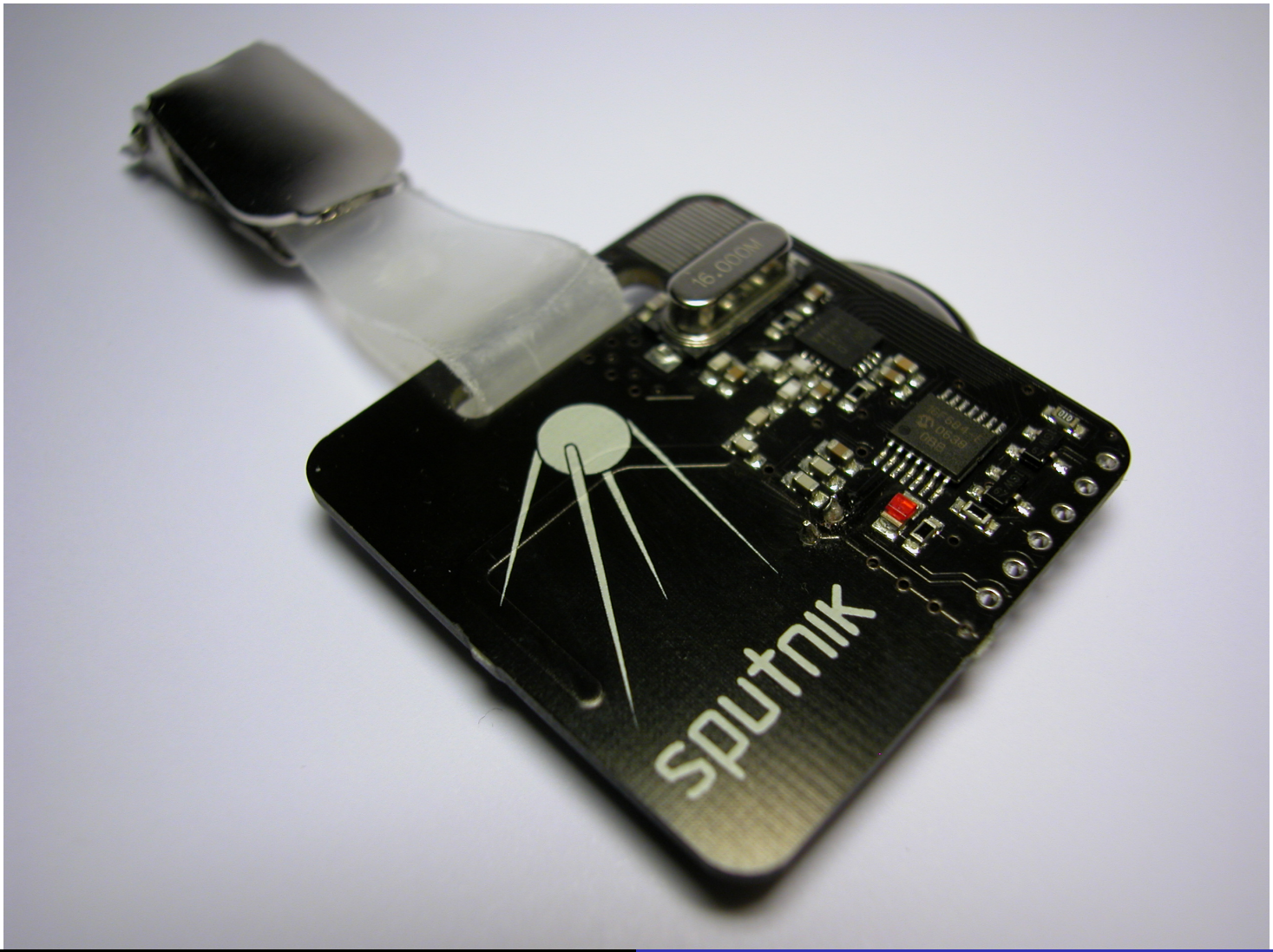
# CCC Sputnik @ datenspuren 2007

Milosch Meriac, Brita Meriac

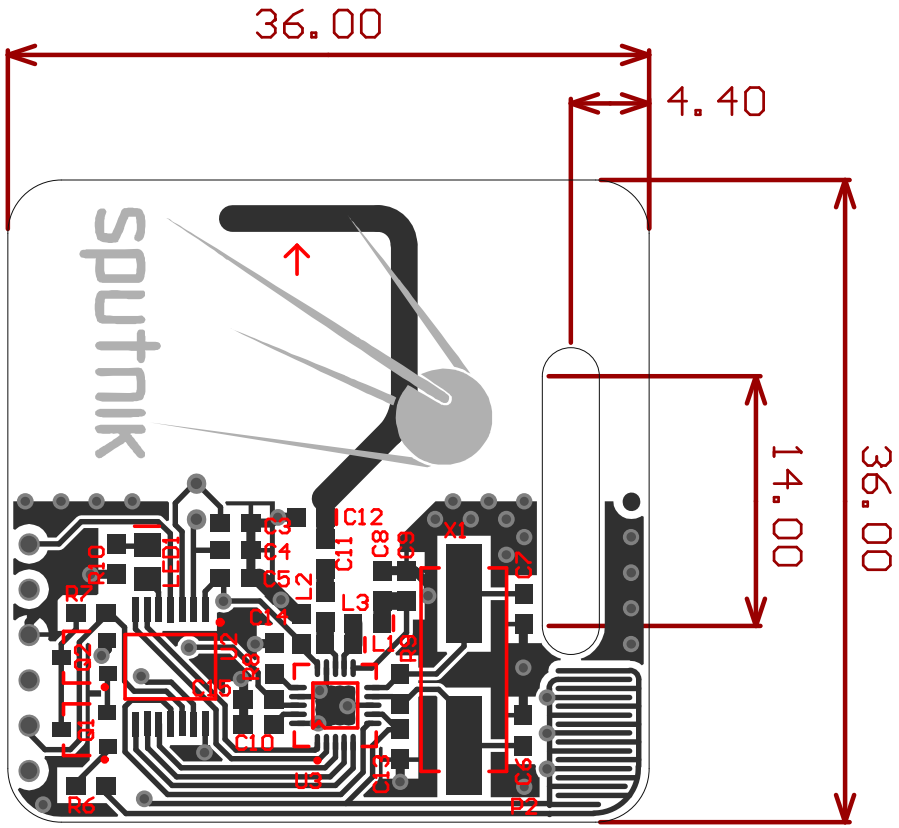
6. Mai 2007

# Inhalt

# Sputnik Tag



# Sputnik Platinenlayout



# Sputnik Hardwareaufbau

- reprogrammierbarer PIC16F684 Prozessor
- nRF24L01 2.4GHz Frontend für bidirektionale Kommunikation
- 2MBit halbduplex mit 2MHz Bandbreite (100 Kanäle)

# Sputnik Hardwareaufbau

- reprogrammierbarer PIC16F684 Prozessor
- nRF24L01 2.4GHz Frontend für bidirektionale Kommunikation
- 2MBit halbduplex mit 2MHz Bandbreite (100 Kanäle)
- CR2032 Knopfzelle als Stromversorgung
- Touchsensor für Interaktion

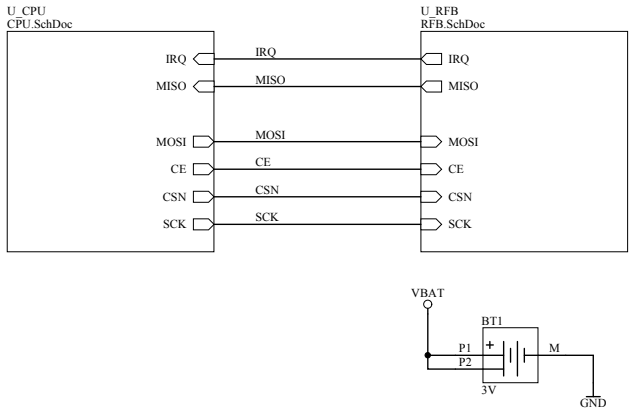
# Sputnik Hardwareaufbau

- reprogrammierbarer PIC16F684 Prozessor
- nRF24L01 2.4GHz Frontend für bidirektionale Kommunikation
- 2MBit halbduplex mit 2MHz Bandbreite (100 Kanäle)
- CR2032 Knopfzelle als Stromversorgung
- Touchsensor für Interaktion

# Sputnik Schaltplan - Übersicht

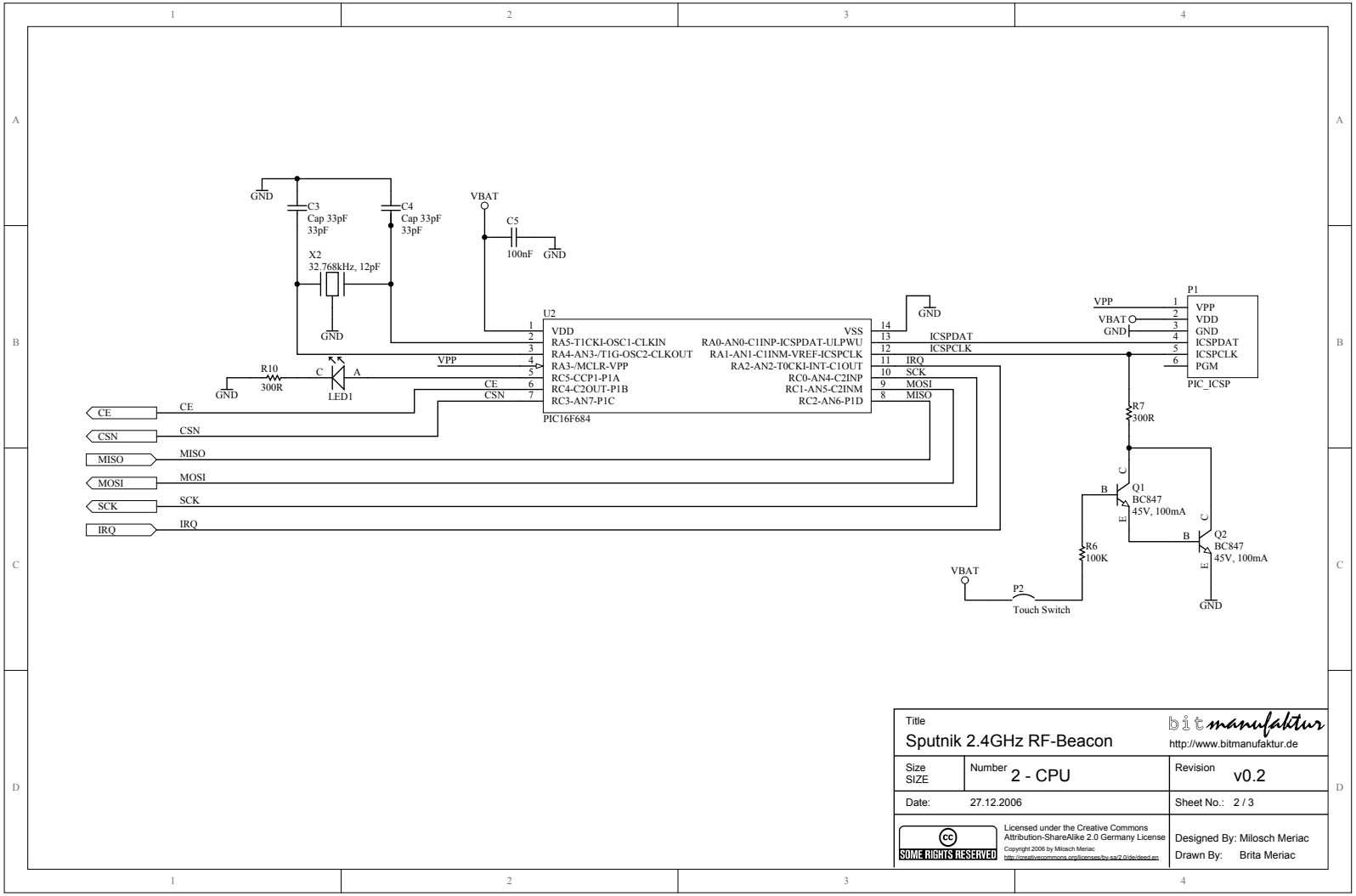
**CCC Sputnik**

Active 2.4GHz RFID Tag

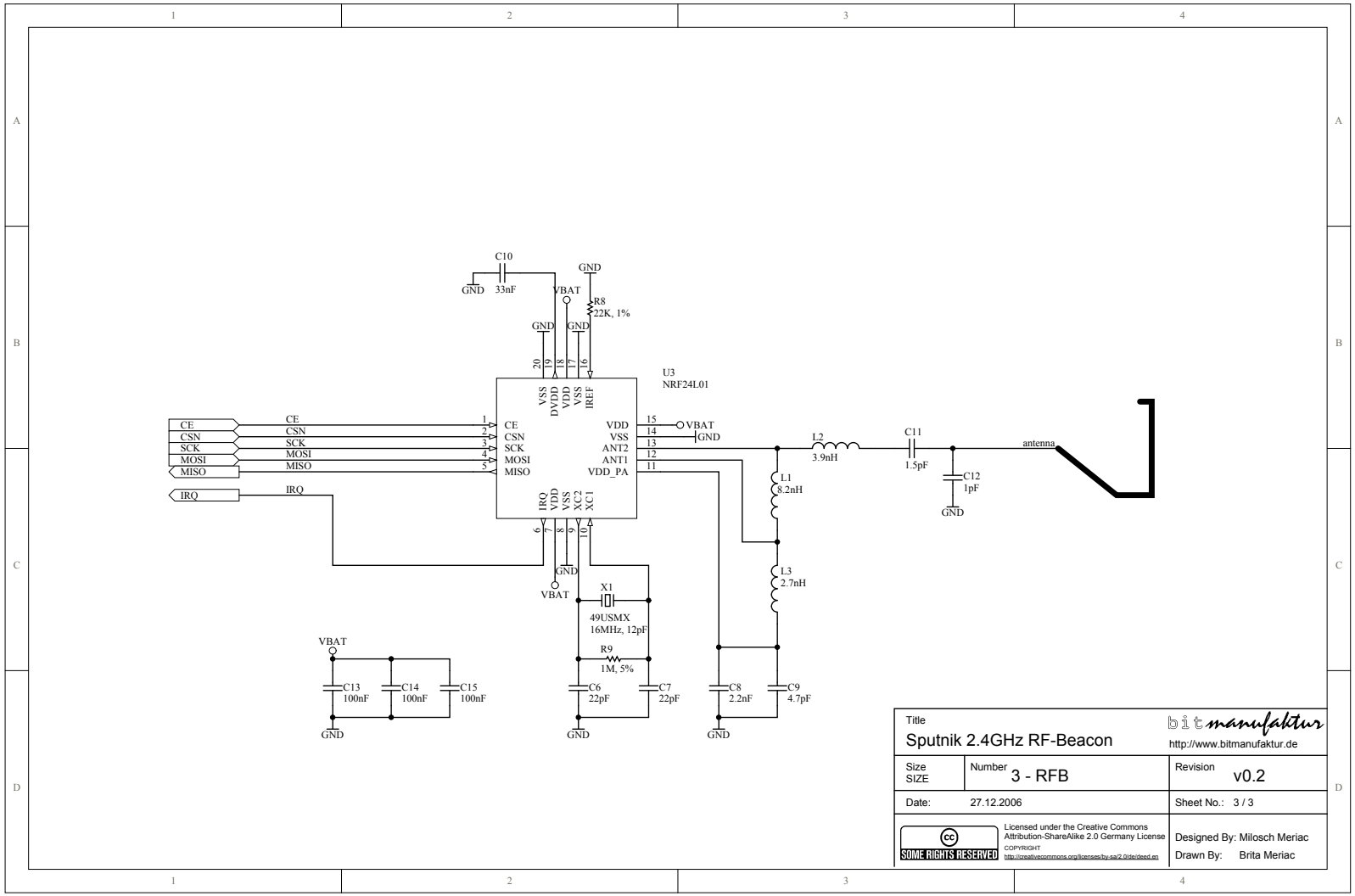



| | | |
|---|---|---|
| Title: Sputnik 2.4GHz RF-Beacon | | bitmanufaktur http://www.bitmanufaktur.de |
| Size: SIZE | Number: 1 - TOP | Revision: v0.2 |
| Date: 27.12.2006 | | Sheet No.: 1 / 3 |
| SOME RIGHTS RESERVED | Licensed under the Creative Commons Attribution-ShareAlike 2.0 Germany License | Designed By: Milosch Meriac<br>Drawn By: Brita Meriac |

# Sputnik Schaltplan - Prozessor



# Sputnik Schaltplan - 2.4GHz Frontend



# Sputnik Funktion

- Tag sendet ungefähr im 1.5-Sekunden-Takt Pakete aus - eine von der Tag-ID abgeleitete zufällige Wartezeit stellt eine Kollosionsvermeidung sicher
- Sendestärke variriert in 4 Stufen (n*0x55)
- über die Empfangswahrscheinlichkeit kann die Entfernung des Tags abgeschätzt werden. Jedes zweite Paket wird mit voller Sendestäke (0xFF) versendet
- alle Basisstationen leiten empfangene Pakete verzögerungsfrei per UDP an zentralen Server (Aggregator) weiter
- eine Positionsschätzung ist möglich, sobald Tag von mehreren Stationen empfangen wird

# Sputnik Funktion

- Tag sendet ungefähr im 1.5-Sekunden-Takt Pakete aus - eine von der Tag-ID abgeleitete zufällige Wartezeit stellt eine Kollosionsvermeidung sicher
- Sendestärke variriert in 4 Stufen (n*0x55)
- über die Empfangswahrscheinlichkeit kann die Entfernung des Tags abgeschätzt werden. Jedes zweite Paket wird mit voller Sendestäke (0xFF) versendet
- alle Basisstationen leiten empfangene Pakete verzögerungsfrei per UDP an zentralen Server (Aggregator) weiter
- eine Positionsschätzung ist möglich, sobald Tag von mehreren Stationen empfangen wird

# Sputnik Privacy

- aus Privacygründen und um Identitätsdiebstahl zu vermeiden wird jedes ausgesendete Paket mit XXTEA blockverschlüsselt (128 bit shared key)
- die verschlüsselten Pakete werden erst auf dem zentralen Server im Aggregator entschlüsselt
- Erfassung der Daten ist somit dem Aufsteller der Anlage vorbehalten, Sniffing ist wertlos, da die Pakete komplett verschlüsselt sind und dadurch keinen Rückschluß auf das Ursprungstag zulassen
- eine auch über Batteriewechsel konsistente Sequenznummer im Paket hilft Replay-Attacken zu vermeiden

# Sputnik Privacy

- aus Privacygründen und um Identitätsdiebstahl zu vermeiden wird jedes ausgesendete Paket mit XXTEA blockverschlüsselt (128 bit shared key)
- die verschlüsselten Pakete werden erst auf dem zentralen Server im Aggregator entschlüsselt
- Erfassung der Daten ist somit dem Aufsteller der Anlage vorbehalten, Sniffing ist wertlos, da die Pakete komplett verschlüsselt sind und dadurch keinen Rückschluß auf das Ursprungstag zulassen
- eine auch über Batteriewechsel konsistente Sequenznummer im Paket hilft Replay-Attacken zu vermeiden

## Historie

- Idee für Pilgertracking in Mekka: Wegleitsysteme/Panikanalyse
- erste Planung für HOPE6, New York, Aug 2006 nicht realisiert aufgrund von Geldmangel des Veranstalters
- Planung im CCC ab Ende Okt. 2006

## Durchführung

- Tim Pritlove (Planung)
- Milosch & Brita Meriac (Idee, Planung, Hardware, Tag- und Reader Firmware, Software), Andy Green (Server Software, Aggregator), Harald Welte (Verbesserungen der Tag Firmware)
- Hannes Mehnert (Datenbank, Benutzerfrontend), Pavel Mayer/ART+COM (Visualisierung), Marten Suhr (3D-Modell des bcc)
- viele Helfer bei Montage, Flashen von 900 Tags, Frontend Software, Auf- und Abbau

## Historie

- Idee für Pilgertracking in Mekka: Wegleitsysteme/Panikanalyse
- erste Planung für HOPE6, New York, Aug 2006 nicht realisiert aufgrund von Geldmangel des Veranstalters
- Planung im CCC ab Ende Okt. 2006

## Durchführung

- Tim Pritlove (Planung)
- Milosch & Brita Meriac (Idee, Planung, Hardware, Tag- und Reader Firmware, Software), Andy Green (Server Software, Aggregator), Harald Welte (Verbesserungen der Tag Firmware)
- Hannes Mehnert (Datenbank, Benutzerfrontend), Pavel Mayer/ART+COM (Visualisierung), Marten Suhr (3D-Modell des bcc)
- viele Helfer bei Montage, Flashen von 900 Tags, Frontend Software, Auf- und Abbau

# Motivation & Umsetzung

## Motivation

- Erfahrung mit 2.4GHz Leiterplatten-Voodoo sammeln
- freies RFID Design für mehr Transparenz etablieren
- Möglichkeiten und Akzeptanzgrenzen der Überwachung und Datenauswertung austesten

## Umsetzung

- 23 Basisstationen in Über-Kopf-Höhe auf drei Ebenen verteilt
- 900 Sputnik Tags zum Verkauf für je 10,-EUR

# Motivation & Umsetzung

## Motivation

- Erfahrung mit 2.4GHz Leiterplatten-Voodoo sammeln
- freies RFID Design für mehr Transparenz etablieren
- Möglichkeiten und Akzeptanzgrenzen der Überwachung und Datenauswertung austesten

## Umsetzung

- 23 Basisstationen in Über-Kopf-Höhe auf drei Ebenen verteilt
- 900 Sputnik Tags zum Verkauf für je 10,-EUR

# 3D Echtzeitvisualisierung

- Anzeige der Position aller Benutzer mit Tag-ID
- Interaktion des Träger mit dem System durch Taster auf Tag - Markierung der Avatare
- freiwillige Verknüpfung der Tag-ID mit Nickname durch optionale Registrierung

# 3D Echtzeitvisualisierung

# Datenspeicherung

## jeder überwacht jeden

- freier Zugang zu den Rohdaten für generische Auswertungen
- Erstellung von Bewegungsprofilen
- Statistik über Vorträge: Anzahl der Zuhöhrer, Fluktuation, Ähnlichkeiten von Benutzervorlieben
- Beziehungen von Personen, Gruppenbildung

## was schief gehen kann, geht schief

ungewollte Anonymisierung der gespeicherten Daten durch Fehler in der Server Software: ID wurde nicht gespeichert.

# Datenspeicherung

## jeder überwacht jeden

- freier Zugang zu den Rohdaten für generische Auswertungen
- Erstellung von Bewegungsprofilen
- Statistik über Vorträge: Anzahl der Zuhöhrer, Fluktuation, Ähnlichkeiten von Benutzervorlieben
- Beziehungen von Personen, Gruppenbildung

## was schief gehen kann, geht schief

ungewollte Anonymisierung der gespeicherten Daten durch Fehler in der Server Software: ID wurde nicht gespeichert.

# Tags über Zeit

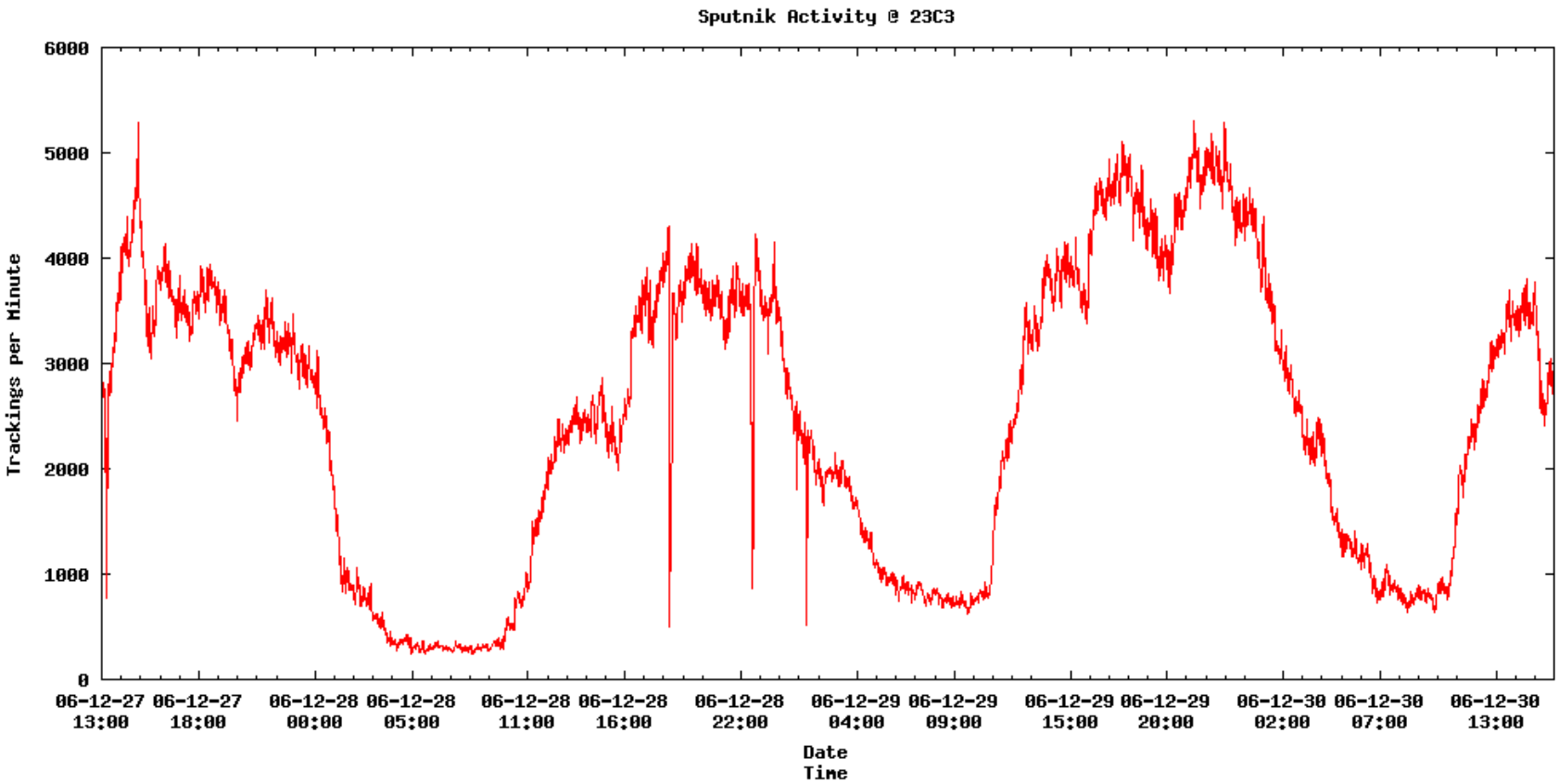



Abbildung: Peter Meerwalds Auswertung (http://pmeerw.net/23C3_Sputnik/)

# Tags über Basisstationen

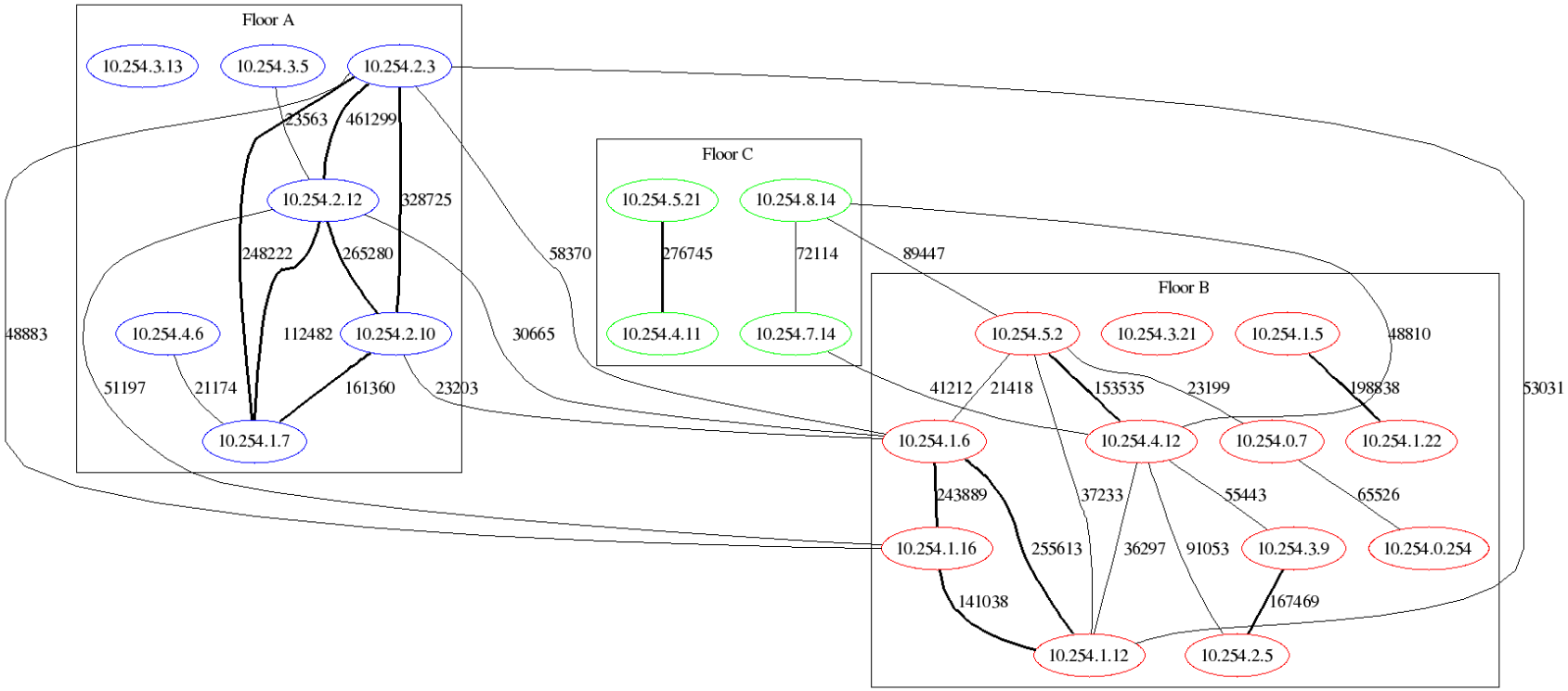



Abbildung: Peter Meerwalds Auswertung (http://pmeerw.net/23C3_Sputnik/)

# Andy Greens Webfrontend

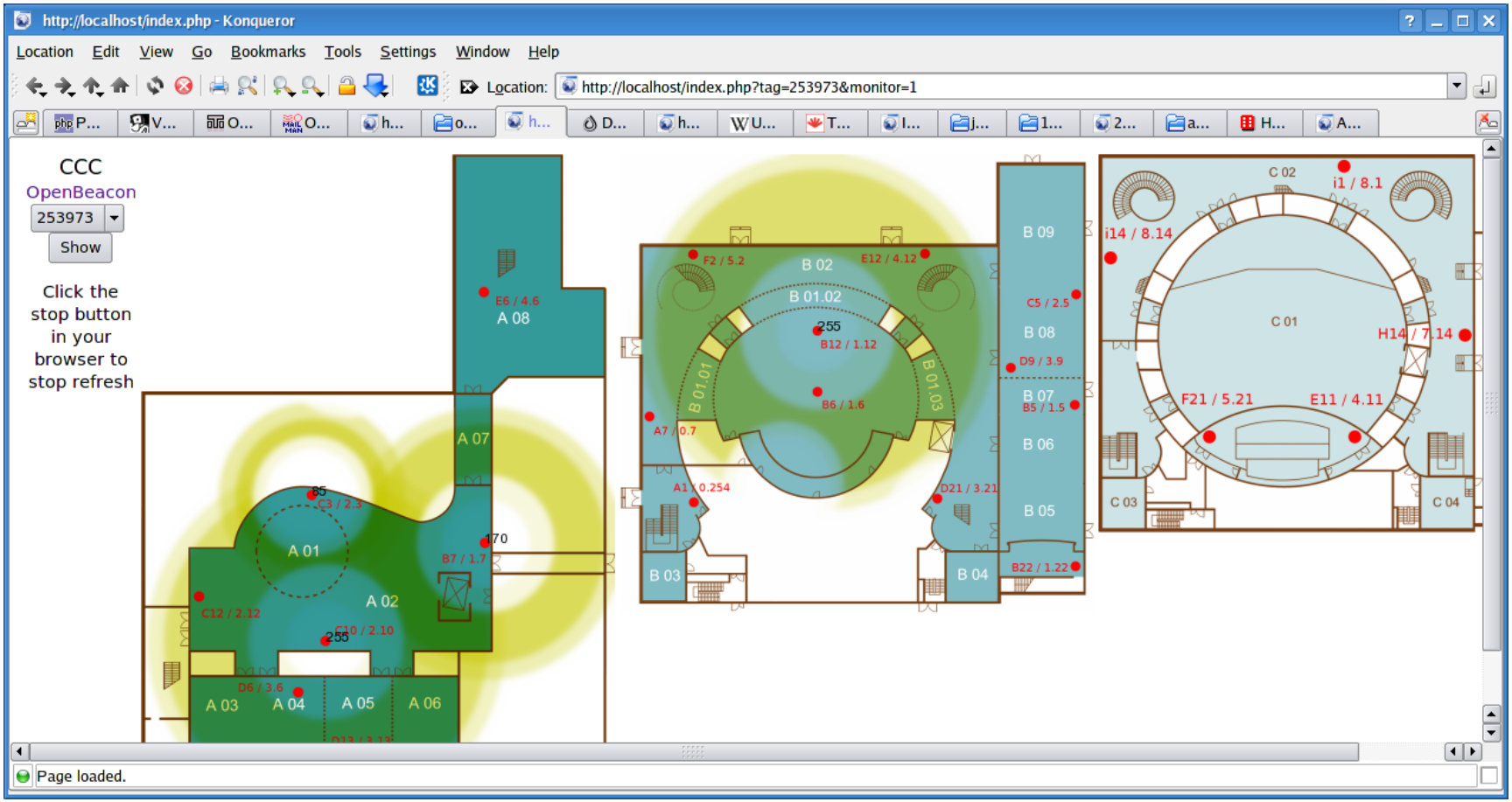



Abbildung: empfangene Entfernung eines einzelnen Tags auf dem 23C3

# Andy Greens Webfrontend

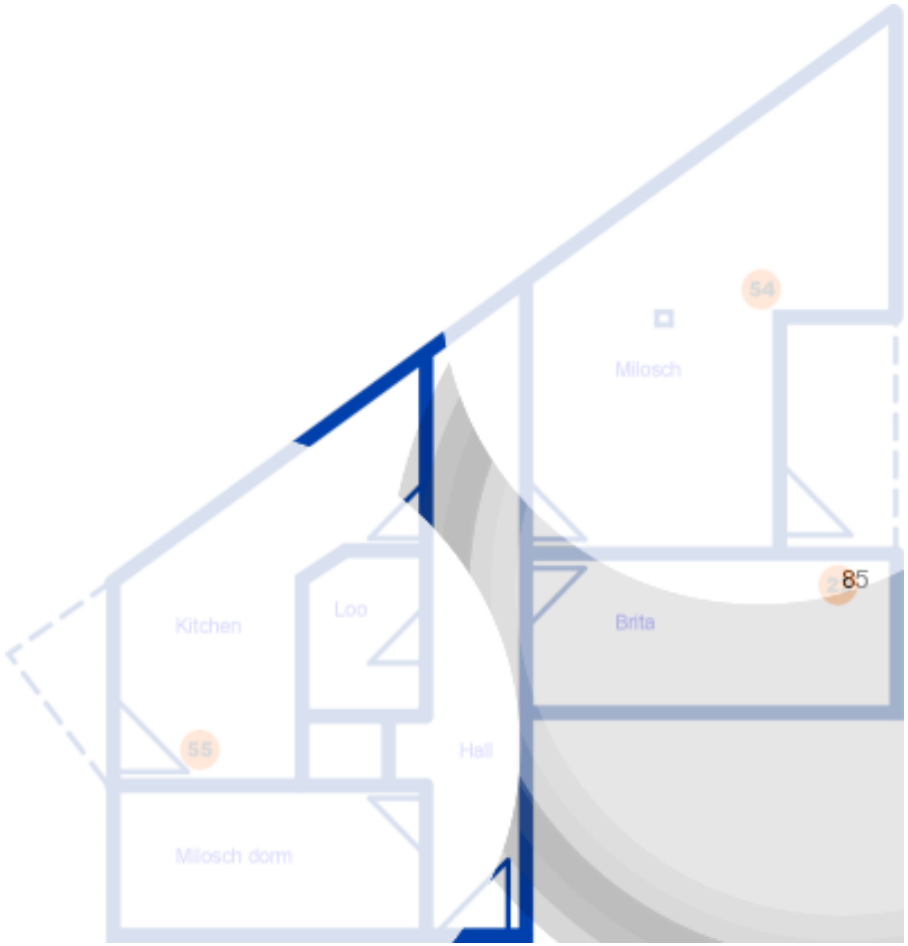



Abbildung: unsere Wohnung - grafische Lösung der Positionsschätzung

# Do-it-yourself-Überwachung: Reaktionen

## Erfahrungen mit freiwilliger Überwachung

- Ausverkauf der 900 Sputnik Tags
- große Neugierde
- positive Erwartungen
- Spieltrieb geweckt

## Akzeptanz durch Transparenz

- offenes Design
- blinkende LED zeigt Sendehäufigkeit
- Basisstation offen sichtbar
- Ausschalten der Tags durch Batterie herausnehmen
- Wiedervervendbarkeit (Chaos Camp!)
- Hackvalue (bidirektionale Funktion der Tags)

# Do-it-yourself-Überwachung: Reaktionen

## Erfahrungen mit freiwilliger Überwachung

- Ausverkauf der 900 Sputnik Tags
- große Neugierde
- positive Erwartungen
- Spieltrieb geweckt

## Akzeptanz durch Transparenz

- offenes Design
- blinkende LED zeigt Sendehäufigkeit
- Basisstation offen sichtbar
- Ausschalten der Tags durch Batterie herausnehmen
- Wiedervervendbarkeit (Chaos Camp!)
- Hackvalue (bidirektionale Funktion der Tags)

# Do-it-yourself-Überwachung: Fragen

## Fragen, die uns gestellt wurden

- wo kann man die Daten runterladen?
- Auswertung der gesammelten Daten
- wie genau ist die Ortung/Positionierung?
- sind Basisstationen außerhalb des BCC?
- ist die 2.4GHz Strahlung gesundheitsschädlich?
- ist das Tag waschbar ;-)?

## Fragen, die uns nicht gestellt wurden

- nur wenige haben sich für die Technik interessiert
- während des Kongress gab es keine Hacks mit der Firmware

# Do-it-yourself-Überwachung: Fragen

## Fragen, die uns gestellt wurden

- wo kann man die Daten runterladen?
- Auswertung der gesammelten Daten
- wie genau ist die Ortung/Positionierung?
- sind Basisstationen außerhalb des BCC?
- ist die 2.4GHz Strahlung gesundheitsschädlich?
- ist das Tag waschbar ;-)?

## Fragen, die uns nicht gestellt wurden

- nur wenige haben sich für die Technik interessiert
- während des Kongress gab es keine Hacks mit der Firmware

## Einsatz

- Uni Passau
- FH Dortmund
- CCC Ulm
- Metalab Wien

## Anfragen für Projekte

- Zeiterfassung z.B. für Radrennen
- Securityanwendung in Kombination mit Infrarotmelder
- Bühnensteuerung für Ballett

## Einsatz

- Uni Passau
- FH Dortmund
- CCC Ulm
- Metalab Wien

## Anfragen für Projekte

- Zeiterfassung z.B. für Radrennen
- Securityanwendung in Kombination mit Infrarotmelder
- Bühnensteuerung für Ballett

## Angedachte Erweiterungen

RGB LEDs, Piezolautsprecher, Mikrofone zur Erkennung von Sprachaktivität, 3D-Bewegungssensoren, Temperatursensoren

## Einsatz

- Uni Passau
- FH Dortmund
- CCC Ulm
- Metalab Wien

## Anfragen für Projekte

- Zeiterfassung z.B. für Radrennen
- Securityanwendung in Kombination mit Infrarotmelder
- Bühnensteuerung für Ballett

## Angedachte Erweiterungen

RGB LEDs, Piezolautsprecher, Mikrofone zur Erkennung von Sprachaktivität, 3D-Bewegungssensoren, Temperatursensoren

# Weiterentwicklung: Power Over Ethernet

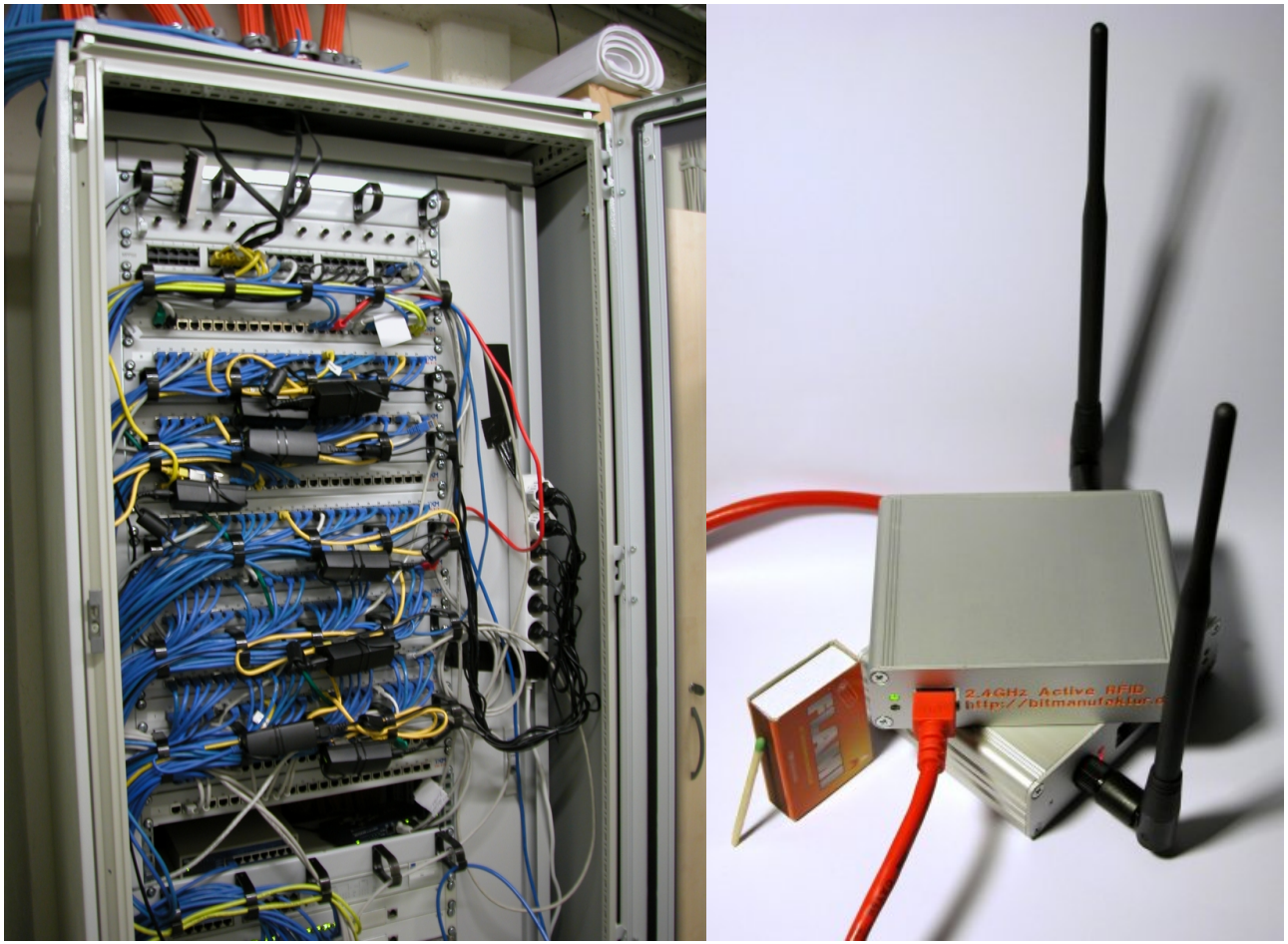



Abbildung: früher Netzteile im Serverschrank / jetzt PoE 802.3af

# Weiterentwicklung: OpenBeacon USB


Abbildung: Autarke Basisstation mit USB-Device Port

# Zusammenfassung & Links

## Überwachung wird akzeptiert wenn ...

- ... die Überwachung einen direkten Nutzen bietet
- ... man die freie Entscheidung über das Wann & Wo hat
- ... man sich sicher sein kann, wer überwacht wird und was mit den Daten passiert

## Links

- http://www.openbeacon.org
- Freies 13.56MHz RFID reader/writer design: http://www.openpcd.org

# Zusammenfassung & Links

## Überwachung wird akzeptiert wenn ...

- ... die Überwachung einen direkten Nutzen bietet
- ... man die freie Entscheidung über das Wann & Wo hat
- ... man sich sicher sein kann, wer überwacht wird und was mit den Daten passiert

## Links

- http://www.openbeacon.org
- Freies 13.56MHz RFID reader/writer design: http://www.openpcd.org