

# Software Defined Radio

Was ist das?

Warum will man das?



Ekki Plicht, DF4OR  
GPN 2015 (v0.2)

# About me

- Funkamateurl seit 40+ Jahren (DF4OR)
- Morsen, Funkfernschreiben und so Kram
- Ein wenig Software (Perl, C++)
- LUG-Landau e.V.
- Job: Berater & Webmaster in nem Laden für Antennen & Funkgeräte usw.

[eplicht@gmail.com](mailto:eplicht@gmail.com)

**PUT A RADIO**



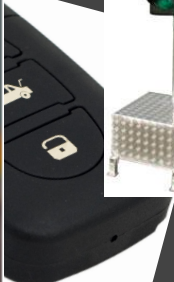
**IN ALL THINGS**

[memegenerator.net](http://memegenerator.net)



**9V Radio-Interlinked Smoke  
Ei3100RF Series**

- 9v battery operated
- Available with Ionisation, Optical and battery operated alarms
- Wireless radio-interlinked - can interlink
- Suitable for BS 5839-6: 2013 Grade F
- Please Note: Alarms are sold individually



# Warum Digitalisierung des Funks?

- Effizientere Nutzung des Spektrums
- Größere Robustheit (Fading, Reflektionen)
- Verschlüsselung
- Nutzungs/Zugangskontrolle

# Funkfrequenzen als Ressource

Funkfrequenzen sind eine begrenzte Ressource, ähnlich wie Grundstücke. Wir können sie nicht beliebig vermehren, nur besser nutzen.

**Digitalisierung** ist *eine* Möglichkeit der besseren Nutzung.

# Funkfrequenzen als Ressource

- Analog TV → DVB-T/S/C
- UKW-Rundfunk → DAB/DAB+
- AM-Rundfunk → DRM
- Autotelefon A/B/C-Netz → D-Netz (2G, 3G, 4G (LTE))
- BOS-Funk (FM) → Tetra

**Digitalisierung** ist *eine* Möglichkeit der besseren Nutzung.

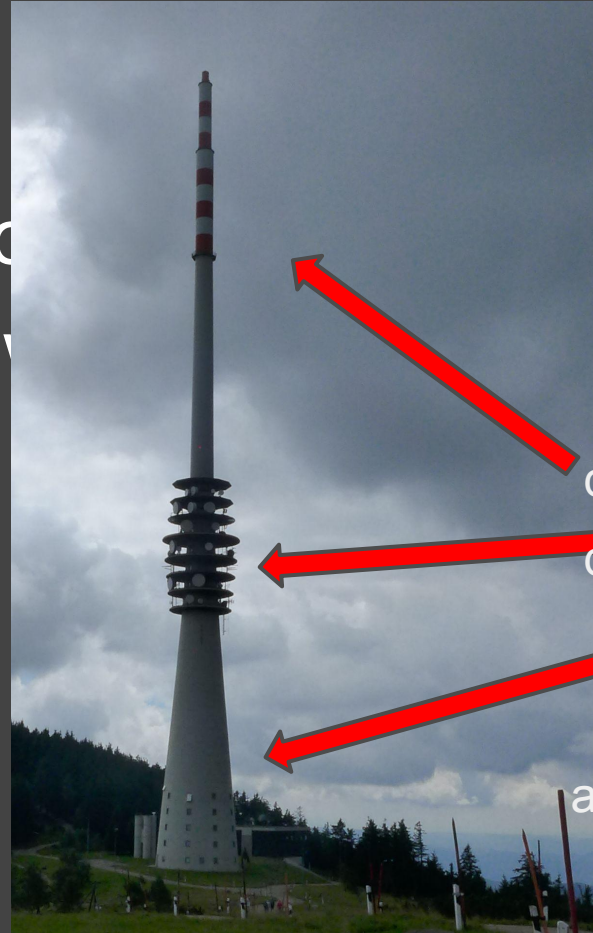
# Das Problem:

Neue, effizientere Modulationsverfahren  
brauchen neue Hardware (Sender, Empfänger)



# Das Problem:

Neue, effizientere Modelle  
brauchen neue Hardware



en  
(Empfänger)

da

da

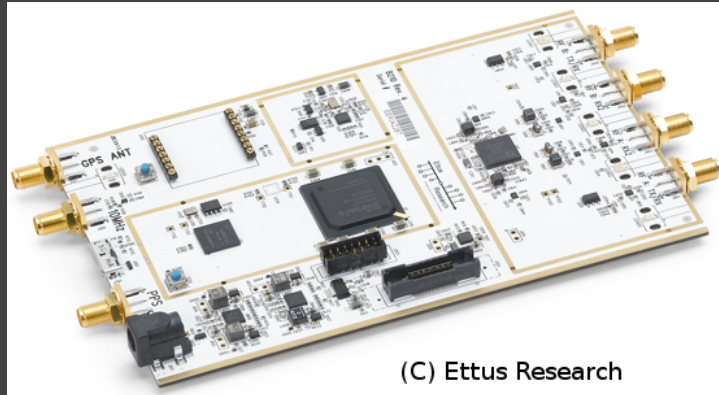
und da

an 30.000 Standorten

# Die Lösung:

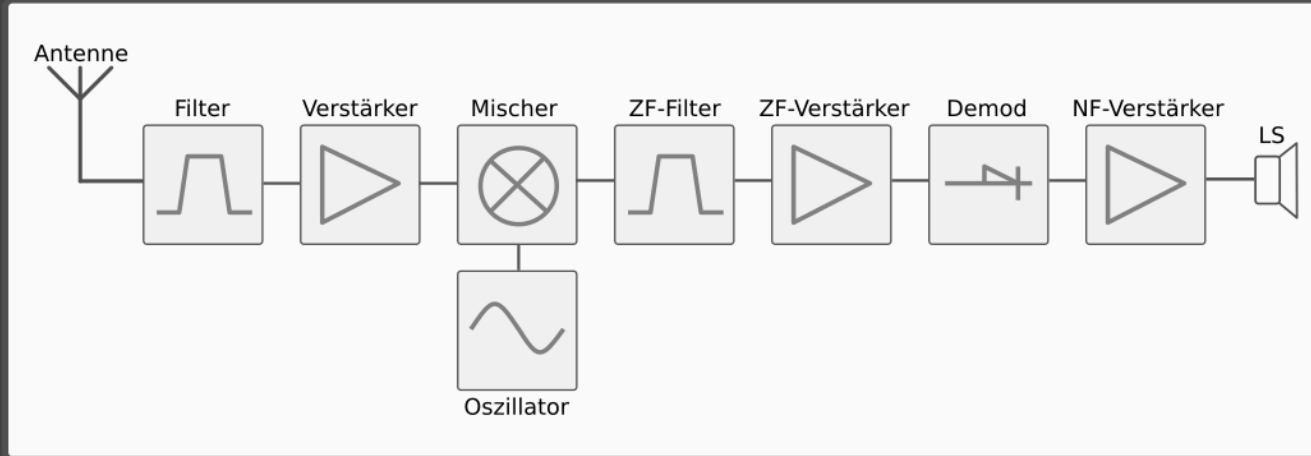
Ein flexibleres Konzept  
aus Hard- und Software

## Software Defined Radio

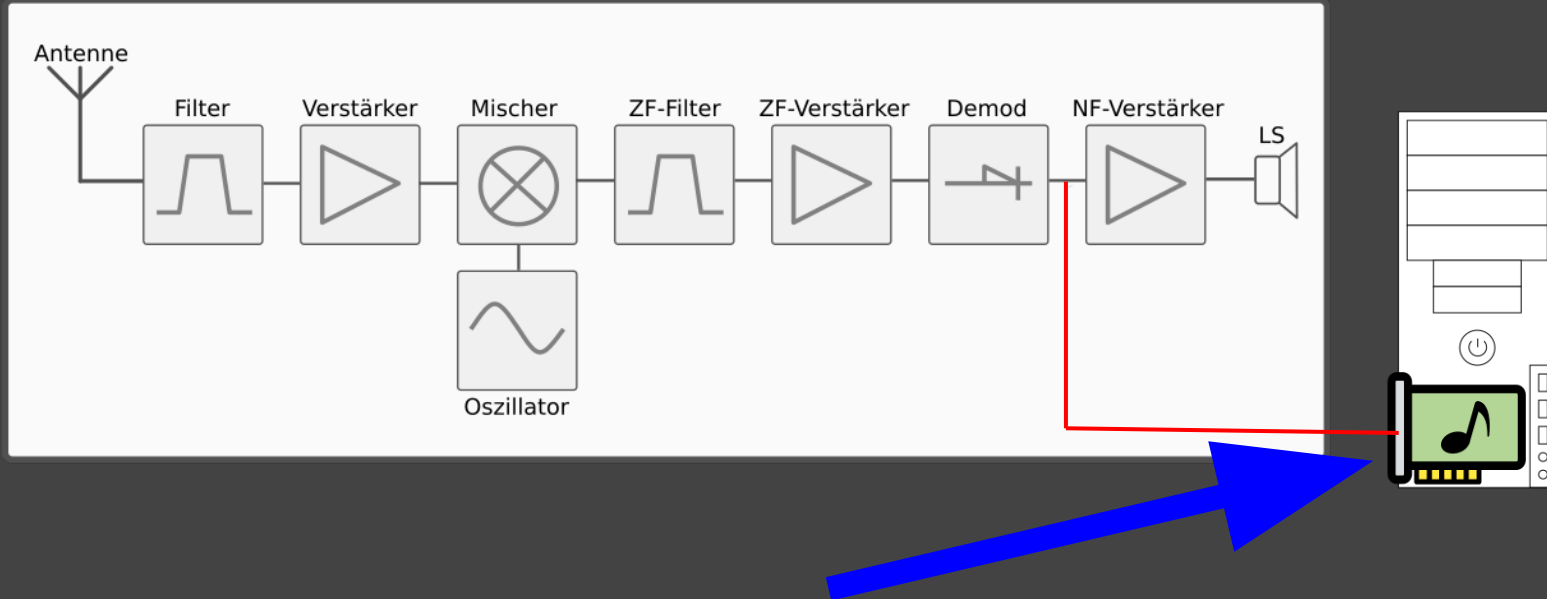


(C) Ettus Research

# Ein analoger Empfänger

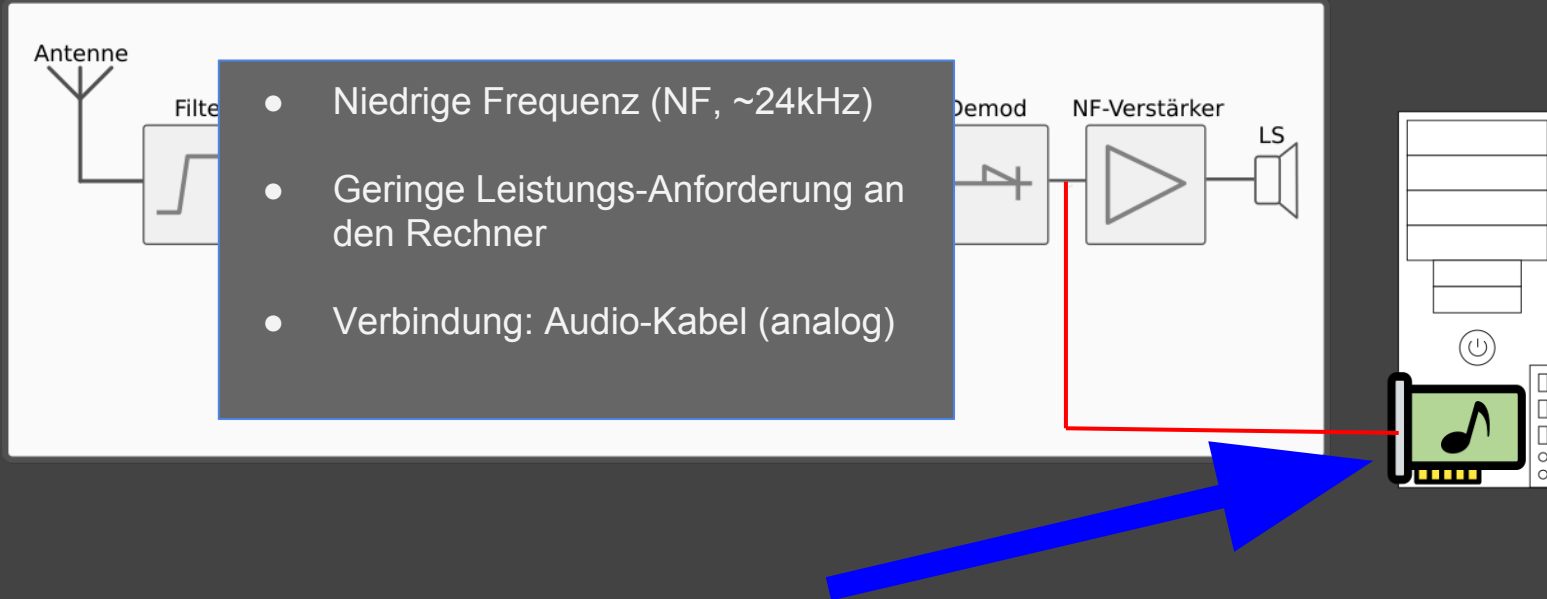


# Digitalisierung mit Soundkarte



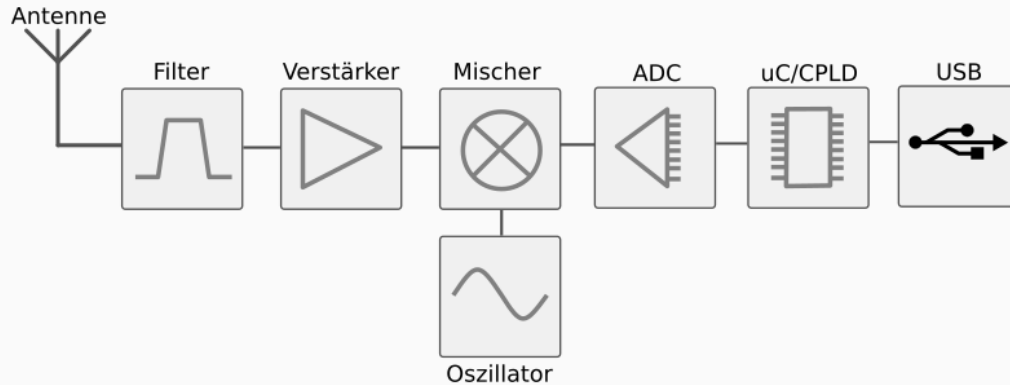
Soundkarte = Analog/Digital-Wandler (ADC)  
~24 kHz

# Digitalisierung mit Soundkarte



Soundkarte = Analog/Digital-Wandler (ADC)  
~24 kHz

# Digitalisierung in der ZF



ADC auf ZF-Ebene

~ wenige hundert kHz bis wenige MHz

# Digitalisierung in der ZF

Antenne

Filter

- Mittlere Frequenz (x00 - x000 kHz)
- Höhere Leistungs-Anforderung an den Rechner (Filter, Demodulation)
- Verbindung: USB (digital, I/Q)

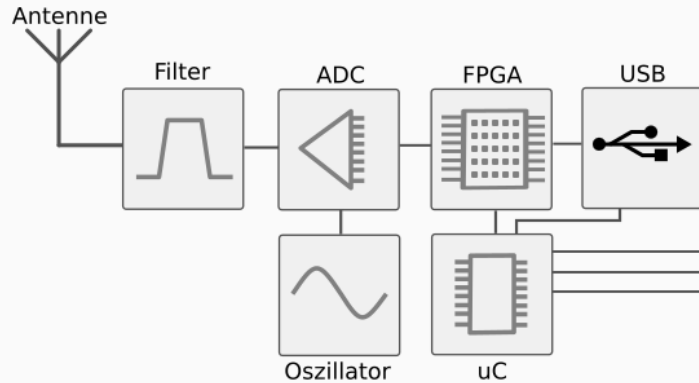
USB



ADC auf ZF-Ebene

~ wenige hundert kHz bis wenige MHz

# Digitalisierung direkt an der Antenne



ADC direkt an der Antenne (mit/ohne Filter)  
bis ca. 100 - 120 MHz  
Nachverarbeitung durch FPGA



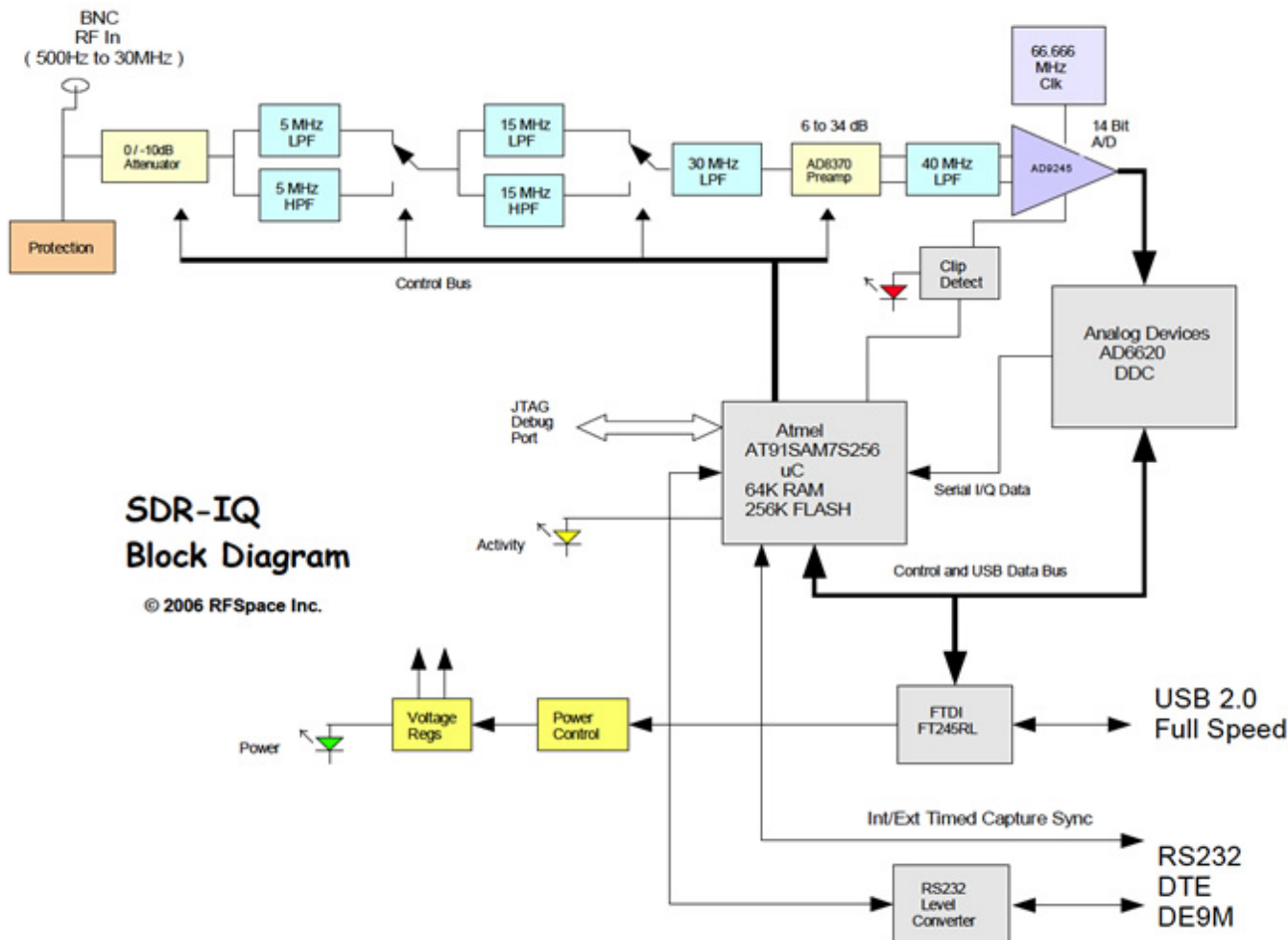
# Digitalisierung direkt an der Antenne

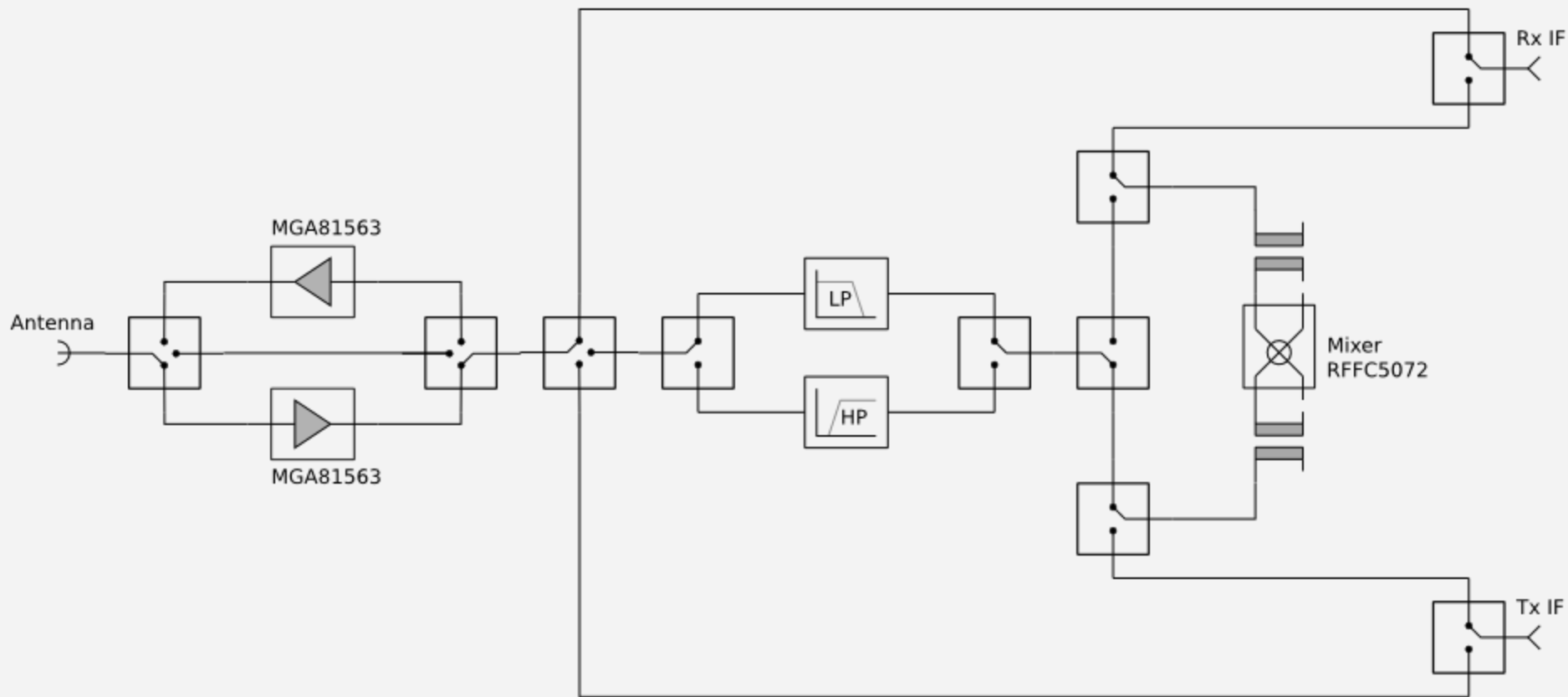
Antenne

Filter

- Hohe Frequenz ( $\sim 100\text{MHz}$ )
- Hohe bis sehr hohe Leistungs-Anforderung an den Rechner (Filter, Demodulation)
- Verbindung: USB oder Ethernet (digital, I/Q)

ADC direkt an der Antenne (mit/ohne Filter)  
bis ca. 100 - 120 MHz  
Nachverarbeitung durch FPGA





### **HackRF One Frontend Block diagram**

based on frontend schema dated 13. Feb. 2014

(C) Ekki Plicht, DF4OR WiMo

# Grenzen der SDRs

- Abtastrate des ADC
  - muss mind 2x der max. Frequenz sein (Nyquist)
- Wortbreite des ADC
  - mehr Bits= größerer Dynamikumfang, bessere Empfindlichkeit
- Übertragungsrate zum PC
  - größeres Spektrum darstellbar

# Grenzen der SDRs

- Abtastrate des ADC
  - muss mind 2x der max. Frequenz sein (Nyquist)
- Wortbreite des ADC
  - mehr Bits= größerer Dynamikumfang, bessere Empfindlichkeit
- Übertragungsrate zum PC
  - größeres Spektrum

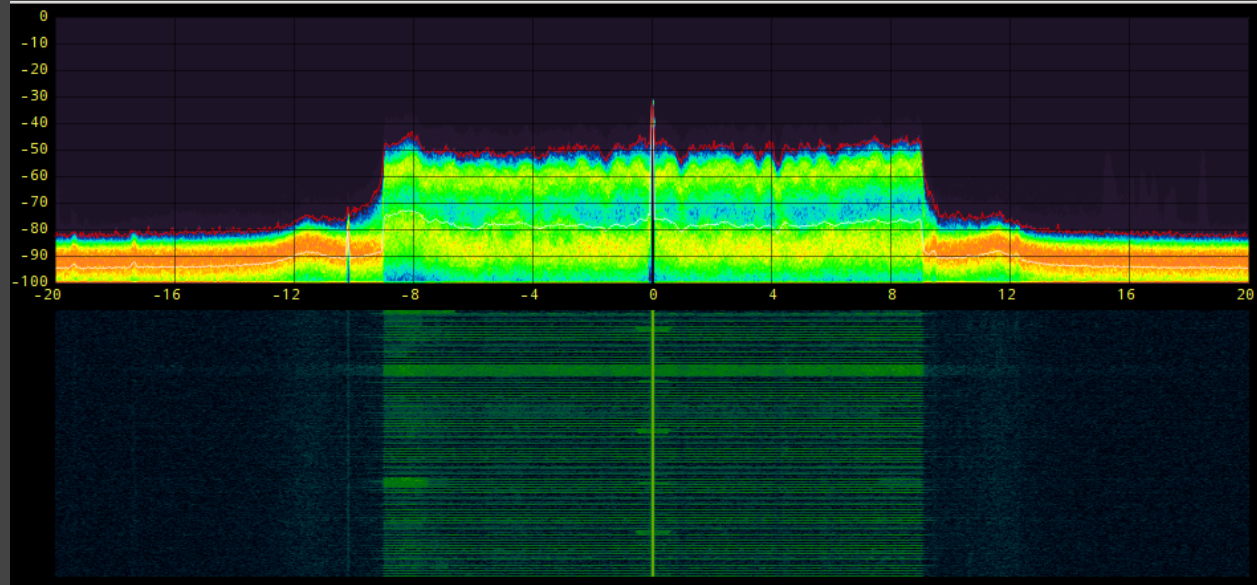
Derzeit max.  
~ 200-220 MS/s

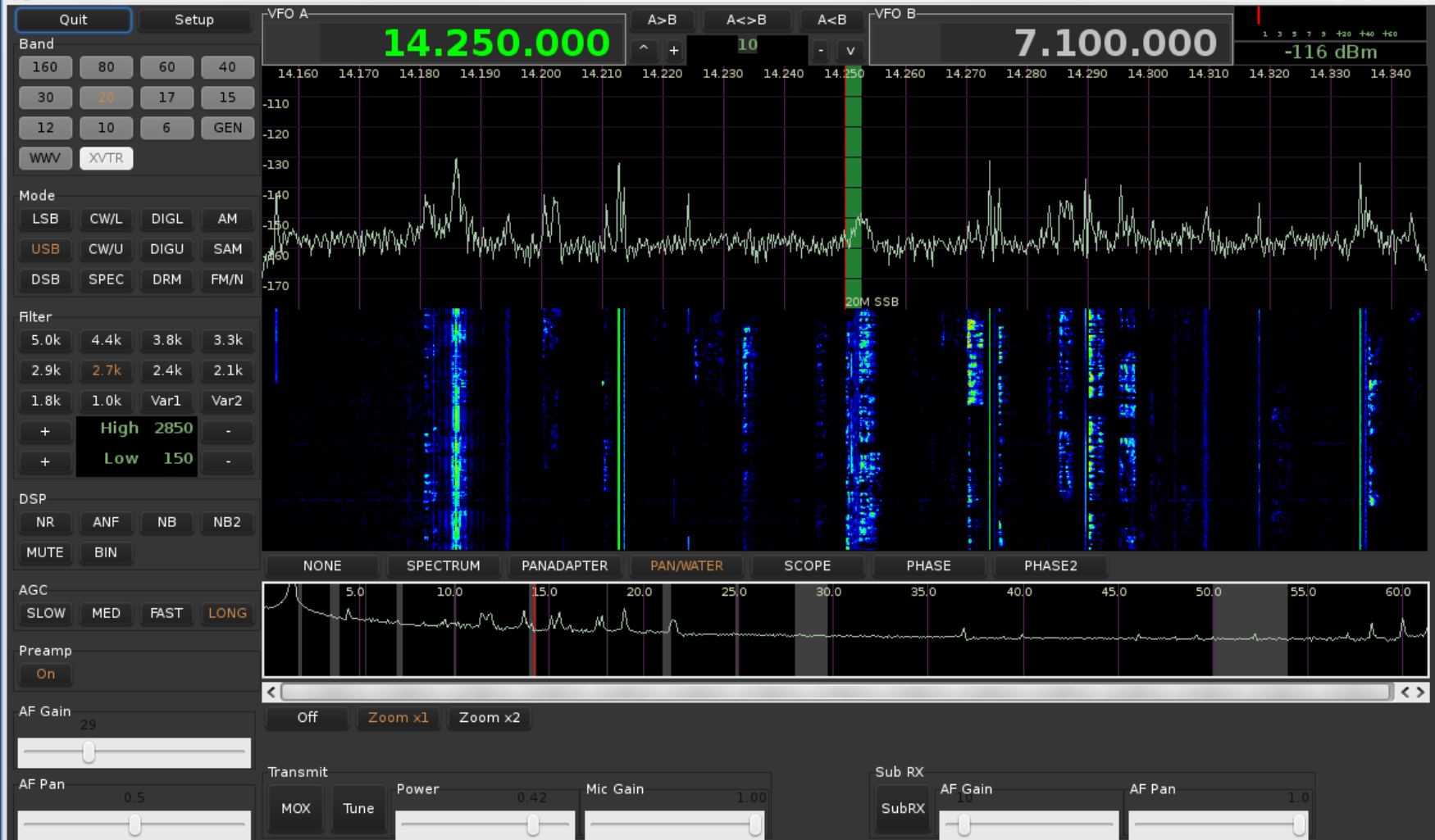
Derzeit max.  
16 Bit

480MBit/s (USB2)  
10GBit/s (USB3)  
100-1000MBit/s (Ethernet)

# Was bekommt man nun dafür?

- Spektrum
- Wasserfall
- Auflösung
- Historie





# Rechtliches

- Was darf ich, was nicht?
  - Das regelt das TKG in DE
  - Nur Sendungen “an Alle” sind legal
  - Rundfunk, Amateurfunk, CB, wenige Dienste auf Kurzwelle (Wetter)
- Was wäre wenn...?
  - Kommt drauf an :)
  - Von Beschlagnahme des Equipments, Ordnungswidrigkeit, Strafbarkeit



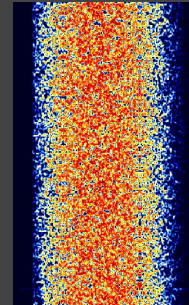
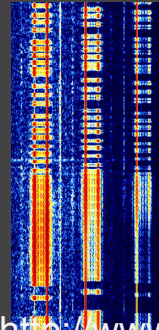
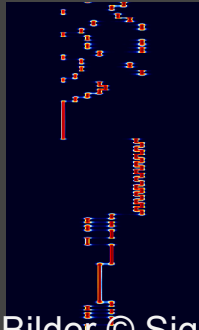
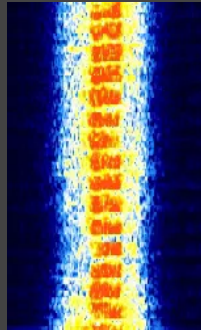
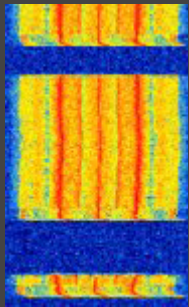
# Hacken mit SDRs

FM RDS (siehe O.Räisänen Blog)

Autoschlüssel auf 433 oder 868 MHz

Wireless Keyboard/Maus

DWD auf Kurzwelle (FAX, RTTY)



# Wie einsteigen?

- Den billigsten DVB-T Dongle kaufen, den man finden kann (RTL-Dongle, ca. 15€)
- rtl\_sdr installieren (Linux)
- SDR# installieren + USB-Stress (Windows)
- Antenne dran  
→ Spaß haben

# Wie einsteigen?

Stop. Bitte  
Nachtrag 1 lesen :)

- Den ~~billigsten~~ DVB-T Dongle kaufen, den man finden kann (RTL-Dongle, ca. 15€)
- rtl\_sdr installieren (Linux)
- SDR# installieren + USB-Stress (Windows)
- Antenne dran  
→ Spaß haben

# Wie einsteigen?

<http://sdr.osmocom.org/trac/wiki/rtl-sdr>

<http://dl3jin.de/sdr.htm>

[http://www.darc.de/uploads/media/SDR\\_Stick\\_neu.pdf](http://www.darc.de/uploads/media/SDR_Stick_neu.pdf)

# Wie einsteigen und mehr lernen?

GNU Radio

<http://gnuradio.org>



- **‘Bessere’ Hardware mit OpenSource Gedanken**
  - **USRP (Ettus)**
  - **SDR-Play**
  - **CloudSDR (RFspace)**
  - **HackRF**
  - **uvm**

# Software Defined Radio

Fragen?

[eplicht@gmail.com](mailto:eplicht@gmail.com)

oder hier auf der GPN15

# Nachtrag 1

Auf der GPN15 hat sich jemand dann gleich einen preiswerten DVB-T Stick gekauft (9,90 €) der prompt nicht funktionierte (VID:PID 187f:0600). Grund: Der Chipsatz ist sehr neu und basiert wahrscheinlich nicht auf den RTL-Chips. Es gibt keinen Treiber für Linux.

Daher besser erstmal auf <http://sdr.osmocom.org/trac/wiki/rtl-sdr> gucken, welche Chipsätze wie unterstützt werden und dann kaufen.

Sorry....

# Nachtrag 2

Den Besuchern, die nach dem Geheimnis hinter den “IQ-Daten” gefragt hatten, seien diese Links empfohlen:

[https://www.youtube.com/watch?v=h\\_7d-m1ehoY](https://www.youtube.com/watch?v=h_7d-m1ehoY)

#170: Basics of IQ Signals and IQ modulation & demodulation - A tutorial  
by w2aew

<http://www.ni.com/tutorial/4805/en/>

Ein Whitepaper von National Instruments