CCC Sputnik @ Chaos Communication Camp 2007

Milosch Meriac

August 8, 2007

Contents

History

- Based on an idea how to guide pilgrims in Mecca / Saudi Arabia decrease stampede possibility
- Tracking of 1000 Tags at 23C3 congress in Berlin by setting up 23 Ethernet readers

CCC Sputnik Team

- Milosch & Brita Meriac
- Henryk Plötz
- Karsten Nohl
- Visualization by ART+COM AG team

History

- Based on an idea how to guide pilgrims in Mecca / Saudi Arabia decrease stampede possibility
- Tracking of 1000 Tags at 23C3 congress in Berlin by setting up 23 Ethernet readers

CCC Sputnik Team

- Milosch & Brita Meriac
- Henryk Plötz
- Karsten Nohl
- Visualization by ART+COM AG team

Motivation & Implementation

Motivation

- gather experience with 2.4GHz PCB layout
- establish a free and open RFID design for more transparency
- evaluating possibilities and acceptancy of surveillance and data mining
- create a generic platform for *cheap* high performance 2.4GHz comminication

Chaos Communication Camp 2007 Setup

- 10 Ethernet based readers mainly in shelters and villages
- 30 Rating Nodes (battery powered to enable rating of locations around the camp)
- 500 Sputnik RFID tags can be bought at Art&Beauty shelter for 15,-EUR each starting on second day

Motivation & Implementation

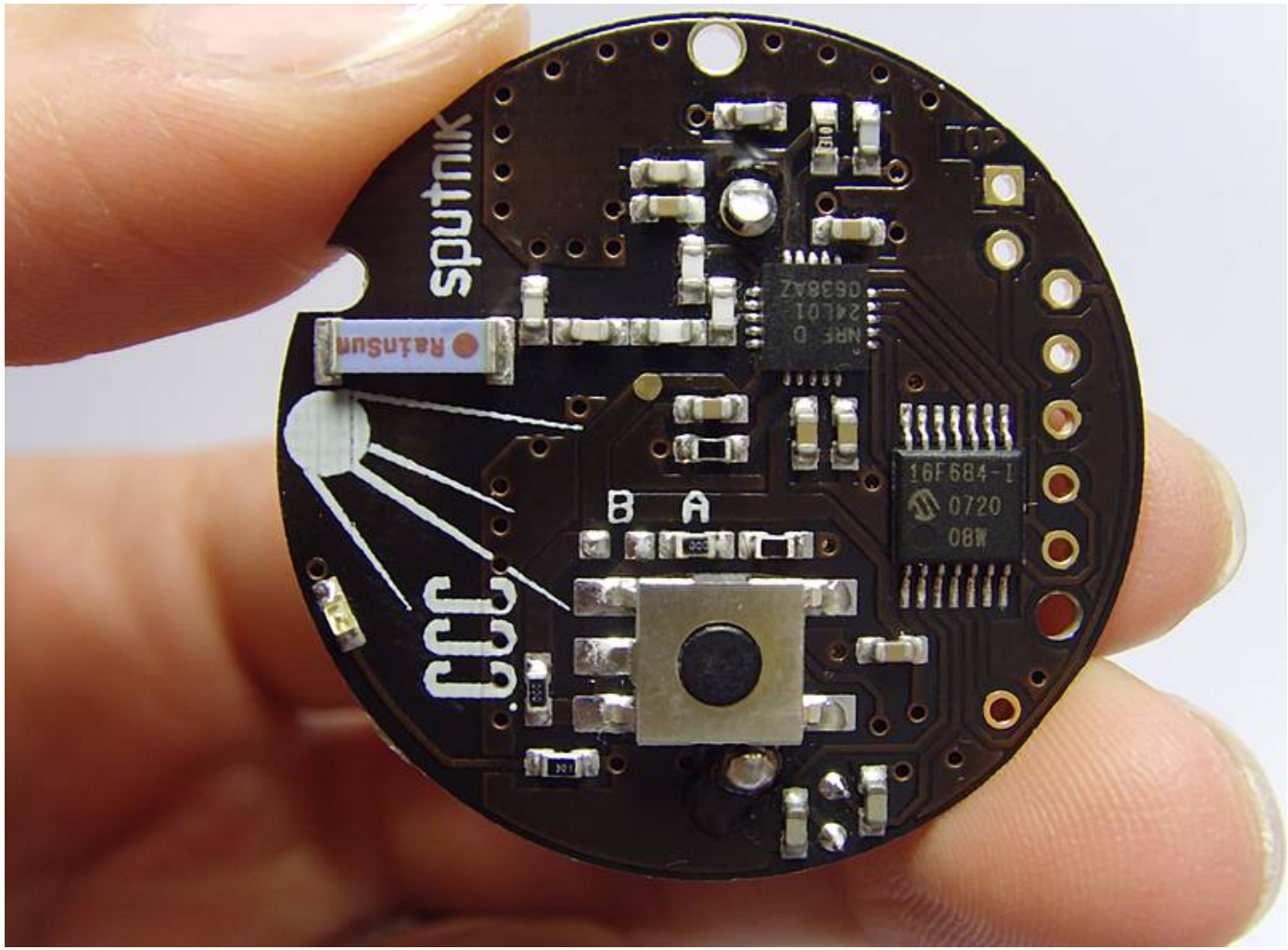
Motivation

- gather experience with 2.4GHz PCB layout
- establish a free and open RFID design for more transparency
- evaluating possibilities and acceptancy of surveillance and data mining
- create a generic platform for *cheap* high performance 2.4GHz comminication

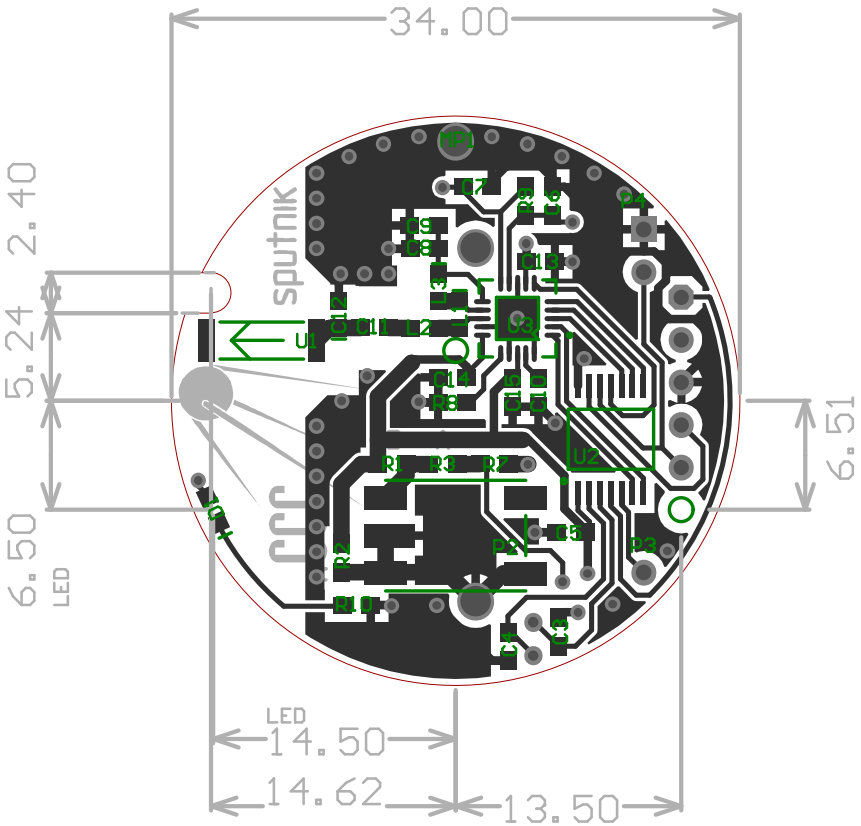
Chaos Communication Camp 2007 Setup

- 10 Ethernet based readers mainly in shelters and villages
- 30 Rating Nodes (battery powered to enable rating of locations around the camp)
- 500 Sputnik RFID tags can be bought at Art&Beauty shelter for 15,-EUR each starting on second day

Sputnik Tag



Sputnik PCB Layout



Sputnik Tag Hardware

- reprogrammable PIC16F684 microprocessor
- nRF24L01 2.4GHz Frontend for bidirectional communication
- 2MBit halfduplex receive & transmit at 2MHz bandwidth (100 channels)

Sputnik Tag Hardware

- reprogrammable PIC16F684 microprocessor
- nRF24L01 2.4GHz Frontend for bidirectional communication
- 2MBit halfduplex receive & transmit at 2MHz bandwidth (100 channels)
- CR2032 lithium ion battery as power supply
- push button for interaction
- prepared for piezo buzzer

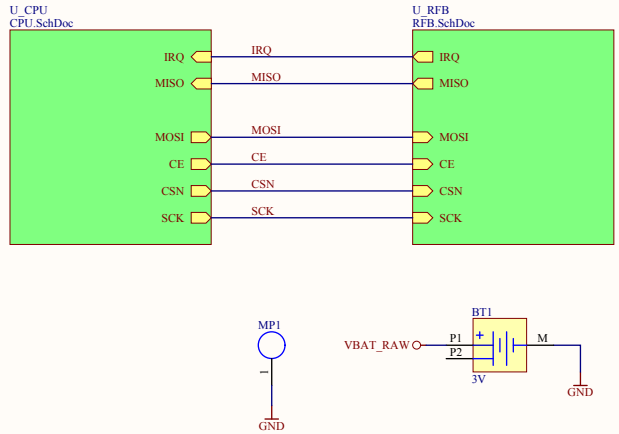
Sputnik Tag Hardware

- reprogrammable PIC16F684 microprocessor
- nRF24L01 2.4GHz Frontend for bidirectional communication
- 2MBit halfduplex receive & transmit at 2MHz bandwidth (100 channels)
- CR2032 lithium ion battery as power supply
- push button for interaction
- prepared for piezo buzzer

Sputnik Tag Circuit - Overview

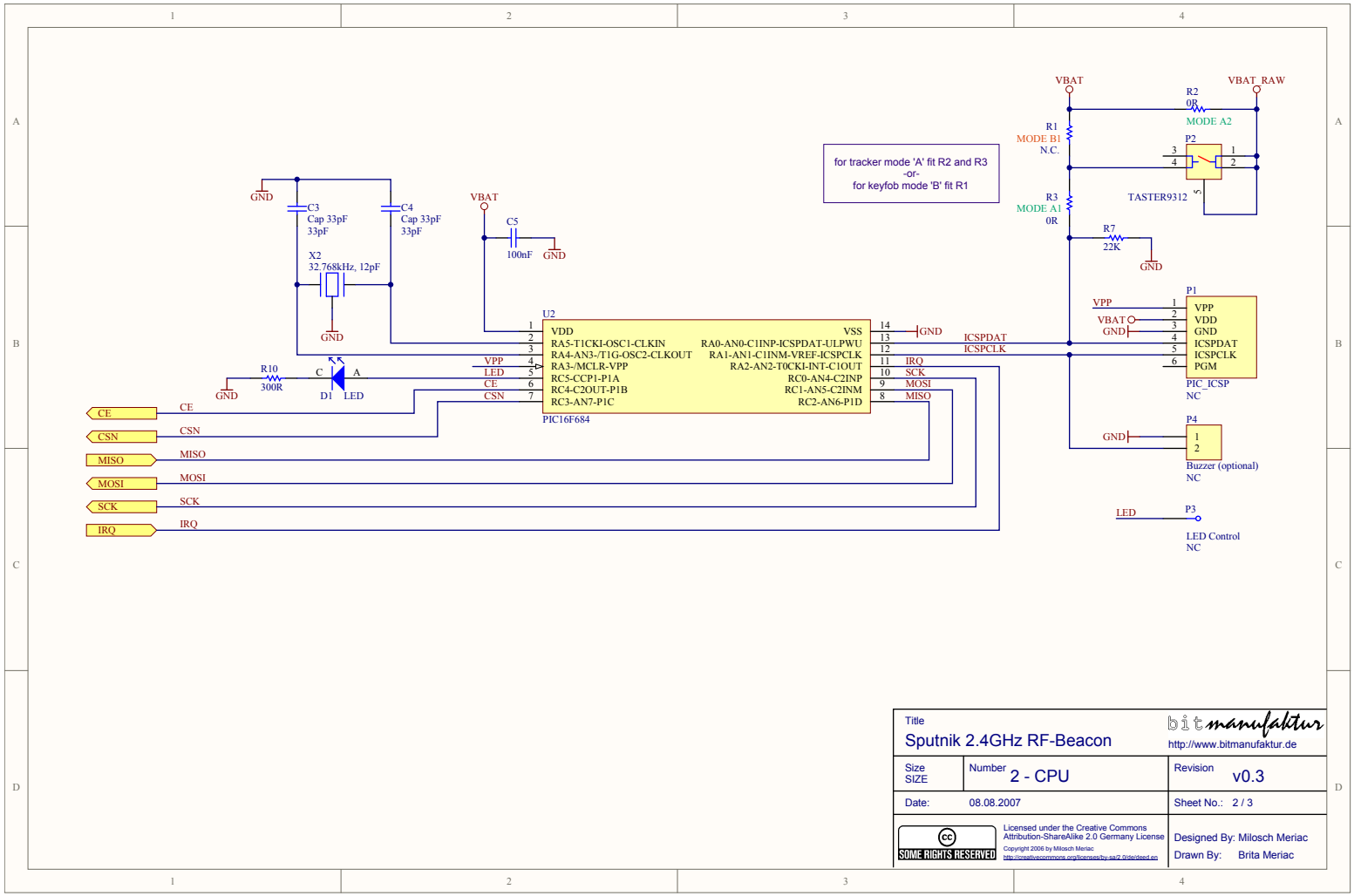
CCC Sputnik

Active 2.4GHz RFID Tag

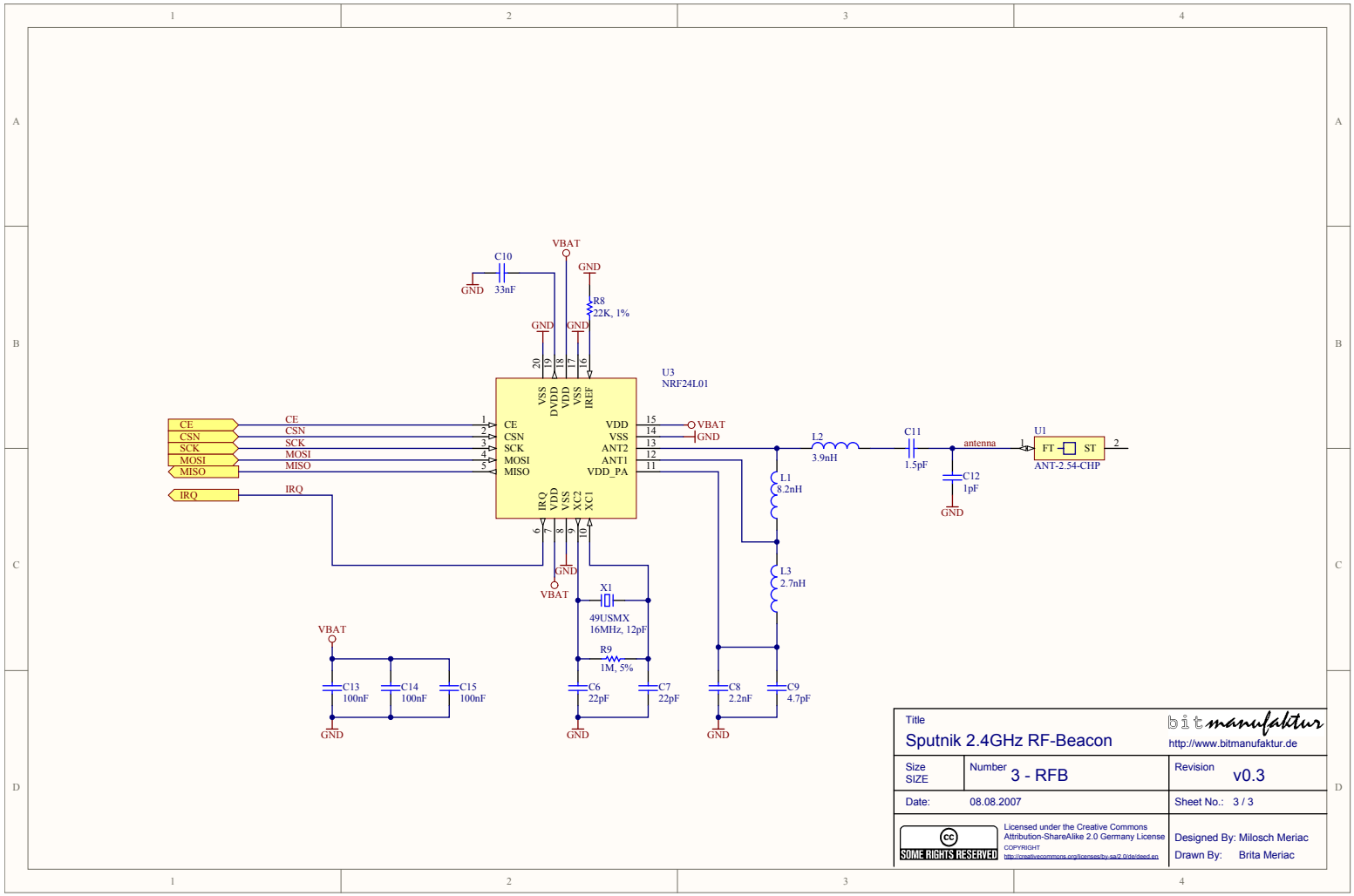


Title: Sputnik 2.4GHz RF-Beacon		bitmanufaktur http://www.bitmanufaktur.de
Size: SIZE	Number: 1 - TOP	Revision: v0.3
Date: 08.08.2007		Sheet No.: 1 / 3
SOME RIGHTS RESERVED	Licensed under the Creative Commons Attribution-ShareAlike 2.0 Germany License	Designed By: Milosch Meriac Drawn By: Brita Meriac

Sputnik Tag Circuit - Prozessor



Sputnik Tag Circuit - 2.4GHz Frontend



Sputnik Functionality

- every Tag transmits six to eight times per second
- a pseudo random generator seeded with a fixed random seed reduces the possibility of packet collosions
- transmit power cycles throug 4 power levels (n*0x55)
- packet loss per power level is used for distance estimation
- packets are transmitted on two channels seperately at two different intervals (channel A/B).
- on channel A packets are transmitted 4 times as often as on channel B

Sputnik Privacy

- replay attacks of encrypted packets are inhibited by using a incrementing sequence number
- because of privacy reasons every packet is XXTEA block encrypted by using a 128bit shared key
- beacause of changing sequence number and encryption practically every packet is totally different
- shared key is protected by CPU copy protection bits
- encrypted packets will be forwarded by an ethernet based readers to a aggregator server where they will be decrypted
- data gathering therefore can be only done by the owner of the tracking system. sniffing packets doesn't help.

Sputnik Privacy

- replay attacks of encrypted packets are inhibited by using a incrementing sequence number
- because of privacy reasons every packet is XXTEA block encrypted by using a 128bit shared key
- beacause of changing sequence number and encryption practically every packet is totally different
- shared key is protected by CPU copy protection bits
- encrypted packets will be forwarded by an ethernet based readers to a aggregator server where they will be decrypted
- data gathering therefore can be only done by the owner of the tracking system. sniffing packets doesn't help.

Prerequisites

- PICkit 2 Programmer (40EUR @ microchip.com / Part Number PG164120)
- HI-TECH PICC-Lite Compiler(free @ htsoft.com) - we will port Firmware to SDCC - Small Device C Compiler at http://sdcc.sourceforge.net/ during next weeks
- average C-compiler skills

Prerequisites

- PICkit 2 Programmer (40EUR @ microchip.com / Part Number PG164120)
- HI-TECH PICC-Lite Compiler(free @ htsoft.com) - we will port Firmware to SDCC - Small Device C Compiler at http://sdcc.sourceforge.net/ during next weeks
- average C-compiler skills
- time

Prerequisites

- PICkit 2 Programmer (40EUR @ microchip.com / Part Number PG164120)
- HI-TECH PICC-Lite Compiler(free @ htsoft.com) - we will port Firmware to SDCC - Small Device C Compiler at http://sdcc.sourceforge.net/ during next weeks
- average C-compiler skills
- time

Porting code to different processors

- replace atomic functions for toggeling & reading the few SPI pins
- have a look at OpenBeacon USB firmware for layered API
- nRF24L01 datasheet is pretty readable - highly suggested if porting code

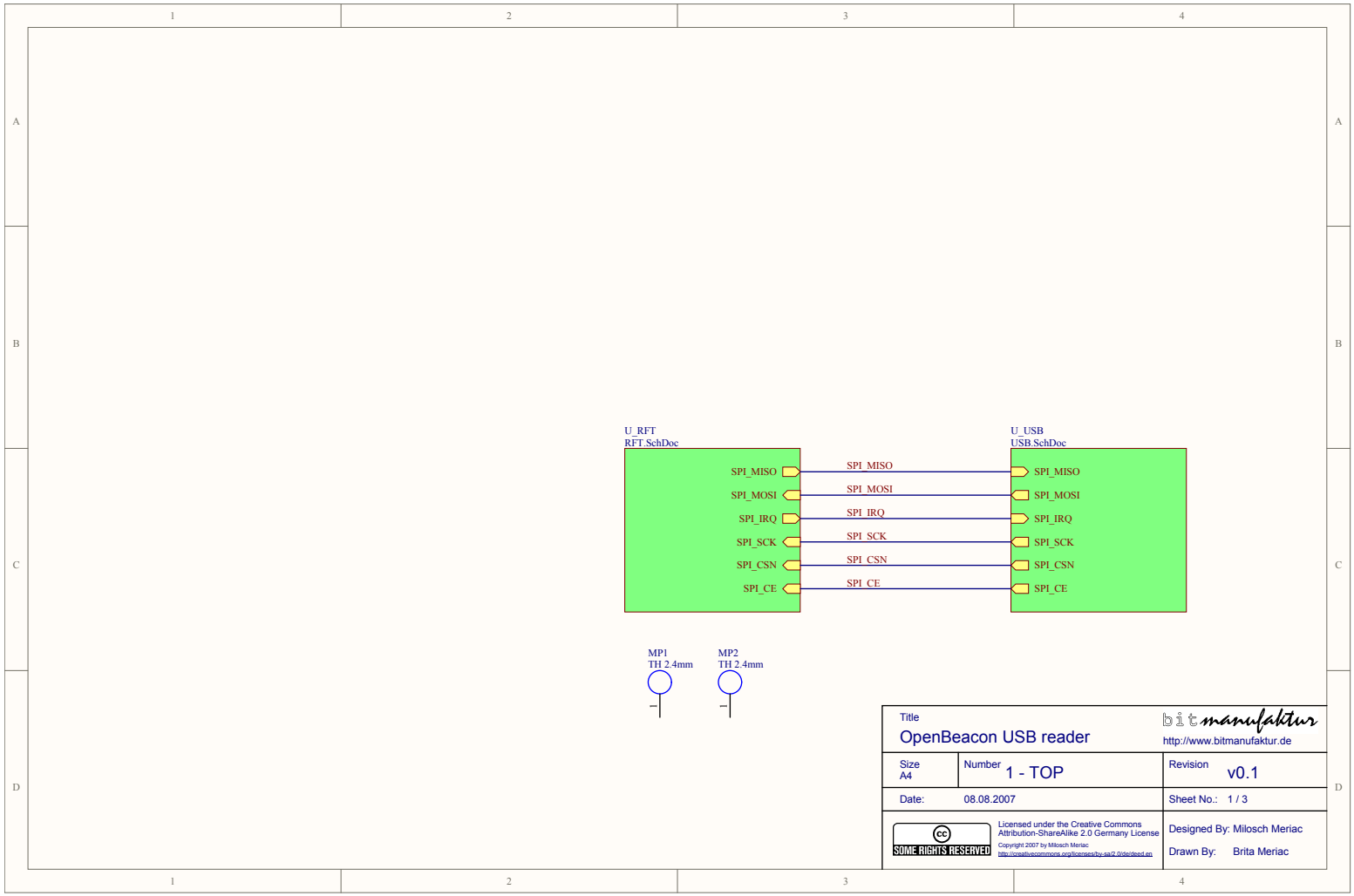
OpenBeacon USB

Figure: autonomous base station

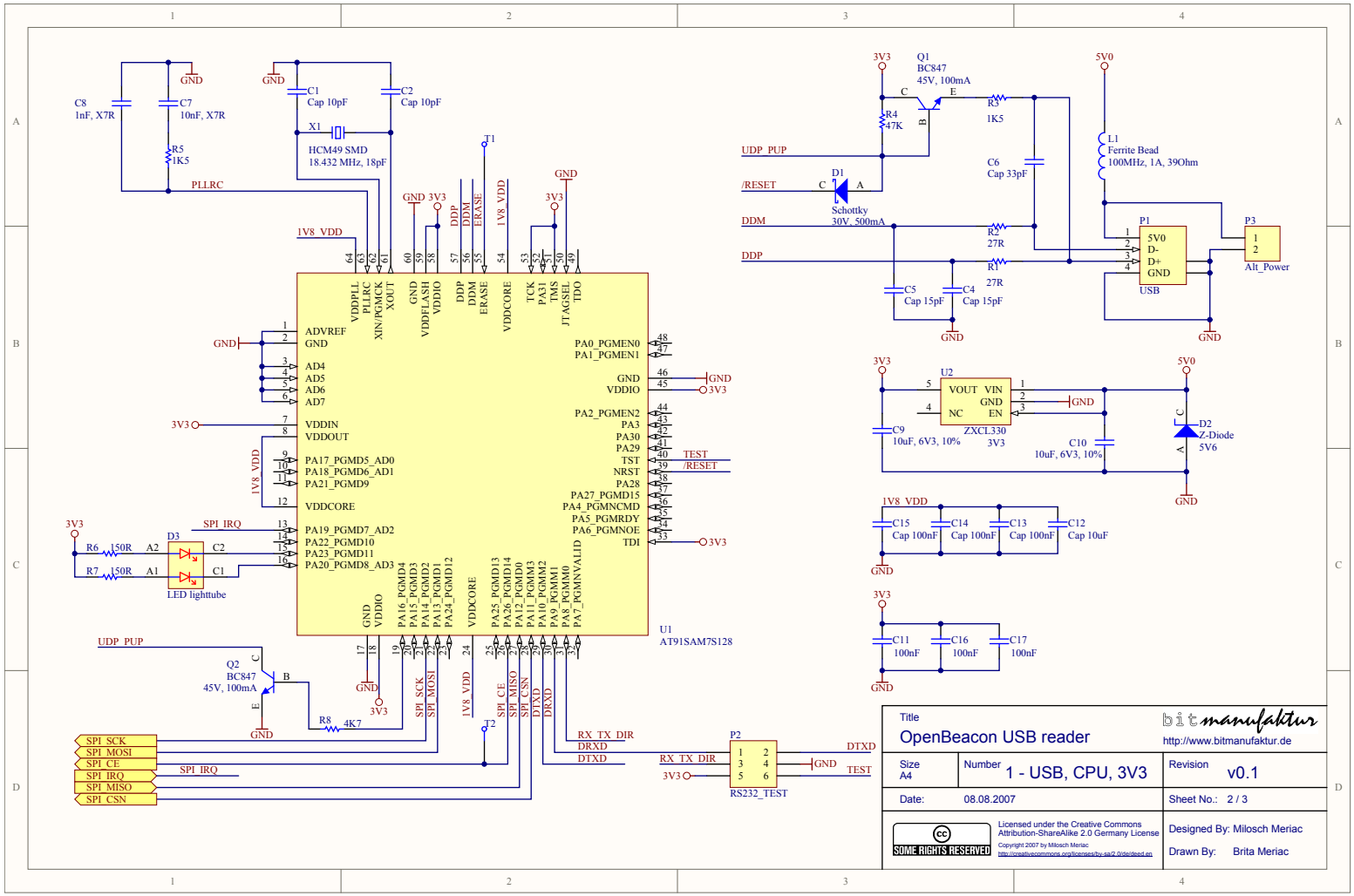
OpenBeacon USB Node Hardware

- very convenient AT91SAM7S128 32 bit ARM processr
- 32kB RAM / 128kB Flash
- again nRF24L01 2.4GHz Frontend
- USB device interface for powering and reprogramming device
- 6 pin header for user extensions: RS232@3.3V serial port
- fully DMA accelerated nRF24L01 for high speed data
- can handle easily 2000 Packets per second
- hardware acceleration for accurate frequency hopping
- nice blinking LED's

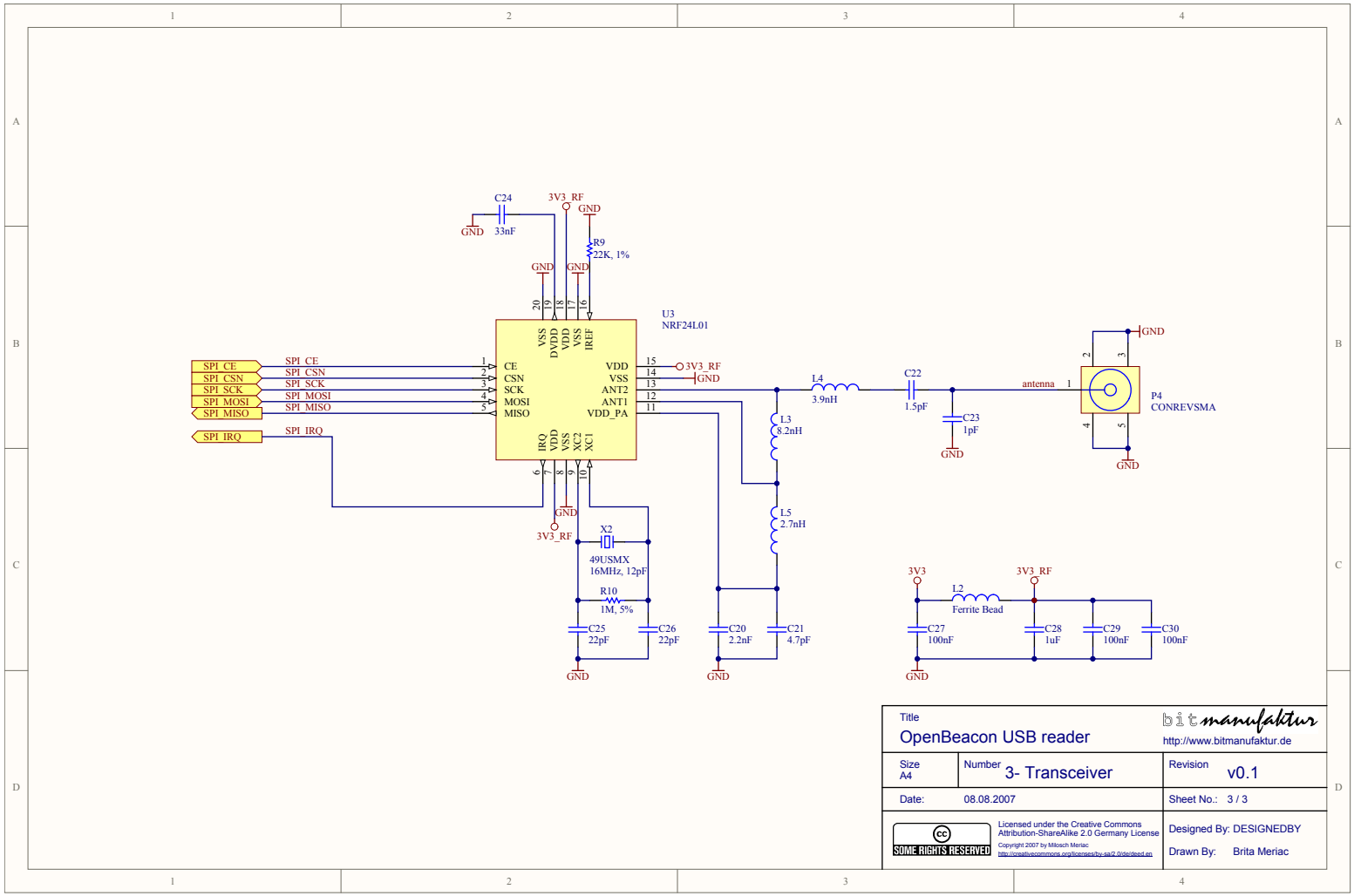
OpenBeacon USB Circuit - Overview



OpenBeacon USB Circuit - CPU



OpenBeacon USB Circuit - 2.4GHz Frontend



Hands on OpenBeacon

- no additional hardware needed for reprogramming OpenBeacon USB
- can be reprogrammed over USB under Linux & Windows
- not brickable - you can always revert to a failsafe USB boot loader
- freely available GNU GCC ARM toolchain - great !
- FreeRTOS used as realtime operation system - loads of documentation available
- emulates a serial port over USB - ASCII terminal software for configuring reader
- Virtual Serial Port recognized out-of-the-box in Linux (modprobe usbserial)
- Multitasking, Queuing & Locking implmented

Tags sightings per base station

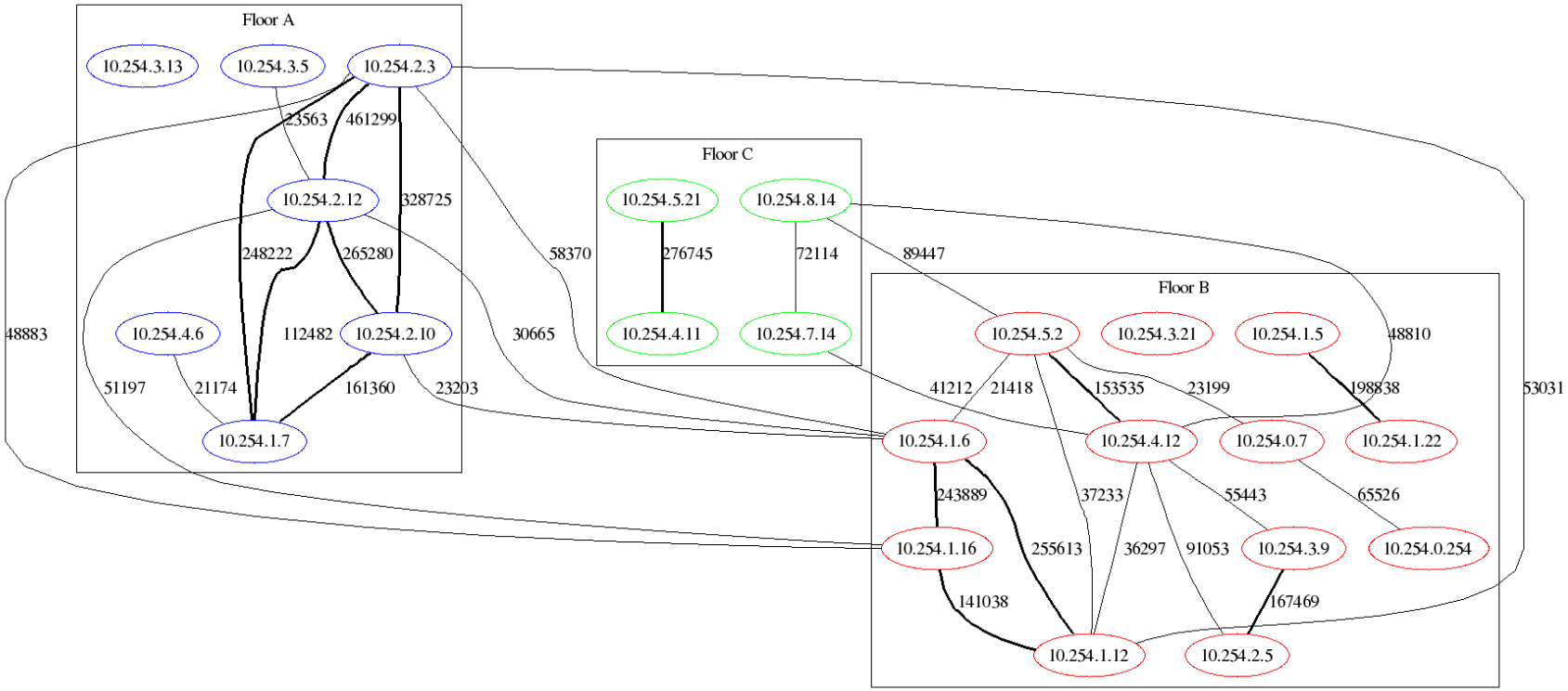


Figure: Peter Meerwald's great analysis (http://pmeerw.net/23C3_Sputnik/)

Andy Greens Webfrontend & Aggregator

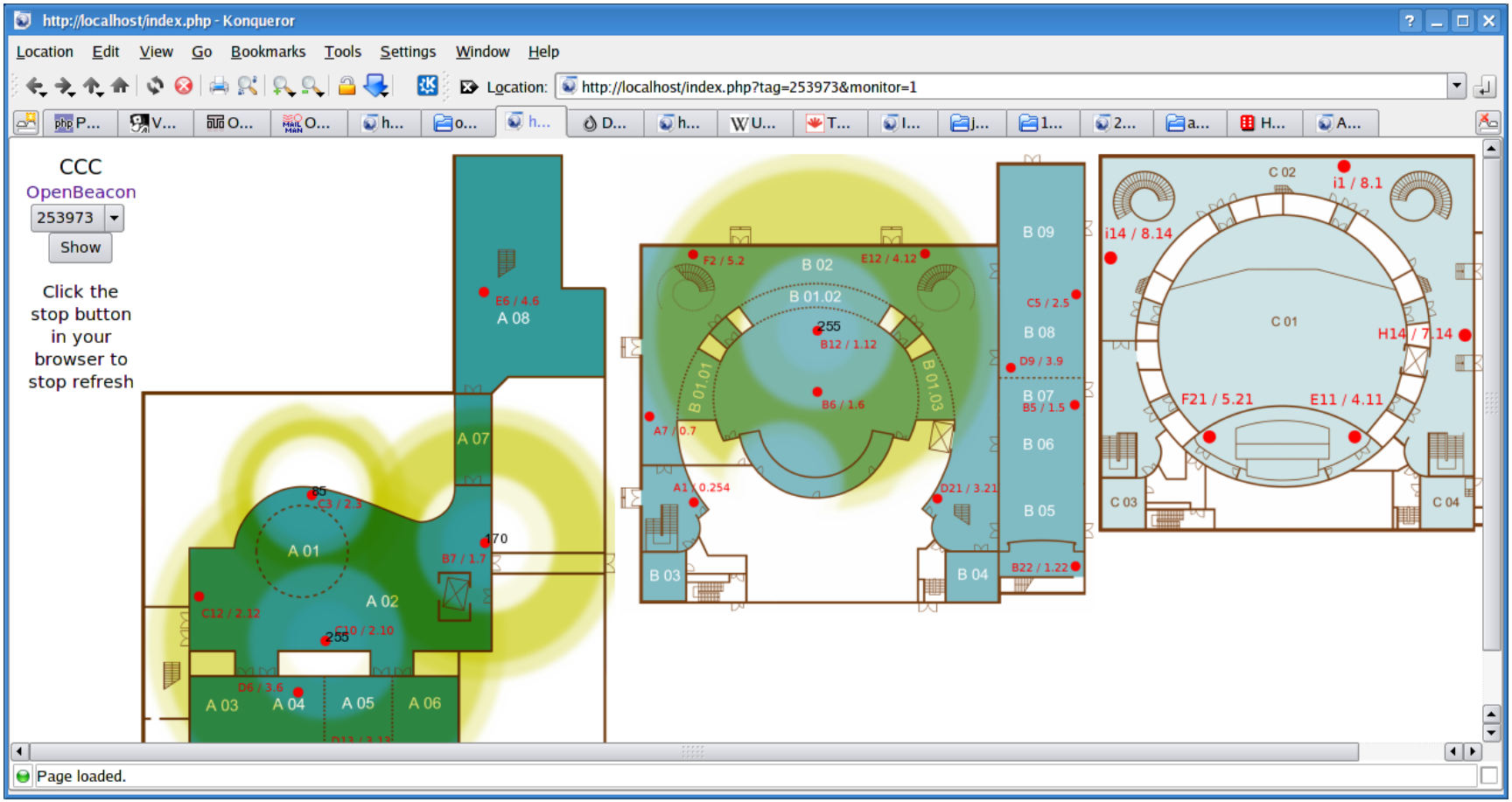


Figure: single Tag and receive strength of surrounding readers

Andy Greens Webfrontend

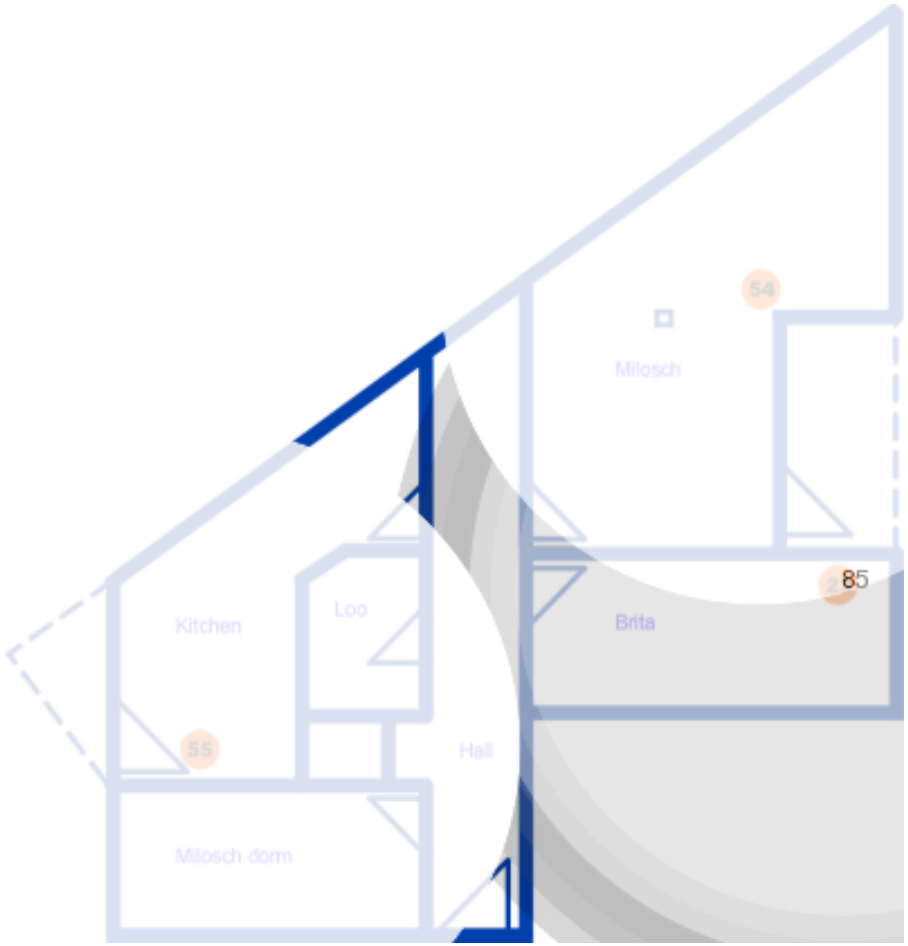


Figure: our flat - prototype for graphical position estimation

802.3af Power Over Ethernet Reader

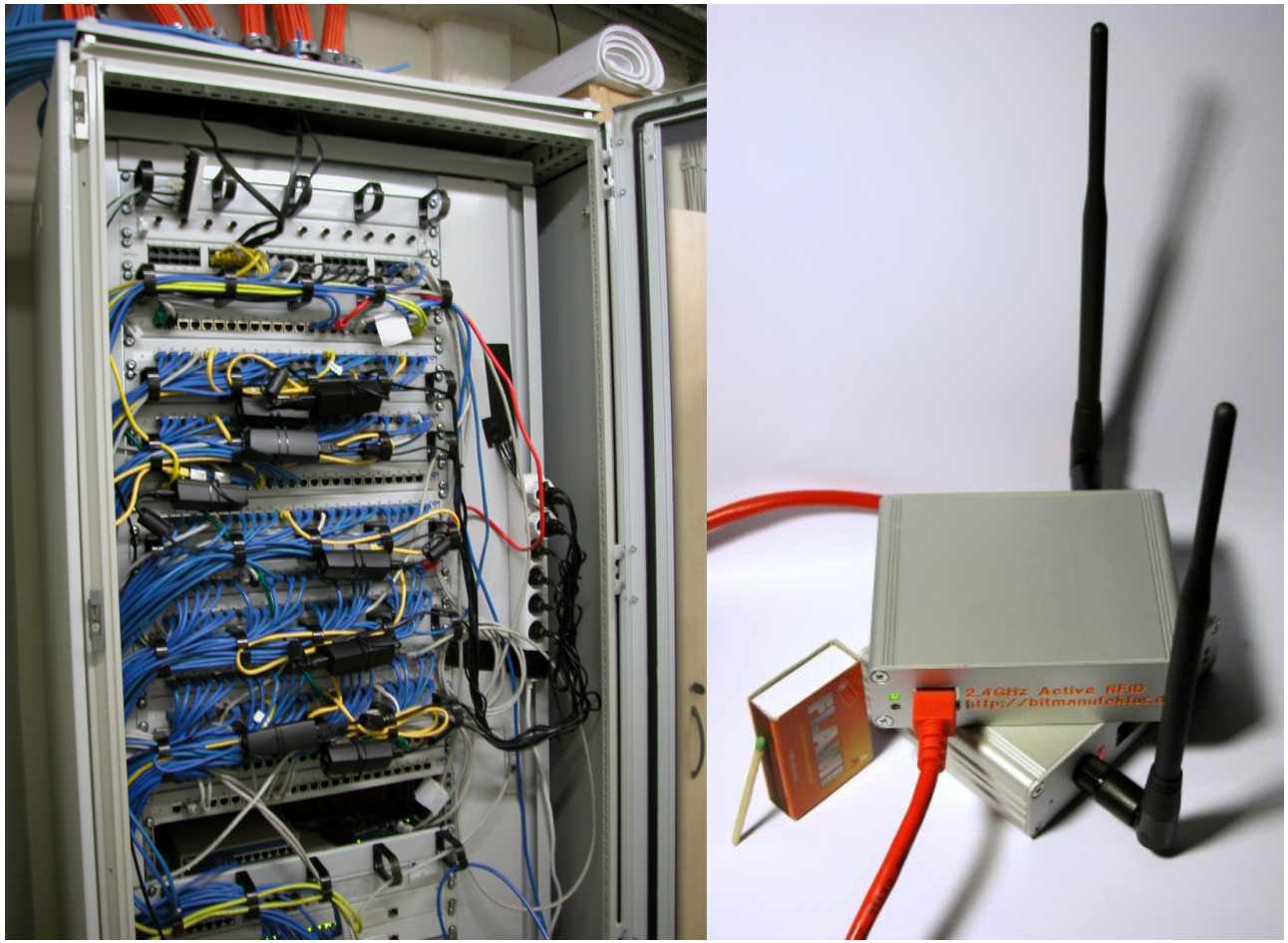


Figure: PoE powered Ethernet reader

Summary

Monitoring is accepted if ...

- ... user have immediate benefits
- ... enveryone can freely decide where & when
- ... users accepts what happens with the data

Links

- Free active 2.45 GHz Active RFID design: http://www.openbeacon.org
- Free 13.56MHz RFID reader/writer design: http://www.openpcd.org
- nRF24L01 2.4GHz transceiver: http://nvlsi.no
- PIC16F84: http://ww1.microchip.com/downloads/en/DeviceDoc/41202F-print.pdf

Summary

Monitoring is accepted if ...

- ... user have immediate benefits
- ... enveryone can freely decide where & when
- ... users accepts what happens with the data

Links

- Free active 2.45 GHz Active RFID design: http://www.openbeacon.org
- Free 13.56MHz RFID reader/writer design: http://www.openpcd.org
- nRF24L01 2.4GHz transceiver: http://nvlsi.no
- PIC16F84: http://ww1.microchip.com/downloads/en/DeviceDoc/41202F-print.pdf