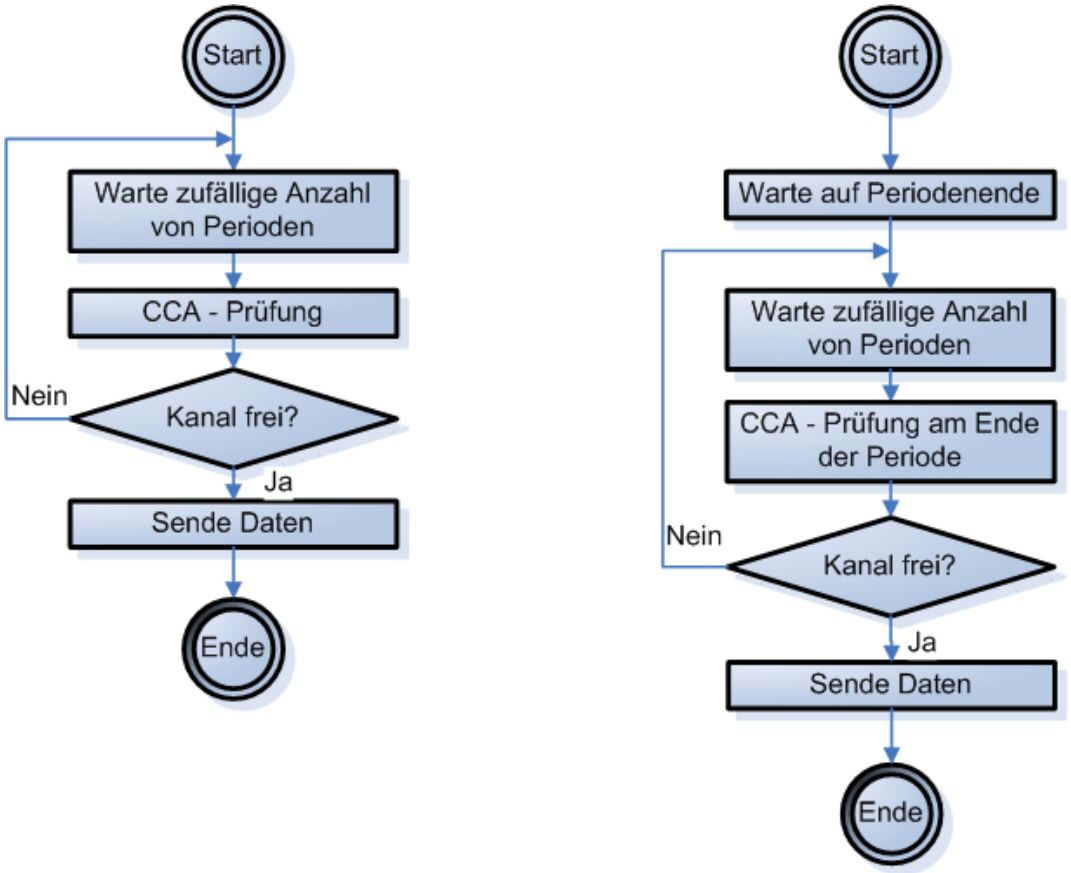

Abbildung 19: IEEE 802.15.4 - CSMA/CA-Mechanismen

2.1.5.4.2 Bestätigung der Pakete

Der erfolgreiche Empfang von Daten oder einem Mac-Kommando kann vom Adressaten durch ein Paket (ACK-Frame) bestätigt werden. Das ACK-Frame ist optional, abhängig von der Anwendung kann auf ein fehlendes ACK durch wiederholte Sendung oder Abbruch reagiert werden.

2.1.5.4.3 Verifikation der Daten

Um fehlerhafte Bits im Datenpaket zu erkennen wird ein Checksummen-Mechanismus (FCS) verwendet. Er entspricht der zyklischen Redundanzprüfung (englisch: cyclic redundancy check - CRC) und ist durch die ITU-T standardisiert. Die Anwendung findet auf jedes Datenpaket statt.

2.1.5.5 Leistungsverbrauch

Die Koordinatoren eines LR-WPAN sind in der Regel an ein Stromversorgungsnetz angeschlossen. Die restlichen Netzteilnehmer sind in der Regel autonome Einheiten, die überwiegend per Batterie versorgt werden. Das Protokoll ist darauf ausgelegt, stromeffizient zu arbeiten.
Die Module befinden sich den Großteil ihrer Laufzeit im Ruhezustand und lauschen regelmäßig auf ihre Kanäle, ob Nachrichten bzw. Daten an sie gerichtet sind und auf sie warten. Somit ist es dem Entwickler möglich, Anwendungen zu erstellen, deren Schwerpunkte geringer Verbrauch und kurze Latenzzeiten sind.

2.1.5.6 Sicherheit

Der in diesem Standard verwendete Sicherheitsmechanismus ist ein symmetrisches Kryptosystem. Schlüssel werden durch höhere Schichten bereitgestellt und auf MAC-Ebene zur Ver- und Entschlüsselung verwendet.
Es ist durch den Programmierer der höheren Schichten auf die ordnungsgemäße Erstellung, Weitergabe und Hinterlegung der Schlüssel zu achten.

2.1.5.6.1 Zugiffskontrolle

Nach dem Prinzip der Zugriffskontrolle führt jedes Gerät eine Zugriffskontrollliste (access control list - ACL). In dieser Liste sind die Geräte aufgeführt, von denen das Gerät den Empfang von Datenpaketen zulässt.

2.1.5.6.2 Datenverschlüsselung

Die Sicherheitsmechanismen in diesem Standard nutzen ein symmetrisches Kryptosystem. Datenverschlüsselung wird auf den Datenbereich von Beacon-, Kommando- und Datenframes angewandt.

2.1.5.6.3 Datenvertrauenswürdigkeit

Diese Sicherheitsleistung ist ein Service, der Pakete mithilfe des MIC (message integrity code) auf seine Vertrauenswürdigkeit prüft. Die fortlaufende Nummer der Pakete wird im verschlüsselten Datenbereich mit übertragen.

Der Empfänger überprüft die laufende Nummer und verwirft Pakete, welche nicht in die Reihenfolge passen. Durch diesen Mechanismus werden z.B. manipulierte Pakete herausgefiltert.
Datenvertrauenswürdigkeit wird auf den Datenbereich von Beacon-, Kommando- und Datenframes angewandt.

2.1.5.6.3.1 Sequenzielle Datenaktualität

Dieser Mechanismus überprüft die Aktualität der empfangenen Datenpakete. Ist ein Paket neuer als das zuvor empfangene, wird es akzeptiert, anderenfalls verworfen. Dadurch ist sichergestellt, dass das aktuelle Paket neuer als das zuvor empfangene ist.

2.2 ZigBee™

Quellen: [ZB_1], [ZB_2], [ZB_3], [ZB_4], [ZB_5], [ZB_6], [ZB_7], [ZB_8], [ZB_9]

2.2.1 Die ZigBee Alliance

Die ZigBee Alliance ist eine Vereinigung von Firmen. Sie arbeiten gemeinsam an Überwachungs- und Steuerungsprodukten, welche auf einem offenen, globalen Standard basieren. Die Produkte haben die Eigenschaften, verlässlich, kostengünstig, stromeffizient und kabellos zu sein.

Das Ziel der ZigBee Alliance ist es, den Verbrauche mit universell einsetzbarer, mobiler und einfach zu handhabender kabelloser Technik, eingebettet in alltägliche Geräte, auszustatten. Eingesetzt werden soll diese Technik in großen Umfang in den Bereichen Verbraucher, Gewerbe, Industrie und Regierung.
Zum 1. Mal gibt es für Firmen eine standardisierte Möglichkeit, kabellose Technik, optimiert auf individuelle Vorstellungen für entfernte Überwachungs- und Steuerungsanwendungen mit den Schwerpunkten Schlichtheit, Verlässlichkeit und Verbrauchseffizienz zu erhalten.

Die ZigBee Alliance setzt sich mit folgenden Aufgabenstellungen auseinander:

- Definition von Netzwerk-, Sicherheits- und Anwendungsschichten
- Bereitstellung der Spezifikationen für Interoperabilität der Geräte und der Konformitätsprüfung
- Weltweite Förderung und Verbreitung der Marke „ZigBee“
- Organisation der Entwicklung der Technologie

Aktuell befinden sich in der ZigBee Alliance 8 Promoter und über 175 weitere Mitglieder.

Der Name ZigBee stammt von der Honigbiene. Sie lebt in einem Bienenstock, der sich aus einer Königin, einigen Männchen und tausenden von Arbeitsbienen zusammensetzt. Um die Gesellschaft aufrecht zu erhalten, ist die ständige Kommunikation untereinander dringend notwendig. Die Art der Kommunikation und das Zickzackmuster der Bewegung der Bienen verleiht ZigBee den Namen.

2.2.2 Architektur

ZigBee verwendet für die eigene Architektur als Basis die IEEE 802.15.4 – Spezifikation und erweitert das Schichtenmodell um zwei weitere Ebenen und Sicherheitsdiensten (*Abbildung 20: ZigBee – Schichtenmodell*):

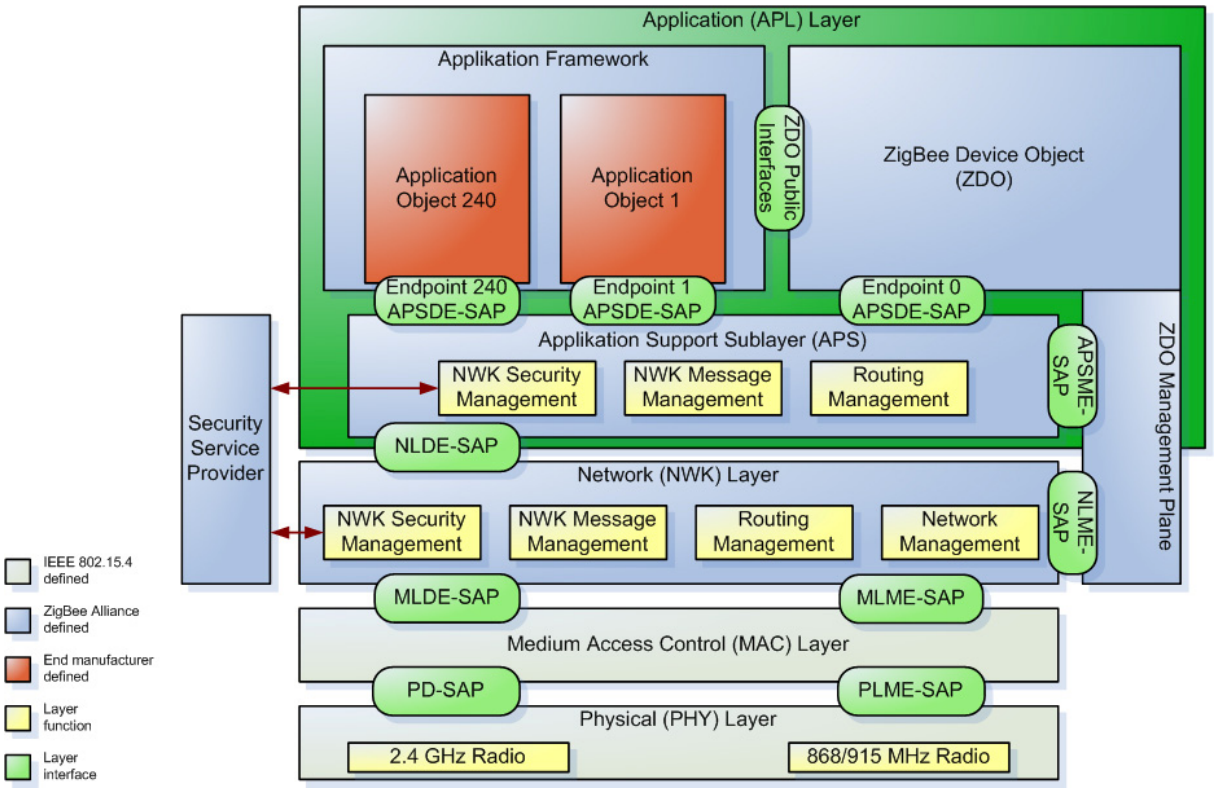

Abbildung 20: ZigBee – Schichtenmodell

Das Aufbau folgt dem Layout des ISO /OSI –Modells. Die Dienste einer jeden Schicht sind für die darauf folgende Ebene über Schnittstellen (engl. service access point - SAP) erreichbar.

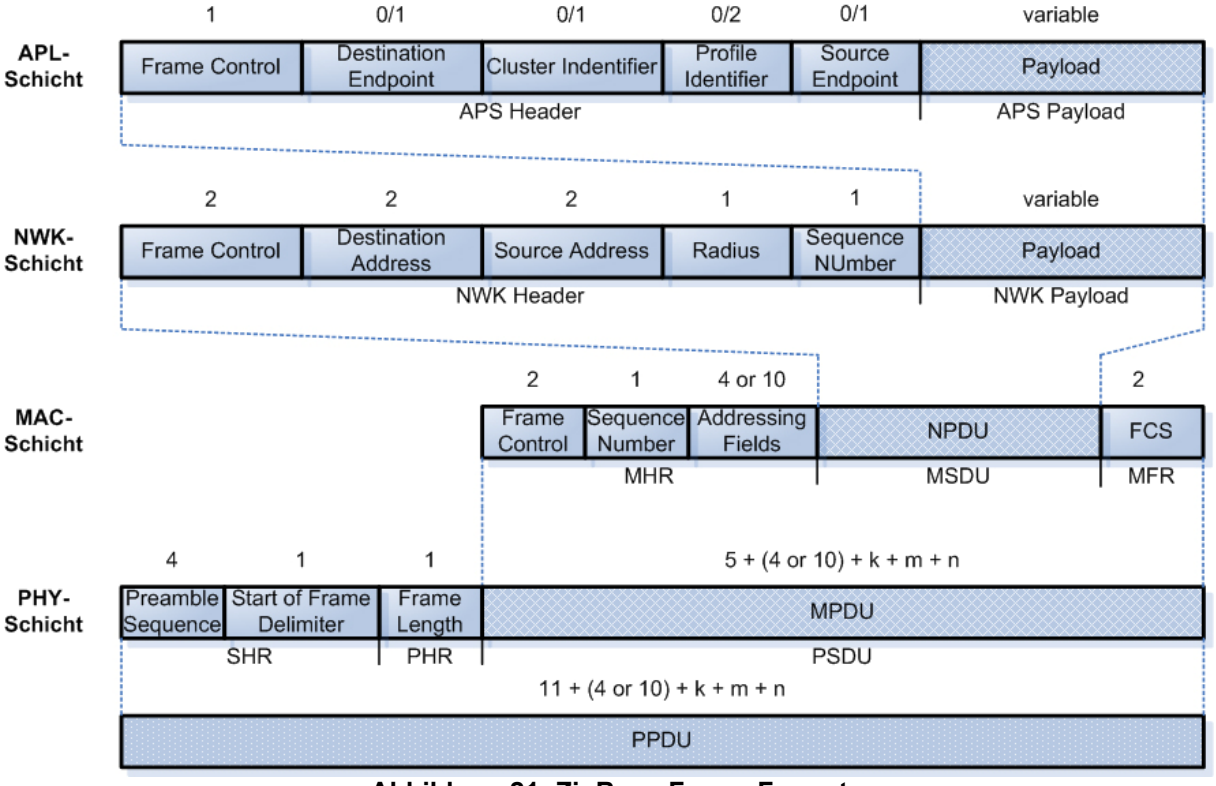

Abbildung 21: ZigBee - Frame-Format

Die beiden unteren Ebenen, die physikalische Schicht (PHY) und die Sicherungsschicht (MAC) sind durch das IEEE 802.15.4-2003 definiert. Die ZigBee Alliance erweitert dieses Grundgerüst durch zwei weitere Ebenen, die Netzwerkschicht (NWK) und die Anwendungsschicht (APL).
Die Grafik *Abbildung 21: ZigBee - Frame-Format* zeigt den gesammten Aufbau der einzelnen Pakete, näher wird hierrauf nicht eingegangen.

2.2.2.1 Anwendungs-Schicht

Die Anwendungsschicht besteht aus mehreren Komponenten:

2.2.2.1.1 Application support sup-layer (APS)

Der APS verbindet die Netzwerk-Schicht und die Komponenten der Anwendungsschicht miteinander, indem zwei Dienste zur Verfügung gestellt werden:

- **APS-Dateneinheit**
  Der Transport von den Dateneinheiten (PDU) der Anwendungen zwischen mindestens zwei im selben Netzwerk befindlichen Geräten wird durch die APSDE gewährleistet.

- **APS-Managementeinheit (APSME)**
  Die APSME ist für das Auffinden und die Anbindung von Geräten sowie für das Pflegen dieser in der Datenbank (AIB) zuständig.

2.2.2.1.2 Anwendungs-Framework

Die Anwendungsobjekte des ZigBee-Gerätes sind in das Anwendungs-Framework eingebettet. Mit dessen Hilfe werden Daten gesendet und empfangen (via APSDE). Die Steuerung und das Verwalten der Anwendungsobjekte erfolgt über die ZDO-Schnittstellen.

Der über die APSDE-Schnittstelle (APSDE-SAP) zur Verfügung gestellte Datendienst beinhaltet die Grundfunktionen für die Datenübertragung:

- **Anforderung**
  Unterstützung des Datentransfers zwischen gleichrangigen Objekten im Anwendungs-Framework

- **Bestätigung**
  Ergebnismeldung einer Anforderung

- **Signalisierung**
  deutet auf den Transport vom APS zum Zielobjekt im Anwendungs-Framework hin

- **Antwort**

Bis zu 240 verschiedene Anwendungsobjekte können im Framework definiert sein, welche die APSDE-Schnittstellen mit den Endpunkten 1 bis 240 nutzen.

Zusätzlich sind zwei weitere Endpunkte reserviert: der Endpunkt 0, welcher die Verbindung zum ZDO herstellt und der Endpunkt 255, über welchen der Broadcast an alle Anwendungsobjekte möglich ist.
Das Anwendungs-Framework bietet den Anwendungs-Objekten zwei Dienste an:

2.2.2.1.2.1 Key Value Pair Service

Der KVP Service ermöglicht die Verwendung von Attributen, die in den Anwendungsobjekten definiert sind. Sie können von außerhalb abgefragt, gesetzt oder eventgetriggert werden. Die Kommunikation wird durch komprimiertes XML realisiert.

2.2.2.1.2.2 Nachrichtendienst

Gerade für einfache Anwendungen ist der Einsatz des KVP-Service überzogen. Hier kann alternativ ein einfacherer Nachrichtendienst verwendet werden, der vom Anwendungsentwickler durch das Profil genauer definiert wird.

2.2.2.1.3 Adressierung

Gemäß dem IEEE 802.15.4-Standard verfügt jeder einzelne Knoten eines LR-WPAN über einen Transceiver und ist somit nur als einzelnes Gerät adressierbar. ZigBee bietet die Möglichkeit, mehrere Anwendungsobjekte auf einem Knoten zu adressieren.

2.2.2.1.4 Grundlagen der Anwendungskommunikation

2.2.2.1.4.1 Profile

In Profilen sind Nachrichten, Nachrichtenformate und Prozessabläufe definiert. Sie ermöglichen die Verwendung von den Grundfunktionen zwischen den Modulen (Anweisungssendung, Datenanforderung, Prozessanforderung/-anweisung), was die Voraussetzung einer verteilten Anwendung ist.
Profile werden durch die jeweiligen Anbieter der Anwendung entwickelt, um den Anforderungen spezieller Problemstellungen zu genügen.
Die ZigBee.org hat drei Profile entwickelt: Home Controls, Building Automation und Plant Control.

2.2.2.1.4.2 Cluster

Cluster bzw. Gruppen werden anhand eines Gruppenidentifikators gekennzeichnet. Innerhalb des jeweiligen Profils sind die Identifikatoren eindeutig. Der Verbund von zwei Geräten findet statt, wenn sie denselben Identifikator haben und die Schnittstelle eines Gerätes als Eingang und die des anderen als Ausgang fungiert.

2.2.2.1.5 Auffinden

2.2.2.1.5.1 Auffinden von Geräten

Mit Hilfe von Anfragen über Broadcast oder Unicast können sich ZigBee-Module gegenseitig finden. Es gibt zwei Möglichkeiten der Adressierung:

- **an die IEEE-Adresse**
  Es handelt sich um einen Unicast und es wird vorausgesetzt, dass die Adresse der NWK-Schicht bekannt ist.

- **an die Adresse der NWK-Schicht**
  Es handelt sich um einen Broadcast, wobei die bekannte IEEE-Adresse im Datenfeld des Paketes übergeben wird.

Die Antwort auf die Anfragen ist vom Typ der Module abhängig:

- **ZigBee Endgeräte** beantworten die Anfrage durch senden ihrer IEEE- bzw. NWK-Adresse.

- Der **ZigBee Koordinator** schickt die eigene sowie zusätzlich sämtliche IEEE- bzw. NWK-Adressen der mit ihm verbundenen Geräte.

- Der **ZigBee Router** schickt die eigene sowie zusätzlich sämtliche IEEE- bzw. NWK-Adressen der mit ihm verbundenen Geräte.

2.2.2.1.5.2 Auffinden von Diensten

ZigBee-Module können in einem Netzwerk nach vorhandenen Diensten suchen. Die Dienste werden an Endpunkten von Geräten zur Verfügung gestellt und können von externen Geräten erkannt und eventuell genutzt werden. Um die Dienste vollständig zu erfassen, können Anfragen auf sämtliche Endpunkte der Geräte gestartet werden.

2.2.2.1.6 Binding

ZigBee unterstützt in der Anwendungsebene das Clustering, was auch als Binding bezeichnet wird – die logische Verbindung von Geräten eines Anwendungsgebietes. Verbindungen zwischen Geräten werden in einer Referenztabelle festgehalten, welche im Koordinator des WPAN implementiert ist.

2.2.2.1.7 Nachrichten

2.2.2.1.7.1 Direkte Adressierung

Sobald Geräte miteinander verbunden sind, können innerhalb des Systems Nachrichten verschickt werden. Eine Nachricht wird an die Zieladresse geleitet, welche sich aus der Adresse der Gerätes (gemäß IEEE 802.15.4) und dem Endpunkt zusammensetzt.
Die direkte Adressierung setzt voraus, dass der Absender bezüglich der Adresse und des Dienstes am adressierten Endpunkt informiert ist.

2.2.2.1.7.2 Indirekte Adressierung

Ist die Adresse eines Gerätes nicht bekannt wird das Feld leer gelassen. Die Anforderung wird an die APSDE- Schnittstelle gesendet. Durch Extrahierung der Absenderadresse und des Endpunktes können in der Binding-Tabelle alle Assoziationen gefunden werden. Die Daten werden an diese weitergeleitet.

2.2.2.1.7.3 Adressierung per Broadcast

Eine Anwendung hat die Möglichkeit, eine Nachricht an alle Endpunkte eines Gerätes zu senden und wird als Anwendungs-Broadcast bezeichnet. Dazu muss als Ziel die 16-bit Netzwerk-Broadcast-Adresse verwendet und der Bitschalter für Broadcast im APS Frame Control Field gesetzt werden.
Zusätzlich befinden sich in dem APS-Paket Quellinformationen, wie der Gruppenidentifikator, der Profilidenifikator und die Endpunktadresse.

2.2.2.1.8 ZigBee Device Objects

Die „ZigBee Device Objects“ (ZDO) bieten eine Schnittstelle zwischen den Anwendungsobjekten, dem Knotenprofil und dem APS. Die ZDO befindet sich zwischen dem Anwendungs-Framework und dem APS. Die Aufgaben des ZDO sind:

- Initialisierung der Anwendungs-Stütz-Unterschicht (APS), der Netzwerkschicht (NWK) und der Sicherheitsspezifikationen (SSS)

- Sammeln von Informationen der Endanwendungen, um das Auffinden, Sicherheitsmanagement, Netzwerkmanagement und Binding Management umzusetzen

2.2.2.1.8.1 Discovery-Management

Das Discovery-Management ermöglicht den Anwendungsobjekten, innerhalb des WPAN nach anderen Knoten zu suchen. Abhängig vom adressierten Knoten erhält das Anwendungsobjekt eine einzelne oder eine Liste von Adressen anderer ZigBee-Knoten.
Zudem ist es den Anwendungsobjekten möglich, nach zur Verfügung gestellten Diensten bestimmter oder aller Knoten zu suchen.

2.2.2.1.8.2 Binding-Management

Anwendungsobjekte haben die Möglichkeit, andere Anwendungsobjekte beliebiger ZigBee-Geräte über Binding-Tabellen an sich zu binden.

2.2.2.1.8.3 Sicherheits-Management

Die ZigBee-Sicherheitsmechanismen können durch die Anwendungsobjekte beliebig aktiviert oder deaktiviert werden.

2.2.2.2 Netzwerk-Schicht

Die Netzwerkschicht wird benötigt, um die korrekte Funktionsweise der MAC-Schicht (gemäß IEEE 802.15.4) zu gewährleisten und stellt der Anwendungsschicht eine geeignete Schnittstelle zur Verfügung. Die Funktionalität wird durch zwei Dienste erreicht, welche über die jeweilige Schnittstelle (NLDE-SAP bzw. NLME-SAP) zur Verfügung gestellt werden:

2.2.2.2.1 Dateneinheit (NLDE)

Die NDLE ermöglicht der Anwendung, Protokolldatenpakete (APDU) zwischen mehreren Geräten innerhalb desselben Netzwerkes zu befördern. Die Aufgaben der NLDE:

- **Erzeugung einer PDU auf Netzwerkebene (NPDU)**: Die NLDE generiert eine NPDU, indem sie die Protokolldateneinheit der Anwendungsschicht in einen geeigneten Protkoll-Header bettet.

- **Routing gemäß der Netzstruktur**: Die NLDE überträgt eine NPDU an einen bestimmten Knoten, der entweder der Zielknoten oder der nächste Knoten auf dem Weg zum Ziel ist.

2.2.2.2.2 Managementeinheit (NLME)

Die NLME ermöglicht der Anwendung durch einen Managementdienst mit dem Stack zu interagieren. Die Aufgaben der NLME:

- **Konfiguration eines neuen Gerätes**
  entweder einen Koordinator und folglich ein neues Netzwerk starten oder als einfache Einheit an einem Netzwerk teilnehmen

- **Erstellung eines Netzwerkes**

- **Beitreten und Verlassen eines Netzwerkes**
  (auch die Veranlassung dazu)

- **Adressierung**
  Adressvergabe an neue Geräte durch Koordinator und Router

- **Ermittlung der Umgebung**
  Entdeckung, Aufzeichnung und Darstellung der direkt benachbarten Knoten

- **Ermittlung der Route:**
  Entdeckung und Aufzeichnung der effektivsten Wege durch das Netzwerk, wodurch Nachrichten geroutet werden.

- **Empfangskontrolle**
  Durch Aktivierung der MAC-Funktionen synchrone Kommunikation oder direkte Adressierung kann die Verfügbarkeit von Geräten getestet werden.

2.2.2.3 Sicherheits-Dienste

2.2.2.3.1 Sicherheitsarchitektur und –design

2.2.2.3.1.1 Prämisse

ZigBee gewährleistet Sicherheitsdienste nur zwischen den Geräten. Zwischen den Schichten innerhalb eines Gerätes bzw. zwischen den Anwendungsobjekten besteht keine gesicherte Kommunikation.

2.2.2.3.1.2 Design

Die Prämisse ergibt die folgenden fünf Richtlinien für das Sicherheitsdesign:

1. Sicherung von Paketen: Es ist die Schicht für die Sicherung des Paketes verantwortlich, in der es entsteht.

2. Soll die Anwendung vor Leistungsdiebstahl (theft of service) geschützt werden, muss der Sicherungsmechanismus der Netzwerkschicht genutzt werden. Dies gilt nicht für Pakete, welche zwischen Router und einem neuen Gerät ausgetauscht werden, damit dieses dem Netzwerk beitreten kann. Somit ist gewährleistet, dass Geräte nur dann über mehr als einen Schritt im Netzwerk kommunizieren können, wenn sie die Authentifizierung bestanden haben.

3. Entsprechend des „open trust modell“ werden Schlüssel zwischen den Schichten wieder verwendet. Beispielsweise kann der aktuelle Schlüssel des NWK-Frame für die Sicherung von APS-Paketen verwendet werden.

4. Da nur Quell- und Zielknoten im Besitz des gemeinsamen Schlüssels sind, kann der Transport bzw. das Routen der Pakete abstrahiert von der Vertrauensebene vollzogen werden.

5. Um die Interoperabilität der Knoten zu vereinfachen, muss das Sicherheitskonzept auf allen Knoten und in allen Schichten eines jeden Knotens dasselbe sein.

Richtlinien an die Anwendungsprofile:

- Behandlung von Fehlern, die bei der Ver- und Entschlüsselung von Paketen auftreten. Fehlerzustände können auf Synchronisationsprobleme oder anstehende Angriffe hinweisen.

- Erkennung und Behandlung von fehlerhaften Zählerzuständen wie Synchronisationsfehler oder Zähleroverflow

- Erkennung und Behandlung von Synchronisationsproblemen des Schlüssels

- Verfall und regelmäßige Aktualisierung von Schlüsseln (bei Bedarf)

2.2.2.3.1.3 Sicherheitsschlüssel

Das ZigBee-Konzept sieht zwei Arten von Sicherheitsschlüsseln für das Netzwerk vor, welche die Geräte durch Transport, selbständige Etablierung oder Vorinstallation erhalten:

- **Verbindungsschlüssel**: Schutz von Punkt-zu-Punkt-Kommunikation (Unicast) von zwei gleichartigen APL-Einheiten durch einen 128-Bit-Schlüssel

- **Netzwerkschlüssel**: Schutz von Broadcast-Kommunikation durch einen 128-Bit-Schlüssel, welcher gemeinsam von sämtlichen Knoten des Netzwerkes genutzt wird

2.2.2.3.1.4 Sicherheitsarchitektur

Sicherheitsmechanismen erstrecken sich auf drei Schichten der ZigBee-Architektur. Gesichert werden die MAC-, die NWK- und die APS-Schicht. Abhängig von den Anforderungen der Anwendung kann die Sicherung der Daten auf jeder Ebene vollzogen werden.

3 Analyse

Welche Funktechnologie eignet sich für die Zielsetzung am Besten?

Quellen: [ATan], [AHac], [BT]

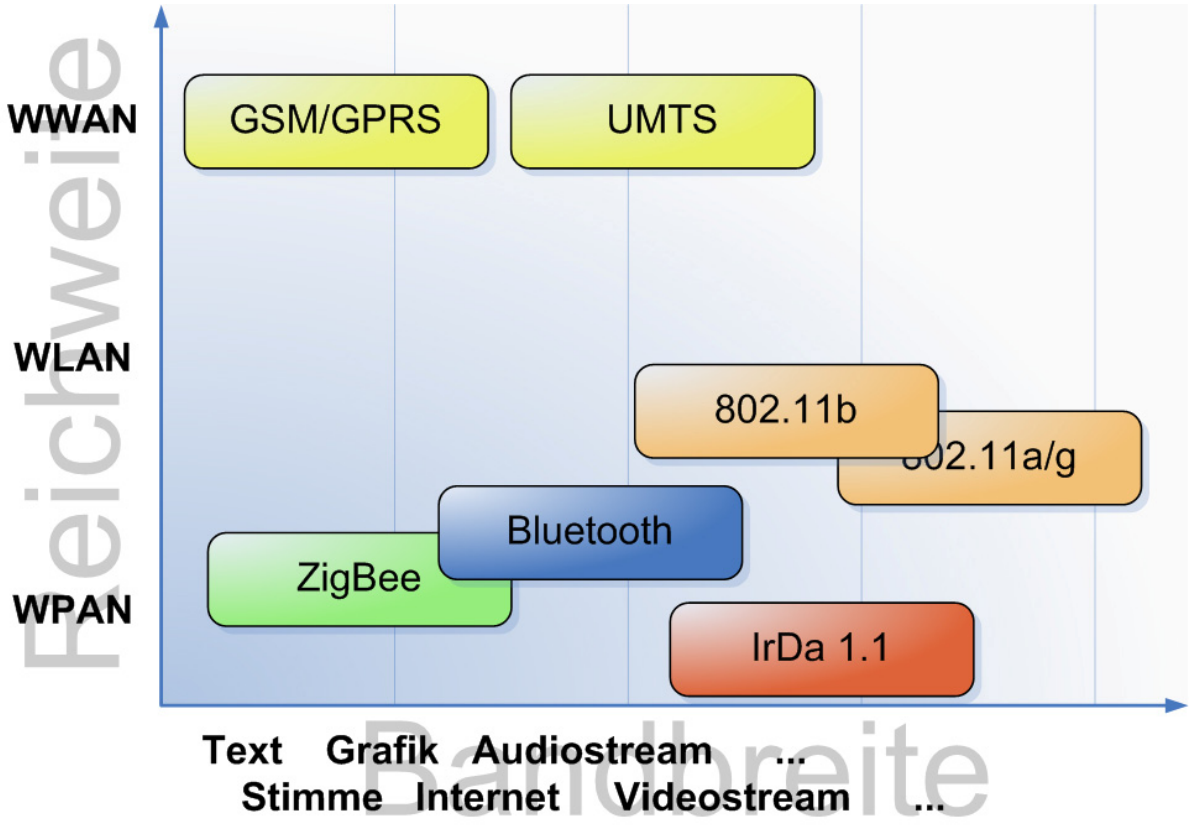

Abbildung 22: Funktechnik - Aktuelle Standards im Vergleich

In Anbetracht der Zielsetzung und der derzeit vorliegenden Standards (siehe *Abbildung 22: Funktechnik - Aktuelle Standards* im Vergleich) kann die Art des Netzwerkes festgelegt werden. Da sich das Netzwerk auf kurze bis mittellange Distanz ausbreitet (10 bis 200 Meter), befindet sich das System im Bereich des Kabellosen Persönlichen Netzwerkes (WPAN) bis hin zu dem Kabellosen Lokalen Netzwerkes (WLAN). Die zu diesen Netzwerkarten zugeordneten standardisierten Technologien sind:

- WLAN
- Infrarot
- Bluetooth
- ZigBee

Die Anforderung an die Übertragungsgeschwindigkeit ist gering. Sensordaten und Kommandos an die Aktoren sind kurze Textnachrichten, die eine geringe Bandbreite erfordern. Rechenbeispiel: In einem Netzwerk befinden sich 400 Knoten. Jeder Teilnehmer sendet pro Sekunde ein 30 Byte großes Datenpaket an das zentrale Modul (10 Byte Informationsgehalt und pauschal 20 Byte Header-Daten). Ein empfangenes Paket wird durch ein 20 Byte großes Antwortpaket bestätigt. Am zentralen Modul kann eine maximale Bitrate von 160 kBit/s entstehen.

Jede der hier betrachteten Technologien gewährleistet diesen Datendurchsatz.

Um die geeignete Technologie zu finden, werden die oben genannten Standards anhand folgender Kriterien miteinander verglichen:

- **Geschwindigkeit/Bandbreite:** Es werden hauptsächlich kleine Datenmengen transportiert. Sensorenwerte und Kommandos für Aktoren werden in Textform übertragen und benötigen nur geringe Datenübertragungsgeschwindigkeiten.

- **Energieverbrauch:** Der Großteil der Module wird mit Batterien bespeist. Dies erfordert eine effiziente Technologie.

- **Reichweite:** Wie oben erwähnt, erstrebt das System die Reichweite eines WLAN.

- **Anzahl der Netzwerkteilnehmer:** Die Anzahl der Knoten ist abhängig von der Art der Anwendung, sie sollte so groß wie möglich sein.

- **Arbeitsspeicher:** Die Größe der Module ist nicht beschränkt, sollte jedoch so klein wie möglich gehalten werden. Die Technologie muss mit so wenig Speicher wie möglich auskommen, was sich letztlich auch auf den Energieverbrauch niederschlägt.

- **Latenzzeiten:** Die Latenzzeit beschreibt die Zeit eines Datenpaketes vom Sender zum Empfänger. Sie setzt sich aus der Zeit der eigentlichen Übertragung und der Verarbeitungszeiten bei Sender und Empfänger zusammen. In dieser Betrachtung steht der zweite Punkt im Vordergrund.

3.1 Grobe Selektion

Die mit Abstand größte Reichweite mit ca. 200 - 300 Metern direkt zwischen zwei Geräten erreicht WLAN, jedoch entfällt diese Technik, da der Ressourcenverbrauch von mindestens einem Megabyte RAM und der Energieverbrauch die Kapazitäten kleiner Module übersteigt.
Ebenfalls ungeeignet ist die Infrarot-Technik, da stets Sichtkontakt zwischen den miteinander kommunizierenden Modulen bestehen muss.
Der eigentliche Vergleich beschränkt sich somit auf die Techniken Bluetooth und ZigBee.

3.2 ZigBee und Bluetooth im Vergleich

- **Geschwindigkeit/Bandbreite:**

  Bluetooth und ZigBee arbeiten in den 2,4 GHz-Bereichen des ISM-Band. Bluetooth verwendet das Frequenzsprung-Verfahren FHSS und erreicht eine Verbindungsrate von 1 MBit pro Sekunde, wobei praktisch eine Datenübertragungsrate von rund 720 kBit pro Sekunde erlangt wird. Durch die Verwendung anderer Modulationsverfahren schafft Bluetooth in der Version 2.0 die bis zu dreifache Verbindungsrate und somit einen Datendurchsatz von etwa 2,2 MBit pro Sekunde.

ZigBee nutzt das Frequenzsprung-Verfahren DSSS und kommt somit auf eine Verbindungsrate von 250 kBit/s.

In Anbetracht der Anforderungen an das verteilte System sind beide Technologien bezüglich der Übertragungsrate geeignet.

- **Reichweite:**

  Die Reichweite von Bluetooth liegt, abhängig von der Klasse, bei 10 bis 100 Metern. Große Entfernungen erfordern erheblich mehr Sendeleistung (Klasse I: 100 m bei 100 mW, Klasse III: 10 m bei 1 mW).
  ZigBee hat eine Reichweite von 10 bis 75 Metern, wobei im Mittel 30 Meter erwartet werden können.

  Um erwartete Netzwerke mit einer Reichweite von bis zu 300 Metern aufzubauen, reichen direkte Verbindungen von Gerät zu Gerät nicht aus. Große Entfernungen fordern das Routing und die Weiterleitung von Paketen innerhalb der Netzwerke, was zwar von beiden Standards unterstützt wird, aber bei Bluetooth mit relativ hohem Aufwand verbunden ist.

- **Anzahl der Netzwerkteilnehmer:**

  Die Architektur des Bluetooth-Netzwerkes unterteilt sich in zwei Komponenten, dem Pico- und dem Scatternetz. Ein Piconetz enthält bis zu 255 Teilnehmer, bestehend aus einem Master und Slaves. Da der Master sieben Sendeslots an die Slaves vergeben kann, können insgesamt lediglich acht Geräte gleichzeitig aktiv sein.
  Einzelne Knoten können sich in mehreren Piconetzen befinden, wodurch ein Scatternetz entsteht.
  ZigBee bzw. die Netzwerkschicht des ZigBee-Stack erlaubt die Bildung eines Netzes mit 2^{16} = 65,536 Einheiten. Adressiert werden die Module auf MAC-Ebene über die 64-Bit-Adresse.

  Bluetooth schränkt die Netzspontaneität durch die geringe Anzahl gleichzeitig verteilbarer Sendeslotts ein, zudem wird die Größe des Netzwerkes durch die Anzahl adressierbarer Knoten beschränkt.

- **Energieverbrauch:**
  Bei Betrachtung des Leistungsverbrauchs der beiden Technologien beim Senden und Empfangen von Daten, sowie im Standby-Modus gibt es kaum Differenzen. Ein unterschiedlicher Energieverbrauch kommt durch die Art und Weise des Sendens und Empfangens zustande.
  Die PHY-Schicht von Bluetooth fordert ständig die Synchronisation der Module untereinander. Somit verweilen die Module kaum im Standby-Modus und verbrauchen verhältnismäßig viel Energie.
  ZigBee bzw. die PHY-Schicht der IEEE 802.15.4-Spezifikation hat das anders gelöst. An ein bestimmtes Gerät adressierte Daten werden beim Koordinator hinterlegt. Der Empfänger überprüft in Abständen, die um ein Vielfaches größer als die bei der Bluetoothsynchronisation sind, ob Daten warten. Somit verbringt das Modul den Großteil seiner Zeit im Standby-Modus.

- **Arbeitsspeicher:**
  Der Verbrauch von Ressourcen wie RAM ist ein wesentliches Kriterium bezüglich Design, Preis und Leistungsverbrauch des zu entwickelnden Moduls.
  Bluetooth benötigt für den 250 Kilobyte großen Protokollstack relativ viel Speicher.
  Der komplette Protokollstack von ZigBee liegt unter 32 Kilobyte. Der Koordinator im Netzwerk benötigt, abhängig von der Anwendung und dem Umfang des Netzwerkes, zusätzlich Speicher für die Datenbank der mit dem Netzwerk assoziierten Geräte, den Transport von Paketen und Referenz- sowie Bindingtabellen. Ein RFD in einem ZigBee-Netzwerk benötigt etwa vier Kilobyte für den Stack.

- **Latenzzeiten:**

	Bluetooth	**ZigBee**
Beitritt in ein Netzwerk	> 3 s	~ 30 ms
Wechsel eines schlafenden Knotens in den aktiven Zustand	~ 3 s	~ 15 ms
Zugriff eines aktiven Knotens	~2 ms	~15 ms

  Große Unterschiede bestehen bei den Beitritts- und Anforderungszeiten zwischen den Technologien.
  Besonders der Zeitaufwand, bis ein Bluetooth-Modul vom schlafenden in den aktiven Zustand gewechselt ist, wird nicht den Anforderungen eines Sensornetzwerkes gerecht.

3.3 Ergebnis

In Anbetracht der Vorteile von ZigBee gegenüber Bluetooth wird als Funktechnik für das Modul ZigBee verwendet.

4 Design und Realisierung

4.1 Gliederung des Entwicklungs-/Erstellungsprozesses

Der Entwicklungsprozess orientiert sich an die im ersten Kapitel festgelegten Anforderungen:

- Anforderungen an das Modul:
  - Anschlussmöglichkeit für beliebige Sensoren und Aktoren
  - normierte Schnittstelle (als Anschlussmöglichkeit für z.B. einen Computer)
  - Stromversorgung per Batterie bzw. Akku

- Anforderungen an das Modul-Netzwerk
  - zentralisierte Steuerung und Monitoring der Knoten
  - Netzwerk beliebig erweiterbar und reduzierbar
  - drahtlose Kommunikation

Die für das Netzwerk festgelegte Funktechnologie ist ZigBee.

Der Ablauf dieses Kapitels gliedert sich in folgende Schritte:

- Der erste Abschnitt befasst sich mit dem grundsätzlichen Aufbau des Moduls. Er beschreibt die Anforderungen an Komponenten und legt diese fest.

- Der zweite Absatz, der Entwurf des Schaltbildes, zeigt den detaillierten technischen Aufbau und die Verbindungen der einzelnen Komponenten im Gesamtsystem anhand von schematischen Entwürfen. Zudem wird ein Einblick in die verwendeten Werkzeuge gegeben.

- Der dritte Abschnitt erläutert das resultierende Platinenlayout.

4.2 Modulaufbau, Festlegung der Hauptkomponenten

Quellen:
[DS_ATM], [DS_CC2], [DS_IDT], [DS_M74], [DS_MAX], [DS_MIC], [DOC_DBK], [DOC_EM]

Bei Betrachtung der Anforderungen an das Modul und an das Modul-Netzwerk ergeben sich folgende Komponenten (Die angegebenen technischen Daten der Bauteile sind in den jeweiligen Datenblättern aufgeführt - Anhang):

4.2.1 RF-Komponente

Da die Kommunikation drahtlos geschieht, ist eine Funkkomponente notwendig. Die RF-Komponente besteht aus einem Funk-Chip, dem Hochfrequenzteil und der Beschaltung. Im dritten Kapitel ist die Technologie ZigBee als geeignet festgestellt worden.

Chips für ZigBee-Technik sind derzeit von 4 Herstellern beziehbar: Chipcon (CC2420), Freescale (MC13192 und MC13193), CompXs (CX1540) und Ember (EM2420, EM250, EM260).
Alle Modelle beinhalten die PHY- und die MAC-Schicht der IEEE 802.15.4-Spezifikation und sind somit für ZigBee-Anwendungen geeignet. Der MC13193 bietet außerdem den kompletten Umfang des ZigBee-Stacks.

Verwendung findet in der RF-Komponente der CC2420 von Chipcon. Der IC kann von 2,1 V bis 3,6 V versorgt werden, in dieser Anwendung werden 3,3 V verwendet. Der Empfangsmodus benötigt bei einer Sensitivität von -94 dBm einen Strom von 19,7 mA, die Sendeleistung kann in Stufen im Bereich von -25 dBm bis maximal 0 dBm geschaltet werden. Eine grafische Darstellung ist in *Abbildung 24: Leistungsbhängige Stromaufnahme* zu finden.

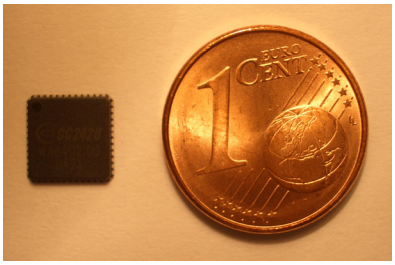

Abbildung 23: CC2420 im QLP(48)-Gehäuse, 7x7 mm

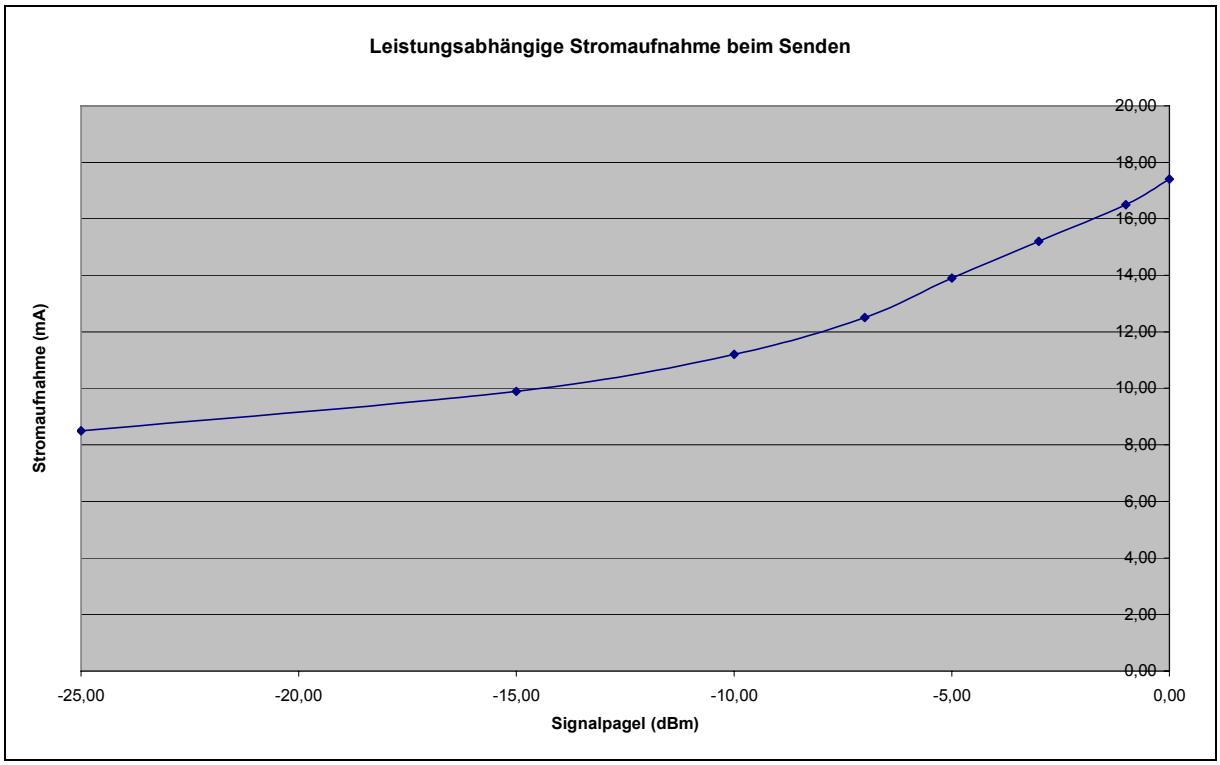

Abbildung 24: Leistungsbhängige Stromaufnahme

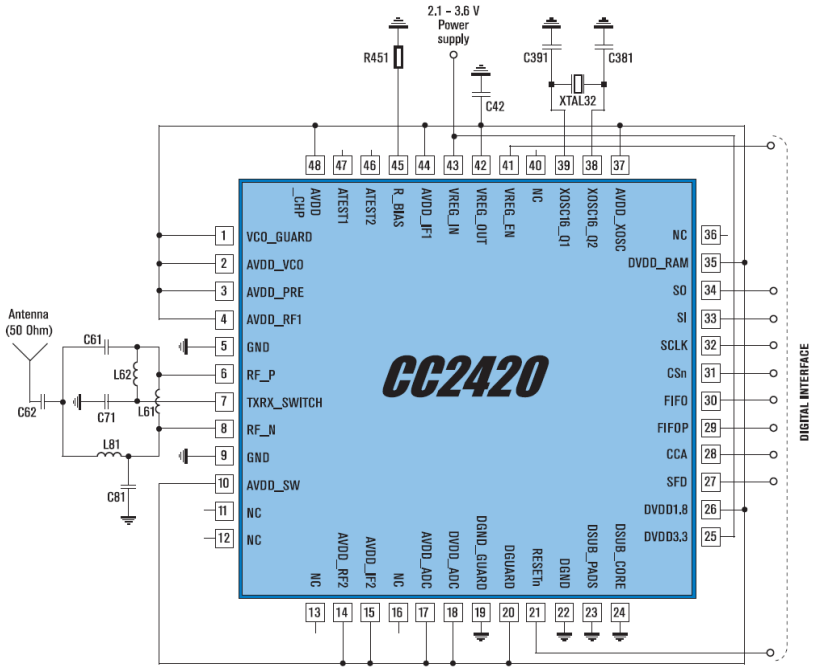

Abbildung 25: CC2420 - Pinbelegung und Zusatzschaltungen

Chipcon bietet eine vollständige RF-Einheit (CC2420EM) an, die den CC2420-Chip, den HF-Teil und den Antennenanschluss beinhaltet.
Der Anschluss des Bauteils erfolgt über zwei Steckerleisten der Firma Samtec (TFM-110-02-S-D-A-TR), alternativ können zwei Stiftleisten mit jeweils 2x10 Pins in einem Lochrastermass von 1,27 mm verwendet werden. Über diesen Anschluss werden die neun für die Kommunikation zwischen Chip und Mikrokontroller benötigten Daten- und Steuerleitungen sowie die Versorgungsspannung und Masse durchgeschleift (*Abbildung 25: CC2420 - Pinbelegung und Zusatzschaltung*).

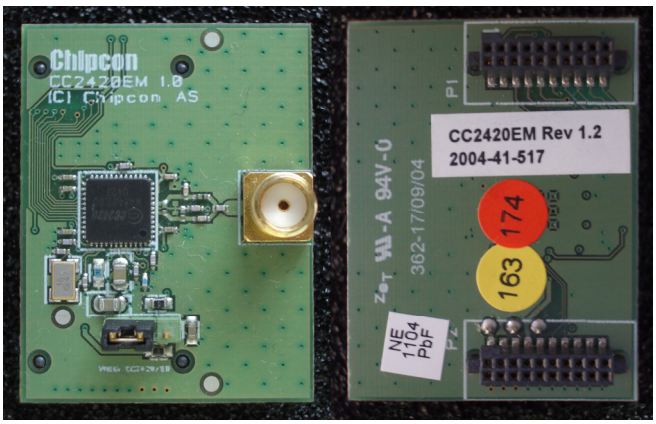

Abbildung 26: CC2420EM Ober- und Unteransicht

4.2.2 Kommunikationsschnittstelle

Das Monitoring und die Interaktion mit dem Netzwerk verlangt eine Schnittstelle an die zentrale Einheit, den Koordinator. In dieser Anwendung findet die Kommunikation mit einem Computer statt.
Es bietet sich aus zwei Gründen die serielle Schnittstelle an: Die Technik ist weit verbreitet und auf nahezu jedem Computer vorhanden. Zudem ist die Implementierung

einfach und es existiert eine direkte Unterstützung für RS232 durch die meisten Mikrokontroller.

Als RS232-Transceiver wird der MAX3233E der Firma Maxim verwendet. Das Bauteil wird mit 3,3 Volt versorgt und ist gegen elektrostatische Entladung von ±15 kV gesichert. Wenn keine Transaktion stattfindet, beträgt der Versorgungsstrom 1 µA. Die maximale Datenübertragungsrate beträgt 250 kBit/s. Interne Kondensatoren ermöglichen ein kleineres Platinenlayout.
Es bestehen Anschlussmöglichkeiten für zwei RS232-Schnittstellen. In diesem Anwendungsfall wird nur eine benötigt (*Abbildung 28: Pinbelegung MAXIM MAX3233E*).

Abbildung 27: MAXIM MAX3233E im SO.300-Gehäuse

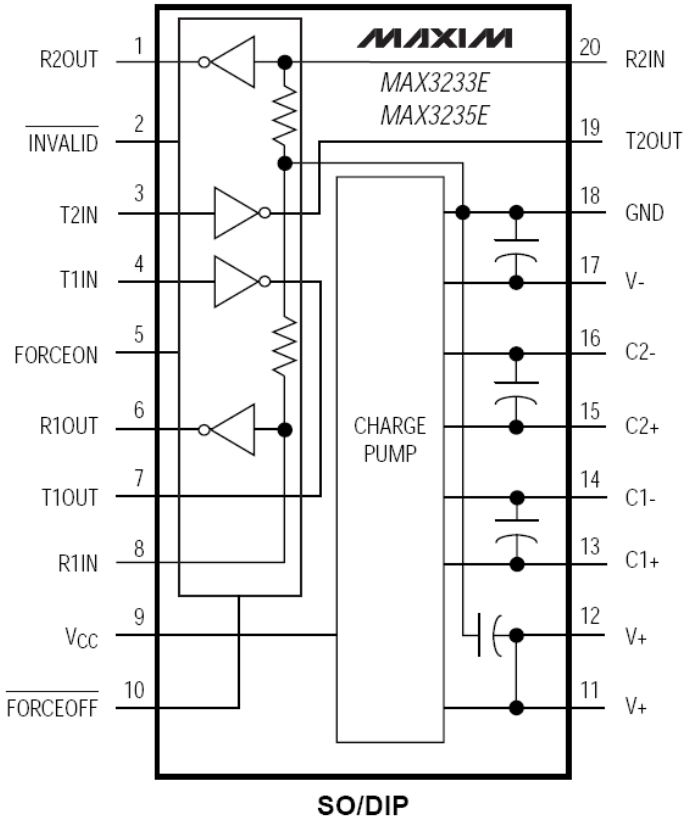

Abbildung 28: Pinbelegung MAXIM MAX3233E

Als Anschlussmöglichkeit an den Computer wird auf dem Modul eine RJ-11-Buchse verwendet. Die Pinbelegung entspricht der auf den Aksen-Boards der Fachhochschule Brandenburg für den Anschluss des Flasher-Kabels.

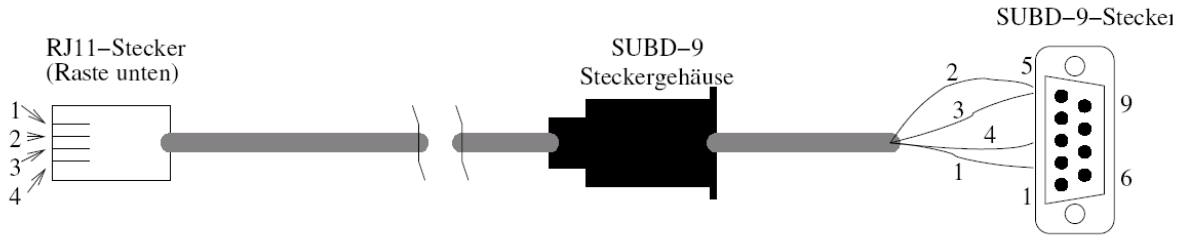

Abbildung 29: Aufbau des Kabels für die serielle Verbindung

4.2.3 Mikrokontroller und Anschlüsse

Der Mikrokontroller ist die zentrale Recheneinheit und bindet die Funkkomponente und die Kommunikationsschnittstelle in das System ein bzw. bildet mit ihnen das System. Zusätzlich stellt er die Anschlussmöglichkeiten für Sensoren und Aktoren zur Verfügung.

Der ATmega128L der Firma ATMEL (*Abbildung 30: ATMEL ATmega128L im MLF-Gehäuse*) erfüllt die Anforderungen und wird in dem System verwendet. Versorgt wird die MCU mit 3,3 Volt, die Taktung beträgt 8 MHz, wodurch die Versorgungsstromstärke im aktiven Modus bei etwa 11 mA und im Leerlauf bei etwa 5 mA liegt.
Der auf der RISC-Architektur basierende 8Bit-Mikrokontroller verfügt über 128K Bytes Flash, 4K Bytes EEPROM, 4K Bytes internen SRAM. Zudem bietet er die Option, extern 64K Bytes Speicher anzusteuern. Durch eine Speichererweiterung ist es folglich möglich, den bis zu 32K Bytes großen ZigBee-Protokoll-Stack einzubinden.

Abbildung 30: ATMEL ATmega128L im MLF-Gehäuse

Programmiert wird der ATMEL über eine SPI-Schnittstelle. Der Anschluss über JTAG ist möglich, jedoch in dieser Anwendung nicht explizt vorgesehen. Auf diesem Board wird die SPI-Schnittstelle direkt über einen eigenen Anschluss zur Verfügung gestellt. Es handelt sich um eine sechspolige Stiftleiste im 2,54 mm Rastermass. Die Pinbelegung für das ISP-Adapter ist unter Abbildung *31* dargestellt.

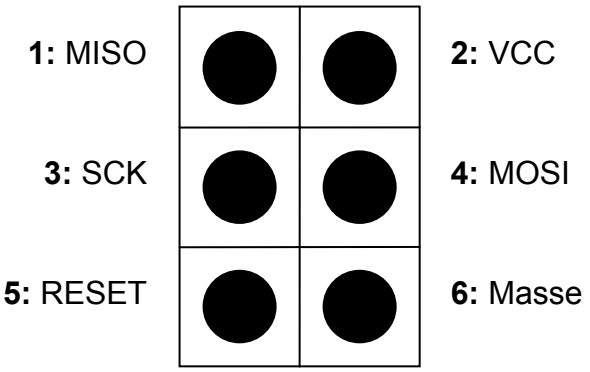

Abbildung 31: Pinbelegung ISP-Schnittstelle

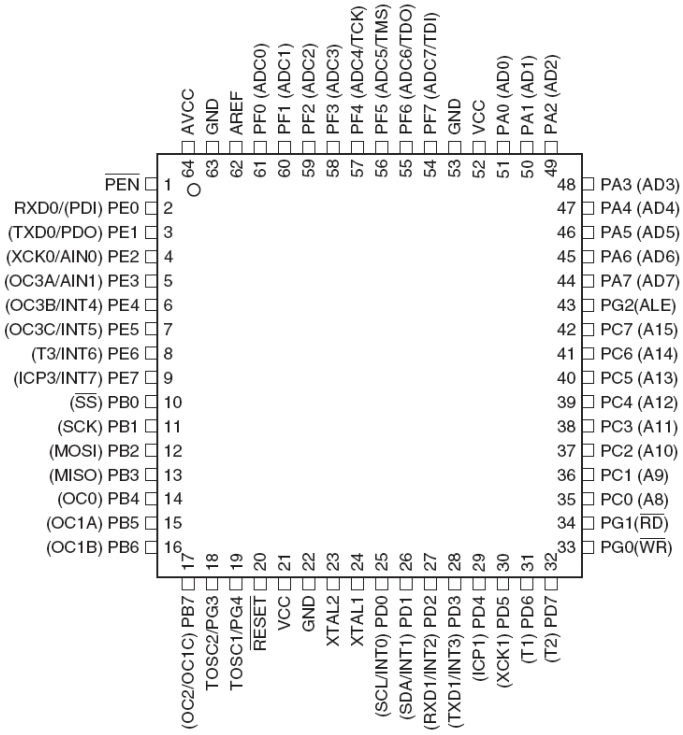

Abbildung 32: Pinbelegung ATmega128L

Der ATmega128 verfügt über sieben Ein-/Ausgabe-Register mit insgesamt 53 Leitungen.

Für den Anschluss von externen Sensoren und Aktoren sowie weiteren Funktionen werden zwei 8-Bit Register zur Verfügung gestellt:

Register PE0 – PE7: Der Port E des ATmega128 bietet verschiedene Möglichkeiten der Nutzung (Die Stromstärke jeder Leitung sollte 10 mA und die Summe aller Leitungen 150 mA nicht überschreiten.):

- Digitale 8-Bit Ein-/Ausgabe-Schnittstelle
  Jede Leitung ist mit einem internen Pull-Up-Widerstand versehen, der bei Bedarf aktiviert werden kann.

- Interrupteingänge
  Die oberen vier Leitungen können als Eingänge der externen Interrupts 4-7 geschaltet werden.
- Timer/Zähler/Pulsweitenmodulation
  Das Register stellt die Leitungen des Timers/Zählers 3 zur Verfügung und ermöglicht den Einsatz von Pulsweitenmodulation.
- UART0
  Über die unteren zwei Leitungen wird der zweite serielle Anschluss zur Verfügung gestellt, allerdings wird ein RS232-Transceiver für den Pegelausgleich benötigt.
- Verwendung des Analog-Komparators

Register PF0 – PF7: Der Port F des ATmega128 bietet verschiedene Möglichkeiten der Nutzung (Die Stromstärke jeder Leitung sollte 10 mA und die Summe aller Leitungen 200 mA nicht überschreiten.):

- Digitale 8-Bit Ein-/Ausgabe-Schnittstelle
  Jede Leitung ist mit einem internen Pull-Up-Widerstand versehen, der bei Bedarf aktiviert werden kann.
- Analoge Eingabe-Schnittstelle
  Die acht Leitungen sind direkt mit dem internen 10-Bit-Analog/Digital-Konverter verbunden.
- Über die oberen vier Leitungen kann der JTAG-Adapter angeschlossen werden.

Der High-Pegel an den Ein-/Ausgängen hat mindestens den Wert von 2,4 Volt, der Low-Pegel hat höchstens den Wert von 0,5 Volt. Um dies zu gewährleisten, darf die Summe der Stromstärken aller Leitungen 400 mA nicht überschreiten.

Angeschlossen werden die Geräte nach demselben Format wie bei den Aksen-Boards der Fachhochschule Brandenburg auf Buchsenleisten. Jedoch steht den Geräten eine Versorgungsspannung von 3,3 Volt anstatt 5 Volt zur Verfügung. Die Pinbelegung sieht folgendermaßen aus:

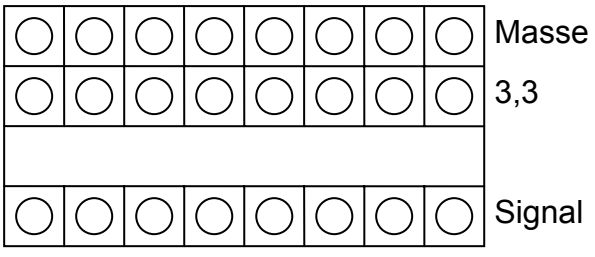

Abbildung 33: Anschlussleiste eines PORTs

4.2.4 Speicher

Da der interne SRAM der MCU nicht ausreicht, um den bis zu 32K Bytes großen ZigBee-Stack zu hinterlegen, ist es nötig externen Speicher in das System einzubinden. Als Speicher wird der SRAM IDT71V256SA20YI der Firma Integrated Device Technology, Inc. genutzt. Im normalen Betrieb beträgt die Versorgungsspannung 3,3 Volt und der Verbrauch an Strom 85 mA. Im Standby-Betrieb sinkt der Wert auf 20 mA.
Der Speicher ist in 32K Registern zu jeweils 8 Bit aufgebaut und wird über das Register C (obere Byte) und das Register A (untere Byte) des ATmega128 adressiert. Das Register A dient ebenfalls als Datenleitung, was die Verwendung eines achtfachen D-Flipflops zur Folge hat. Hier wird das M74HC573 des Herstellers ST verwendet.

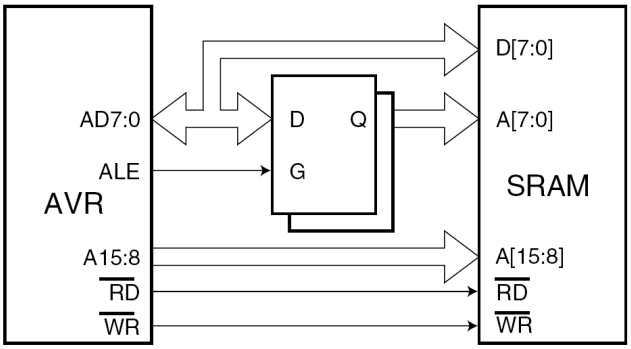

Abbildung 34: Schaltbild µC und SRAM

4.3 Entwurf des Schaltbildes

4.3.1 Werkzeuge

Das Schaltbild wird mithilfe der Entwicklungsumgebung Protel DXP 2004 von Altium entworfen. Das Programm bietet die komplette Unterstützung bei der schematischen Entwicklung bis hin zum Layout der Platine.

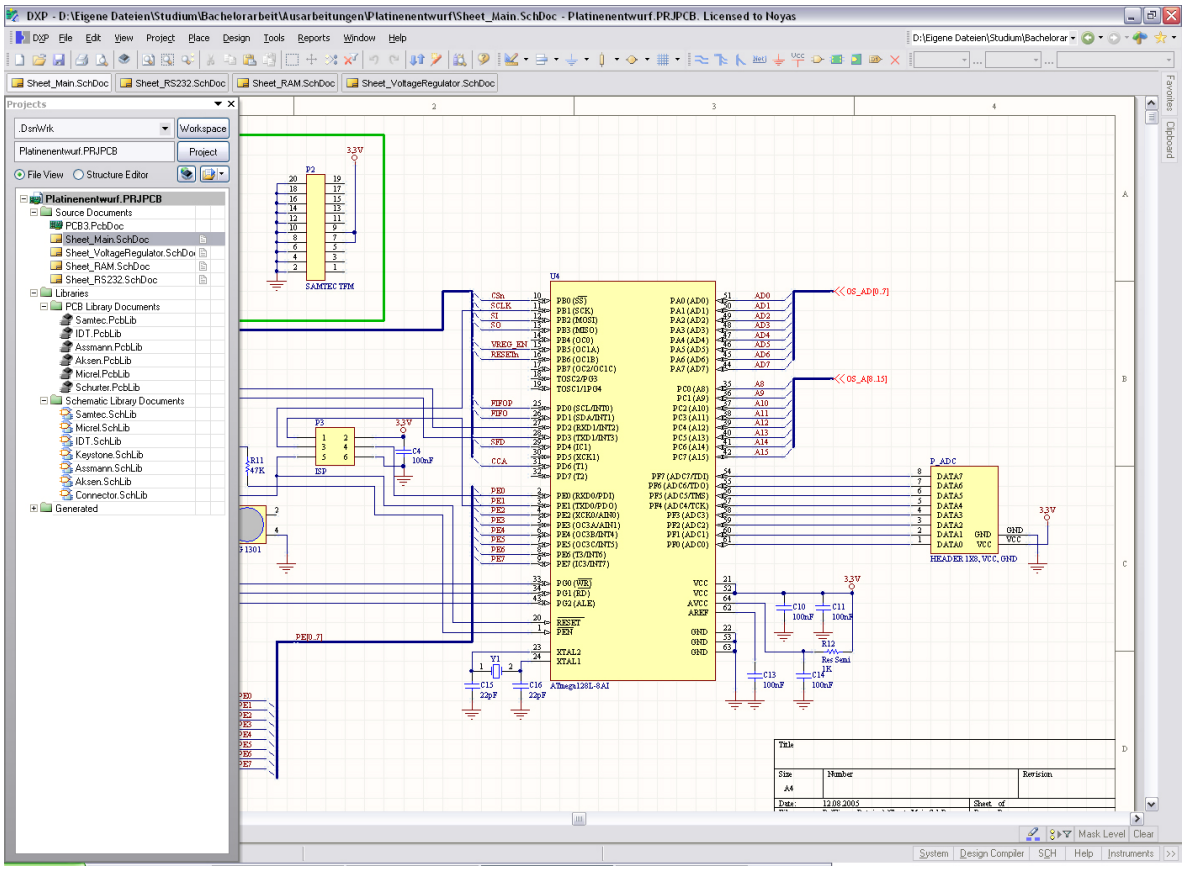

Abbildung 35: Werkzeuge - Protel DXP Schematisches Layout

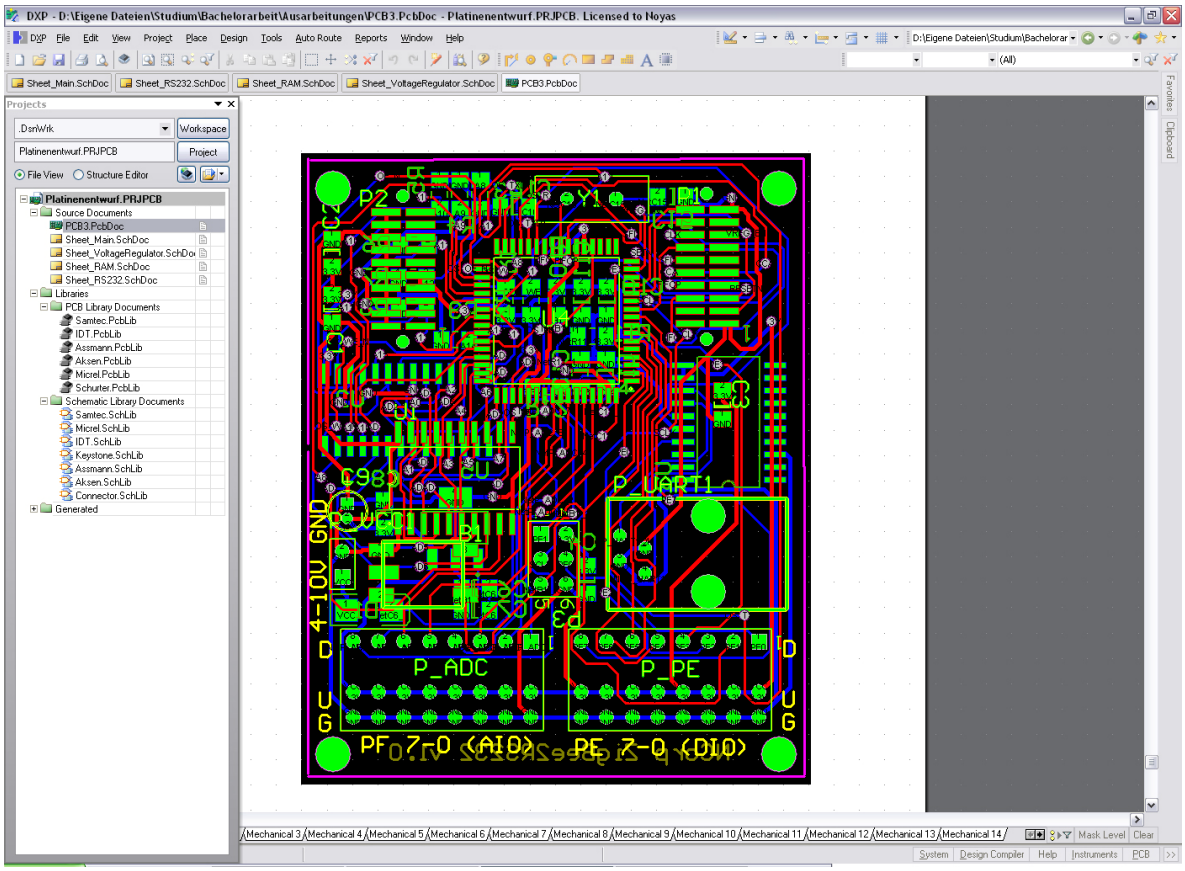

Abbildung 36: Werkzeuge - Protel DXP PCB-Layout

4.3.2 Ergebnis – Schematisches Layout

Die oben festgelegten Komponenten werden in einen Schaltplan zusammengeführt (*Abbildung 37: Schematischer Aufbau - Blockschaltbild*) und mit spezifischen Vorschaltungen erweitert.
Um die Spannung auf 3,3 Volt zu regeln, wird der Spannungsregulator MIC5209-3.3BS der Firma Micrel verwendet.

Da die RF-Komponente mit dem ZigBee-Chip als komplettes Bauteil von Chipcon bezogen wird, ist eine eigenständige Anfertigung eines Schaltplans nicht notwendig. Die Schaltung ist auf der Homepage der Firma Chipcon zur Verfügung gestellt.

4.3.2.1 Blockschaltbild

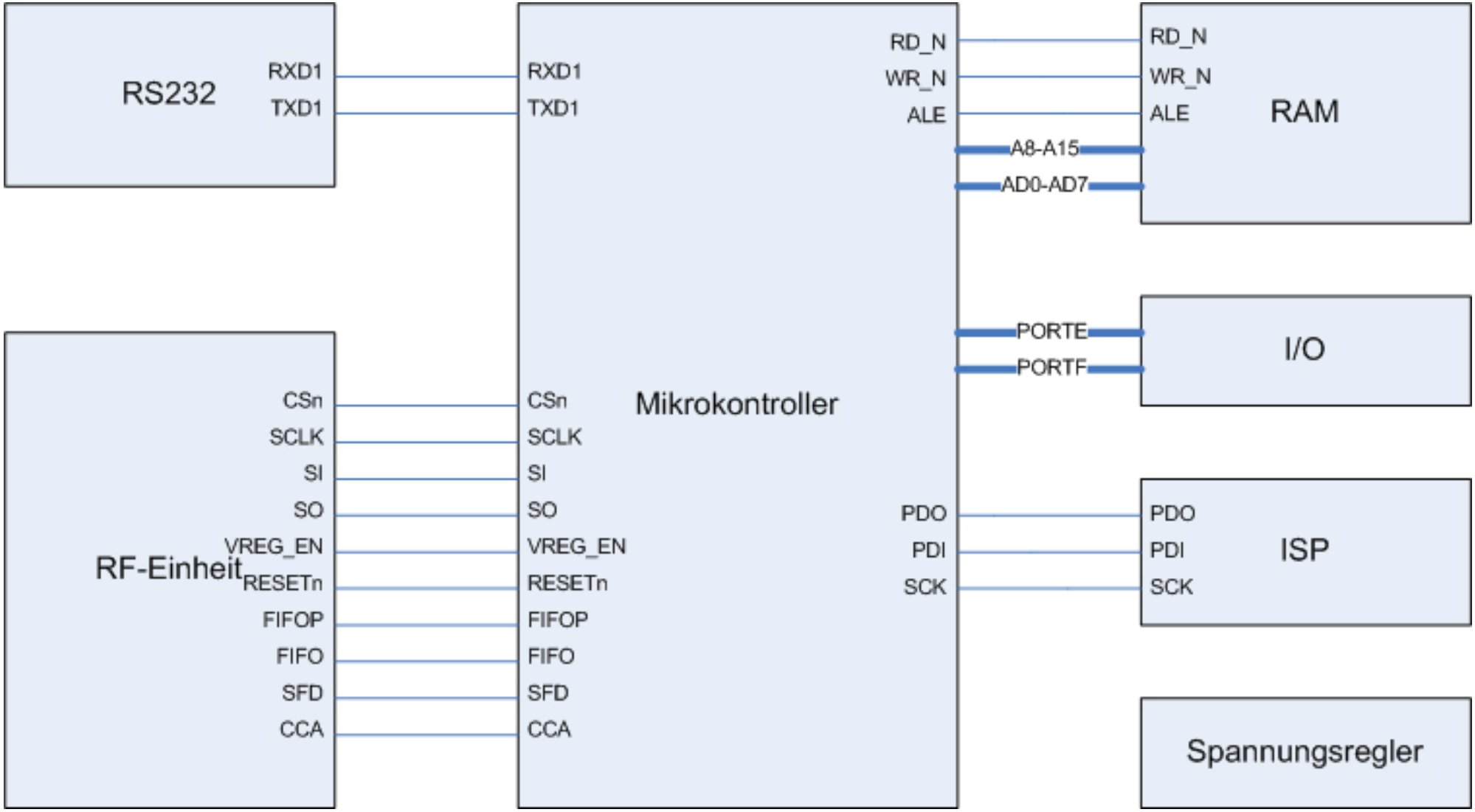

Abbildung 37: Schematischer Aufbau - Blockschaltbild

4.3.2.2 RF-Komponente

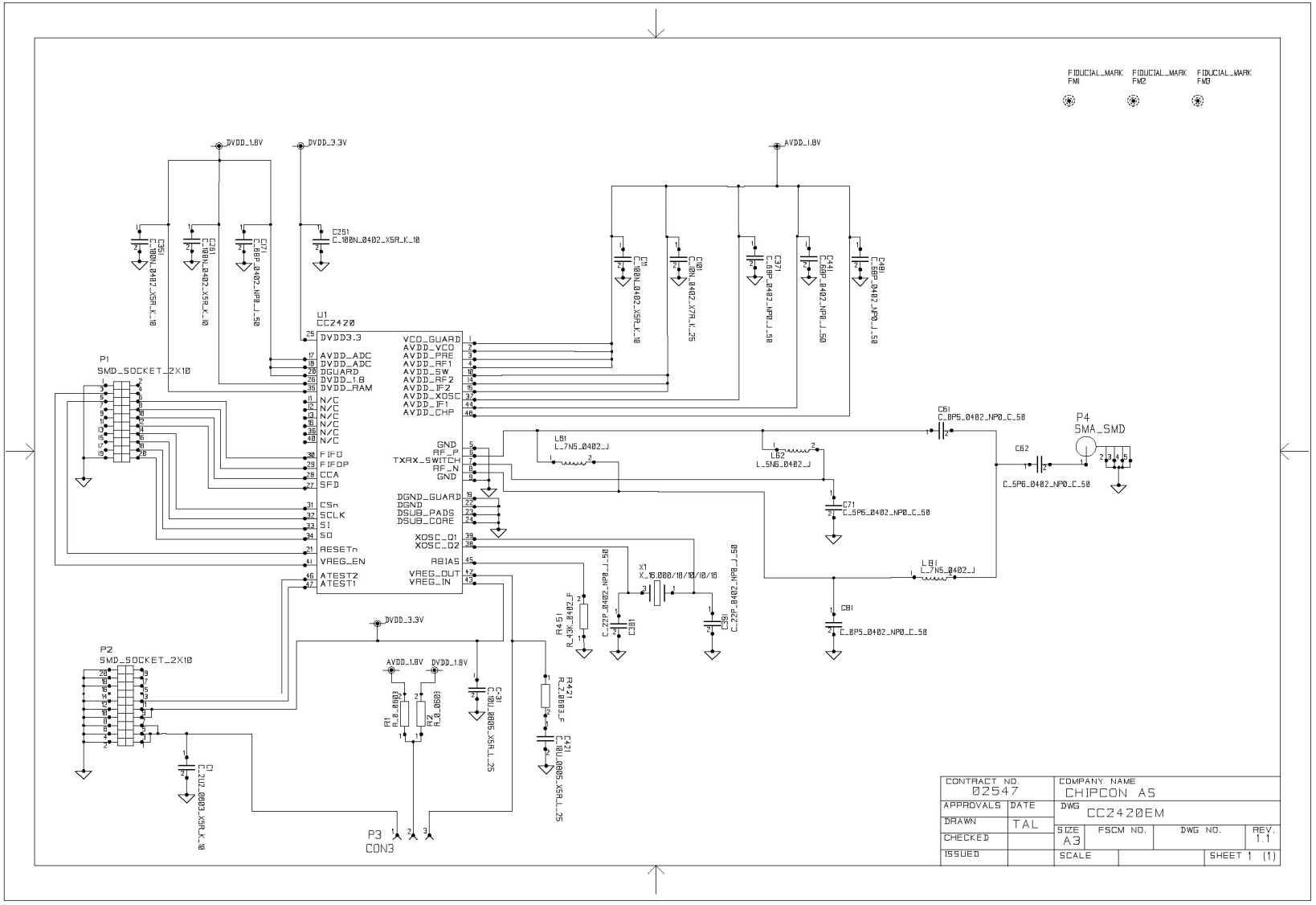

Abbildung 38: Schematischer Aufbau - Chipcon CC2420EM

4.3.2.3 Kommunikationsschnittstelle

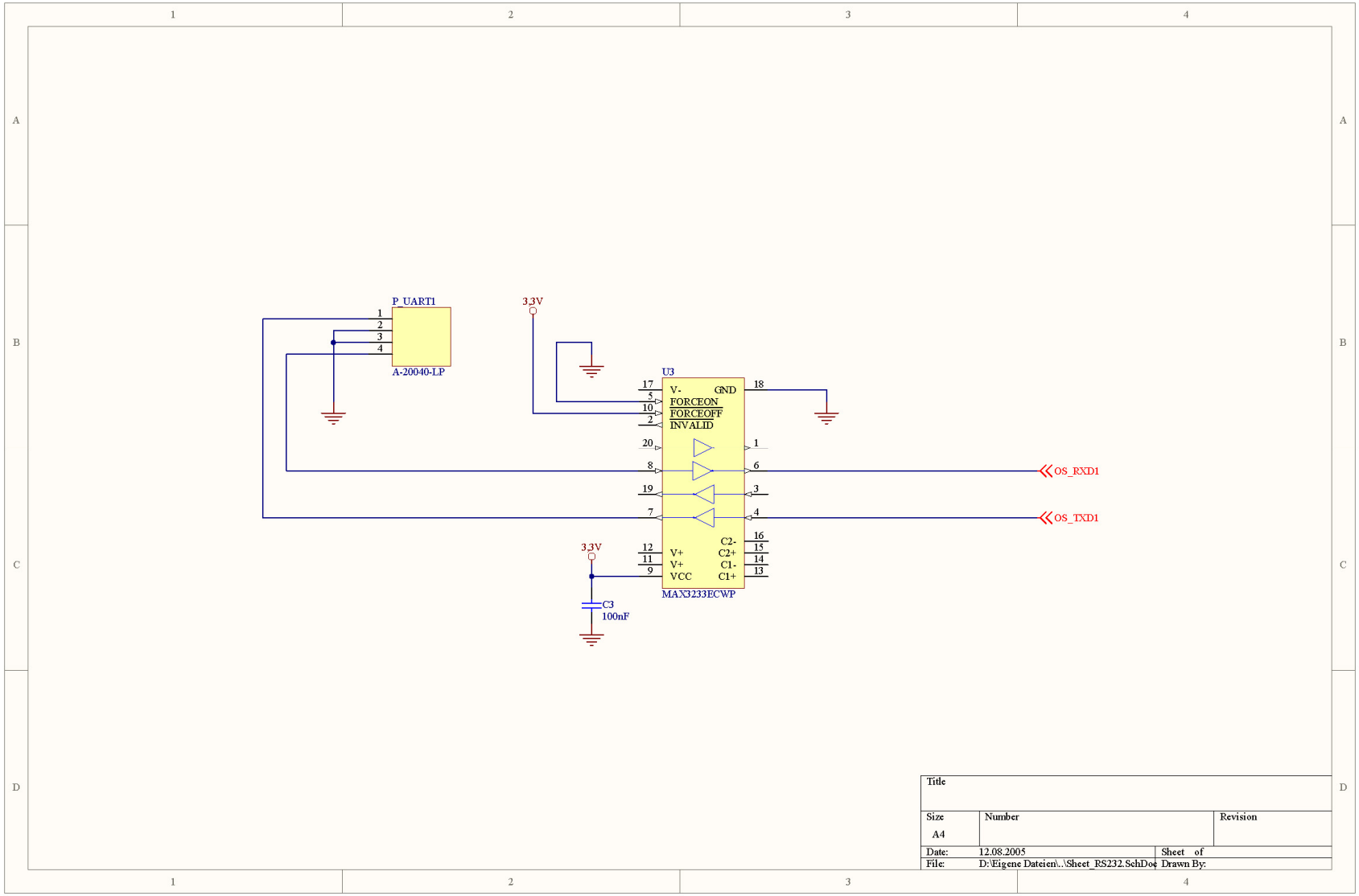

Abbildung 39: Schematischer Aufbau - RS232

4.3.2.4 Mikrokontroller und Anschlüsse

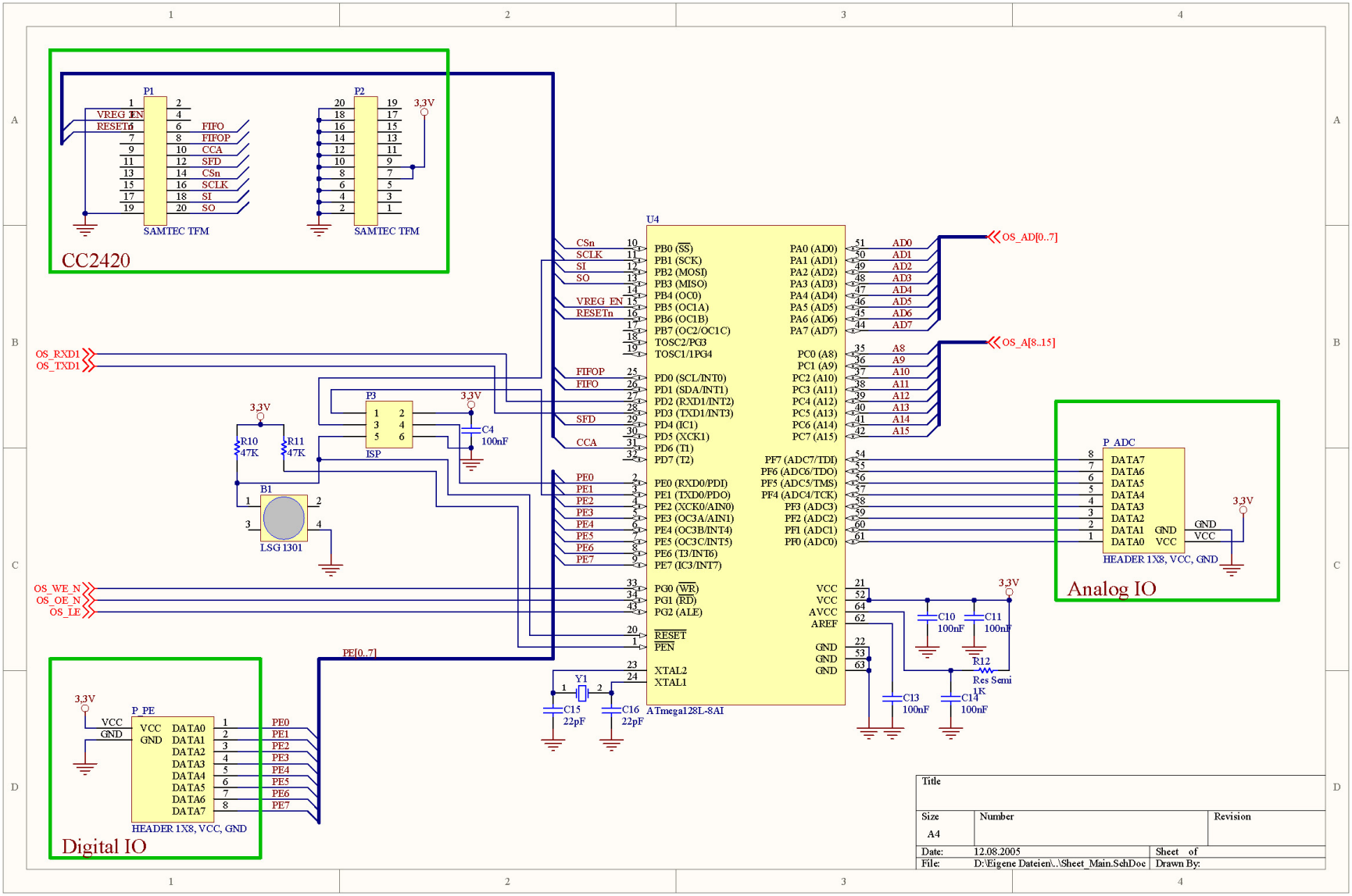

Abbildung 40: Schematischer Aufbau - Mikrokontroller und Anschlüsse

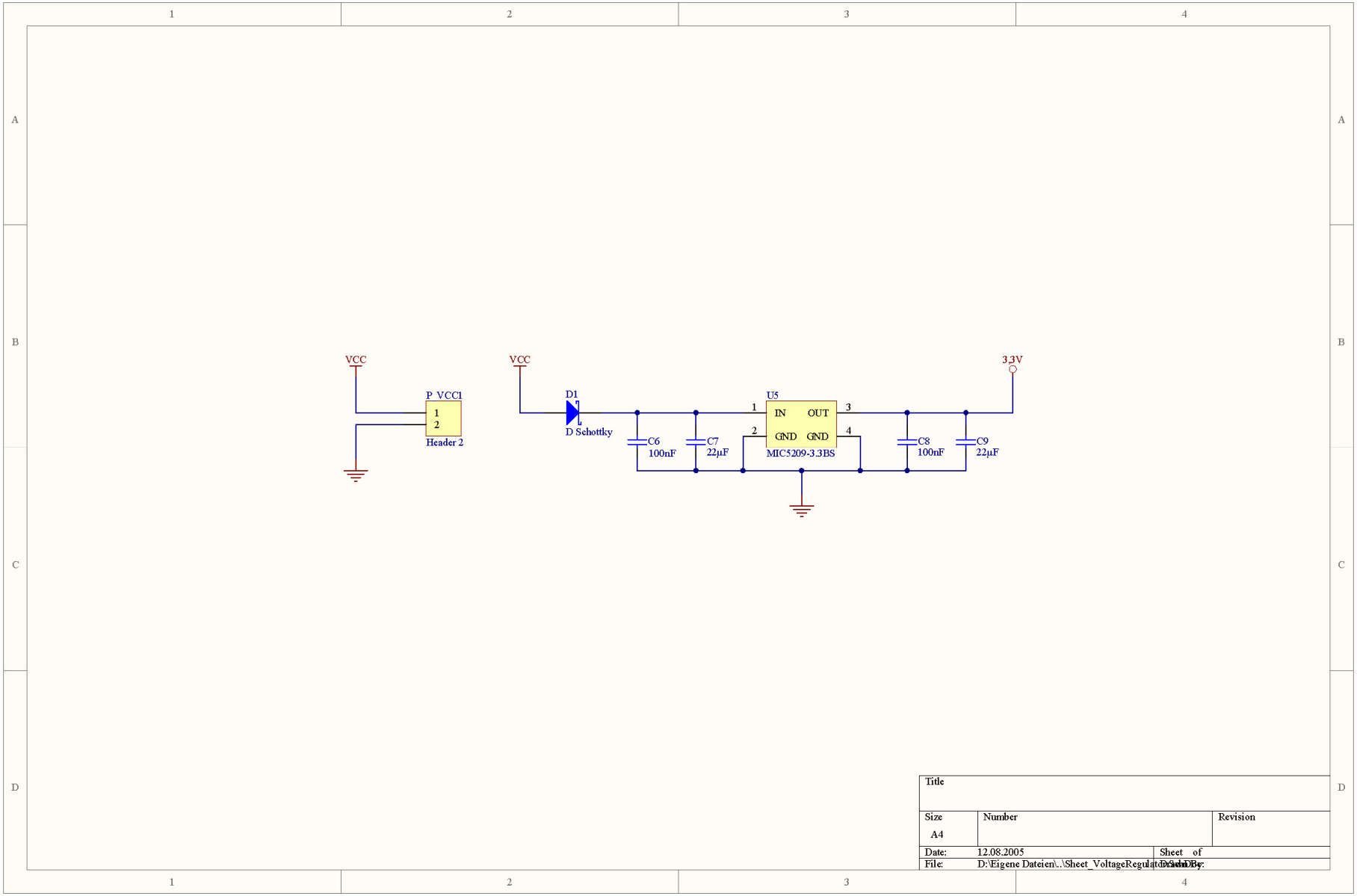

Abbildung 41: Schematischer Aufbau - Spannungsreglung

4.3.2.5 Speicher

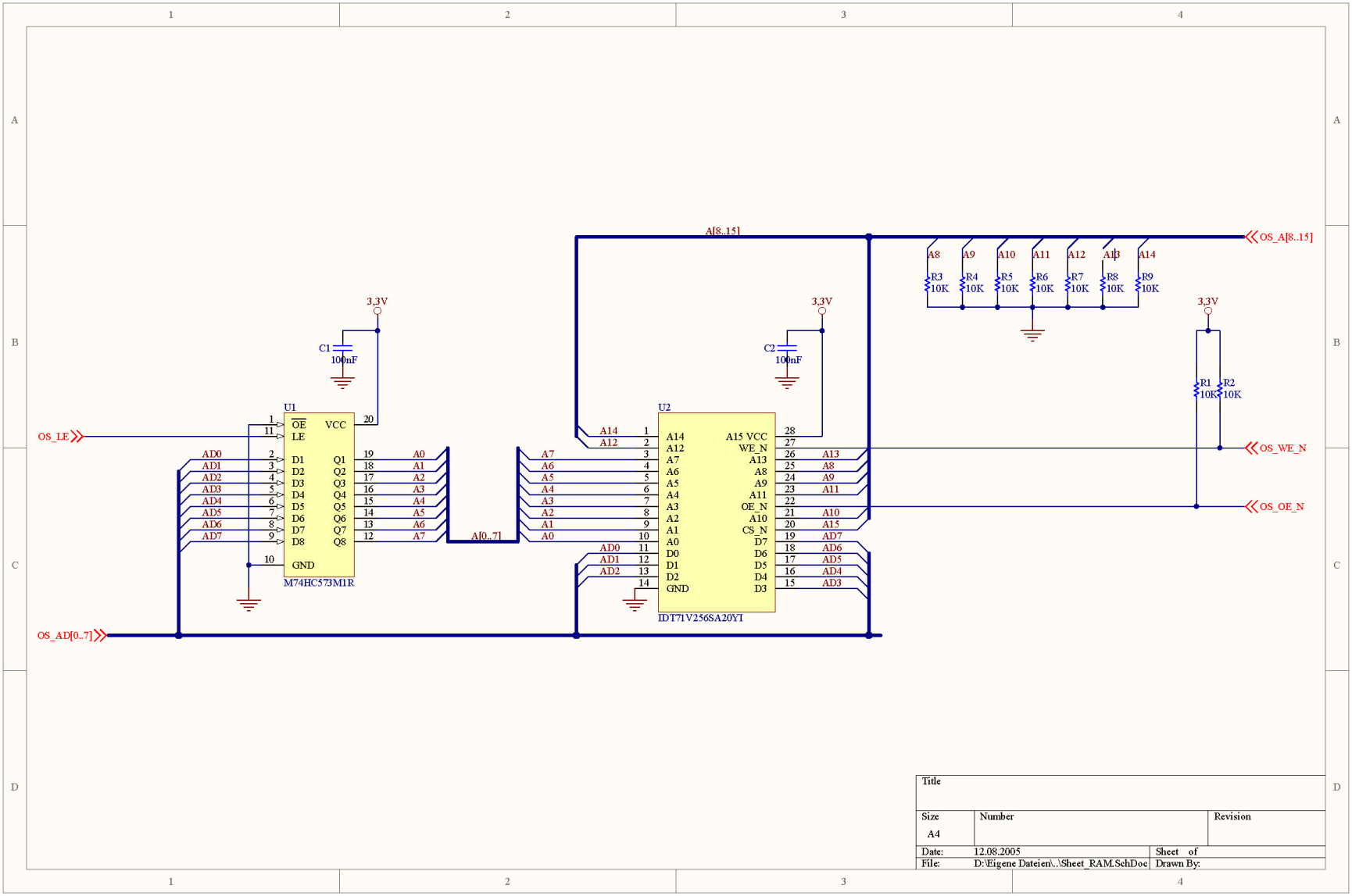

Abbildung 42: Schematischer Aufbau - Speicher

4.3.3 Ergebnis – PCB Layout

Die Positionierung der Komponenten wird von Hand realisiert. Das doppelseitige Bestücken der Platine mit überwiegend oberflächenmontierten Bauelementen (SMD) ermöglicht geringe Abmessungen der Leiterplatte, jedoch wird nur eine Lage verwendet. Das Setzen der Verbindungen (Routen) übernimmt der programminterne Autorouter. Das fertige PCB-Layout ist unter Abbildung 44 dargestellt.

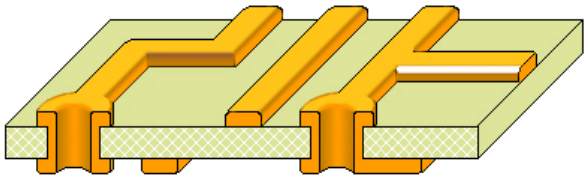

Abbildung 43: Aufbau der Platineschichten

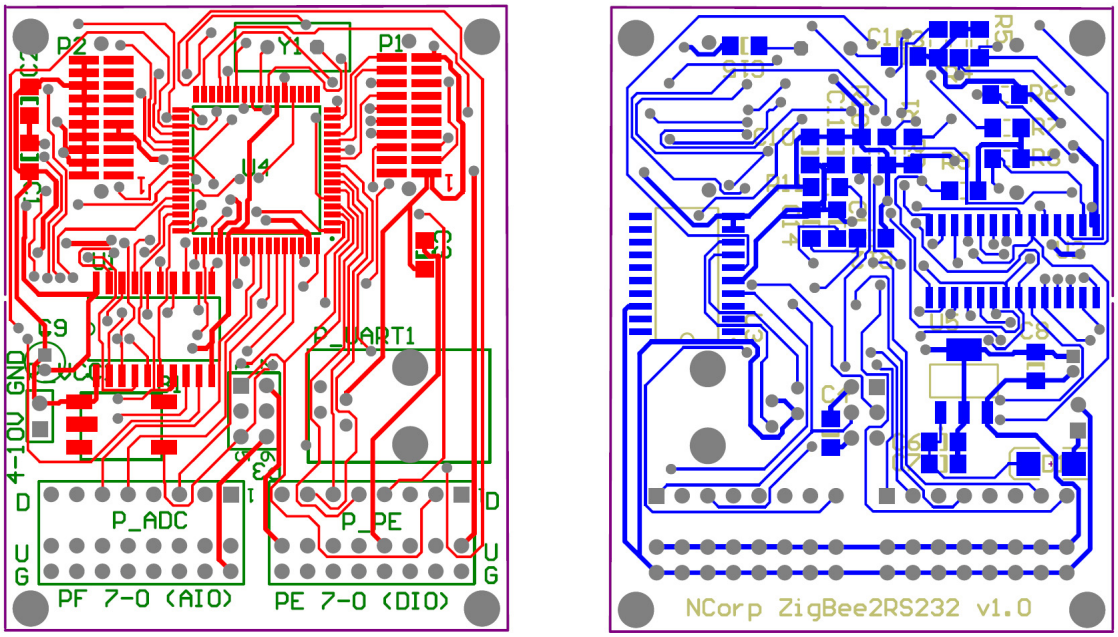

Abbildung 44: PCB-Layout, Ober- und Unterseite

5 Das Modul

Die Platinen wurden gemäß dem Entwurf aus Kapitel vier durch die Firma „Beta LAYOUT GmbH“ als Prototyp hergestellt. Anschließend wurden diese durch manuelles Löten mit den erforderlichen Bauteilen bestückt.

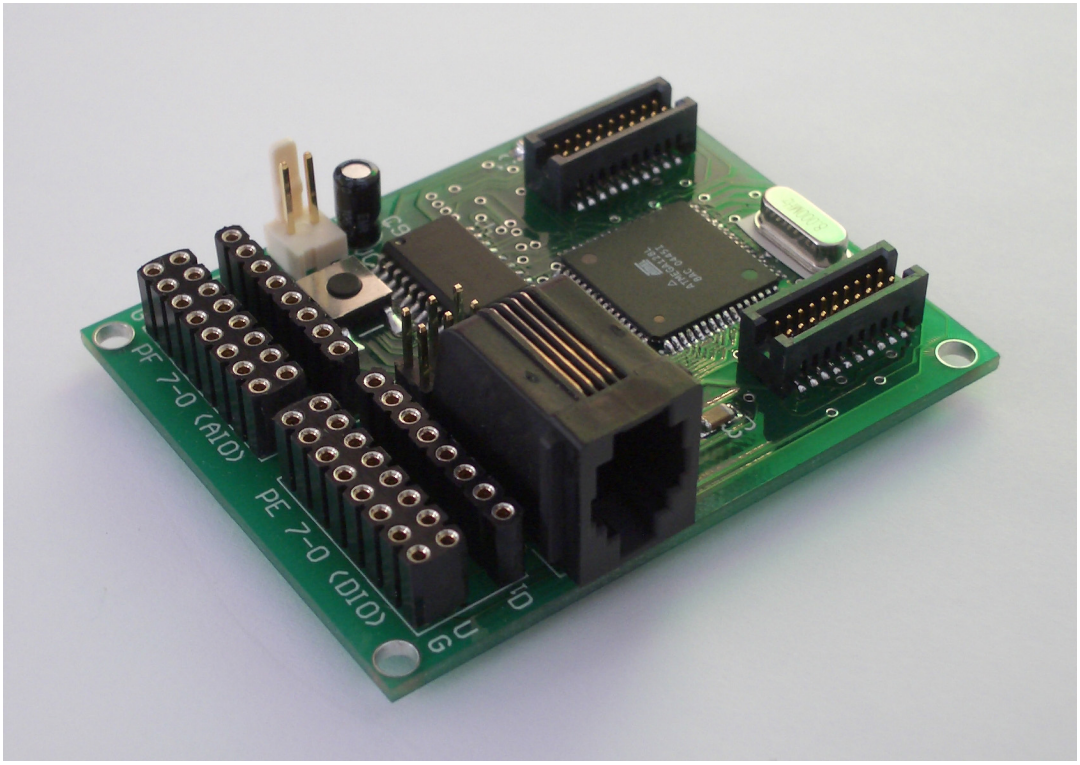

Abbildung 45: Modul - Seitenansicht ohne Funkeinheit

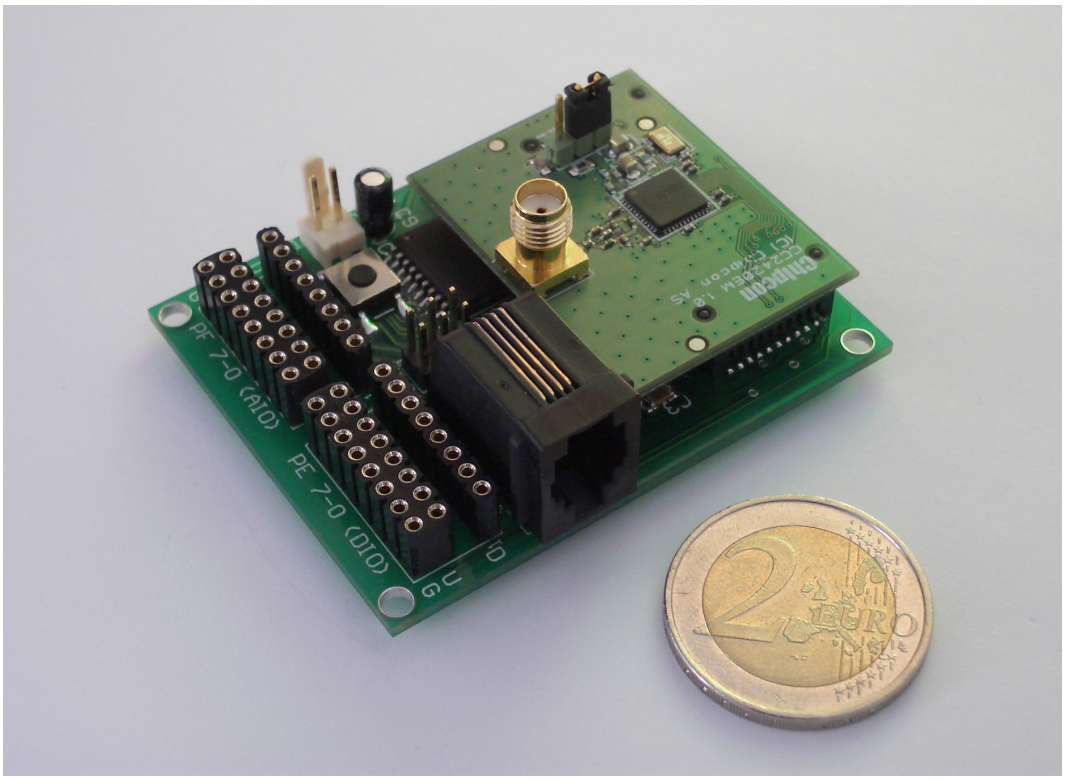

Abbildung 46: Modul - Seitenansicht mit Funkeinheit

5.1 Beschreibung

Mit aufgesteckter RF-Einheit misst das entstandene Modul 62 mm x 50 mm und ist 24 mm hoch. Das Gerät wird mit 4 – 10 Volt Gleichspannung versorgt.

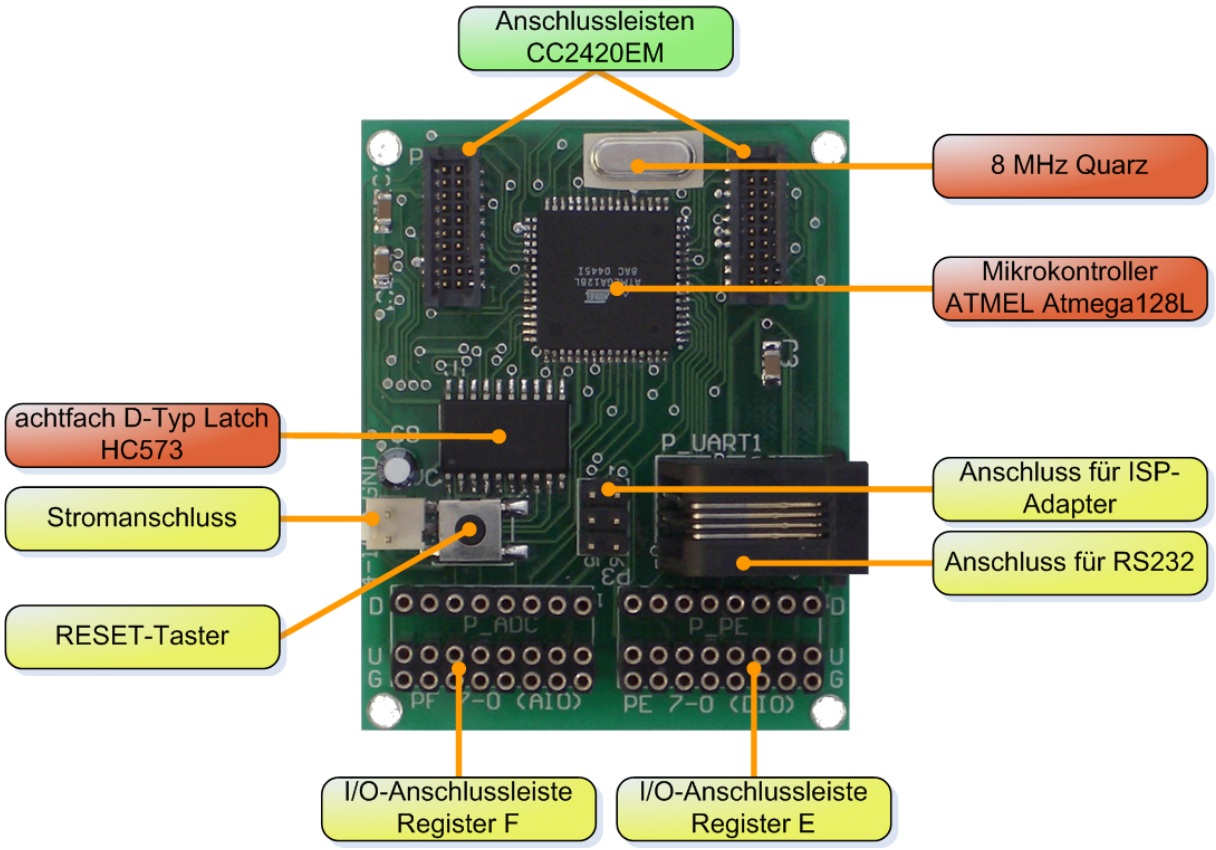

Abbildung 47: Modul - Oberansicht

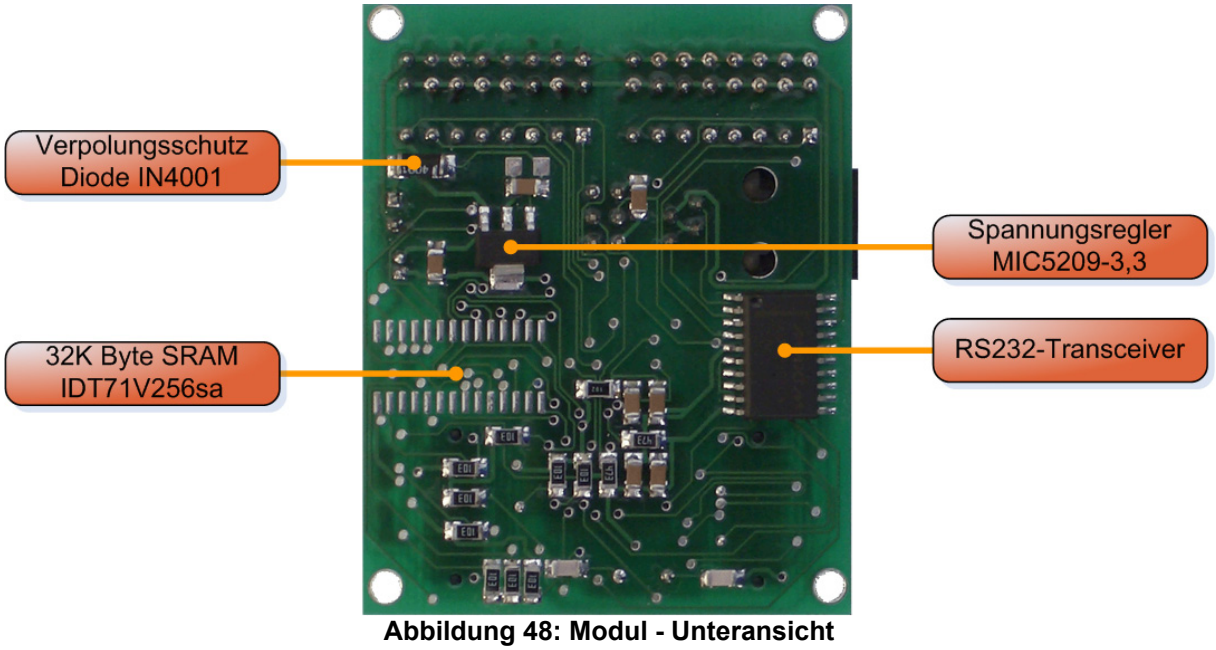

Abbildung 48: Modul - Unteransicht

5.2 Kosten

Für die Erstellung eines Moduls wurden folgende Kosten aufgebracht:

- **Bauteile**
  Die aktuellen Preise der Bauteile sind unter Tabelle *1* aufgelistet.
  Es handelt sich um Stückpreise, welche bei der Produktion in Serie deutlich sinken würden.

- **Platine**
  Da die Platine als Prototyp gefertigt wird, fallen für drei Exemplare (Fertigung auf 1.00 dm² großen Platine) 77 € Kosten an. Der Preis für eine Leiterplatte liegt bei 26 €. Zum Vergleich: bei Vergabe eines Kleinserienauftrags von 150 Platinen sinkt der Stückpreis auf 2,59 €.

- **RF-Modul**
  Das Funkmodul von Chipcon (CC2420EM) ist für einen Stückpreis von 50 € erhältlich.
  In dieser Arbeit wurde von der selbständigen Entwicklung Abstand genommen, da die notwendige Bestückung der Platine aufgrund der IC-Größe nur mit speziellen Gerätschaften bzw. nur unter hohem Aufwand möglich ist.
  Die erhebliche Reduktion der Stückpreise kann im Zuge einer Kleinserienproduktion veranschaulicht werden: die Platinengröße beträgt 30 mm x 39 mm, was bei einer Fertigung von 160 Stück (20 x 1 dm² Platinen) zu einem Stückpreis von 1,88 € führt. Die Kosten für die Produktion einer Prototyp-Platine mit 8 Einheiten liegen bei 6,68 € pro Stück.
  Der einzelne CC2420 liegt etwa bei 5 € pro IC, die restlichen Komponenten können für insgesamt 15 € erworben werden (Einzelstückpreise).

Die Gesamtkosten für die Erstellung eines Moduls im Rahmen dieser Arbeit belaufen sich auf 107, 61 €.

Tabelle 1: Bauteilkosten

Beschreibung	Hersteller	Bauteil	An-zahl	Artikel-preis (€)	Gesamt-preis (€)
Mikrokontroller	ATMEL	ATmega128L 8 ai oder au	1	10,30	10,30
RS232-Transceiver	MAXIM	Max3233EEWP	1	6,67	6,67
Speicher	IDT	IDT71V256sa	1	4,30	4,30
Achtfach D-Typ Latch	Motorrola	HC573	1	0,31	0,31
Spannungsregler	Micrel	MIC5209-3,3BS	1	1,35	1,35
Quarz			1	0,49	0,49
Anschlussleisten (CC2420EM)		Stiftleiste 2x10-polig, Raster: 1,27	2	1,05	2,10
Reset-Taster			1	0,23	0,23
Verpolungsschutz		Diode 1N 4001	1	0,08	0,08
Stromanschluss		Printstecker 2-polig	1	0,78	0,78
Modulareinbau-buchse			1	0,38	0,38
SMD-Kondensator 22 pF			2	0,05	0,10
SMD-Kondensator 100 nF			10	0,09	0,90
SMD-Widerstand 1,0 kΩ			1	0,10	0,10
SMD-Widerstand 10 kΩ			9	0,10	0,90
SMD-Widerstand 47 kΩ			2	0,10	0,20
Subminiatur-Elko, radial 22µF/10V			1	0,07	0,07
Stiftleiste 2x3-polig, Raster: 2,54mm		Stiftleiste 2x10-polig	1	0,13	0,13
Buchsenleiste 2x 2x8-polig		Buchsenleiste 2x17-polig	1	2,22	2,22
				Gesamtpreis:	31,61 €

6 Applikation

Quellen: [DOC_PP], [DOC_AVR], [JDK], [GKru], [AVR_1], [AVR_2]

Um die Funktionalität der erstellten Geräte zu überprüfen und einen kleinen Einblick in die praktische Anwendung zu geben, wurde ein beispielhaft ein einfaches Programm entwickelt.
Einem Anwender wird über die grafische Oberfläche an einem PC die Möglichkeit gegeben, ein sternförmiges Netzwerk zu administrieren. Die Endknoten sind jeweils mit einem achtpoligen Piano-Dip-Schalter auf der Eingangsseite ausgestattet, welcher einen Sensor simulieren soll. Aktoren werden auf der Ausgangsseite durch Leuchtdioden simuliert.
Es ist möglich, dem Netzwerk neue Teilnehmer hinzuzufügen. Ferner können die Werte eines jedes Knotens ausgelesen und Aktoren angesteuert werden.

6.1 Ansatz

Folgende Softwarekomponenten werden unterschieden: einerseits das auf dem Modul und somit auf dem ATMEL ATmega128 laufende Programm. Andererseits eine entsprechende Applikation auf dem Computer, um dem Anwender die Möglichkeit zu geben, über den Koordinator mit dem gesamten Netz zu interagieren.

6.2 Programmierumgebung und Werkzeuge

Das Programm für den Mikrokontroller wird in C geschrieben und mithilfe des freien C-Compilers avr-gcc übersetzt. Da die Entwicklung unter dem Betriebssystem Windows XP stattfindet, kommt die Softwaresammlung WinAVR [WA] in der Version 20050214 zum Einsatz. Sie beinhaltet neben dem Compiler und anderen Tools die Laufzeitbibliotheken [avr-libs] und die zugehörige Dokumentation. Um den Quellcode zu schreiben, wird der Texteditor Programmers Notepad [PN] in der Version 2.0.5.48 verwendet (*Abbildung 49: Werkzeuge - Programmers Notepad*).

Da der ZigBee-Stack nicht zur Verfügung stand, arbeitet diese Applikation gemäß IEEE 802.15.4 auf der MAC-Ebene. Die Laufzeit-Bibliotheken [CC_libs] stammen von der Firma Chipcon. Sie decken nicht den kompletten Funktionsumfang ab, reichen jedoch für diese Anwendung aus.

Der durch den Compiler übersetzte Maschinencode wird via ISP-Schnittstelle auf den ATMEL Atmega128 übertragen. Als Programm eignet sich das freie PonyProg [PP], welches die gängigsten Adapter unterstützt (*Abbildung 50: Werkzeuge - PonyProg*).

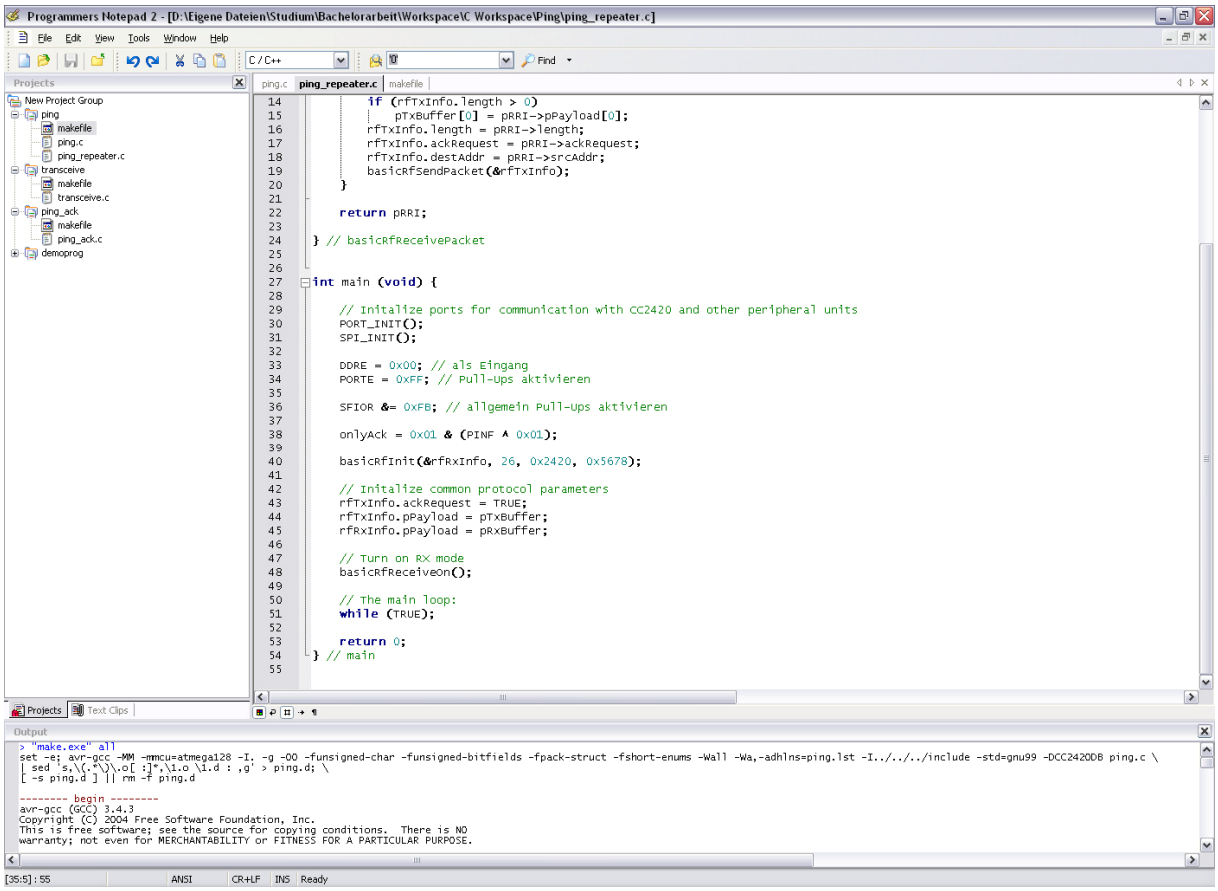

Abbildung 49: Werkzeuge - Programmers Notepad

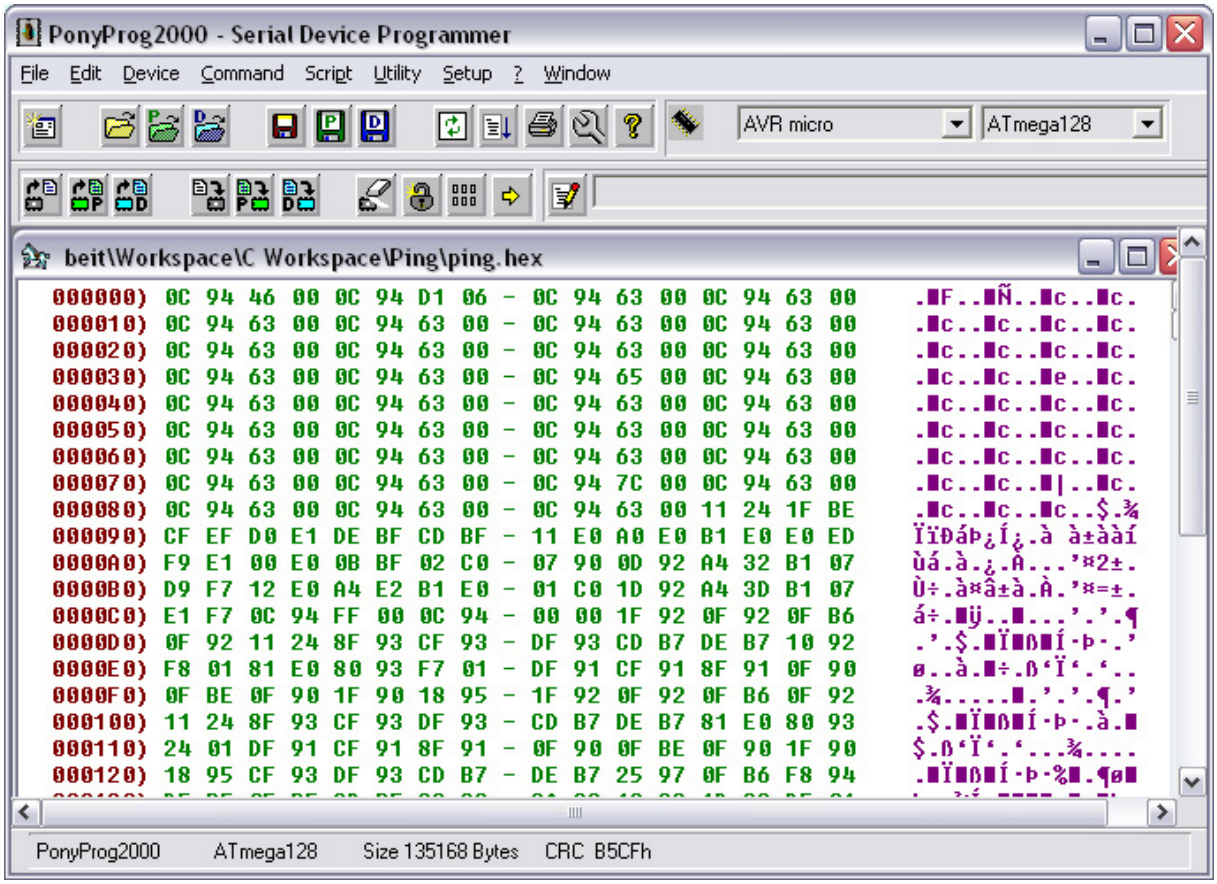

Abbildung 50: Werkzeuge - PonyProg

Die Kommunikation zwischen Mikrokontroller und Computer wird über die serielle Schnittstelle realisiert. Die einzige Anforderung an die Programmiersprache für das Computerprogramm ist die Möglichkeit, auf das serielle Interface zugreifen zu können. Um die Anwendung und damit den Anwender nicht fest an ein Betriebssystem zu binden, wird als Programmiersprache JAVA 1.5.0_04 verwendet.
Die Entwicklung findet unter Windows XP statt, als Entwicklungsumgebung bietet sich das freie Eclipse [EC] (Abbildung 51: Werkzeuge - Eclipse) in der Version 3.1 an.

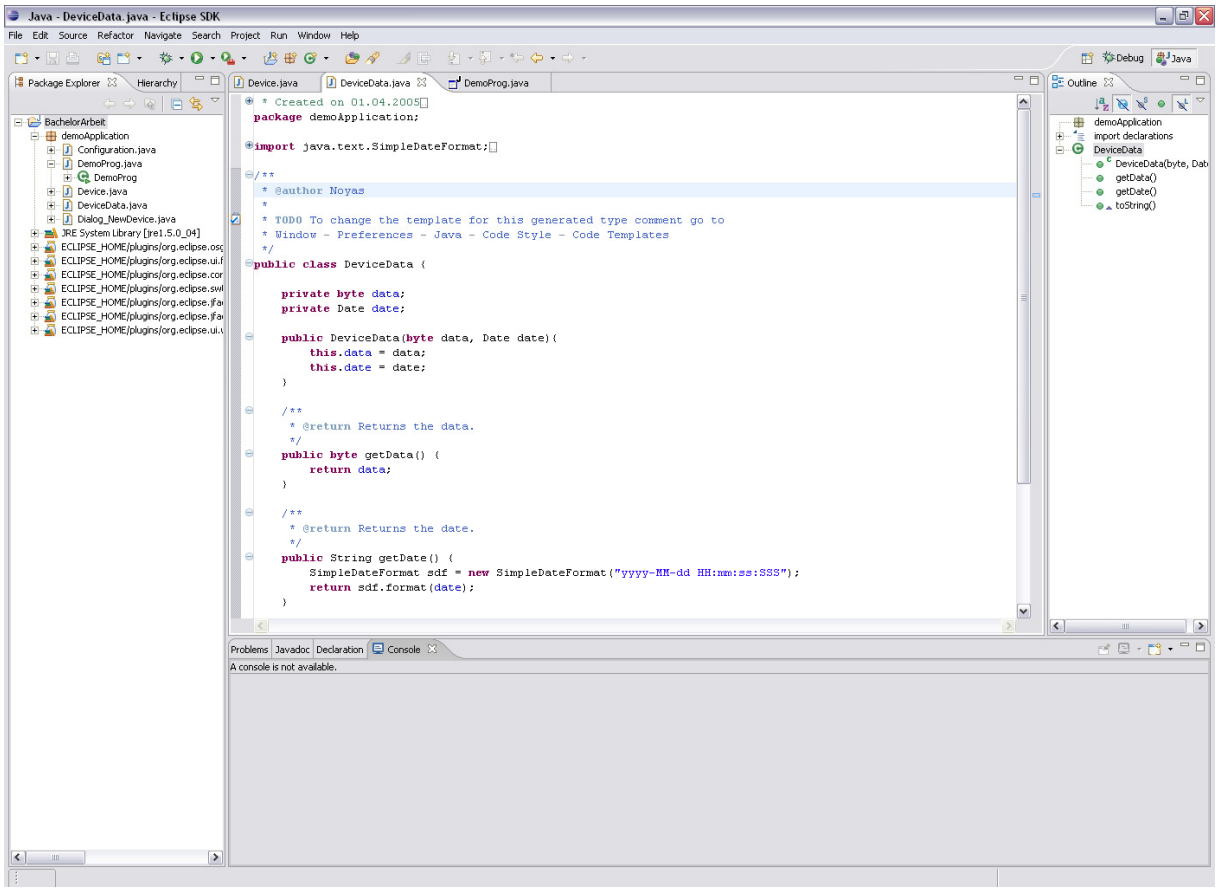

Abbildung 51: Werkzeuge - Eclipse

Die Eclipse Foundation stellt zusätzlich eine Bibliothek für das Design von grafischen Benutzeroberflächen zur Verfügung: die SWT-Bibliothek. Der Vorteil ist, dass die Programmoberfläche genauso aussieht wie das darunter liegende Betriebssystem.

6.3 Funktionen und Programmablauf

6.3.1 Modul-Software

Das Netzwerk in dieser Anwendung besteht aus zwei verschiedenenen Modulen: dem Koordinator und dem Endknoten. Auf die Funktionsweisen der einzelnen Module wird in den jeweiligen Abschnitten näher eingegangen.
Es befindet sich auf beiden Geräten dieselbe Software, jedoch werden, abhängig vom Zustand des Netzes, verschiedene Codeabschnitte abgearbeitet: Das erste Gerät, welches das „Netz“ betritt, wird zum Koordinator, alle nachfolgenden Geräte werden zu Endknoten, die über den Koordinator mit dem PC kommunizieren. Es bildet sich eine Sterntopologie. Abgebildet in *Abbildung 52: Netzstruktur der Anwendung*.

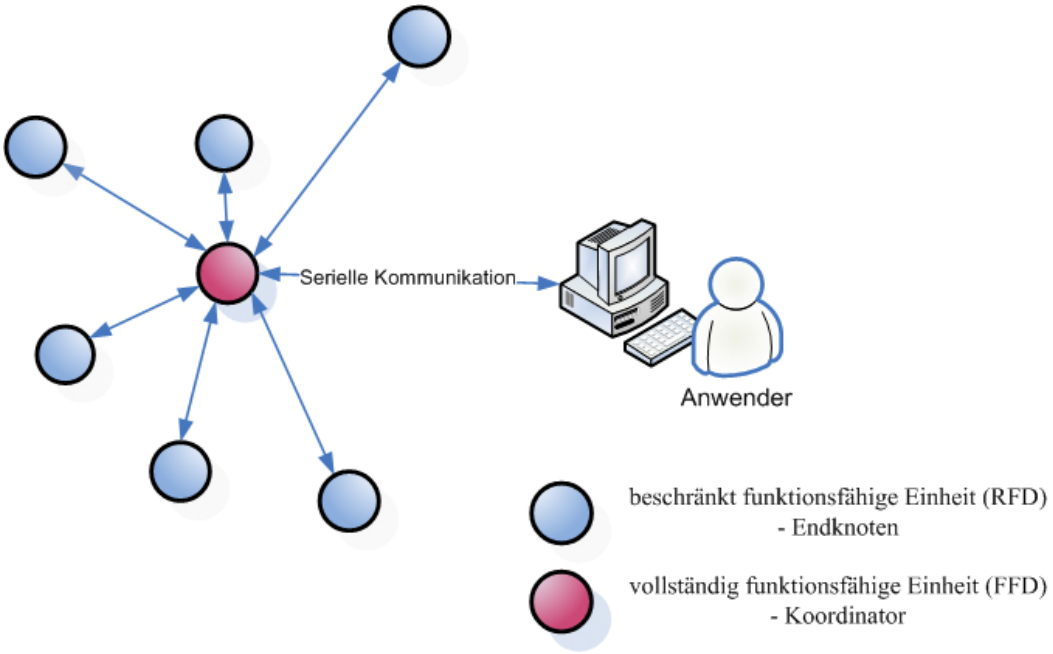

Abbildung 52: Netzstruktur der Anwendung

Der Initialisierungsprozess entscheidet über den auszuführenden Code. Zusammengefasst ergibt sich folgender Ablauf: wird ein Gerät gestartet, initialisiert es die Schnittstellen und die Funkeinheit mit der Standardadresse für neue Geräte (0x00). Um zu überprüfen, ob bereits ein Koordinator vorhanden ist, wird ein leeres Paket an die für den Koordinator reservierte Adresse (0xFF) gesendet. Die Nachricht erfordert eine Empfangsbestätigung.
Erfolgt diese nicht, wird davon ausgegangen, dass kein Koordinator verfügbar ist. Das Gerät initialisiert seine Funkeinheit neu mit der Adresse 0xFF, wird somit zum Koordinator und geht in Wartestellung für Anfragen und Kommandos.
Sollte zuvor eine Empfangsbestätigung eingetroffen sein, wird das Gerät zu einem Endknoten und wechselt ebenfalls in Wartestellung. Dargestellt ist dieser Prozess in *Abbildung 53: Prozess - Initialisierung des Gerätes*.

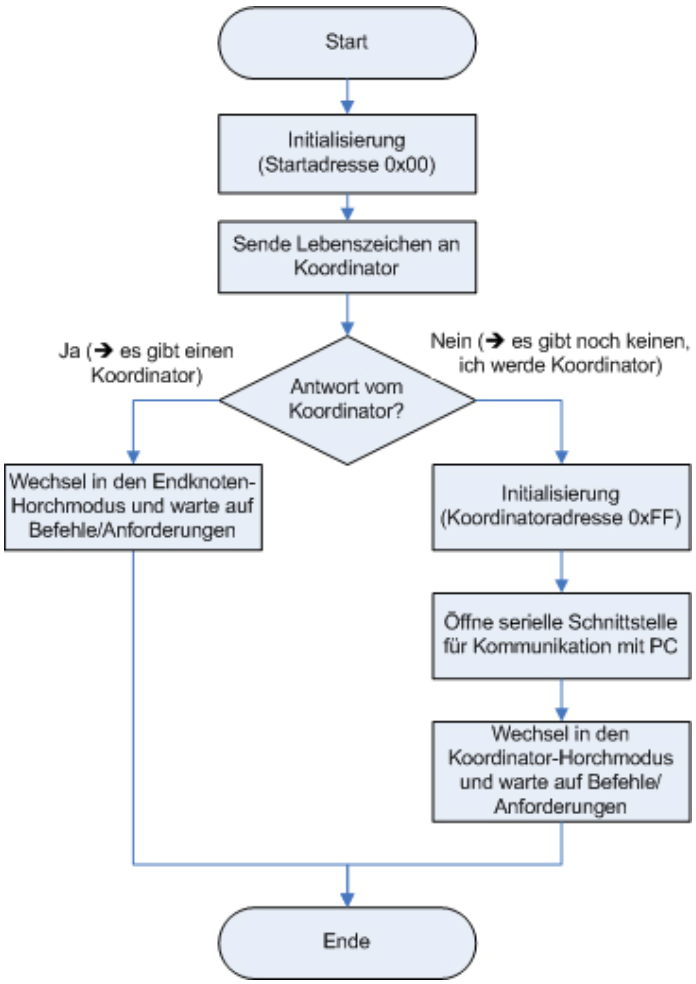

Abbildung 53: Prozess - Initialisierung des Gerätes

6.3.1.1 Koordinator

Nach der Initialisierung befindet sich der Koordinator, wie oben beschrieben, im Wartezustand.
Erreicht ihn über die serielle Schnittstelle eine Nachricht vom PC, wird diese in Adressat und Nachrichteninhalt zerlegt. Der Koordinator setzt ein Paket mit dem Inhalt zusammen und schickt es an den Adressaten.
Wird ein Paket eines Endknotens (über Funk) empfangen, sendet der Koordinator dieses an den PC weiter. Hierbei werden Information und Absenderadresse zusammengefasst und via RS232 weitergeschickt.

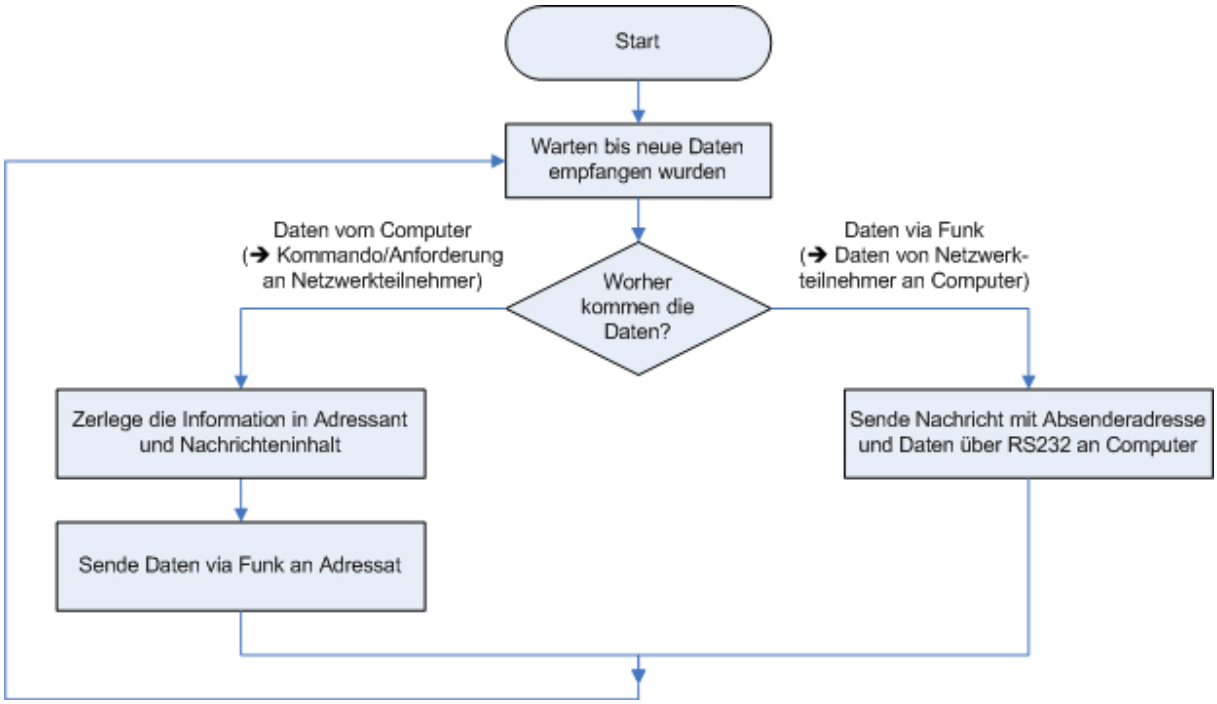

Abbildung 54: Prozess - Koordinator

6.3.1.2 Endknoten

Ebenso wie der Koordinator verharrt der Endknoten nach Abschluss des Initialisierungsprozesses in einem Wartezustand. Sobald ihn via Funk Daten erreichen, werden diese ausgewertet. Es gibt zwei Kommandos: das Modul wird angewiesen, die eigene Adresse auf eine Übergebene zu ändern. Dies geschieht direkt nach der Initialisierung, da die Initialisierungsadresse (0x00) für neue Geräte reserviert ist. Die Funkeinheit wird mit dieser Adresse neu gestartet.
Das zweite Kommando ist die Aufforderung, den aktuell laufenden Modus zu wechseln. Hier werden die Modusinformationen aus dem empfangenen Paket extrahiert und auf das Modul übertragen. Details zu den Modi werden im Zuge der Erläuterung der PC-Software vermittelt.

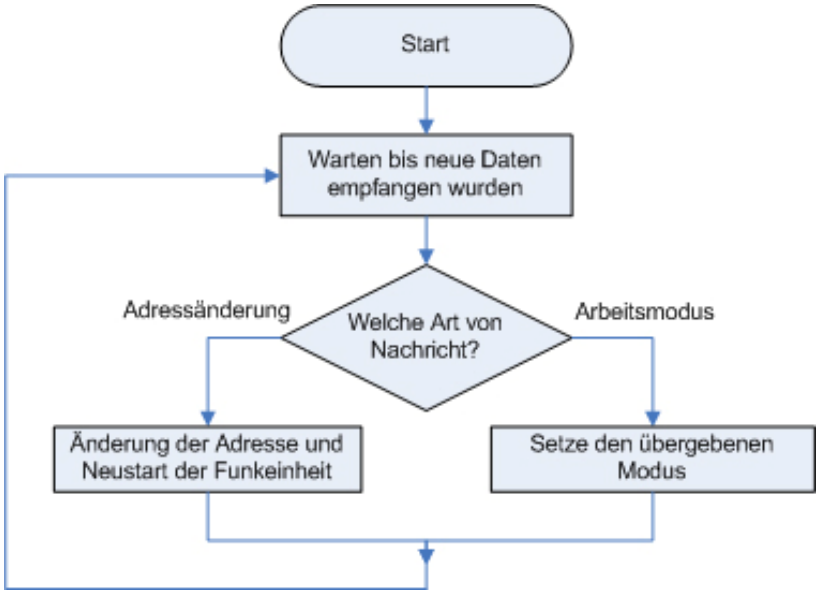

Abbildung 55: Prozess - Endknoten

6.3.2 PC-Software

Der Anwender erhält durch die PC-Software die Möglichkeit, das Netzwerk zu administrieren. Der Ablauf ist folgender:
Die Schnittstelle zum Koordinator wird unter „1“ geöffnet, wobei der Koordinator noch nicht vorhanden sein muss. Sobald das erste Gerät als Koordinator deklariert wurde, können Geräte als Endknoten hinzugefügt werden.
Gelangt ein neues Gerät in den Bereich des Netzes und stellt die Anfrage nach dem Koordinator, wird ihm über den Koordinator vom PC-Programm eine Adresse zugewiesen. Ist dieser Vorgang abgeschlossen, erscheint in der Bedienoberfläche ein Dialog, um dem Gerät einen Namen zu vergeben („2“). Im gleichen Zug wird der Knoten in die Liste („3“) aufgenommen und ist ab sofort administrierbar. Wird (unter „3“) ein Knoten selektiert, können auf der rechten Seite (roter Rand) Kommandos erteilt und Anforderungen versandt werden.
Das Gerät kann in drei verschiedene Modi gesetzt werden („6“):

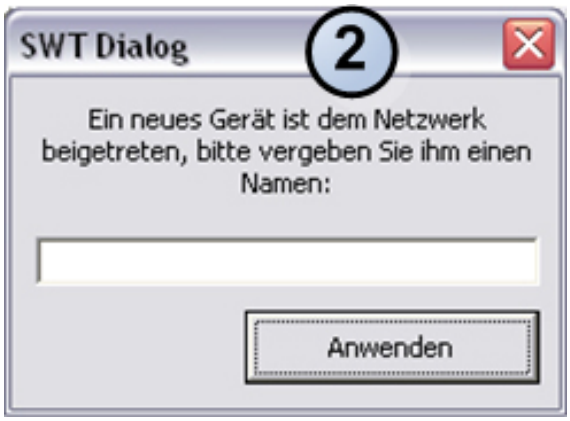

Abbildung 56: Programm-Dialog

1. **Wartemodus**
   Im Wartemodus verharrt das Gerät solange im aktuellen Status, bis ein neuer Befehl eintrifft. Es liefert keine neuen Sensorenwerte und sendet den Aktoren keine neuen Kommandos.

2. **Intervallmodus**
   Bei Aktivierung des Intervallmodus wird dem Gerät zusätzlich die eingestellte Periodendauer übergeben, nach welcher es die anliegenden Sensorwerte übertragen soll. Die Erneuerung der Werte erfolgt kontinuierlich bis zum nächsten Moduswechsel.

3. **Grenzwertmodus**
   Dem Endknoten wird mitgeteilt, in welchem Bereich sich Sensorwerte befinden dürfen. Verlässt ein Wert den Bereich, wird der Anwender durch eine Nachricht darüber informiert.

Empfangene Daten werden für jedes Gerät in einem Protokollfeld aufgenommen („4“) und sind jederzeit abrufbar.
Zusätzlich gibt es die Möglichkeit, eine einmalige, direkte Abfrage des Sensorwertes zu starten oder den Wert am Ausgang einmalig zu ändern („5“). Der aktuell laufende Modus wird dazu kurz unterbrochen und nach erfolgter Ausführung sofort wieder aufgenommen.
Ereignisse, wie das Ein- und Austreten von Geräten in das bzw. aus dem Netzwerk oder wichtige Programmdetails werden unter „7“ protokolliert.

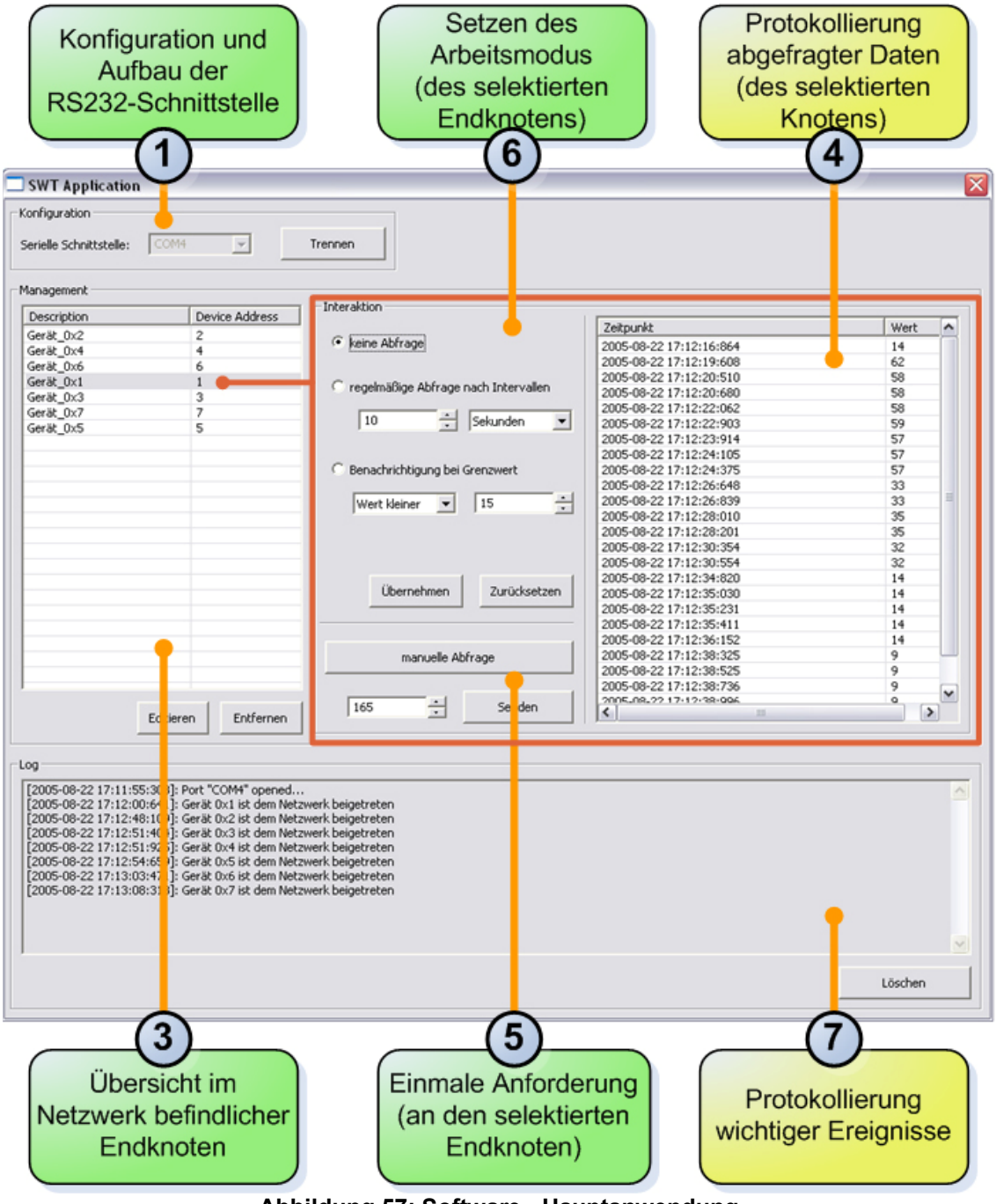

Abbildung 57: Software - Hauptanwendung

7 Validierung und Tests

7.1 Reichweite

Die Ermittlung der praktischen Reichweite erfolgt nach einem einfachen Prinzip. Zwei Module werden solange von einander wegbewegt, bis die Kommunikation abbricht. Eine Software signalisiert den Verbindungszustand für jedes Modul über zwei Leuchtdioden. Eine deutet auf den Empfang und die andere auf das erfolgreiche Senden von Paketen hin. Somit kann überprüft werden, ob die Sende- bzw. Empfangsleistungen der Geräte stark voneinander abweichen.
Es werden drei Situationen nachgestellt:

7.1.1 Direkte Verbindung, freie Strecke

Die Module werden im Freien bei stetigem Sichtkontakt voneinander entfernt. Eine Kommunikation ohne sichtbare Beeinträchtigung (kein Flackern der LED's) findet bis zu einer Entfernung von etwa 180 Metern statt. Die maximale Entfernung für regelmäßige Kommunikation, jedoch mit hoher Fehlerrate, liegt bei 210 Metern. Wird in dieser Entfernung etwas in die Sichtlinie gebracht, bricht der Kontakt sofort ab.

7.1.2 Natürliche Umgebung

Der Test in einer natürlichen Umgebung bezeichnet den Einsatz in einem von Pflanzen bewachsenen Gebiet. Zwei Module werden in einem Garten zwischen Gewächsen auf dem Boden positioniert.
Die Reichweite für eine fehlerfreie Kommunikation ist stark abhängig von der Dichte und Anzahl der umliegenden Pflanzen. Befinden sich die Geräte in Erdmulden, ist eine Kommunikation so gut wie gar nicht möglich. Bei relativ guten Bedingungen, wobei der Untergrund eben ist, die Module von Sträuchern umgeben sind und sich keine Bäume in der Luftlinie befinden, werden Reichweiten von 20 bis 50 Meter erzielt.

7.1.3 Innerhalb von Gebäuden

Gemessen wurde die Verbindung in einem massiven Haus mit zwei Etagen und einer maximalen Entfernung (Luftlinie) von etwa 20 Metern, durch eine Decke und zwei Wände hindurch. Eine Beeinträchtigung der Kommunikation erfolgte, wenn sich die Module unmittelbar hinter Gegenständen befanden.

7.2 Datenübertragungsgeschwindigkeit

Aus den IEEE 802.15.4-Spezifikationen geht hervor, dass physikalisch Übertragungsgeschwindigkeiten von bis zu 250 kBit/s möglich sind. Interessant ist der Vergleich dieses theoretischen Wertes mit den in der Praxis ermittelten Werten.
Eine Anwendung auf den Modulen führt drei verschiedene Testläufe durch und dokumentiert die Ergebnisse in der Konsole. Die Daten werden in eine Excel-Tabelle importiert und weiter verarbeitet.
Diese Anwendung befindet sich auf einem Modul, die Wahl des Testlaufes erfolgt über Dip-Schalter. Das andere Gerät agiert als Repeater, es bestätigt das Eintreffen von Nachrichten und sendet abhängig von der Konfiguration Pakete zurück.
Die entscheidenden Kriterien sind die transferierte Datenmenge und die dafür benötigte Zeit.

Eine einheitliche Zeitmessung ist nicht realisierbar, da sich auf den Modulen keine aufeinander abgestimmten Echtzeituhren befinden. Folglich muss der Sender die Zeit bis zum Eintreffen eines Echos der gewünschten Nachricht dokumentieren.
Die Zeitmessung erfolgt mithilfe des 16-Bit-Zählers (Timer/Counter 1) des Mikrokontrollers. Bei 8 MHz Taktfrequenz wird mit dem Vorteiler 256 eine Laufzeit von maximal etwa zwei Sekunden erreicht, bevor das Zählregister überläuft und ein Overflow-Interrupt (wird als Timeout angewandt) ausgelöst wird.
Um die Messungen nicht durch Spitzenwerte zu verfälschen, wird jede einzelne Sendung von Paketen 255-mal wiederholt und daraus das arithmetische Mittel gebildet.

7.2.1 Datenpaket senden, ACK-Frame empfangen

Pakete mit 1 bis 115 Byte großem Dateninhalt werden nacheinander versandt. Die Gegenstelle antwortet bei Empfang des Paketes mit einem durch Hardware generiertes Bestätigungspaket (ACK-Paket). Die Dauer vom Absenden des Paketes bis zum Eintreffen der Bestätigung wird notiert.

7.2.2 Datenpaket senden, Echo-Datenpaket empfangen

Für diesen Test wird die hardwaretechnische Empfangsbestätigung deaktiviert. Ankommende Pakete werden von der Gegenstelle direkt zurückgeschickt (Echo). Aus einem unbestimmten Grund können abgesendete Pakete erst ab einem fünf Byte großen Dateninhalt von der Gegenstelle erkannt werden. Somit findet der Test mit Paketgrößen von 5 bis 115 Byte Informationen statt. Gemessen wird die Zeit vom Versenden bis zum Empfang der Echo-Nachricht.

7.2.3 Datenpaket senden, Echo-Datenpaket empfangen – mit ACK

Im vorherigen Anwendungsfall war der Durchlauf mit 1 bis 4 Byte großem Dateninhalt nicht durchführbar. Da die Verwendung der ACK-Funktion dies ermöglicht, wird der zweite Fall mit Aktivierung dieser wiederholt. Es ist mit einer leichten Verzögerung der Antwort zu rechnen.

7.2.4 Grafische Darstellung

Die Auswertung der Ergebnisse erfolgt durch Diagramme.
Das erste Diagramm (*Abbildung 58: Auswertung - Pingdauer*) vermittelt einen Eindruck der praktischen Laufzeiten von Paketen in einem IEEE 802.15.4-Netz.
Die blaue Linie visualisiert die Abhängigkeit von Zeit und Anzahl der verschickten Pakete. Es wird das ACK-Paket als Echo verwendet (7.2.1).
Die Verwendung des ursprünglichen Paketes als Rückantwort (7.2.2) wird durch die rosafarbene Linie gezeigt.
Die wachsende Differenz der Funktionswerte nach dem Schnittpunkt entsteht durch das stetig größer werdende Echo-Paket. Das ACK-Paket hat eine konstante Größe.

Die zweite Grafik (*Abbildung 59: Auswertung - Übertragungsgeschwindigkeit*) präsentiert die Bitraten bezogen auf den Netto- (Dateninhalt) und Brutto- (PPDU – komplettes Paket) Datendurchsatz. Bei Verwendung der ACK-Funktion fällt im Anfangsbereich (bis ca. 75 Datenpakete) der erhebliche Performanzverlust auf.

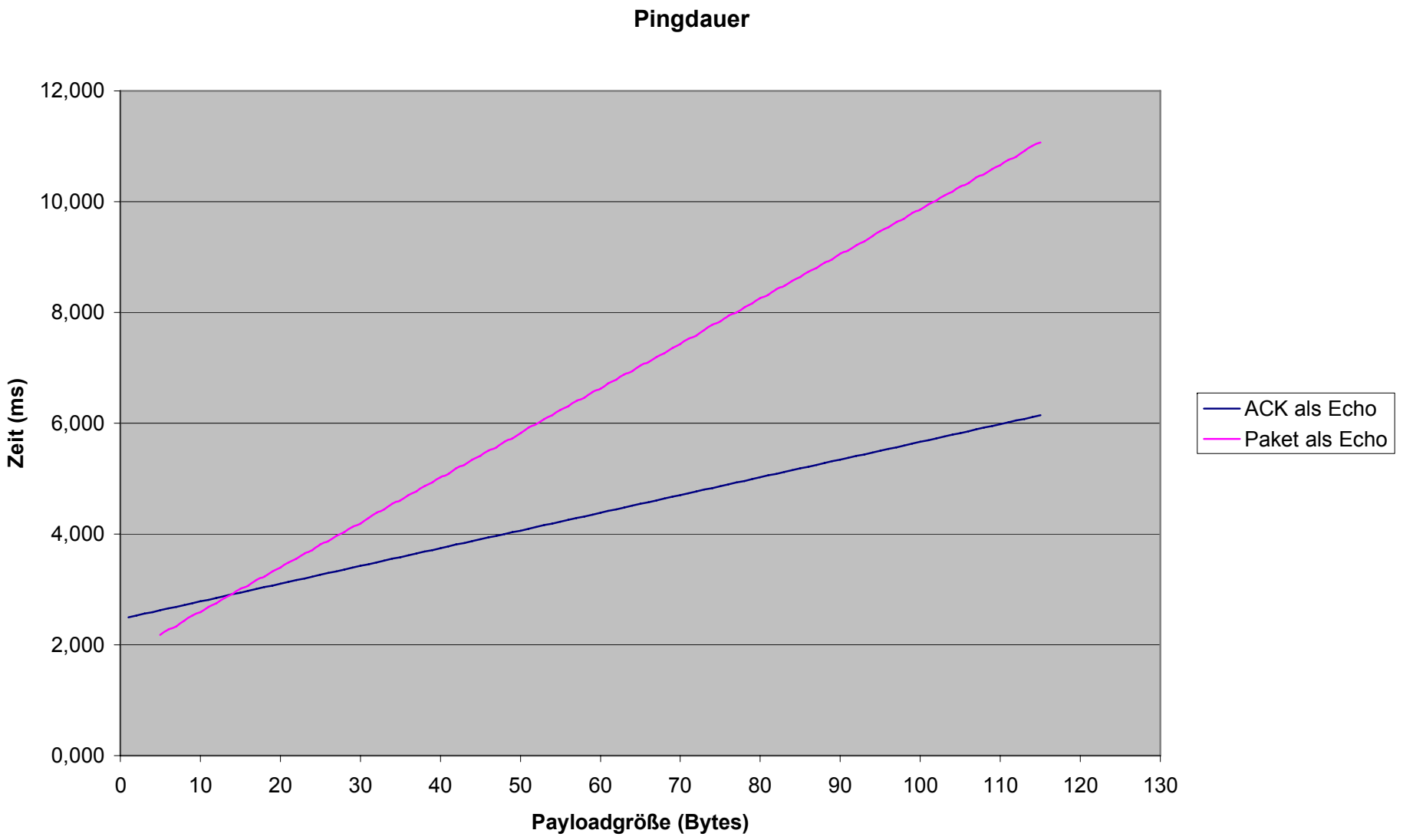

Abbildung 58: Auswertung - Pingdauer

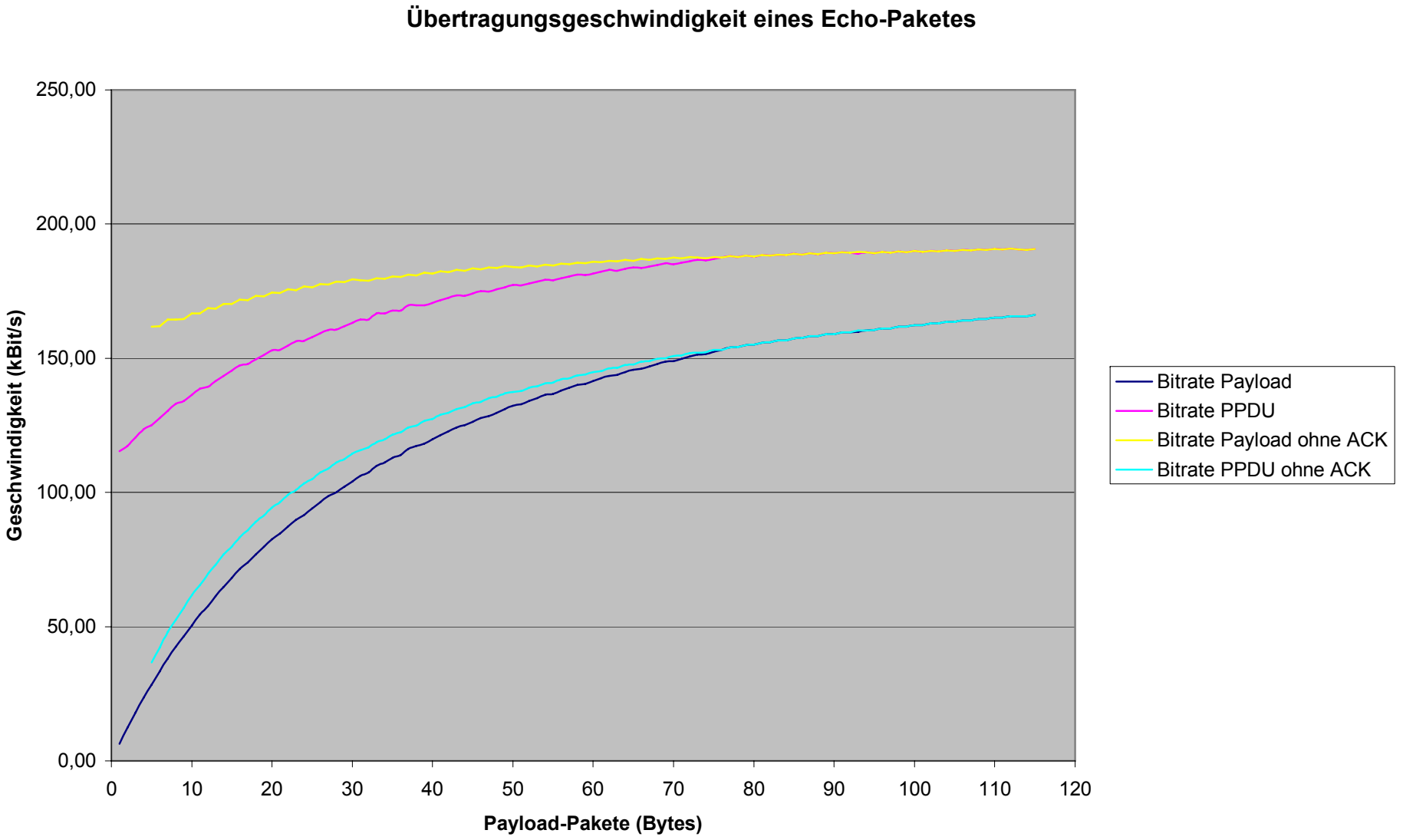

Abbildung 59: Auswertung - Übertragungsgeschwindigkeit

8 Verwendungsmöglichkeiten

Das Gerät unterstützt den Einsatz von Funknetzen gemäß IEEE 802.15.4-Spezifikation und ist somit ein geeignetes Produkt für den Aufbau einfacher Netzwerke. Im Speziellen ist es für die Verwendung der ZigBee-Technologie konzipiert. Aufgrund dieser Tatsache wird erläutert, in welchen Bereichen ZigBee interessant ist:

8.1 Für welche Bereiche ist ZigBee interessant?

Bei Systemen, in denen ZigBee-Technologie zum Einsatz kommt, handelt es sich um Sensoren/Aktoren-Netzwerke mit einer großen Anzahl von Knoten und geringen Übertragungsgeschwindigkeiten, bei denen die Batterielaufzeit eine wesentliche Rolle spielt.
Die Anforderungen an die Netzstruktur sind eindeutig: sie muss sehr robust sein und gewährleistet selbständig durch Sicherungsmechanismen die Qualität des Netzes. Das Einbinden von Knoten erfolgt ohne das Eingreifen durch externe Anwender, im Fall von Veränderungen des Netzaufbaus bei zum Beispiel Ausfällen von Knoten werden neue Routen bestimmt.
Die Anforderung an Batterielaufzeiten beträgt mehrere Monate bis hin zu Jahren, die Kosten der Installation und der einzelnen Geräte müssen sehr niedrig sein. Das System soll einfach administrierbar und die Größe der Komponenten sehr gering sein.
Die Komponenten sind aufgrund ihrer Eigenschaften universell einsetzbar und können an beliebigen Orten angebracht werden.

Bereiche, für die ZigBee vorgesehen ist:

8.1.1 Heim- und Gebäudeautomatisierung

Die Automatisierung von Gebäuden schlägt sowohl im privaten Umfeld (Heim, Garten), als auch im gewerblichen Zweig nieder. Zu den Anwendungsfeldern gehören die Gebäudesicherheit, Klima- und Heizungssteuerung, Lichtschaltung und Zugangssteuerung.
Beispielsweise werden Knoten mit Temperatursensoren und Knoten mit Aktoren an Sprinkleranlagen verteilt, um im Falle eines Feuers dieses automatisch zu bekämpfen oder im Falle von Trockenheit den Garten zu bewässern.
In einem Hotel können Sensoren angebracht sein, welche dem System melden, sobald ein Raum vom Gast verlassen wurde, woraufhin bestimmte elektronische Geräte abgeschaltet werden können um Strom zu sparen.
Grundstücke, die über einen bestimmten Zeitraum menschenleer sind, wie beispielsweise eine Firma am Wochenende oder ein Familienhaus während eines Urlaubs, bemerken über Sensoren plötzlich geöffnete Fenstern oder Türen und alarmieren direkt die Polizei.

8.1.2 Überwachung und Steuerung in der Industrie

Die Aspekte aus der Heim- und Gebäudeautomatisierung sind ohne weiteres übertragbar auf industrielle Gebäude im Großgewerbe wie beispielsweise Fabriken. Hinzu kommt hier der Einsatz der ZigBee-Technologie in der Prozesssteuerung di-

rekt bei der Fertigung, dem Bestandsmanagement im Bereich der Spedition und Logistik und dem Energiemanagement.
Eine Speditionsfirma könnte ihre Container mit Knoten versehen, welche während des Transportes den Zustand der Ware vermitteln oder beim Be- und Entladen den aktuellen Status und die Präsenz mitteilen.

8.1.3 Unterstützung im Gesundheitswesen

Eine beständige Überwachung der körperlichen Zustandswerte von Patienten oder Personen im privaten Bereich wird durch Etablierung eines ZigBee-Systems erreicht. Beispielsweise liefert die am Körper eines Patienten befindliche Sensorik regelmäßig aktuelle Werte über den Gesundheitszustand direkt an den Arzt.
Ferner kann auch die Überwachung der Vitalfunktionen während sportlicher Betätigung realisiert werden.

8.1.4 Konsumentenbereich

Kommunikation zwischen Technischen Geräten im Konsumentenbereich kann durch ZigBee stattfinden.
Die drahtlose Steuerung von Multimediageräten via Infrarot, wie zum Beispiel dem Fernseher, Videorekorder und DVD/CD-Spieler, kann durch die Funktechnik ersetzt werden.
Der Anschluss von Peripheriegeräten an den Computer, wie Maus, Tastatur und Joystick, erfolgt über ZigBee.

9 Zusammenfassung

Das ursprüngliche Ziel wird wiederholt dargestellt und mit dem tatsächlich erreichten Ergebnis verglichen. Nachträglich erkannte Schwachstellen werden erläutert und eventuell mit Lösungsansätzen versehen.
Herausgearbeitet werden Ansatzpunkte, wie die Arbeit weitergeführt werden kann.

9.1 Ausgangslage

Die technologische Entwicklung bringt eine Erleichterung von Arbeit und Aufwand für den Menschen. Technische Geräte werden kompakter und ansehnlicher. Die Zahl der computergestützten Aufgaben im Alltag wächst unaufhaltsam, der Trend geht zu „Ubiquitärem Computing“ – Computer sind überall vorhanden, der Mensch bemerkt sie nicht mehr.
Diese Arbeit hat die Aufgabe, ein spezielles Alltags-Szenario dem heutigen Fortschritt anzupassen und als Resultat die manuelle Arbeit zu verringern. Im Vordergrund steht dabei die hardwaretechnische Entwicklung eines Sensornetzwerkes.
In diesem Zuge wird eine Analyse der aktuell vorhandenen Funkstandards, insbesondere ZigBee durchgeführt. Es folgt der Entwurf eines energieeffizienten, unauffälligen und robusten Systems mit geringer Komplexität. Die Erstellung der Hardware und beispielhafter Software vervollständigt die Arbeit, durch abschließende Tests werden praktische Erfahrungen vermittelt.
Ein Ausblick erläutert das breite Spektrum an Einsatzmöglichkeiten dieses Systems.

9.2 Resümee

Mit Rückblick auf das ursprüngliche Szenario aus Kapitel 1.2 wird folgender Schluss gezogen:
Die hardwaretechnische Entwicklung eines Netzwerkes und der benötigten Module ist gemäß der Zielsetzung aus Kapitel 1.3 erfolgreich beendet. Es konnte eine Funktechnologie gefunden werden, welche die Anforderungen erfüllt. Die hergestellten Geräte in Verbindung mit dem ausgewählten Standard ZigBee sind geeignet für die Umsetzung eines Sensor/Aktor-Netzwerkes. Verstärkt wird diese Aussage durch die in Kapitel 7 durchgeführten Tests.
Offen geblieben ist die Entwicklung einer Netzwerkanwendung gemäß den ZigBee-Spezifikationen. Die Applikation aus Kapitel 6 ist zunächst eine befriedigende Lösung, die noch Optimierungsbedarf hat.

9.3 Kritik, Verbesserungsmöglichkeiten

9.3.1 Modul

Die Verwendung von professionellen Gerätschaften, mit denen es möglich ist, IC’s im QLP-Gehäuse verarbeiten zu können, erlaubt ein erheblich kleineres Design. Das Funkmodul von Chipcon ist eine schnelle Möglichkeit mit ZigBee praktisch in den Kontakt zu treten. Die Abmaße der Platine sind jedoch für die Anzahl und Größe der Bauteile sehr großzügig gewählt. Praktisch gibt es von fast jedem Bauteil kleinere Ausfertigungen, die Gesamtgröße des Moduls kann um einen großen Teil reduziert werden.
Es sind kleine Optimierungsmöglichkeiten im Design des Moduls vorhanden: Die ISP-Schnittstelle sollte verpolungssicher sein, derzeit kommt der Kontakt durch eine

doppelreihige Stiftleiste zustande, die falsch angeschlossen werden kann. Ein Wannenstecker schafft hier Abhilfe. Die Pinbelegung der Anschlussleiste entspricht nicht dem AVR-Standard.
Die Kompatibilität zum Aksen-Board bezüglich des RS232-Anschlusses ist nicht vollständig gewährleistet. Aktuell befinden sich auf den Platinen Modularbuchsen für Stecker mit maximal vier Leitungen. Es sollten Buchsen sein für Stecker mit sechs Vorrichtungen, wobei im Endeffekt nur vier Adern genutzt werden.
Interessant wäre ein Spannungsteiler, verbunden mit dem Mikrokontroller, um den aktuellen Spannungswert angeben zu können. Bei zu geringer Eingangsspannung könnte ein Alarm ausgelöst werden.

9.3.2 Technologie

Obwohl das Thema dieser Arbeit ZigBee ist, konnte der praktische Kontakt zu dieser Technologie leider nicht hergestellt werden, da der Stack nicht verfügbar war. Somit blieben die Ideen von ZigBee leider nur interessante Theorie. Die Funktionen gemäß IEEE 802.15.4 sind besonders im Hinblick auf Komplexität und Leistung beeindruckend.

9.4 Aussichten, Weiterführung

Es gibt Ansatzmöglichkeiten in diese Arbeit. Der nächste Schritt ist der praktische Einsatz von ZigBee. Die Module sind für diese Technik konzipiert und bilden die hardwaretechnische Basis. Die ZigBee-Spezifikation offeriert viel versprechende, umfangreiche Einsatzmöglichkeiten, hinzu kommt auf der einen Seite die Kompatibilität der Geräte untereinander, auf der anderen Seite die Eigenschaft, sich an spezielle Probleme individuell anpassen zu können.

9.5 Kommentar

Quelle: [MWei]

Mit "The Computer for the Twenty-First Century." hat Mark Weiser (1952-1999) im September 1991 dargestellt, wie seiner Meinung nach die Zukunft aussehen wird, und den Begriff „Ubiquitous computing“ geprägt.
Tatsächlich verläuft die Entwicklung vieler heutiger Technologien mehr denn je in diese Richtung. Diese Arbeit geht einen Schritt mit und hat sich mit einer Technik auseinandergesetzt, die mit der Standardisierung einer Anwendungsumgebung für ein LR-WPAN einen großen Schwung in diese Entwicklung bringen könnte – ZigBee. Die Industrie reagiert positiv auf das Konzept der ZigBee Alliance. Die Anzahl der Mitglieder stieg diesen August auf über 175 und Chipcon konnte einen Vertrieb von über eine Million „ZigBee ready“ / IEEE 802.15.4-Chips verzeichnen.

10 Glossar

ACL	access control list
CAP	contention access periode
CCA	clear channel assessment
CFP	contention free periode
CRC	cyclic redundancy check
CSMA/CA	carrier sense multiple access with collision avoidance
DSSS	direct sequence spread spectrum
ED	energy detection
FCS	frame check sequence
FFD	full-function device
GTS	guaranteed time slot
LLC	logical link control
LQ	link quality
LQI	link quality indication
LR-WPAN	low-rate wireless personal area network
MAC	medium access control
MFR	MAC footer
MHR	MAC header
MIC	Message integry code
MLME	MAC sublayer management entity
MLME-SAP	MAC sublayer management entity-service access point
MPDU	MAC protocol data unit
MSDU	MAC service data unit
OSI	open system interconnection
PDU	protocol data unit
PHR	PHY header
PHY	physical layer
PPDU	PHY Protocol data unit
PSDU	PHY service data unit
RFD	reduced-function device
RSSI	received signal strength indication
SAP	service access point
SDU	service data unit
SPDU	SSCS protocol data unit
SSCS	service specific convergence sublayer
UML	unified modeling language
WLAN	wireless local area network
WPAN	wireless personal area network

11 Literaturverzeichnis

[AHac] Wireless Sensor Network Designs
Anna Hac
ISBN 0-470-86736-1

[ATan] Computernetzwerke
Andrew S. Tanenbaum
4. Auflage, 2003, Pearson Studium
ISBN 3-8273-7046-9

[AVR_1] AVR-GCC-Tutorial
http://www.mikrocontroller.net/articles/AVR-GCC-Tutorial

[AVR_2] AVR Tutorial
http://www.mikrocontroller.net/tutorial/uart

[BT] Informationen Bluetooth
http://de.wikipedia.org/wiki/Bluetooth

[DC] Disappearing Computer
http://www.disappearing-computer.net/

[DOC_AVR] Dokumentation - AVR Bibliotheken
http://www.nongnu.org/avr-libc/user-manual/index.html

[DOC_DBK] Manual – Chipcon CC2420 DBK Rev. 1.3
http://chipcon.com/; CC2420DBK_User_Manual_1_3.pdf

[DOC_EM] Schematisches Layout – Chipcon CC2420EM
http://chipcon.com/; CC2420EM_1_1.pdf

[DOC_PP] PonyProg Documentation
http://www.lancos.com/e2p/ponyprog2000.html

[DOC_WAV] User Manual - WinAVR
http://winavr.sourceforge.net/WinAVR-user-manual.html

[DS_ATM] Datasheet ATMEL ATmega128L
http://atmel.com/dyn/resources/prod_documents/doc2467.pdf

[DS_CC2] Datasheet – CC2420 Rev 1.2
http://chipcon.com; CC2420_Data_Sheet_1_2.pdf

[DS_IDT] Datasheet – IDT71V256SA
http://www.farnell.com/datasheets/1137.pdf

[DS_M74] Datasheet – M74HC573M1R
http://www.st.com/stonline/products/literature/ds/8026/m74hc573m1r.pdf

[DS_MAX] Datasheet MAXIM MAX3233E
http://pdfserv.maxim-ic.com/en/ds/MAX3233E-MAX3235E.pdf

[DS_MIC] Datasheet - Micrel MIC5209-3.3
http://www.micrel.com/_PDF/mic5209.pdf

[EC] Eclipse und SWT-Bibliothek
http://www.eclipse.org/

[GKru] Handbuch der Java-Programmierung
Guido Krüger
ISBN 3-8273-2201-4

[IEEE 802.15.4] IEEE 802.15.4 - Specification for Low-Rate Wireless Personal Area Networks (LR-WPANs)
http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf
IEEE, 1. Oktober 2003

[JDK] JDK 5 Dokumentation
http://java.sun.com/j2se/1.5.0/docs/index.html

[JGut] IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: E-nabling Wireless Sensor Networks
Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett
ISBN 0-7381-3557-7

[MWei] The Computer for the 21st Century
http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html
Mark Weiser, 01. September 1991

[ZB_1] ZigBee Spezifikation (ZigBee Document 053474r06, Version 1.0)
http://zigbee.org; 053474r05_TSC-ZigBee-Specification.pdf

[ZB_2] ZigBee Technology: Wireless Control that Simply Works
Patrick Kinney, 2. Oktober 2003
http://zigbee.org; 031418r00ZB_MG-ZigBeeTechnology.doc

[ZB_3] Zigbee: “Wireless Control That Simply Works”
William C. Craig
http://zigbee.org; 041427r00ZB_MG-ZigbeeWireless.pdf

[ZB_4] ZigBee and Bluetooth – Competitive or Complementary?
Venkat Bahl, September 2002
http://zigbee.org; 021412r00ZB_MG-ZigBeeandBluetooth.pdf

[ZB_5] Emerging Wireless Standards
George Karayannis
http://zigbee.org; 031426r00ZB_MG-EmergingWireless.ppt

[ZB_6] Emerging Standards: Where does ZigBee Fit
Bob Heile, Oktober 2004
http://zigbee.org; 041411r00ZB_MG-ZigBeeOverview.ppt

[ZB_7] Designing with 802.15.4 and ZigBee
Jon Adams, 9. März 2004
http://zigbee.org; 041415r00ZB_MG-Designingwith802.15.4.ppt

[ZB_8] CES 2004
http://zigbee.org; ZigBee_CES_January_2004_FINAL.pdf
Bob Heile; 9. Januar 2004

[ZB_9] „What You Should Know About the ZigBee Alliance“
http://zigbee.org; 031413r00ZB_MG-WhatYouShouldKnow.ppt
Jon Adams, 24. September 2003

12 Anhang

Im Anhang befindet sich eine CD-ROM mit folgendem Inhalt:

- diese Bachelorarbeit als Dokument im PDF-Format
- die Datenblätter der verwendeten Bauteile

- den Sourcecode (Beta) der Anwendung aus Kapitel 6
- den Sourcecode der Testprogramme aus Kapitel 7

- die Daten der Tests aus Kapitel 7

Versicherung über die Selbständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §22(4) ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Ort, Datum Unterschrift