**Examensarbete**
LITH-ITN-ED-EX--05/015--SE

# Zigbee for wireless networking

Johan Lönn
Jonas Olsson

2005-03-15

Linköpings universitet
TEKNISKA HÖGSKOLAN

**Department of Science and Technology**
**Linköpings Universitet**
**SE-601 74 Norrköping, Sweden**

**Institutionen för teknik och naturvetenskap**
**Linköpings Universitet**
**601 74 Norrköping**

LITH-ITN-ED-EX--05/015--SE

# Zigbee for wireless networking

Examensarbete utfört i Elektronikdesign
vid Linköpings Tekniska Högskola, Campus
Norrköping

Johan Lönn
Jonas Olsson

Handledare Shaofang Gong
Examinator Shaofang Gong

Norrköping 2005-03-15

**Avdelning, Institution**
Division, Department

Institutionen för teknik och naturvetenskap

Department of Science and Technology

**Datum**
Date

**2005-03-15**

**Språk**
Language

☐ Svenska/Swedish
☒ Engelska/English

☐ ________________

**Rapporttyp**
Report category

Examensarbete
☐ B-uppsats
☐ C-uppsats
☒ D-uppsats

☐ ________________

**ISBN**

**ISRN** **LITH-ITN-ED-EX--05/015--SE**

**Serietitel och serienummer** **ISSN**
Title of series, numbering

**URL för elektronisk version**
**http://www.ep.liu.se/exjobb/itn/2005/ed/015/**

**Titel**
Title
Zigbee for wireless networking

**Författare**
Author
Johan Lönn, Jonas Olsson

**Sammanfattning**
Abstract

The past several years have witnessed a rapid development in the wireless network area. So far wireless networking has been focused on high-speed and long range applications. However, there are many wireless monitoring and control applications for industrial and home environments which require longer battery life, lower data rates and less complexity than those from existing standards. What the market need is a globally defined standard that meets the requirement for reliability, security, low power and low cost. For such wireless applications a new standard called ZigBee has been developed by the ZigBee Alliance based upon the IEEE 802.15.4 standard.
The aim of this diploma work is to design fully functional ZigBee and IEEE 802.15.4 modules, and to evaluate an application in a sensor network.
This diploma work has resulted in two fully functional ZigBee and IEEE 802.15.4 modules, respectively. It is also shown that ZigBee sensors can be networked wirelessly. Eventually it is the authors hope that the modules will be used within ITN, and also be developed further for new applications.

**Nyckelord**
Keyword
ZigBee, modules, networks, sensors

# ZigBee for wireless networking

Johan Lönn
Jonas Olsson

15th March 2005

# Preface

This report is the result of a Master Thesis work done at Linköping University. The diploma work was done at the Department of Science and Technology (ITN), in Norrköping.

The authors would like to thank Professor Shaofang Gong, Pär Håkansson and Andreas Kingbäck at ITN for useful discussions and suggestions during the project.

Special thanks to all the people from Chipcon, Atmel, NDK, gigaAnt and ACTE for supplying devices, and also for the technical support.

# Abstract

The past several years have witnessed a rapid development in the wireless network area. So far wireless networking has been focused on high-speed and long range applications. However, there are many wireless monitoring and control applications for industrial and home environments which require longer battery life, lower data rates and less complexity than those from existing standards. What the market need is a globally defined standard that meets the requirement for reliability, security, low power and low cost. For such wireless applications a new standard called ZigBee has been developed by the ZigBee Alliance based upon the IEEE 802.15.4 standard.

The aim of this diploma work is to design fully functional ZigBee and IEEE 802.15.4 modules, and to evaluate an application in a sensor network.

This diploma work has resulted in two fully functional ZigBee and IEEE 802.15.4 modules, respectively. It is also shown that ZigBee sensors can be networked wirelessly.

Eventually it is the authors hope that the modules will be used within ITN, and also be developed further for new applications.

# Sammanfattning

De senaste åren har det skett en mycket snabb utveckling inom området trådlösa nätverk. Hittills har fokus legat på snabba överföringar och lång räckvidd. Dock finns det ett otal applikationer inom t ex. industrin för övervakning och kontroll, vilka kräver längre batteritid, lägre överföringshastighet och framförallt mindre komplexitet än dagens standarder. Det som dessa marknader behöver är en global standard som nogrannt fyller kraven på säkerhet, tillförlitlighet, låg effektförbrukning och låg kostnad. För dessa typer av applikationer har en ny standard utvecklats av ZigBee Alliance, vilken baseras på standarden IEEE 802.15.4.

Målet med detta examensarbete är att designa och tillverka fullt fungerande trådlösa ZigBee och IEEE 802.15.4 moduler, samt att utvärdera en applikation i ett sensor nätverk.

Examensarbetet har resulterat i två olika fullt fungerande ZigBee och IEEE 802.15.4 moduler. Rapporten beskriver också att det är möjligt att ansluta olika typer av sensorer till ett ZigBee nätverk.

Slutligen är det författarnas förhoppningar att modulerna kommer att användas inom ITN, samt även utvecklas ytterligare för nya applikationer.

# Contents

# List of Figures

# List of Tables

# Terminology

| Abbreviation | Explanation |
|---|---|
| ADS | Advanced Design System. |
| BalUn | Balanced to Unbalanced |
| BOM | Bill Of Material |
| CCA | Clear Channel Assessment |
| CTS | Clear To Send |
| dBm | decibel-milliwatt |
| ED | Energy Detection |
| ESR | Equivalent Series Resistans |
| EVM | Error-Vector Magnitude |
| FFD | Full Function Device |
| GPIO | General Purpose Input/Output |
| GTS | Guaranteed Time Slot |
| IEEE | Institute of Electrical and Electronics Engineers |
| I | In-phase carrier |
| ISP | In-System Programmer |
| LOS | Line Of Sight |
| LQI | Link Quality Indication |
| MAC | Medium Access Control |
| MIC | Message Integrity Code |
| MSK | Minimum Shift Keying |
| MN | Matching Network |
| OQPSK | Offset Quadrature Phase-Shift Keying |
| PA | Power Amplifier |
| PAN | Personal Area Network |

| Abbreviation | Explanation |
|---|---|
| PCB | Printed Circuit Board |
| PER | Packet Error Rate |
| PPDU | PHY Protocol Data Unit |
| PHY | Physical Layer |
| Q | Quadrature-phase carrier |
| RF | Radio Frequency |
| RFD | Reduced-Function Device |
| RTC | Real Time Clock |
| RTS | Ready To Send |
| RX | Receiver |
| SMD | Surfaced Mounted Device |
| TX | Transmitter |
| WLAN | Wireless Local Area Network |

# Chapter 1

# Introduction

The past several years have witnessed a rapid growth of wireless networking. However, up to now wireless networking has been mainly focused on high-speed communications, and relatively long range applications such as the IEEE 802.11 Wireless Local Area Network (WLAN) standards. The first well known standard focusing on Low-Rate Wireless Personal Area Networks (LR-WPAN) was Bluetooth. However it has limited capacity for networking of many nodes. There are many wireless monitoring and control applications in industrial and home environments which require longer battery life, lower data rates and less complexity than those from existing standards. For such wireless applications, a new standard called IEEE 802.15.4 has been developed by IEEE. The new standard is also called ZigBee, when additional stack layers defined by the ZigBee Alliance are used.

## 1.1 Background

This project has been performed as a diploma work for a Master of Science degree in Electrical Engineering at Linköping University. The project has been done at ITN, Campus Norrköping. The Communication Electronics research group, lead by professor Shaofang Gong, has a big interest in new wireless standards and applications. Since there is no standard covering the wireless sensor networking, it is of interest to investigate and evaluate this new standard. One of the questions are how to handle a large number of wireless sensors in the same network. Another interesting task is how to optimize the battery life time of a wireless sensor.

## 1.2 Goal

The goal of this project is to develop fully functional wireless ZigBee and IEEE 802.15.4 modules. This includes design using Protel DXP 2004, and implementation of the ZigBee protocol stack. To evaluate the new standard, a literature study must be performed. A test application will also be developed, in order to test the functionality of the ZigBee modules.

## 1.3 Method

The work is divided into several different sections. Firstly, a literature study is performed. Secondly, to be able to test the ZigBee and IEEE 802.15.4 standards a laboration kit is purchased. Thirdly, Protel DXP 2004 is used for design of the ZigBee modules. The modules are then manufactured outside the university, but the assembly is preformed in-house. After the hardware development, implementation of the software stack is performed. Finally a test application is developed.

The information to the project is obtained mainly from the Internet, but also from specific literatures.

## 1.4 Outline

The report is divided into several sections, and a brief overview of the sections are described here.

- Chapter 2 - Theory. This is a description of the ZigBee and IEEE 802.15.4 standards.
- Chapter 3 - Design Process. The design process and the different parts of the system are described.
- Chapter 4 - Implementation. The implementation of the modules are described.
- Chapter 5 - Development Tools. The software and hardware required to run and develop the modules are described.
- Chapter 6 - Test Application. The developed test application is described.
- Chapter 7 - Results. The results of the project is presented here.
- Chapter 8 - Discussions. Discussions regarding the results obtained from this project are presented.
- Chapter 9 - Conclusions. Conclusions drawn from the project.
- Chapter 10 - Further work. Further work to be done in the area.

# Chapter 2

# Theory

This chapter briefly describes some of the technology background that has been used in this thesis work.

## 2.1 ZigBee Alliance

The ZigBee Alliance is an association of companies working together to define an open global standard for making low-power wireless networks. The intended outcome of ZigBee Alliance is to create a specification defining how to build different network topologies with data security features and interoperable application profiles. The association includes companies from a wide spectrum of categories, from chip manufactures to system integration companies. The number of members in the association is rapidly growing and is currently over 125 (Q1 2005). Among the members one can find Philips, Samsung, Motorola and LG.

The first specification was ratified in Q4 2004 and the first generation of ZigBee products may reach the market sometime in 2005. A big challenge for the alliance is to make the interoperability to work among different products. To solve this problem, the ZigBee Alliance has defined different profiles, depending on what type of category the product belongs to. For example there is an profile called Home Lightning that exactly defines how different brands of home lightning-products should communicate with each other.

To get access to the specification one must currently (Q1 2005) become a member of the ZigBee Alliance, but it will become public later in this year (2005).

Currently there are three different types of ZigBee profiles:

- Private profile
  Interoperability NOT important. No ZigBee stamp on the product, but one can claim "based on a ZigBee platform"

- Published profile
  A private profile is shared with others. No ZigBee stamp on the product, but one can claim "based on a ZigBee platform"

- Public profile
  The official ZigBee profile.

## 2.2 The name ZigBee

The name ZigBee is said to come from the domestic honeybee which uses a zig-zag type of dance to communicate important information to other hive members. This communication dance (the "ZigBee Principle") is what engineers are trying to emulate with this protocol – a bunch of separate and simple organisms that join together to tackle complex tasks.

## 2.3 IEEE 802.15.4

The goal IEEE had when they specified the IEEE 802.15.4 standard was to provide a standard for ultra-low complexity, ultra-low cost, ultra-low power consumption and low data rate wireless connectivity among inexpensive devices. The raw data rate will be high enough (maximum of 250 kb/s) for applications like sensors, alarms and toys.

### 2.3.1 Components of the IEEE 802.15.4

IEEE 802.15.4 networks use three types of devices:

- The network Coordinator maintains overall network knowledge. It is the most sophisticated one of the three types, and requires the most memory and computing power.
- The Full Function Device (FFD) supports all IEEE 802.15.4 functions and features specified by the standard. It can function as a network coordinator. Additional memory and computing power make it ideal for network router functions or it could be used in network-edge devices (where the network touches the real world).
- The Reduced Function Device (RFD) carries limited (as specified by the standard) functionality to lower cost and complexity. It is generally found in network-edge devices. The RFD can be used where extremely low power consumption is a necessity.

### 2.3.2 Network topologies

IEEE 802.15.4 can manage two types of networks, i.e., star topology or the peer-to-peer topology. Both the topologies are illustrated in Figure 2.1. In ZigBee, these two topologies can be combined to build so-called mesh networks.

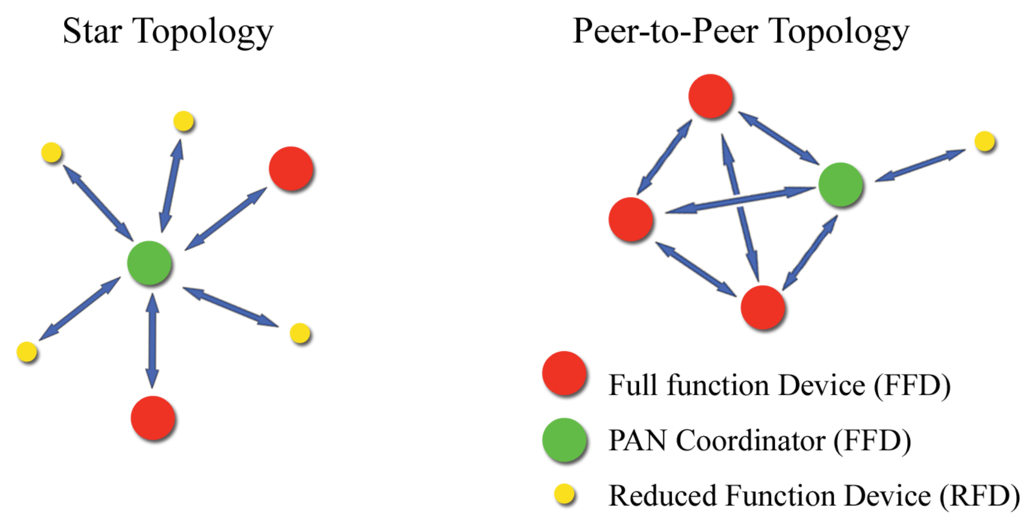



Figure 2.1: Network topologies

#### Star network formation

The first FFD that is activated may establish its own network and become a Personal Area Network (PAN) coordinator. Then both FFD and RFD devices can connect to the PAN coordinator. All networks within the radio sphere of influence must have a unique PAN identity. All nodes in a PAN must talk to the PAN Coordinator.

#### Peer-to-Peer network formation

In the peer-to-peer topology there is also a PAN coordinator, but it differs from the star topology in that any device can communicate with any other device as long as they are in the range of one another. The peer-to-peer topology allows more complex network formations to be implemented, such as the mesh topology.

### 2.3.3 OSI Overview

The Open System Interconnection (OSI) reference model, was developed by the International Organization for Standardization (ISO) as a model for the computer protocol architecture, and as a framework for developing protocol standards. The entire point of the model is to separate networking into several distinct functions that operate at different levels. Each layer is responsible for performing a specific task or set of tasks, and dealing with the layers above and below it. An illustration of the general OSI-model and where ZigBee is defined in the model can be seen in Figure 2.2.

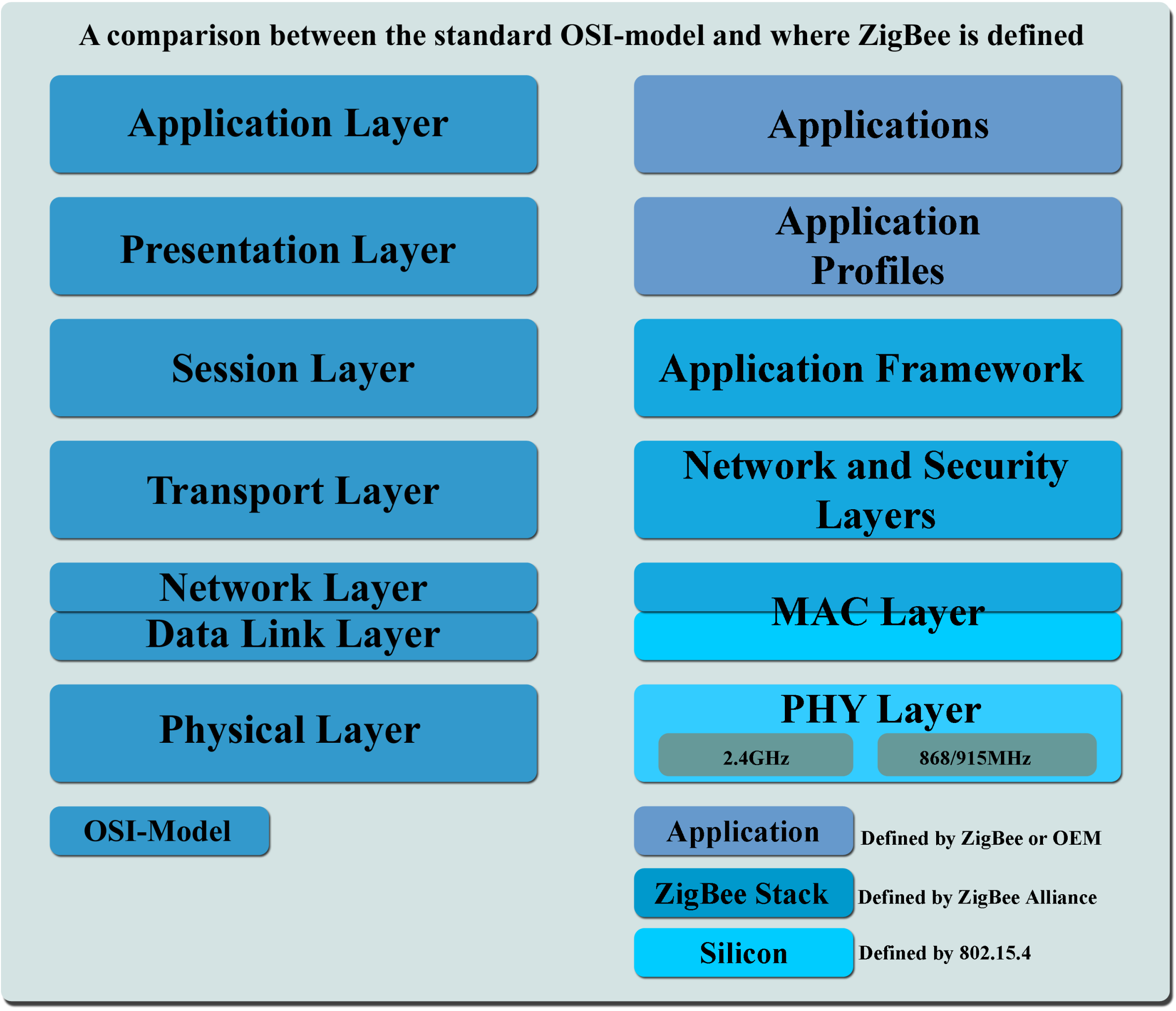



Figure 2.2: OSI model

### 2.3.4 Physical Layer

The IEEE 802.15.4 specification defines three different frequency bands, in order to conform with regulations in Europe, Japan, Canada and the United States. Table 2.1

describes the frequency bands and data rates. Totally 27 channels are available across the different frequency bands, as described in Table 2.2.

Table 2.1: Frequency bands and data rates

| PHY (MHz) | Frequency band (MHz) | Chip rate (kchips/s) | Modulation | Bit rate (kb/s) | Symbol rate (ksymbol/s) | Symbols |
|---|---|---|---|---|---|---|
| 868 | 868-868.6 | 300 | BPSK | 20 | 20 | Binary |
| 915 | 902-928 | 600 | BPSK | 40 | 40 | Binary |
| 2450 | 2400-2483.5 | 2000 | O-QPSK | 250 | 62.5 | 16-ary Orthogonal |

Table 2.2: Channels and how to calculate them

| Center frequency (MHz) | Number of channels (N) | Channel (k) | Channel center frequency (MHz) |
|---|---|---|---|
| 868 | 1 | 0 | 868.3 |
| 915 | 10 | 1 - 10 | 906+2(k-1) |
| 2450 | 16 | 11 - 26 | 2405+5(k-11) |

### Modulation/Spreading

The conversion of the binary data to a modulated signal in the 2450 MHz frequency band can be described as the functional block diagram in Figure 2.3. The numbers show how the binary data "0000b" is converted to a baseband chip sequence with pulse shaping.

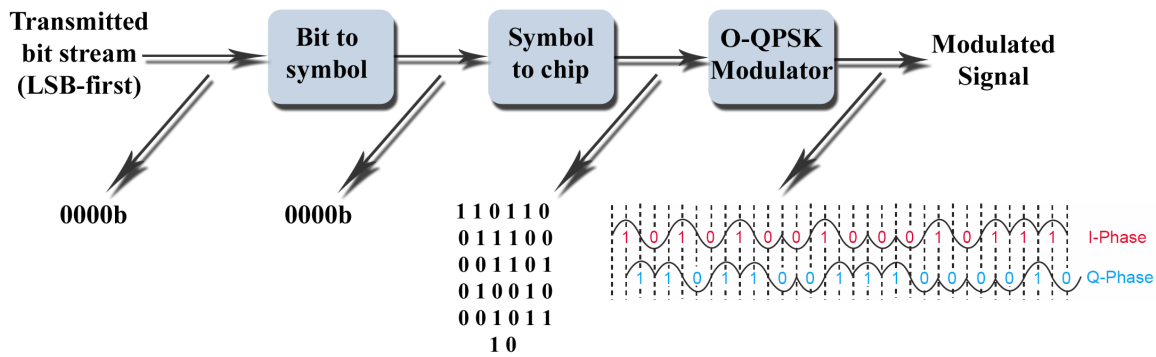



Figure 2.3: Modulation and spreading

### Bit to symbol

The first step is to encode all the data in the PHY Protocol Data Unit (PPDU) from binary data to symbols. Each byte is divided into two symbols and the least significant symbol is transmitted first. For multi-byte fields, the least significant byte is transmitted first, except for security related fields where the most significant byte is transmitted first.

### Symbol to chip

Each data symbol is mapped into a Pseudo-random (PN) 32-chip sequence. The chip sequence is then transmitted at 2 MChip/s with the least significant chip ($c_0$) transmitted first for each symbol. Table 2.3 shows the data symbol with corresponding chip values.

Table 2.3: Symbol to chip mapping

| Data symbol (decimal) | Chip values ($c_0$ $c_1$... $c_{30}c_{31}$ ) |
|---|---|
| 0 | 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 |
| 1 | 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 |
| 2 | 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 |
| 3 | 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 |
| 4 | 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 |
| 5 | 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 |
| 6 | 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 |
| 7 | 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 |
| 8 | 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 |
| 9 | 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 |
| 10 | 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 |
| 11 | 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 |
| 12 | 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 |
| 13 | 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 |
| 14 | 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 |
| 15 | 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 |

### O-QPSK Modulation

The modulation format is Offset - Quadrature Phase Shift Keying (O-QPSK) with half-sine pulse shaping, equivalent to Minimum Shift Keying (MSK). QPSK is an efficient way to use the often limited bandwidth. Each signal element represents two bits, the equation below shows how the O-QPSK can be expressed. By using Offset, phase changes in the combined signal never exceeds 90°. In the case using QPSK the maximum phase change is 180°. O-QPSK provides a greater performance than QPSK when the transmission channel has components with significant nonlinearity.

$$s(t) = \frac{1}{\sqrt{2}} I(t) cos 2\pi f_c t - \frac{1}{\sqrt{2}} Q(t - T_c) sin 2\pi f_c t \tag{2.1}$$

where $f_c$ is the center frequency and $T_c$ is the time that Q is delayed to get the 90° phase change. Equation 2.1 describes the O-QPSK modulated signal, $I$ is the in-phase carrier and $Q$ the quadrature-phase carrier.

The use of half-sine pulse shaping eliminates any amplitude variation and turns the O-QPSK into a constant envelope modulation. Equation 2.2 describes the half sine pulse shaping.

$$p(t) = \begin{cases} \sin\left(\pi \frac{t}{2T_c}\right), 0 \leq t \leq 2T_c \\ 0, otherwise \end{cases} \tag{2.2}$$

### Error-vector magnitude

The modulation accuracy of an IEEE 802.15.4 transmitter is determined with an Error Vector Magnitude (EVM) measurement, see Figure 2.4. EVM is the scalar distance between the two phasor end points representing the ideal and the actual measured chip positions. Expressed in another way, it is the residual noise version of the signal and distortion remaining after an ideal version of the signal has been stripped away.

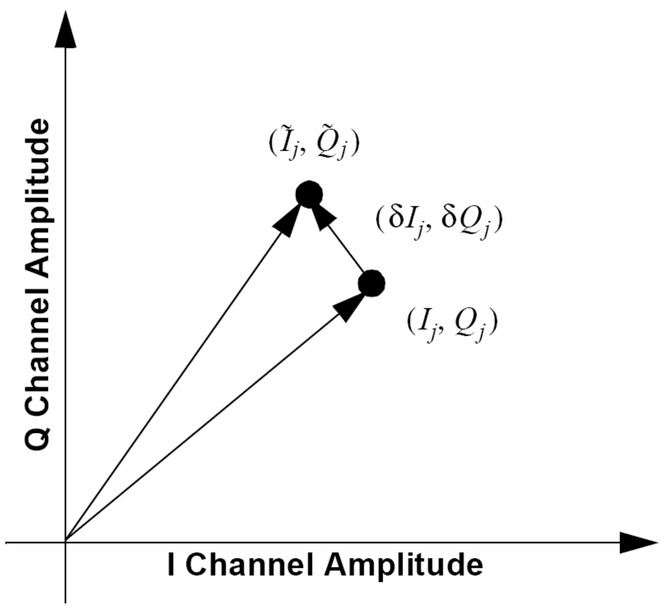



Figure 2.4: Error vector

$$(\tilde{I}_j, \tilde{Q}_j) = (I_j, Q_j) + (\delta I_j, \delta Q) \tag{2.3}$$

The EVM for IEEE 802.15.4 is defined as shown in Equation 2.4.

$$EVM \equiv \sqrt{\frac{\frac{1}{N}\sum_{j=1}^{N}(\delta I_j^2 + \delta Q_j^2)}{S^2}} * 100\% \tag{2.4}$$

where S is the magnitude of the vector to the ideal constellation point, ($\delta I_j$, $\delta Q_j$) is the error vector. The transmitter shall have EVM values of less than 35% when measured with 1000 chips.

### Transmit power

The transmitter should be capable of transmitting at least -3 dBm. The device should transmit as low power as possible to reduce interference to other devices and systems. The definition of dBm is shown in Equation 2.5.

$$Power_{dBm} = 10log\frac{Power_{mW}}{1mW} \tag{2.5}$$

Note the following relationships:

$$0dBm = 1mW \tag{2.6}$$

$$+30dBm = 0dBW \tag{2.7}$$

$$0dBm = -30dBW \tag{2.8}$$

### Receiver sensitivity

The receiver sensitivity is defined by two terms. One is Packet Error Rate (PER) which is the average fraction of transmitted packets that are not detected correctly. The other term is the threshold input signal power that yields a specified PER. In IEEE 802.15.4 a compliant device shall have a sensitivity of -85 dBm or better.

### Receiver ED

The receiver Energy Detection (ED) is intended to be used by the network layer as part of a channel selection algorithm. It is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel. No attempt is made to identify or decode signals on the channel. The ED time shall be equal to 8 symbol periods.

### LQI

The Link Quality Indication (LQI) is a characterisation of the strength and/or quality of a received packet. The measurement may be implemented using receiver ED, a Signal to Noise Ratio (SNR) estimation, or a combination of these methods. The use of the LQI result by the network or application layer is not part of the IEEE 802.15.4 standard.

### CCA

Clear Channel Assessment (CCA) is used to decide whether the channel is busy or idle and one of the following methods must be supported.

- CCA Mode 1: Energy above threshold. CCA shall report a busy medium upon detecting any energy above the ED threshold.
- CCA Mode 2: Carrier sense only. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4. This signal may be above or below the ED threshold.
- CCA Mode 3: Carrier sense with energy above threshold. CCA shall report a busy medium only upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4 with energy above the ED threshold.

A busy channel shall be indicated by the Physical Layer Management Entity Confirm (PLME-CCA.confirm) primitive with a status of BUSY. A clear channel shall be indicated by the PLME-CCA.confirm primitive with a status of IDLE.

## 2.3.5 Medium Access Control Layer

The Medium Access Control (MAC) layer handles the network association and disassociation and has an optional super frame structure with beacons for time synchronisation, and a Guaranteed Time Slot (GTS) mechanism for high priority communications.

## 2.4 Hardware

There are currently an increasing number of manufactures of IEEE 802.15.4 2.4 GHz transceiver chips. Table 2.4 shows a short comparison of the 2.4 GHz transceiver chips that are currently (Q1 2005) on the market.

Table 2.4: 2.4GHz transceivers

| Manufacturer | Chip | $I_{RX}$ (mA) | $I_{TX}$ (mA) | Sensitivity Rx (dBm) | Output Power (dBm) | Voltage (volts) |
|---|---|---|---|---|---|---|
| Chipcon | CC2420 | 19.7 | 17.4 | -94 | 0 | 2.1-3.6 |
| Ember | EM2420 | 19.7 | 17.4 | -94 | 0 | 2.1-3.6 |
| Freescale | MC13191 | 37 | 30 | -91 | 3.6 | 2-2.4 |
| Freescale | MC13192 | 37 | 30 | -92 | 3.6 | 2-3.4 |
| Freescale | MC13193 | 37 | 30 | -92 | 3.6 | 2-3.4 |
| CompXs | CX1540 | 57 | 56 | -90 | 3 | 2.7-3.3 |
| Ubec | uz2400 | x | x | -93 | 0 | x |

The table does not show if the chip has extra features, such as an built-in ZigBee stack, ADC or DAC. Currently (Q1 2005) there is no single chip solution (Radio + Microcontroller) on the market, but there may be single chip solutions on the market later in this year (2005).

## 2.5 Security

There are three types of security modes defined: unsecured mode, access control list and secured mode.

### 2.5.1 Unsecured mode

No security used.

### 2.5.2 Access control list

No encryption used, but the network rejects frames from unknown devices.

### 2.5.3 Secured mode

In the secured mode the devices can use the following security services.

- Access control list.
- Data encryption using the Advanced Encryption Standard (AES) 128 bit encryption algorithm.

- Frame integrity is a security service that uses a Message Integrity Code (MIC) to protect data from being modified by parties without the cryptographic key. It further provides assurance that data come from a party with the cryptographic key.
- Sequential freshness is a security service that uses an ordered sequence of inputs to reject frames that have been replayed. When a frame is received, the freshness value is compared with the last known freshness value.

## 2.6 ZigBee Stack

In this project the ZigBee software stack from Figure 8 Wireless has been used. Currently (Q1 2005) there are just a few companies providing the stack for ZigBee. A short list can be seen in Table 2.5. Since the official standard (ver. 1.0) is not published yet (Q1 2005), there might be some small changes in the stacks that are currently released.

Table 2.5: ZigBee stack

| Provider | Comment |
|---|---|
| Figure 8 | The one used in this thesis |
| Stonestreet one | |
| Ember | |
| Microchip | Free stack, but not complete |
| Luxoft Labs | |
| Helicomm | |

## 2.7 ZigBee Networking

ZigBee can use so-called mesh networking, which may extend over a large area and contain thousands of nodes. Each FFD in the network also acts as a router to direct messages. The routing protocol optimizes the shortest and most reliable path through the network and can dynamically change, so as to take evolving conditions into account. This enables an extremely reliable network, since the network can heal itself if one node is disabled. This is very similar to the redundancy employed in the Internet. ZigBee

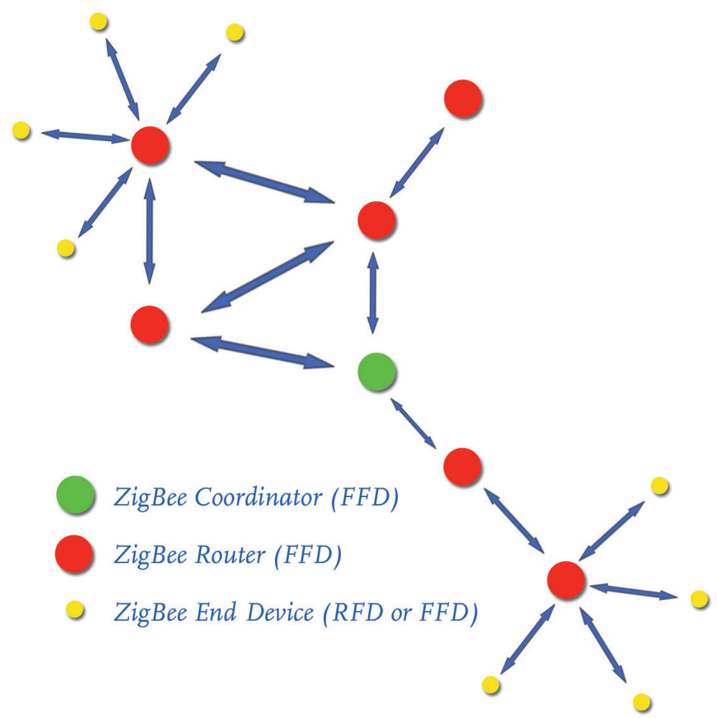



Figure 2.5: Mesh network

networks are primarily intended for low duty cycle sensor networks (<1%). A new network node may be recognized and associated in about 30 ms. Waking up a sleeping node takes about 15 ms, as does accessing a channel or transmitting data. ZigBee applications benefit from the ability to quickly attach information, detach, and go to deep sleep, which results in low power consumption and extended battery life.

# Chapter 3

# Design Process

The design is made using the CAD program Protel DXP 2004. By using DXP 2004 it is possible to have the schematics and layout designs in the same program environment. The design process is basically carried out in two steps. First, the schematics is designed. Second, the schematics is transferred to a layout. With the layout it is possible to manufacture Printed Circuit Boards.

As previously mentioned the main task of the project was to develop fully functional ZigBee modules. It was decided to develop two different modules. One module that contains both an Radio Frequency part (RF) and a Microcontroller part (MCU), which is called "RF+MCU module". The other module only contains the RF part of the system, hereafter called "RF module". The RF module can be used when different MCUs are evaluated. The RF+MCU module is preferably used when developing a completely new application. The RF-part is in the two modules identical.

## 3.1 Design Description

Figure 3.1 shows the block diagram of the RF+MCU module. The circuit is described in detail in the following sections. Note that the complete schematic and Bill Of Materials (BOM) for both modules are included in Appendix C and D.

## 3.2 Components

The system is divided into two main parts i.e., RF and MCU. The RF part handles the actual radio system, including Balanced to Unbalanced (BalUn) components, a matching network (MN) and an antenna. The MCU part handles the digital interface and the control circuit.

### 3.2.1 Microcontroller Unit

The MCU used is the ATmega128L chip from Atmel. The ATmega128L chip is fully capable of operating the ZigBee software stack, since it contains 128 kB of Flash memory. For an FFD the required memory size is up to 32 kB. The circuit shown in Figure 3.2 shows only the essential connections for this application. These are the connections

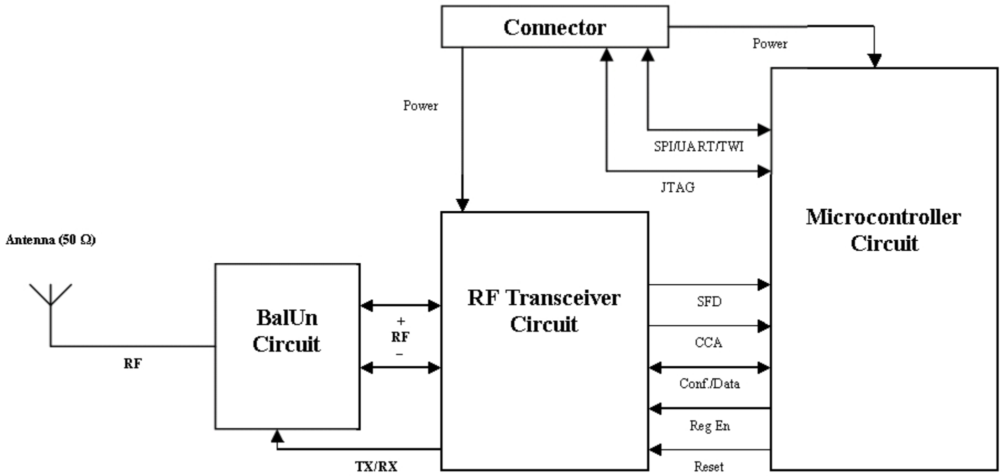



Figure 3.1: RF+MCU module block diagram

required to program and communicate with the device, and to interface the microcontroller with the RF transceiver. The complete schematic can be found in Appendix C.

### Programming

The modules are designed to support In-System Programming (ISP) via the JTAG interface. The connections required to program the device using an in-system programmer are listed in Table 3.1. In this design, these signals are routed to a connector (JP1) which then connects to a programmer. To convert the connector style to a standard JTAG connector a converter is needed. See Appendix D for details. The used in-system programmer is the AVR JTAGICE mkII from Atmel. It is a very powerful programmer that also supports debugging using the JTAG interface.

Table 3.1: Atmel ATmega128L JTAG interface

| Connection Name | Pin Number (Port) | Function |
|---|---|---|
| TDI | 54 (PF7) | Test Data Input |
| TDO | 55 (PF6) | Test Data Output |
| TMS | 56 (PF5) | Test Mode Select |
| TCK | 57 (PF4) | Test Clock |
| 3.3V | 21, 52 | Target Power |
| GND | 22, 63 | Common Ground |
| Reset | 20 | Target Reset Input |

The JTAG programming method is just one of many different alternatives. It is up to the user to decide which one is the most suitable alternative. For more information on alternative programming interfaces, one can refer to [5].

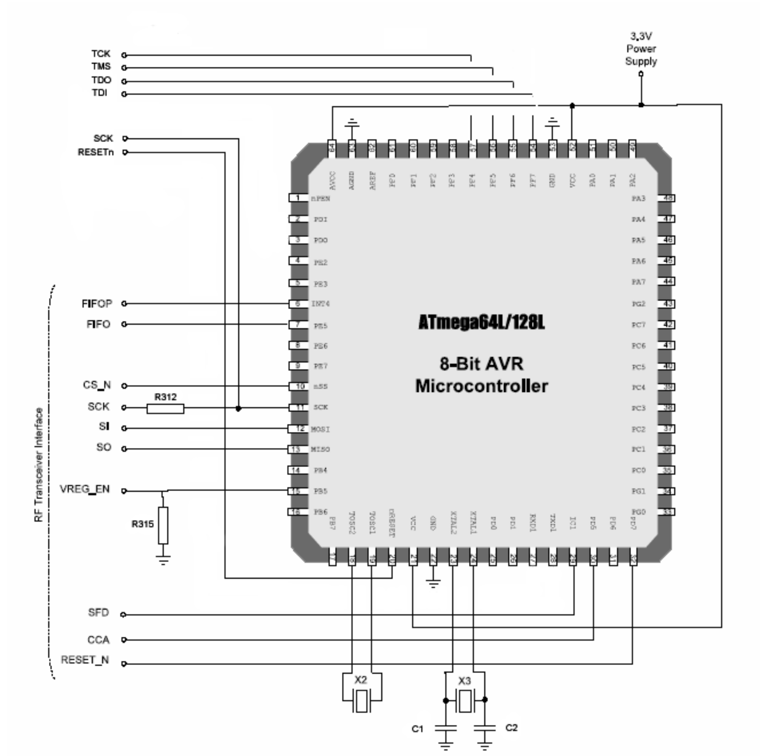



Figure 3.2: MCU circuit

### Data Interface

The RF+MCU module has a wide range of external data interfaces, this allows the MCU to communicate with almost any external device. As already mentioned the JTAG interface is very useful when debugging an application. The JTAG interface is also used to program the MCU. The Serial Peripheral Interface (SPI) is used to communicate with the RF transceiver. The SPI interface can also be used to connect other devices to the module. The SPI interface is described more in the Section 3.2.2. One very commonly used interface is the Universal Synchronous and Asynchronous Serial Receiver and Transmitter (USART). The USART is used to communicate with for example a RS-232 or USB chip. The USART uses in particular two pins: Receive Data (RXD) and Transmit Data (TXD). Some devices, i.e., modems, also use for example Ready To Send (RTS) and Clear To Send (CTS) signals. There are several I/O pins that can be used for that purpose. The USART allows the MCU to communicate with any logic-level USART device that supports standard baud rates. There are two USARTs on the module connector. To add even more functionality to the module, the Two Wire Interface (TWI) is routed to the connector. The TWI is fully compatible with the well known I2C standard from Philips. The TWI uses only two pins; one clock pin and one data pin. The interface can be used to communicate with a wide range of devices. There are several pins on the module connector that can be used as General Purpose Input/Output (GPIO) pins. Even some analog pins are routed to the connector, which allows for the user to use the integrated 10-bit ADC of the MCU. For additional information please see [5].

**Crystals**

As shown in Figure 3.2, two external crystals are required for the microcontroller circuit. First, an 8.000 MHz crystal (X2) is used along with two loading capacitors (C1 and C2) to generate the system clock of the MCU. It is also possible to use the internal RC-clock, but to meet the timing accuracy requirement of the IEEE 802.15.4 it is necessary to use an external crystal. Since the crystal is ultimately used to generate the MAC timing, it must have an overall accuracy of $\pm 40$ ppm. Please note that the total accuracy includes initial tolerance, temperature drift and aging. There are several factors to consider when selecting the 8.000 MHz crystal. One of the goal for this module was to reduce the size as much as possible, therefore a 5x7 mm crystal is used. For applications that are more cost-sensitive, a larger package such as the industry-standard HC-49 can be used. To reduce the cost even more the temperature tolerance can be relaxed. Which package to use is of course application dependent.

The second external crystal, X3, is the Real Time Clock (RTC). The RTC is a 32.768 kHz watch crystal. This crystal is required for the internal low-frequency timer/counter oscillator which is used when the device is in power-save mode. The MCU has integrated loading capacitors, which makes external loading capacitors unnecessary. The frequency of the RTC is chosen such that it is possible to use hours and minutes for the wake-up time of the device, for instance.

### 3.2.2 RF Transceiver/Microcontroller Configuration and Data Interface

The interface between the RF and MCU parts is illustrated in Figure 3.1. Table 3.2 provides a description of these interface signals.

The SPI interface is a commonly used interface for connecting several peripheral units to one microcontroller. The interface uses four lines, i.e., CSn, SCLK, SI and SO, as described in Table 3.2. To be able to connect several devices on the SPI bus it is necessary to connect a 0 $\Omega$ resistor (R312) in series on the SCLK line, to avoid contention on the line. See Figure 3.2. The resistor allows other devices to drive the SCLK line without damaging the CC2420 chip.

The VREG_EN signal is connected to a pull-down resistor (R315) to make sure that the internal voltage regulator is disabled when the microcontroller is reset.

Please note that both the series resistor (R312) and the pull-down resistor (R315) are not implemented on the RF module, because different MCUs has different ways of connecting to the SPI bus.

More information about the RF Transceiver/Microcontroller Configuration and Data Interface can be found in [4].

### 3.2.3 RF Circuit

The RF circuit is shown in Figure 3.3. The figure shows all the external components required for the CC2420 to work properly. Note that no decoupling capacitors are

Table 3.2: RF Transceiver/Microcontroller interface

| RF Num. | RF Name | Description | MCU Num. | MCU Name |
|---|---|---|---|---|
| 21 | RESETn | Asynchronus, active low digital reset. | 16 | PB6 |
| 27 | SFD | Start of Frame Delimiter. | 29 | PD4 |
| 28 | CCA | Clear Channel Assessment. | 31 | PD6 |
| 29 | FIFOP | Asserted when last packet has been received or FIFO size has exceeded threshold. | 6 | INT4 |
| 30 | FIFO | Asserted when data is present in FIFO. | 7 | PE5 |
| 31 | CSn | SPI Chip Select, active low. | 10 | SSn |
| 32 | SCLK | SPI Clock input, up to 10 MHz. | 11 | SCK |
| 33 | SI | SPI Slave Input. Sampled on the positive edge of SCLK. | 12 | MOSI |
| 34 | SO | SPI Slave Output. Updated on the negative edge of SCLK. Tristate when CSn is high. | 13 | MISO |
| 41 | VREG_EN | Internal voltage regulator enable, active high. | 15 | PB5 |

included in the schematic. It is important to note that in this design the RF transceiver is configured for unbalanced (or single-ended) operation. The RF transceiver can also be used for balanced (or differential) operation. However, this is not discussed in this document.

### BalUn and Matching Network

The RF input/output port of the RF transceiver is a differential and high impedance port. To be able to use the RF transceiver in single-ended mode, a BalUn circuit is needed. BalUn stands for Balanced-Unbalanced. The optimal differential load for the RF transceiver is 115+j180 Ω.

The BalUn circuit in this design is used for different functions. The typical function of a BalUn is to convert the differential RF input/output signal to a single-ended port. In Figure 3.3 component pairs L62/C61 and L81/C81 accomplish this task by shifting signals RF_P and RF_N by 90°. This is equivalent to shifting the phase 180° relative to each other, resulting in an single-ended signal.

The second function performed by the BalUn is impedance matching. All the values of the components are carefully chosen so that the impedance "looking into" the BalUn is 50 Ω. The values of the components are exactly the same as the reference design available from Chipcon, however the values are carefully controlled and re-calculated using the Smith Chart Utility in Advanced Design System 2003C (ADS2003C). For more information refer to Appendix A.

The last function of the BalUn is to provide the needed DC bias to the internal PA and LNA in the RF transceiver. A DC patch must exist from the pin TXRX_SWITCH to the pins RF_P and RF_N. This is accomplished by the inductors L61 and L62.

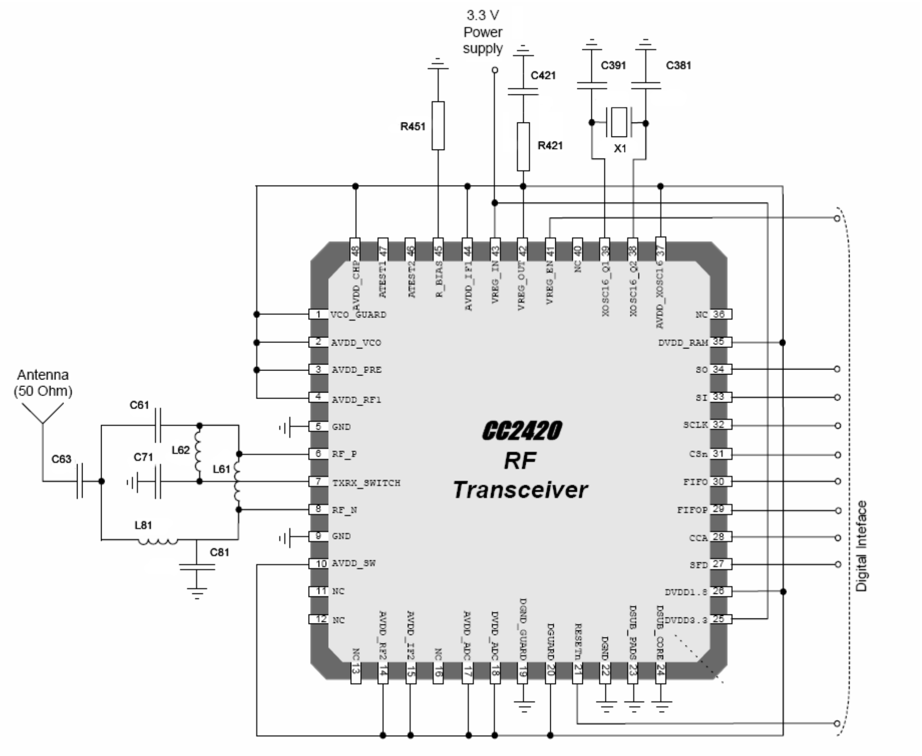



Figure 3.3: RF circuit

The capacitor C71 is used for decoupling. Finally the capacitor C63 is a DC blocking capacitor to the antenna and matching network.

### Antenna

The antenna used in the design is the Mica antenna from gigaAnt AB. It is a relatively small antenna of SMD type which requires a ground plane for proper placement. The antenna has a length of a quarter wave length at 2.4 GHz. One important factor when designing the modules was the radio range. The Mica antenna has a fairly high efficiency, 75%, which results in a good range of the radio link.

### Crystal

An external 16.000 MHz crystal (X1) is needed for the RF transceiver to work. Two loading capacitors (C381 and C391), shown in Figure 3.3, are required for the internal oscillator circuit. When selecting the crystal it is important to notice that the Equivalent Serial Resistans (ESR) must be 60 Ω or less. Otherwise one can not guarantee the start-up time of the internal oscillator. Another thing to notice is that the overall accuracy must not exceed ±40 ppm. The overall accuracy includes temperature drift, initial tolerance and aging. For applications where IEEE 802.15.4 compliance is not required the overall accuracy can be relaxed to ±60 ppm.

#### Bias Resistor

The bias resistor (R451), shown in Figure 3.3, is used to set an accurate current for the internal current regulator. A 43 kΩ resistor with 1% tolerance must be used.

#### Voltage Regulator

The RF transceiver is equipped with an internal voltage regulator which is used to power all of the 1.8V power supply. A 10 $\mu$F tantalum capacitor (C421) is required to secure the stability of the regulator. The ESR of the tantalum capacitor must be between 0.5 and 5 Ω. As seen in Figure 3.3 a series resistor (R421) is used to prevent the ESR to drop below 0.5 Ω. The ESR will vary with the temperature.

#### Power Supply Decoupling

To ensure optimal performance a good power supply decoupling is needed. As usual the placement and size of the decoupling capacitors are very important. The placement of the decoupling capacitors is described more closely in the Chapter 4.

### 3.2.4 Connector

The connector used in the design is a small SMD connector from HRS. The connector has 20 pins which is enough for all important signals. When designing the modules one primary task was to make it easy to connect the modules with different kinds of applications. This is fulfilled with this connector. Since the only connection of the module to the application board is via the connector, the stability of the connector is important. The used connector has a "snap-in" function, so the stability is ensured.

### 3.2.5 Power Supply

The power to the RF+MCU module is supplied by a low drop-out voltage regulator REG102 from Texas Instruments Inc. The new DMOS topology provides a very low drop-out and good protection against transients. The REG102 has thermal and over current protection functions, including a fold back current limit. The regulator also has very low output noise (typically 28 $\mu V_{RMS}$ for $V_{OUT}$ 3.3 V), which makes it ideal for use in small communications devices.

## 3.3 Printed Circuit Board Layout

A proper designed Printed Circuit Board (PCB) is very important for the operation of the RF Transceiver. This section describes the layout design process of the modules.

### 3.3.1 PCB Overview

The PCB of the two modules is a 4 layer standard FR-4 board. The board is 0.95 mm in thickness. The dimensions of the RF+MCU module is 23x40 mm, and the RF module is

18x25 mm. The components on the RF+MCU module are placed on both the top and bottom layer, as shown in Figure 3.4. The only component on the RF module which is placed on the top side is the antenna, while the rest of the components are placed on the bottom layer, see Figure 3.5.

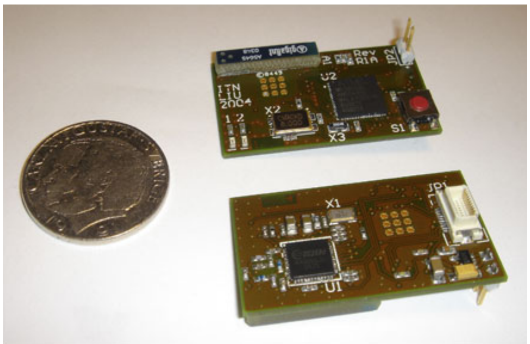


Figure 3.4: RF+MCU module

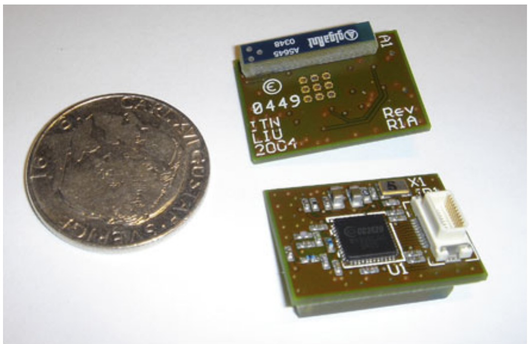


Figure 3.5: RF module

The board is composed of four layers shown in Figure 3.6. The two internal layers are used for power and ground. While the top and bottom layers are used for routing. On the top and bottom a copper pour connected to ground is used. The complete set of PCB layout files can be found in Appendix B. All the design parameters are selected for fabrication in a standard low-cost production process. The smallest via diameter is 0.3 mm, and the smallest trace width is 0.15 mm. The components used on the two modules are mainly of size 0402.

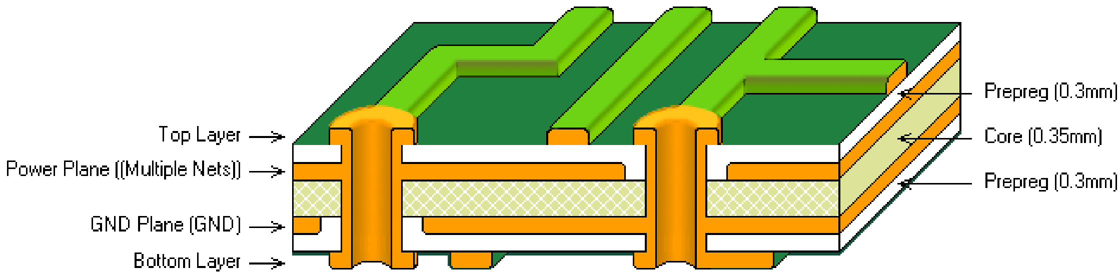



Figure 3.6: Layer stackup

### 3.3.2 General Layout Guidelines

One very important factor when working with RF designs is that power supply decoupling is implemented properly on the PCB. All decoupling capacitors should be as small as possible (preferably 0402) to reduce parasitics. For best results decoupling capacitors should be placed as close to the chip pins as possible. To maximize the effectiveness of decoupling, the capacitors were placed between the pins and the via to the internal power plane. Placing vias between the supply pin and the capacitor should be avoided.

All connections to ground for component pins and decoupling capacitors should be as short as possible. It is very important that every connection to ground is made via an individual connection to the internal ground plane. It is not recommended to rely solely on the top and bottom layer copper pour, as it can result in floating ground planes.

The traces between the 16.000 MHz crystal and the RF transceiver should be very short. The loading capacitors are placed in-line with the traces.

The connection between the antenna and the single-ended port of the BalUn is made via a controlled impedance microstrip line. The width of the microstrip line is determined based on several parameters, including 50 Ω impedance, ground plane separation and the dielectric constant of the PCB substrate. To calculate the width of the microstrip line the function "characteristic impedance driven width" in Protel DXP 2004 is used. The width is calculated to be 0.4917 mm to obtain a 50 Ω micro strip line. The antenna is placed on the top layer, connected via the microstrip line through a via to the BalUn.

### 3.3.3 BalUn Layout

The layout of the BalUn is very important for the performance of the RF transceiver. As Figure 3.7 shows, the components included in the BalUn are placed in a symmetrical topology. The length of the two signal traces should be made equal. The two traces should be sufficiently wide, but it is not necessary to design the traces for 50 Ω impedance. No copper whatsoever is allowed under the BalUn, whether it is in the form of signal traces or plane area. The only copper allowed under the BalUn is the copper pour on the top plane.

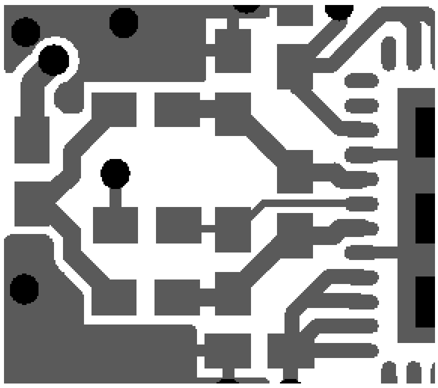


Figure 3.7: BalUn layout

### 3.3.4 GND Vias

Both the RF transceiver (CC2420) and the MCU (ATmega128L) contain a ground pad inside of the component package. The devices use the ground pad for both electrical connectivity and heat dissipation. Because of that it is important to place vias under the two devices, which connect the two devices to the internal ground plane. An array of

3x3 vias is used for both devices, which minimizes the thermal resistance and provides a solid ground connection. This is shown in Figure 3.8.

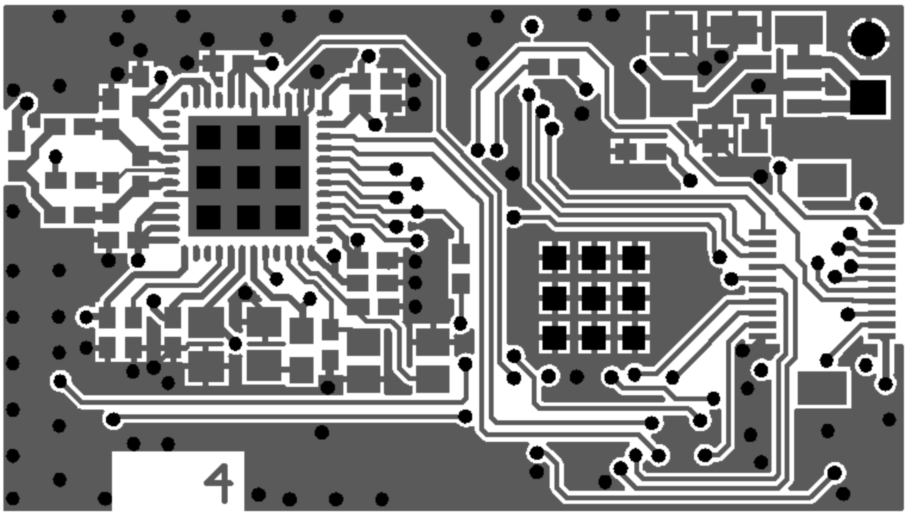



Figure 3.8: Ground vias (bottom view)

To avoid floating ground planes and parasitic effects the copper pour areas are connected to the internal ground plane with several vias. This will prevent unwanted resonances that could potentially impact the RF performance.

# Chapter 4

# Implementation

This chapter describes the implementation of the design, and the fully functional ZigBee modules developed.

## 4.1 PCB Manufacturing

Since the PCBs in this design have four layers, it is not possible to manufacture it in the PCB lab at the university. The company Elektrotryck AB was contracted to manufacture the modules. Elektrotryck handled all the panelization of the modules. A total of 40 modules was manufactured, 20 pieces of each module.

Before manufacturing the layout files must be converted into a format that can be managed by the PCB manufacturer, in this case Gerber RS274X. This results in a set of files, where each file contains information about a specific layer.

For this design the following layers were used:

- Topoverlay - Component print on top.
- Topsolder - Top solder mask.
- Top - Copper on top layer.
- Plane1 - Power/ground plane, negative.
- Plane2 - Ground plane, negative.
- Bottom - Copper on bottom layer.
- Bottomsolder - Bottom solder mask.
- Bottomoverlay - Component print on bottom.
- Drill - Drill file, in .exc format.
- Profile - The milling file, i.e., the shape of the modules.

## 4.2 Assembly

All the assembly was performed at the university. Since there was no flip-chip mounting equipment at the institution, the most difficult part of the assembly was the mounting of the ICs. The assembly was performed with a microscope.

## 4.3 Soldering

To make it possible to manufacture the small modules in-house, a reflow soldering oven was purchased. With a reflow soldering oven it is pretty easy to get a good result when soldering small components.

## 4.4 Bill Of Material

The Bill Of Material (BOM) for the two modules is to be seen in Appendix D. The BOM is created using Protel DXP 2004.

## 4.5 Assembled Modules

The overall dimension of the RF+MCU module is 23x40 mm, and the RF module is 18x23 mm. Table 4.1 shows the dimensions that have been used for the RF+MCU module.

Table 4.1: PCB dimensions for RF+MCU module

| Description | Dimension |
|---|---|
| Standard track width | 0.2 mm |
| Via hole size | 0.3 mm |
| Via pad size | 0.6 mm |
| Standard component size | 0402 |
| No of vias | 131 |
| No of components | 50 |

Table 4.2 shows the pin list of the RF+MCU module, and Table 4.3 shows the pin list of the RF module. For more information about the these modules please refer to Chapter 3.

Table 4.2: RF+MCU module pin list

| Pin no. | Pin Name | Description and internal MCU connection |
|---|---|---|
| 1 | SCLK | SPI interface clock, PB1. |
| 2 | SI | SPI interface Slave Input, PB2. |
| 3 | SO | SPI interface Slave Output, PB3. |
| 4 | SCL | TWI (I2C) clock, PD0. |
| 5 | SDA | TWI (I2C) data, PD1. |
| 6 | PD2 | UART RXD1, Digital I/O, PD2. |
| 7 | PD3 | UART TXD1, Digital I/O, PD3. |
| 8 | PD5 | Digital I/O, PD5. |
| 9 | PD7 | Digital I/O, PD7. |
| 10 | GND | GND |
| 11 | 3.3V | Power |
| 12 | AREF | Analogue ref. for internal ADC. |
| 13 | RESET | Reset |
| 14 | TXD0 | UART TXD0, Digital I/O, PE1. |
| 15 | RXD0 | UART RXD0, Digital I/O, PE0. |
| 16 | PF3 | Digital or Analogue I/O, PF3. |
| 17 | TCK | Digital or Analogue I/O, JTAG TCK, PF4. |
| 18 | TMS | Digital or Analogue I/O, JTAG TMS, PF5. |
| 19 | TDO | Digital or Analogue I/O, JTAG TDO, PF6. |
| 20 | TDI | Digital or Analogue I/O, JTAG TDI, PF7. |

Table 4.3: RF module pin list

| Pin no. | Pin Name | Description |
|---|---|---|
| 1 | VREG_EN | Internal voltage regulator enable, active high. |
| 2 | SFD | Start of Frame Delimiter. |
| 3 | CCA | Clear Channel Assessment. |
| 4 | FIFO | Asserted when data is present in FIFO. |
| 5 | FIFOP | Asserted when last packet has been received or FIFO size has exceeded threshold. |
| 6 | CS | SPI Chip Select, active low. |
| 7 | SCLK | SPI Clock input, up to 10 MHz. |
| 8 | SI | SPI Slave Input. Sampled on the positive edge of SCLK. |
| 9 | SO | SPI Slave Output. Updated on the negative edge of SCLK. Tristate when CSn is high. |
| 10 | VREG_IN | Power, 3.3V |
| 11 | GND | GND |
| 12 | NC | No Connection. |
| 13 | NC | No Connection. |
| 14 | NC | No Connection. |
| 15 | NC | No Connection. |
| 16 | NC | No Connection. |
| 17 | NC | No Connection. |
| 18 | NC | No Connection. |
| 19 | RESETn | Asynchronous, active low digital reset. |
| 20 | GND | GND |

# Chapter 5

# Development Tools

A range of different software and hardware tools are used to compile and configure the modules. The development environment is a combination of the programs and devices presented here.

## 5.1 CC2420 ZigBee DK Development Kit

The CC2420 ZigBee DK Development Kit was purchased from Chipcon, and used to evaluate the ZigBee and IEEE 802.15.4 standards. The kit contains seven laboration cards with different integrated sensors and devices. One packet sniffer is also included in the kit. The packet sniffer is used to read out the packets sent over the air. It is a very useful tool when working with wireless devices. The CC2420 ZigBee DK Development Kit also contains the ZigBee software stack. The stack is reconfigured for use with the two developed modules. The complete kit is shown in Figure 5.1.


Figure 5.1: CC2420 ZigBee DK Development Kit

## 5.2 ATmega128L Tools

The use of the microcontroller ATmega128L from Atmel is based on some different tools.

### 5.2.1 AVR GCC Tool

The free GNU AVR GCC development tools are used to generate the files for the RF+MCU module running on the ATmega128L controller. The GNU AVR GCC compiler is used when compiling files with Programmer's Notepad. Please see [13] in order to obtain detailed insight in compiler options and make-files etc.

### 5.2.2 Atmel AVR Studio

The AVR Studio is used to download code to the microcontroller on the RF+MCU Module. Together with the programmer AVR JTAG ICE mkII is also used for debugging. Figure 5.2 shows the user interface of AVR studio.

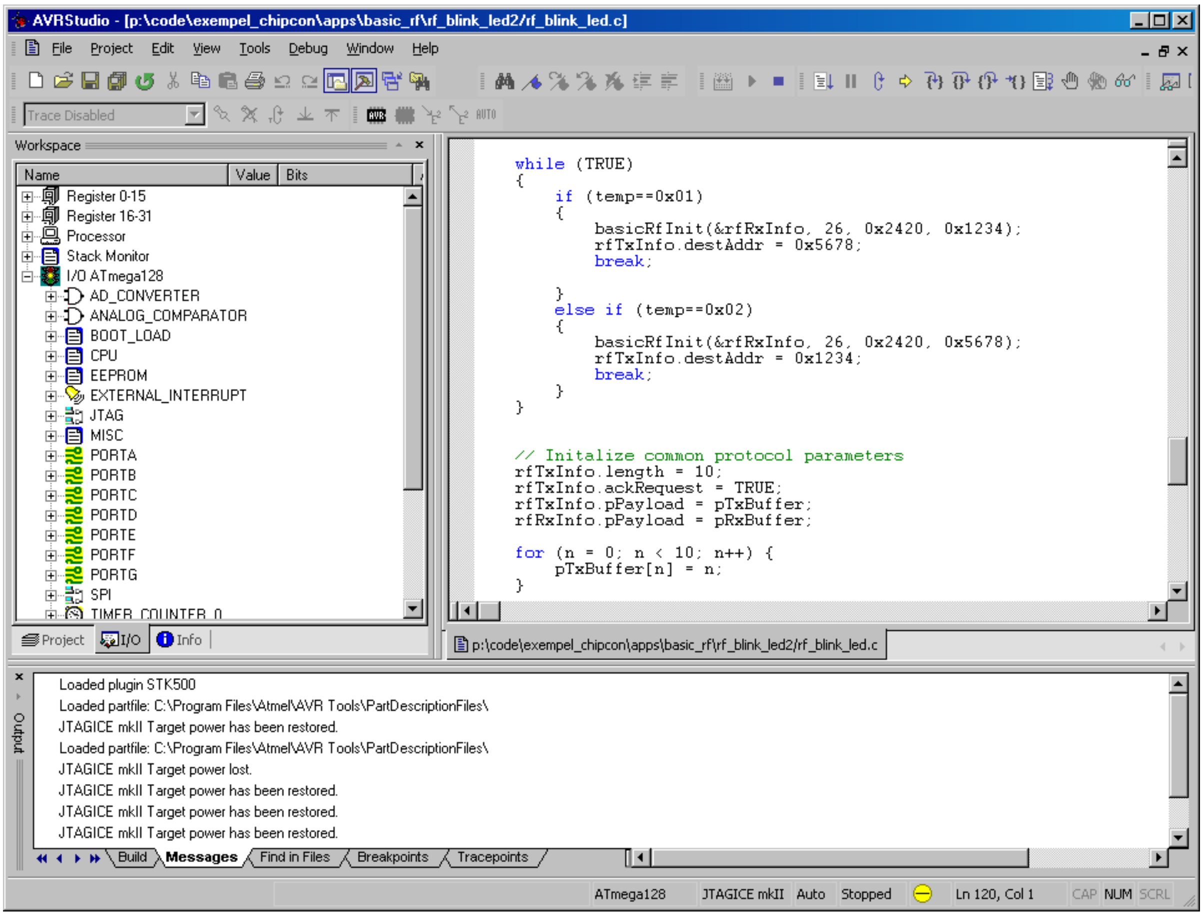



Figure 5.2: AVR studio

### 5.2.3 Programmer's Notepad

A text editor such as Programmer's Notepad with highlighting is used for source code writing. The editor is configured to run the make-files, by use of macros linked to the make-files for AVR GCC. As seen in Figure 5.3 the code is divided automatically into different sections.

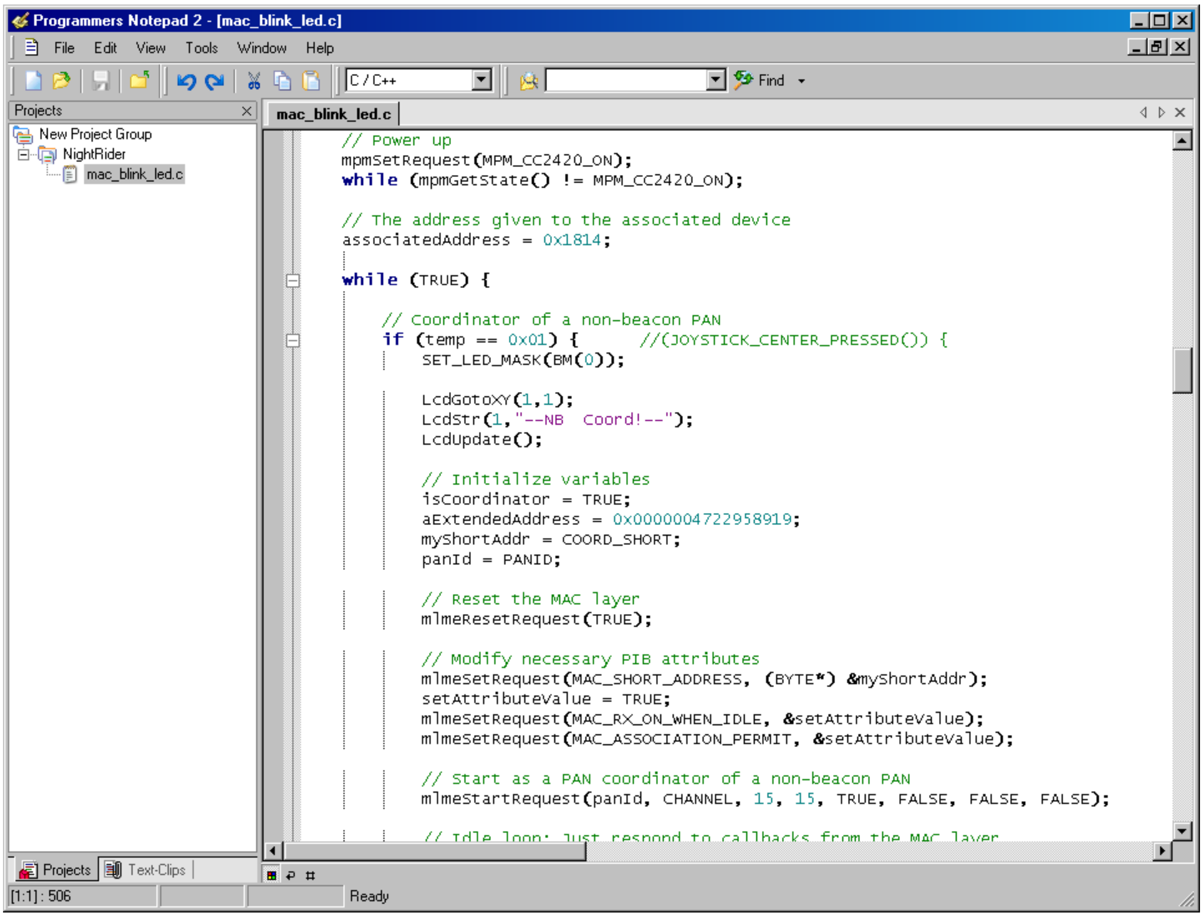



Figure 5.3: Programmer's Notepad

## 5.3 PCB Tool

Protel DXP 2004 is used to design the schematic and the layout of the modules. Protel DXP 2004 is a very powerful tool with many useful functions. For example it has a "rule check" function; the user defines a set of different rules that is to be followed, and then the PCB is designed using the rules. Figure 5.4 shows the Protel DXP 2004 layout environment.

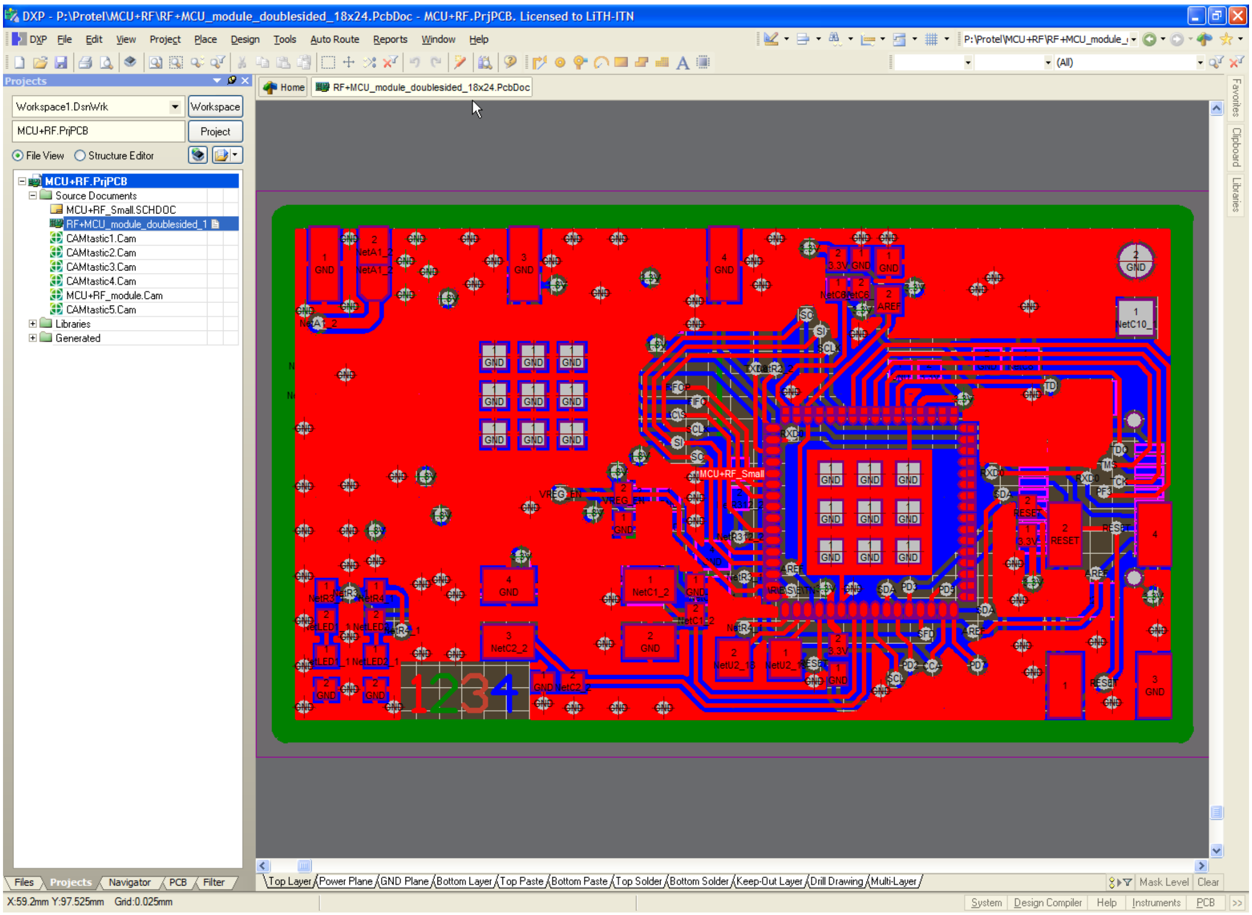



Figure 5.4: Protel DXP 2004 layout environment

# Chapter 6

# Test Application

To test and evaluate the developed ZigBee and IEEE 802.15.4 modules a test application has been developed. The test application consists of two devices: a network coordinator which displays the temperature value on a display, and a temperature sensor which reports the current temperature value to the coordinator. The ZigBee and IEEE 802.15.4 modules are connected to the test devices. As previously stated that the developed ZigBee modules should be able to easily connect themselves to different types of applications. The two test devices has been developed and assembled in-house.

## 6.1 Temperature Coordinator

The coordinator display device consists of a 2-layer PCB, as seen in Figure 6.1. The ZigBee module is connected via a connector to the PCB. The display is connected to the MCU on the module via the same SPI interface as the RF transceiver (CC2420). The coordinator device in the test application is responsible for setting up a network. When the network is set up, the coordinator device initiates the display, and then it waits for the temperature sensor device to report a temperature value. When a value is received the coordinator device converts it to ASCII characters, and the ASCII value are displayed. Figure 6.2 shows the complete MCU program flow.

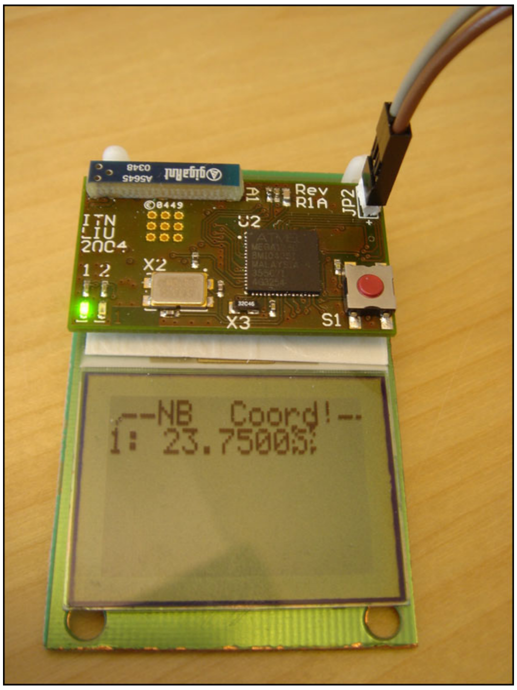



Figure 6.1: Temperature coordinator

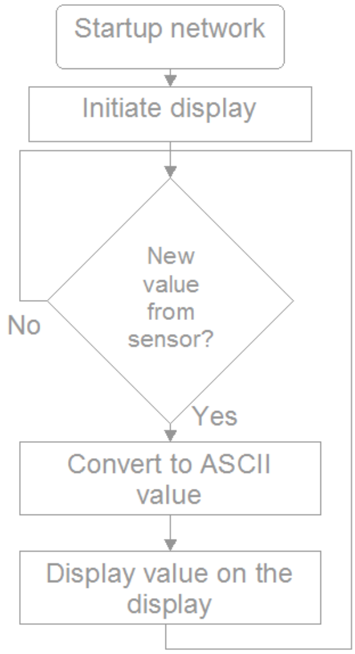



Figure 6.2: Temperature coordinator flow

## 6.2 Temperature Sensor

The temperature sensor device is developed with the temperature sensor DS1631 from Maxim/Dallas Semiconductor. The temperature sensor is connected to the MCU on the ZigBee and IEEE 802.15.4 module via the TWI (I2C) bus, see Figure 6.3.

The temperature sensor device in the test application connects itself wirelessly to the coordinator of the network. When the temperature sensor device is connected to the network the temperature sensor is initiated. A 12-bit value from the temperature sensor is then read and sent to the coordinator device. After that the temperature device is in rest for about two seconds, and then a new value is read from the temperature sensor. Figure 6.4 shows the complete MCU program flow.

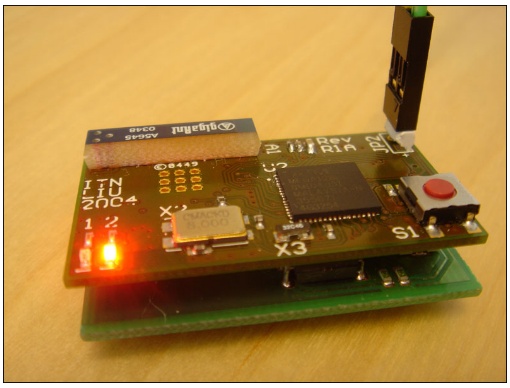



Figure 6.3: Temperature sensor flow

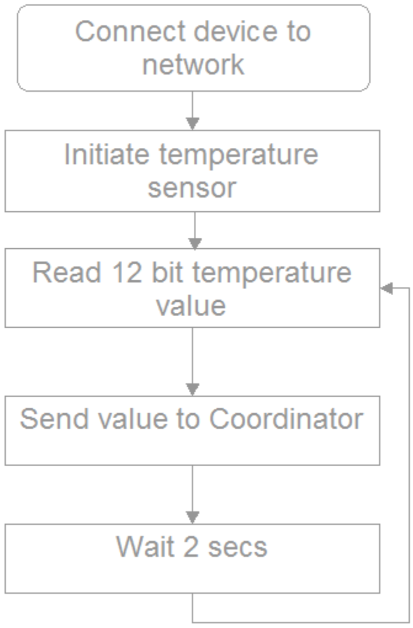



Figure 6.4: Temperature sensor flow

# Chapter 7

# Results

This thesis work has shown that ZigBee can be seen as a complement to other standards, i.e., Bluetooth and IEEE 802.11 WLAN. ZigBee is not competing in the same market segment as either Bluetooth or WLAN. One very important factor for the success of ZigBee is the interoperability. A remote controller from, i.e., Philips must be able to operate a Samsung TV. The three major advantages of ZigBee are low price, long covering range and low energy consumption.

The developed modules can be used for quick prototyping of small wireless sensors, and build large sensor networks. To verify the functionality of the modules, a test application has also been developed. The test application consists of a PAN coordinator and a temperature sensor FFD device. The temperature sensor device reports the temperature to the coordinator which displays the temperature on a display.

The other module, i.e., the RF module is preferably used when evaluating different MCUs. When developing new ZigBee applications the RF+MCU module will be used.

# Chapter 8

# Discussions

The market for wireless sensor networks is expected to grow rapidly in the near future. Our developed ZigBee-ready modules may contribute to this development, since they can easily be connected to various type of sensors and to build up wireless networks.

Our modules are small, but the size can be reduced even more, when a single-chip solution is on the market. *(Which is expected in Q2 2005.)*

If the ZigBee interoperability work between different brands of ZigBee devices, the ZigBee standard may be the dominating standard for wireless sensor networks in the future.

One important advantage of ZigBee over other wireless standards is the low price. The price for one IEEE 802.15.4 transceiver chip is currently as low as $<$ \$3. One should also notice that the IEEE 802.15.4 transceiver can be used to build custom networks, without using the ZigBee network structure.

# Chapter 9

# Conclusions

We believe that there is definitely a place on the market for ZigBee, since no global standard exists today in the wireless sensor network area.

Two fully functional ZigBee/802.15.4 modules have been developed. It is possible to design a module with RF parts on a low cost FR-4 PCB substrate. By using a four layer PCB the size is reduced significantly.

Finally it is shown that a temperature sensor can be integrated with the developed ZigBee-ready modules.

# Chapter 10

# Further work

Some suggestions of further work are given below.
The modules can be improved by:

- Smaller PCB.
- New RF-chip with integrated MCU *(May be released from Chipcon in Q2 2005)*.
- Smaller or integrated antenna.
- Integrated sensors on the module.

Suggested further work for ZigBee enabled applications are:

- USB gateway, for easy communication with a PC.
- Different kinds of sensors, e.g., temperature, pressure, flow, moisture, humidity and accelerometers, etc.
- PC program for control of the ZigBee network.

# Bibliography


[1] Reinhold Ludvig and Pavel Bretchko, *RF Circuit Design - Theory and Applications*, Prenctice Hall 2000, ISBN 0-13-095323-7.

[2] William Stallings, *Wireless Communication and Networking*, Prenctice Hall 2002, ISBN 0-13-040864-6.

[3] *IEEE Standards 802.15.4*, IEEE 2003, ISBN 0-7381-3677-5 SS95127.

[4] Chipcon AS, *Chipcon AS SmartRF CC2420 Preliminary Data sheet (rev 1.2)*

[5] Atmel Corporation, *ATmega128L Data sheet Rev. 2467M-AVR-11/04*

[6] ZigBee Alliance, http://www.zigbee.org, 2005-03

[7] Freescale Semiconductor, http://www.freescale.com, 2005-03

[8] Maxim-Ic, http://www.maxim-ic.com, 2005-03

[9] Atmel Corporation, http://www.atmel.com, 2005-03

[10] Chipcon, http://www.chipcon.com, 2005-03

[11] gigaAnt, http://www.gigaant.com, 2005-03

[12] Figure 8 Wireless, http://www.figure8wireless.com, 2005-03

[13] AVR Freaks, http://www.avrfreaks.com, 2005-03

[14] Texas Instruments, http://www.ti.com, 2005-03

# Appendices

# Appendix A

# Tools

The Smith Chart tool in ADS can be used to create matching networks.

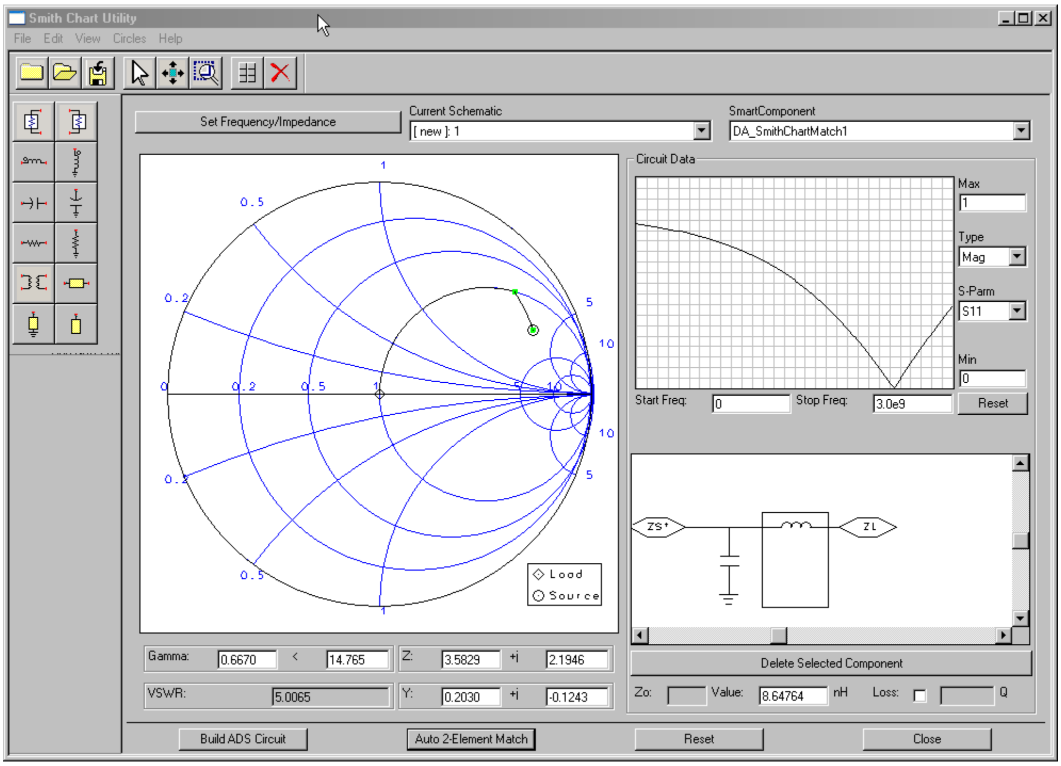



Figure A.1: Smith Chart tool in ADS

# Appendix B

# PCB Layout

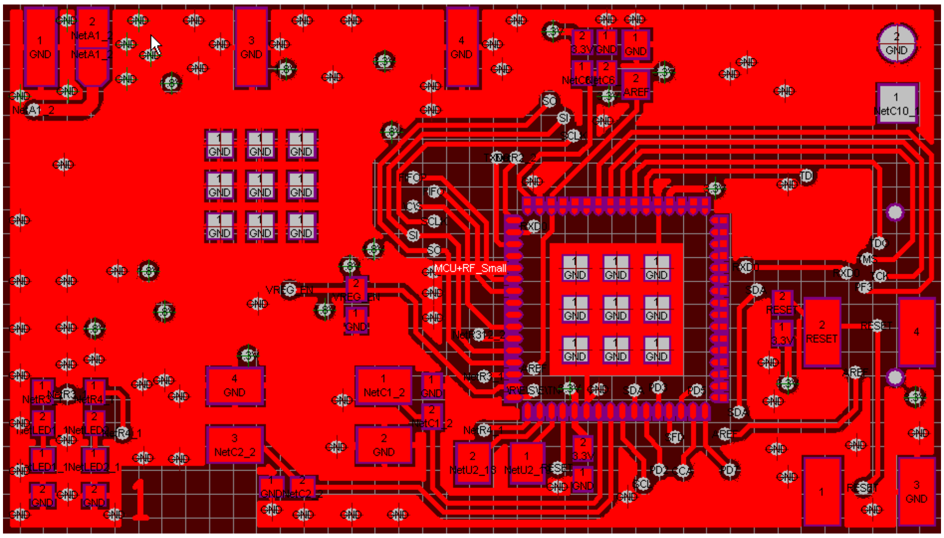


Figure B.1: RF+MCU module top layer

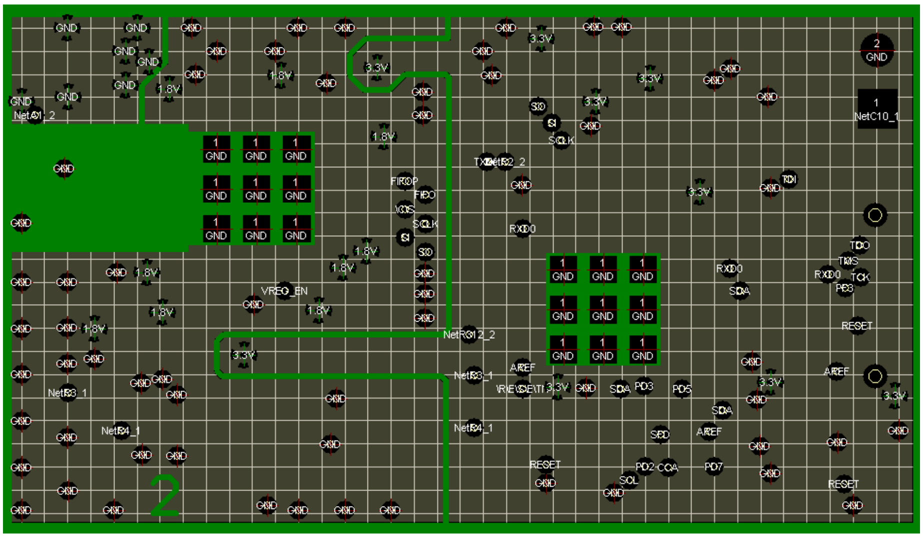


Figure B.2: RF+MCU module power/GND plane, negative

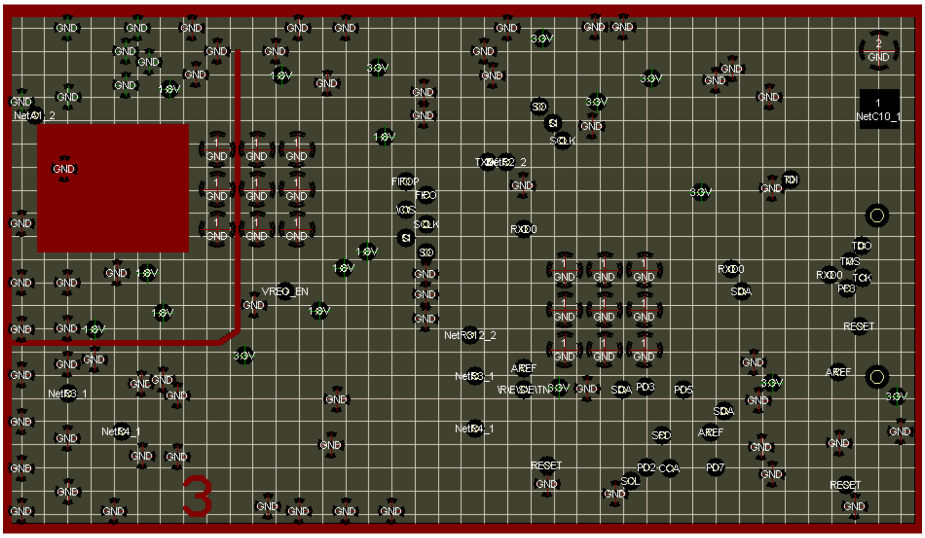


Figure B.3: RF+MCU module GND plane, negative

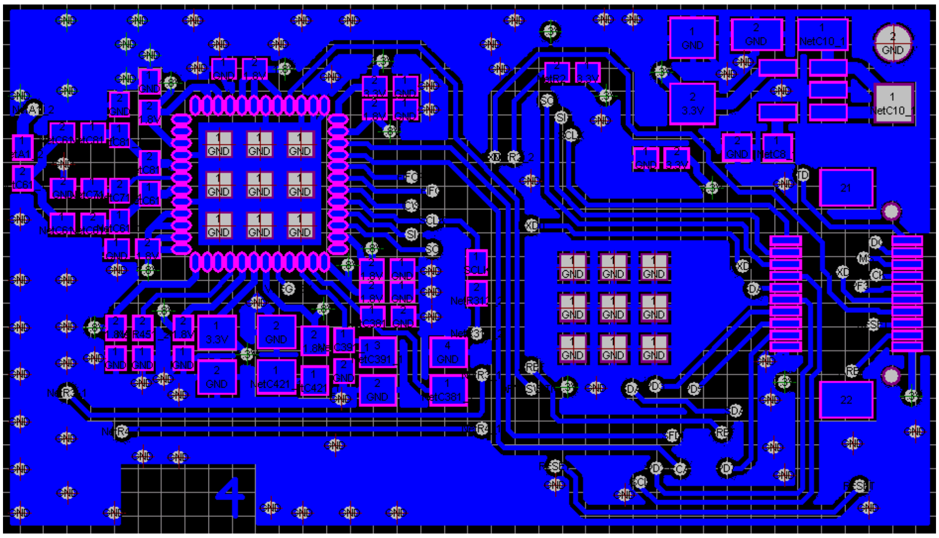


Figure B.4: RF+MCU module bottom layer

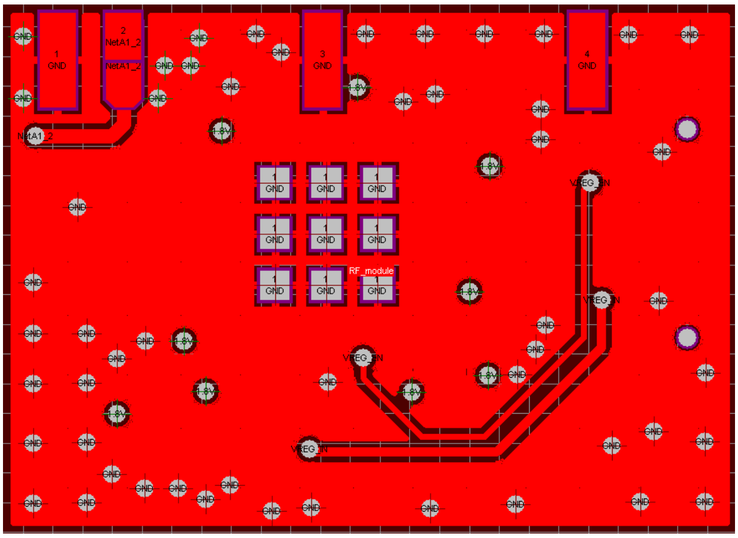


Figure B.5: RF module top layer

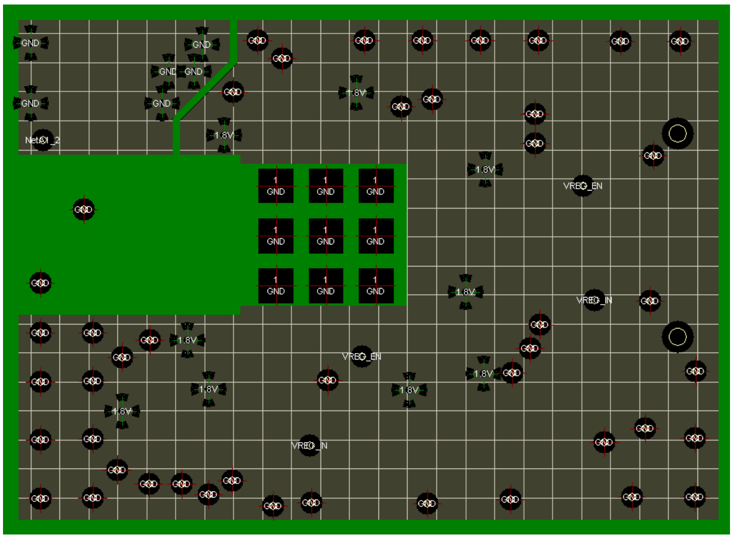



Figure B.6: RF module power/GND plane, negative

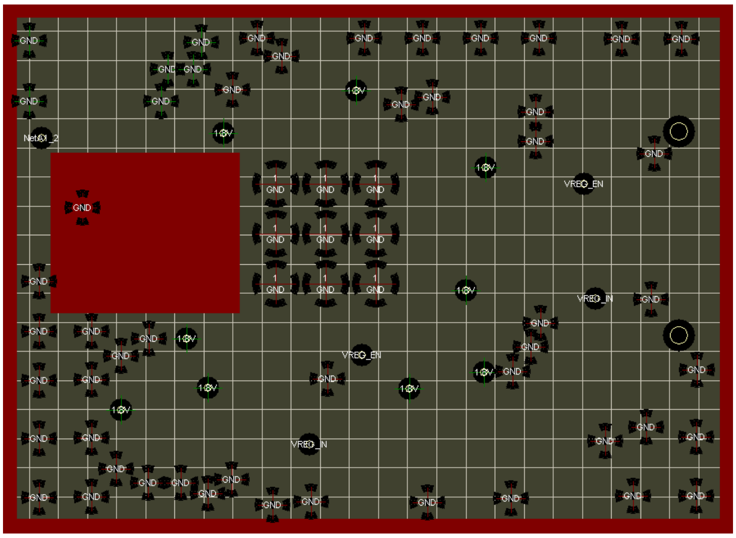



Figure B.7: RF module GND plane, negative

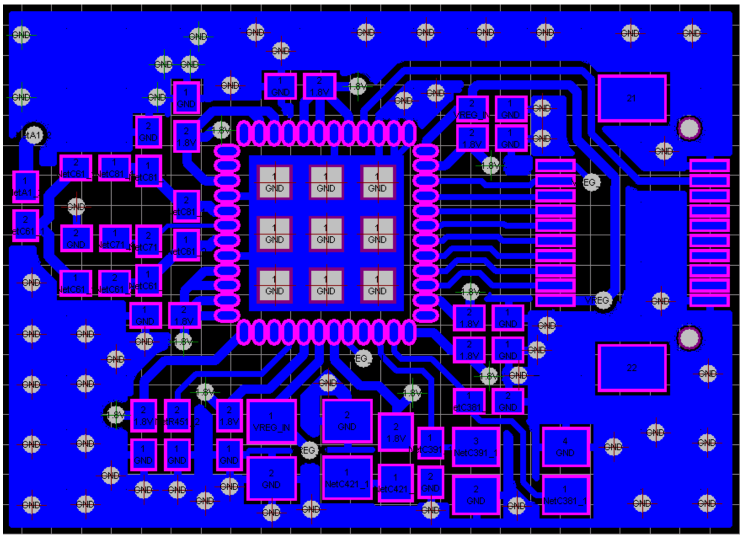


Figure B.8: RF module bottom layer

# Appendix C

# Schematics

Schematics for the RF+MCU Module, the RF Module and the JTAG connector is presented here.

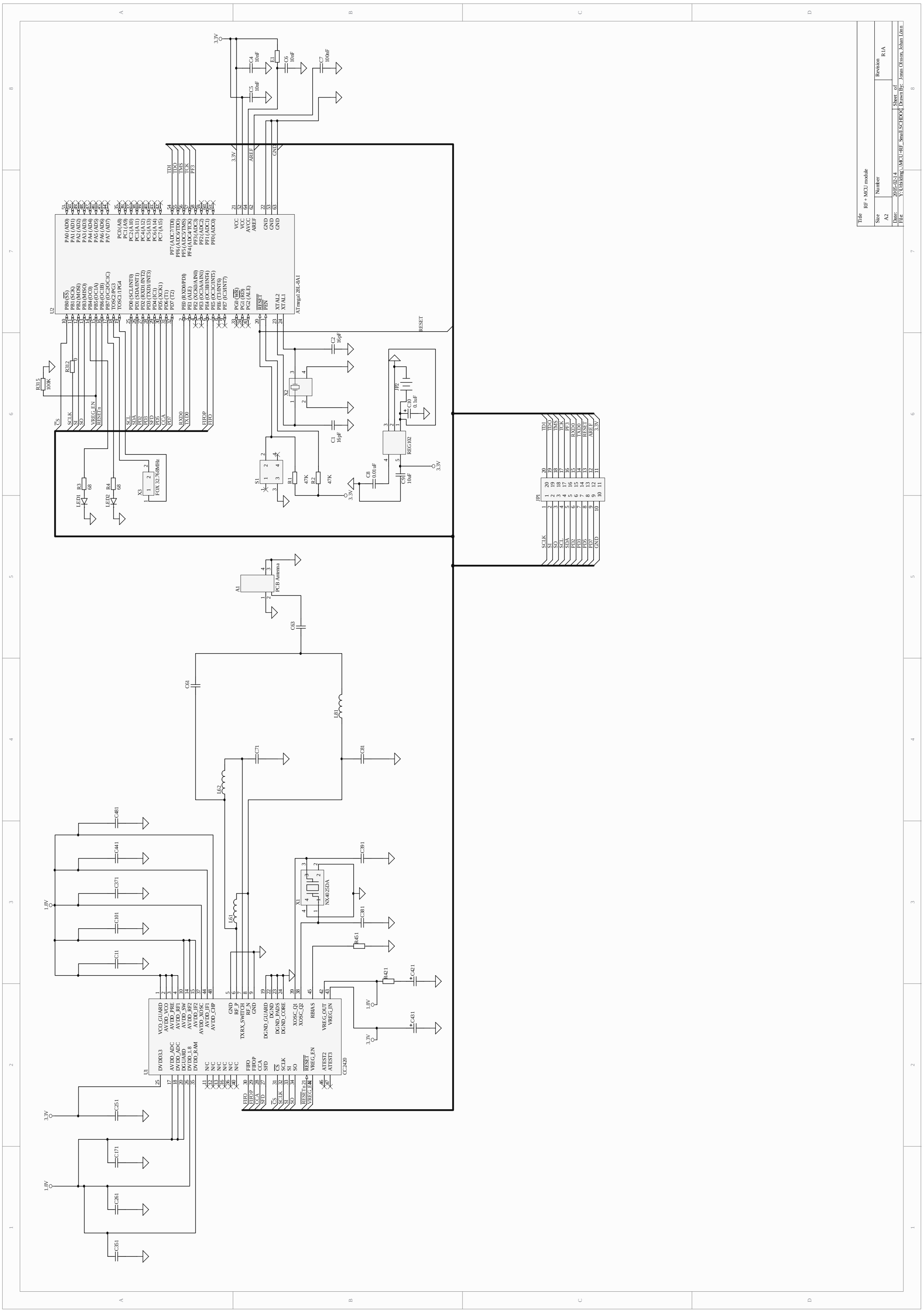


Figure C.1: Schematic of RF+MCU module

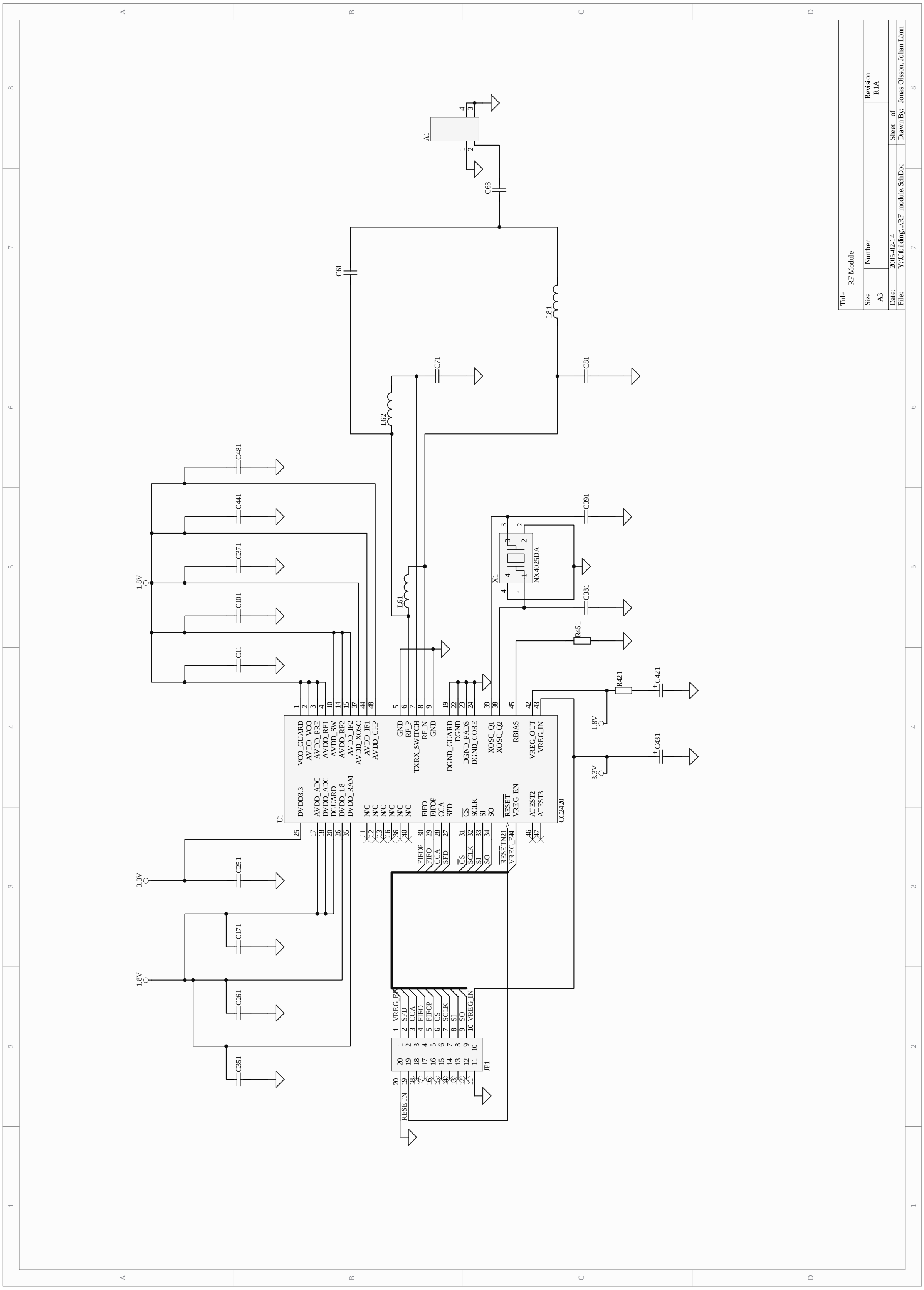



Figure C.2: Schematic of RF module

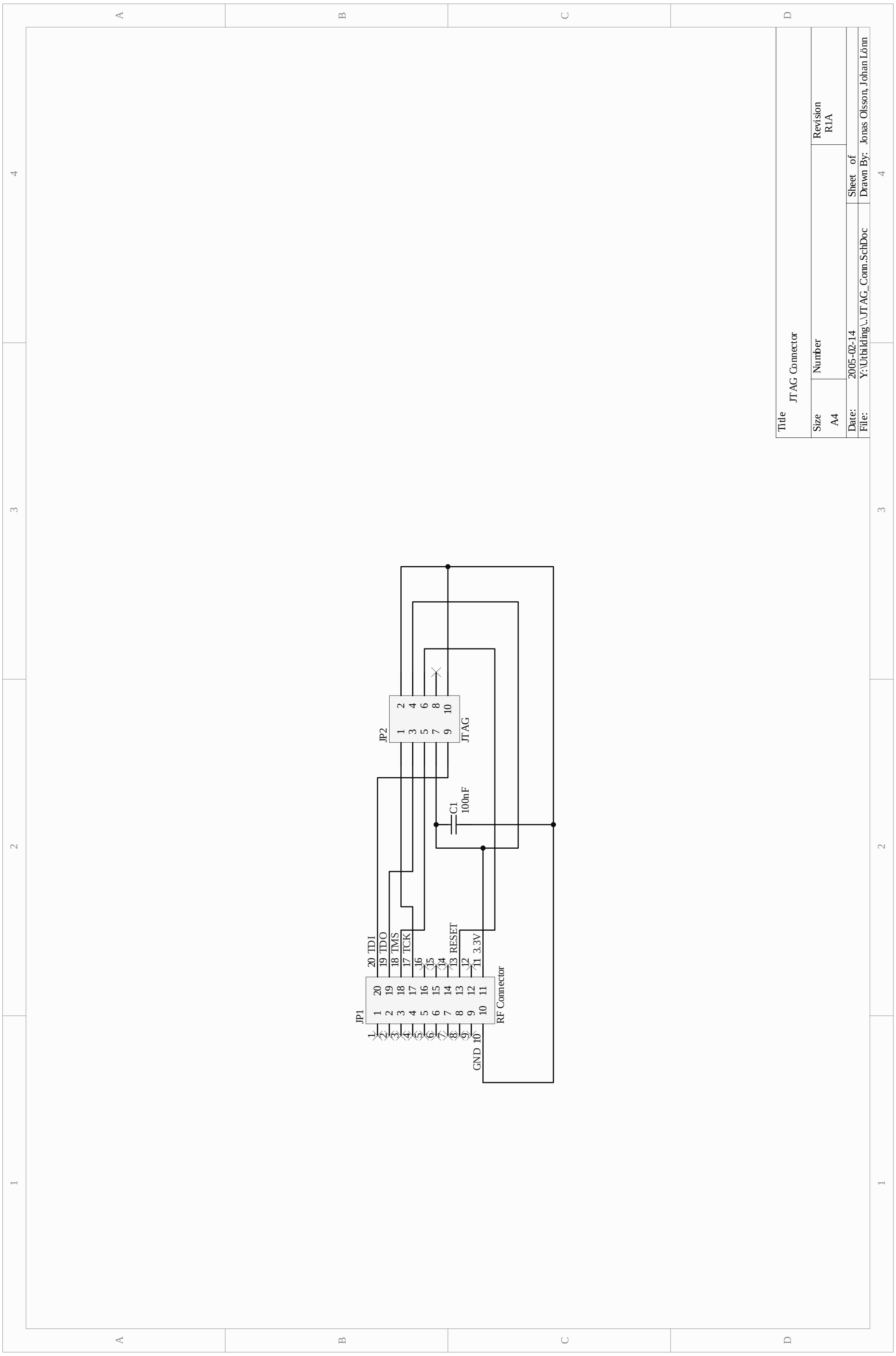



Figure C.3: Schematic of JTAG connector

# Appendix D

# Bill of Material

The Bill of Material for the two different modules is presented here.

**Report Generated From DXP**

| Description | Designator | Footprint | LibRef | Quantity | Value |
|---|---|---|---|---|---|
| SMD Antenna Mica | A1 | PCB_Antenna_Mica | PCB Antenna Mica | 1 | |
| Capacitor (Semiconductor SIM Model) | C1 | CC1005-0402 | Cap Semi | 1 | 16pF |
| Capacitor (Semiconductor SIM Model) | C2 | CC1005-0402 | Cap Semi | 1 | 16pF |
| Capacitor (Semiconductor SIM Model) | C4 | CC1005-0402 | Cap Semi | 1 | 10nF |
| Capacitor (Semiconductor SIM Model) | C5 | CC1005-0402 | Cap Semi | 1 | 10nF |
| Capacitor (Semiconductor SIM Model) | C6 | CC1005-0402 | Cap Semi | 1 | 10nF |
| Capacitor (Semiconductor SIM Model) | C7 | CC1608-0603 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C8 | CC1608-0603 | Cap Semi | 1 | 0.01uF |
| Capacitor (Semiconductor SIM Model) | C9 | CC3216-1206 | Cap Semi | 1 | 10uF |
| Solid Tantalum Chip Capacitor, Standard T494 Series - Low ESR, Industrial Grade | C10 | A | T494A | 1 | 0.1uF |
| Capacitor (Semiconductor SIM Model) | C11 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C61 | CC1005-0402 | Cap Semi | 1 | 0.5pF |
| Capacitor (Semiconductor SIM Model) | C63 | CC1005-0402 | Cap Semi | 1 | 5.6pF |
| Capacitor (Semiconductor SIM Model) | C71 | CC1005-0402 | Cap Semi | 1 | 5.6pF |
| Capacitor (Semiconductor SIM Model) | C81 | CC1005-0402 | Cap Semi | 1 | 0.5pF |
| Capacitor (Semiconductor SIM Model) | C101 | CC1005-0402 | Cap Semi | 1 | 10nF |
| Capacitor (Semiconductor SIM Model) | C171 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C251 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C261 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C351 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C371 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C381 | CC1005-0402 | Cap Semi | 1 | 27pF |
| Capacitor (Semiconductor SIM Model) | C391 | CC1005-0402 | Cap Semi | 1 | 27pF |
| Polarized Capacitor (Surface Mount) | C421 | CC2012-0805 | Cap Pol3 | 1 | 10u |
| Polarized Capacitor (Surface Mount) | C431 | CC2012-0805 | Cap Pol3 | 1 | 10u |
| Capacitor (Semiconductor SIM Model) | C441 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C481 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Semiconductor Resistor | E1 | CR1005-0402 | Res Semi | 1 | 1K |
| HRS Connector | JP1 | HRS_conn20b_header | HRS DF17 Conn20 | 1 | |
| Multicell Battery | JP2 | BAT-2 | Battery | 1 | |
| Inductor | L61 | C1005-0402 | Inductor | 1 | 7.5nH |
| Inductor | L62 | C1005-0402 | Inductor | 1 | 5.6nH |
| Inductor | L81 | C1005-0402 | Inductor | 1 | 7.5nH |
| LED | LED1 | LiteOn_LED_0603 | LiteOn | 1 | |
| LED | LED2 | LiteOn_LED_0603 | LiteOn | 1 | |
| Semiconductor Resistor | R1 | CR1005-0402 | Res Semi | 1 | 47K |
| Semiconductor Resistor | R2 | CR1005-0402 | Res Semi | 1 | 47K |
| Semiconductor Resistor | R3 | CR1005-0402 | Res Semi | 1 | 68 |
| Semiconductor Resistor | R4 | CR1005-0402 | Res Semi | 1 | 68 |
| Semiconductor Resistor | R312 | CR1005-0402 | Res Semi | 1 | 0 |
| Semiconductor Resistor | R315 | CR1005-0402 | Res Semi | 1 | 100K |
| Semiconductor Resistor | R421 | CR1608-0603 | Res Semi | 1 | 2ohm |
| Semiconductor Resistor | R451 | CR1005-0402 | Res Semi | 1 | 43K |
| Regulator 3.3V Texas Instrument | REG102 | SO-G5/P.95 | REG102 | 1 | |
| Pushbutton, ALPS, 6x6mm | S1 | Switch | SKHUAF_ALPS | 1 | |
| RF Transceiver | U1 | CC2420 | CC2420 | 1 | |
| 8-Bit AVR Microcontroller | U2 | QFN9X9-64 | ATmega128L-8AI | 1 | |

*februari 14, 2005 4:45:12 PM* *Page 1 of 2*

Figure D.1: The BOM for the RF+MCU module

| Description | Designator | Footprint | LibRef | Quantity | Value |
|---|---|---|---|---|---|
| Crystal NX4025DA | X1 | NDK_NX4025 | NX4025DA | 1 | |
| SMD Quartz Crystal 8.000 MHz | X2 | 12SMXB | 12SMXB | 1 | |
| RTC Clock | X3 | FOX FSN327 | FOX FSN327 | 1 | |

februari 14, 2005 4:45:13 PM

Page 2 of 2

Figure D.2: The BOM for the RF+MCU module

## Report Generated From DXP

| Description | Designator | Footprint | LibRef | Quantity | Value |
|---|---|---|---|---|---|
| SMD Antenna Mica | A1 | PCB_Antenna_Mica | PCB Antenna Mica | 1 | |
| Capacitor (Semiconductor SIM Model) | C11 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C61 | CC1005-0402 | Cap Semi | 1 | 0.5pF |
| Capacitor (Semiconductor SIM Model) | C63 | CC1005-0402 | Cap Semi | 1 | 5.6pF |
| Capacitor (Semiconductor SIM Model) | C71 | CC1005-0402 | Cap Semi | 1 | 5.6pF |
| Capacitor (Semiconductor SIM Model) | C81 | CC1005-0402 | Cap Semi | 1 | 0.5pF |
| Capacitor (Semiconductor SIM Model) | C101 | CC1005-0402 | Cap Semi | 1 | 10nF |
| Capacitor (Semiconductor SIM Model) | C171 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C251 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C261 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C351 | CC1005-0402 | Cap Semi | 1 | 100nF |
| Capacitor (Semiconductor SIM Model) | C371 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C381 | CC1005-0402 | Cap Semi | 1 | 27pF |
| Capacitor (Semiconductor SIM Model) | C391 | CC1005-0402 | Cap Semi | 1 | 27pF |
| Polarized Capacitor (Surface Mount) | C421 | CC2012-0805 | Cap Pol3 | 1 | 10u |
| Polarized Capacitor (Surface Mount) | C431 | CC2012-0805 | Cap Pol3 | 1 | 10u |
| Capacitor (Semiconductor SIM Model) | C441 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Capacitor (Semiconductor SIM Model) | C481 | CC1005-0402 | Cap Semi | 1 | 68pF |
| Connector HRS | JP1 | HRS_conn20b_header | HRS DF17 Conn20 | 1 | |
| Inductor | L61 | C1005-0402 | Inductor | 1 | 7.5nH |
| Inductor | L62 | C1005-0402 | Inductor | 1 | 5.6nH |
| Inductor | L81 | C1005-0402 | Inductor | 1 | 7.5nH |
| Semiconductor Resistor | R421 | CR1608-0603 | Res Semi | 1 | 2ohm |
| Semiconductor Resistor | R451 | CR1005-0402 | Res Semi | 1 | 43K |
| RF Transceiver | U1 | CC2420 | CC2420 | 1 | |
| Crystal NX4025DA | X1 | NDK_NX4025 | NX4025DA | 1 | |

*februari 14, 2005 4:37:38 PM* *Page 1 of 1*

Figure D.3: The BOM for the RF module

# Appendix E

# Datasheets

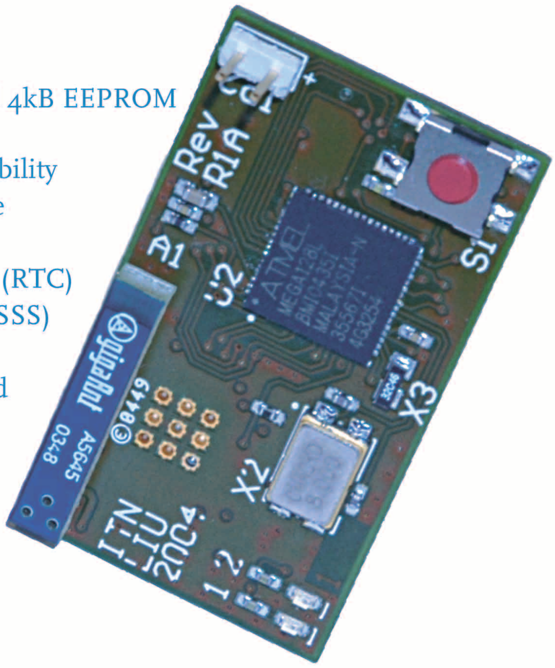
Datasheets for the two different modules.

# ZigBee™

## *ZigBee™-Ready module for wireless networking*

### *Features*

- 23 x 40 mm compact module
- IEEE 802.15.4 compliant
- 128kB Flash memory, 4kB SRAM and 4kB EEPROM
- Full Function device (FFD) and Reduced Function Device (RFD) capability
- 2 UART, SPI, TWI and JTAG interface
- 5 digital I/O ports, 5 10bit ADC ports
- On board 32.76kHz Real Time Clock (RTC)
- Direct Sequence Spread Spectrum (DSSS)
- Integral antenna
- 16 Channels in the 2.4 GHz ISM-band
- Data rate 250 kbit/s
- 2.7 - 10V power supply




### *Applications*

*Prototyping and production of:*

- Stand alone sensors
- Home and building automation
- Industrial control
- OEM equipment

### *General Description*

The ZigBee Ready module is a very compact module that is suitable for star and mesh networks based on the IEEE 802.15.4 compliant PHY and MAC layers.
The module supports both Fully Functional Device (FFD) and Reduced Functional Device (RFD).

*Linköpings Universitet*
*ITN, Norrköping*
*Communication Electronics*
*Professor, Shaofang Gong*
*Tel: +46 (0)11 363459*
*Mobile: +46 (0)73 0647836*
*E-mail: shago@itn.liu.se*
*www.comelec.itn.liu.se*

Linköpings universitet

*(Brief Datasheet Rev1.0a)* 

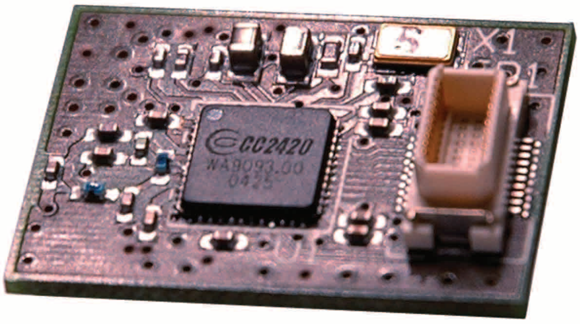
Figure E.1: Datasheet for the RF+MCU module

# ZigBee™

## *IEEE 802.15.4 Radio Module*

### *Features*

- IEEE 802.15.4-compliant PHY and MAClayer
- 18 x 25 mm compact module
- Data rate 250 kbit/s
- 16 channels in the 2.4 GHz ISM-band
- Direct Sequence Spread Spectrum (DSSS)
- Integral antenna
- SPI interface to microcontroller
- 2.1 - 3.6V power supply




### *Applications*

- *2.4 GHz IEEE 802.15.4-compatible systems*
- *ZigBee systems*
- *Home and building automation*
- *Industrial control*
- *Wireless sensor networks*

### *General description*

The IEEE 802.15.4 Radio Module can be integrated into a system using the standard Serial Peripheral Interface (SPI). Adding the module simplifies the implementation of IEEE 802.15.4 or ZigBee to an exsiting system.

*Linköpings Universitet*
*ITN, Norrköping*
*Communication Electronics*
*Professor, Shaofang Gong*
*Tel: +46 (0)11 363459*
*Mobile: +46 (0)73 0647836*
*E-mail: shago@itn.liu.se*
*www.comelec.itn.liu.se*

Linköpings universitet



Figure E.2: Datasheet for the RF module