Software Defined Radio

Beertalk 2017

Reto Schädler

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Themen

- Was bedeutet SDR
- SDR Hardware
- Sinus Signal / Schnelle Fourier-Transformation
- Funktionsweise eines SDR
- Replay Attacken
- Modulationen
- Signale identifizieren mit GQRX und Inspectrum
- Türgong: Signal Analyse mit GNU-Radio
- GPS-Spoofing mit SDR

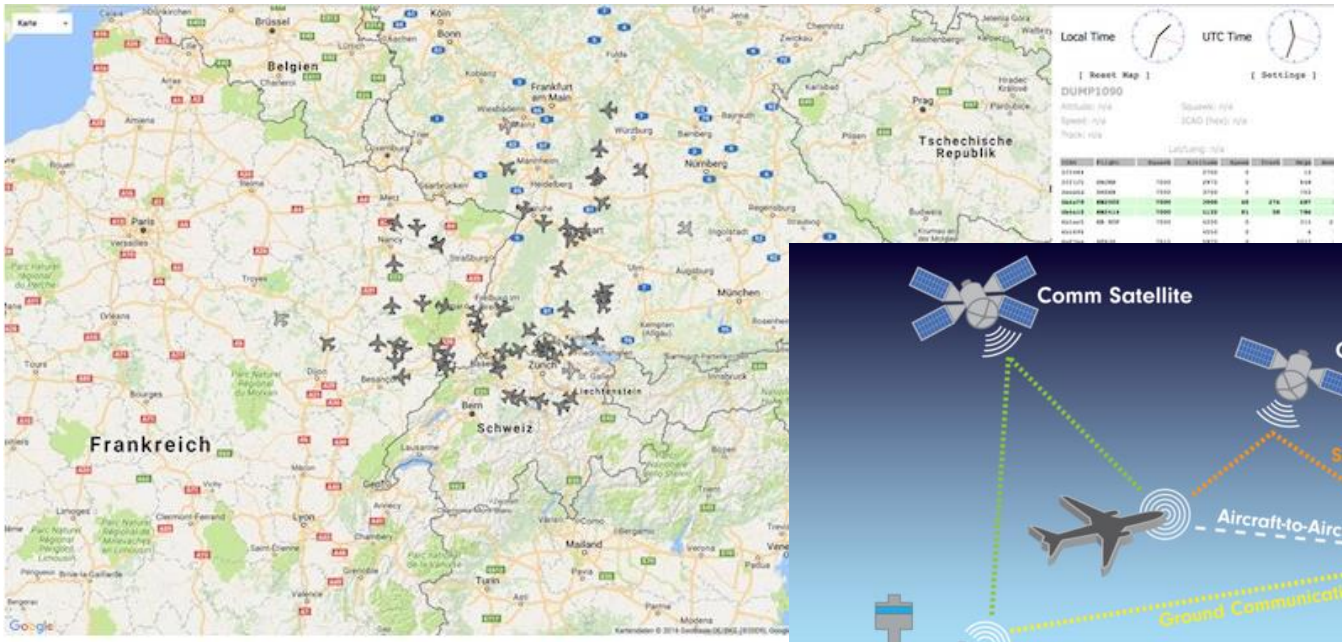
Die Zeit vor SDR

Früher musste für jede Anwendung eine eigene Hardware gebaut werden.

- Z.B. DCF77 Sender

Was bedeutet SDR

- Funk Empfänger / Sender
- Ein Grossteil der Signalverarbeitung erfolgt im Computer
- Dadurch universell einsetzbar, z.B. decodieren von ADS-B:



SDR

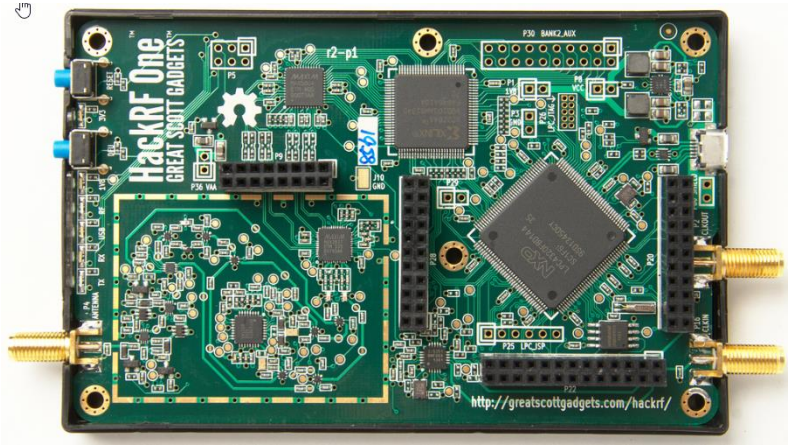
RTL-SDR

- Nur Empfangen
- ~20$
- 24MHz-1766MHz

SDR

HackRF One

- Senden / Empfangen
- 299$
- 1MHz-6000MHz



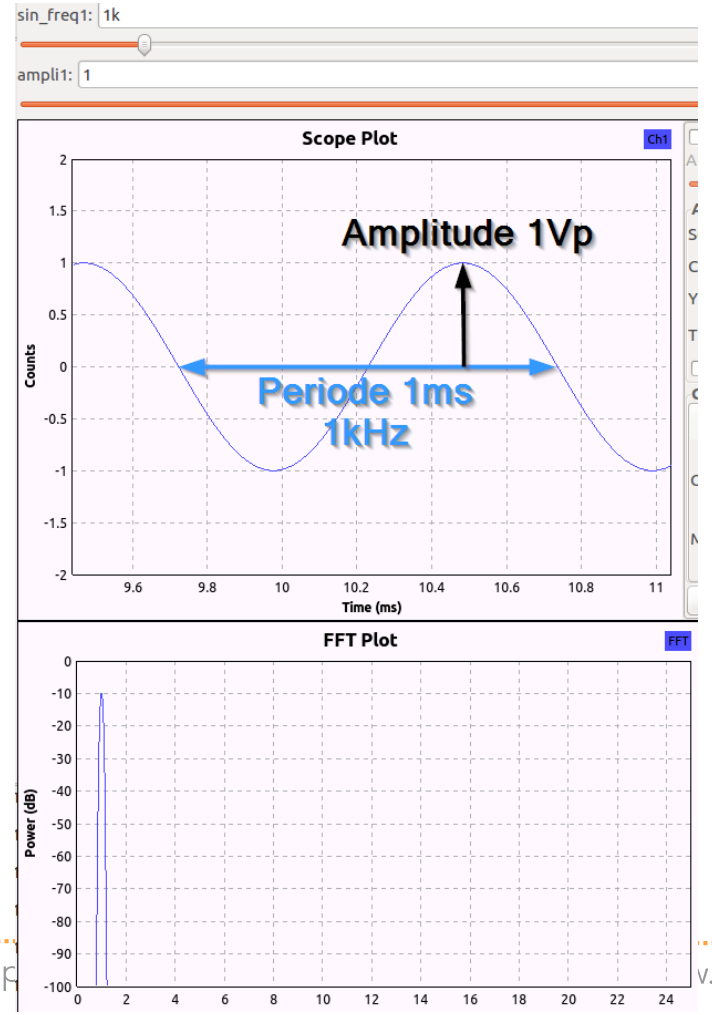
Ettus – SDR

- Gleichzeitig senden und empfangen
- Z.B. für GSM Basisstation
- Frequenzbereich je nach eingesetzten Modulen
- > 2000$

Kurze Theorie

Sinus

Frequenz + Amplitude in Scope + FFT Ansicht – zwei verschiedene Darstellungen



f=1/T

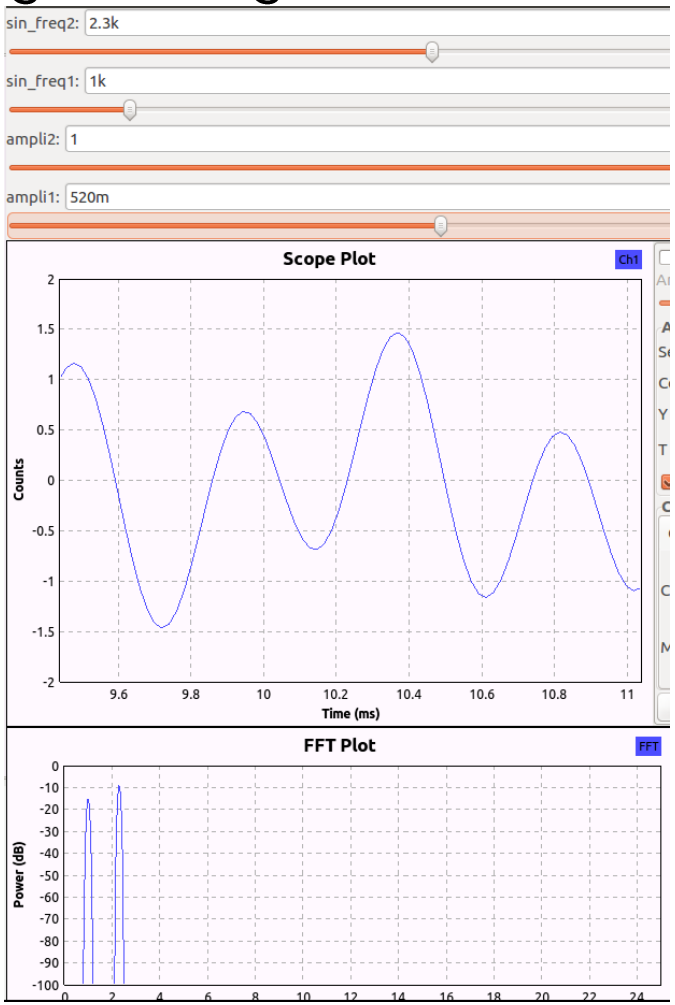
T[s]

f [Hz]

Schnelle Fourier-Transformation

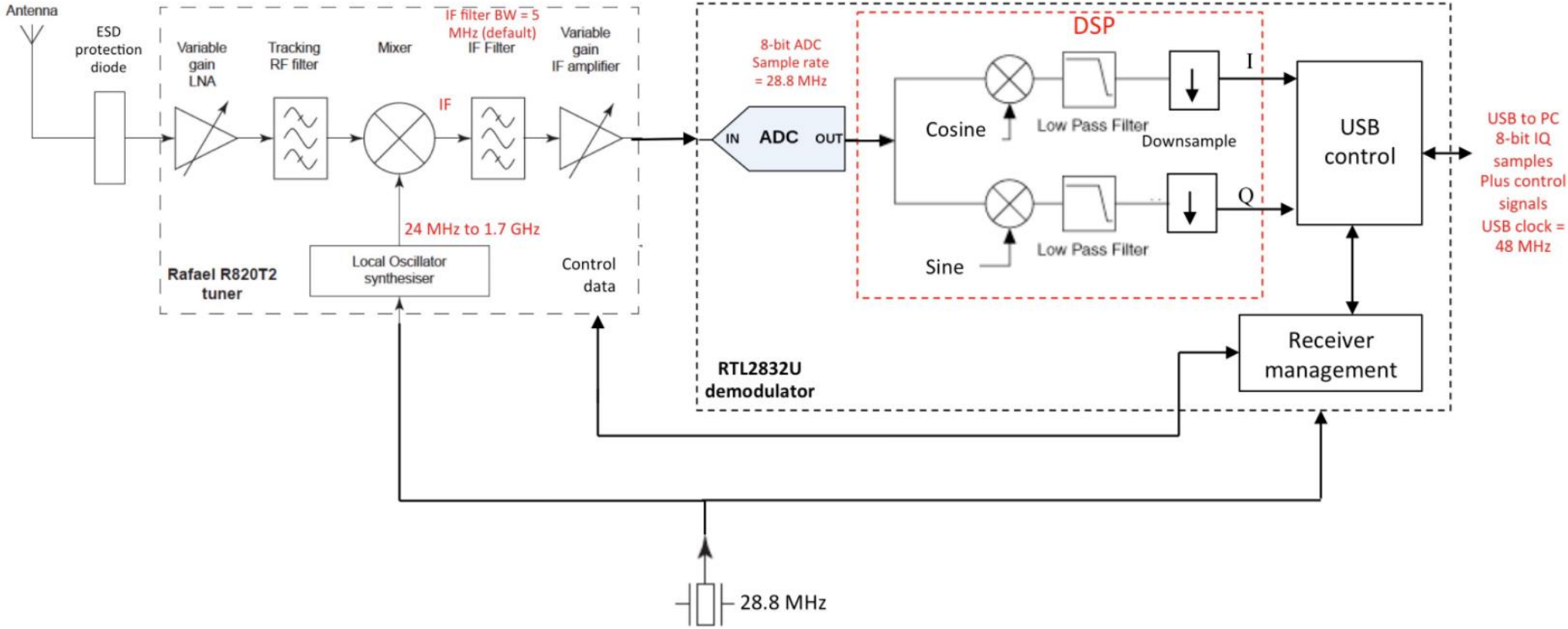
Mehrere Frequenzen

Zwei Frequenzen gleichzeitig



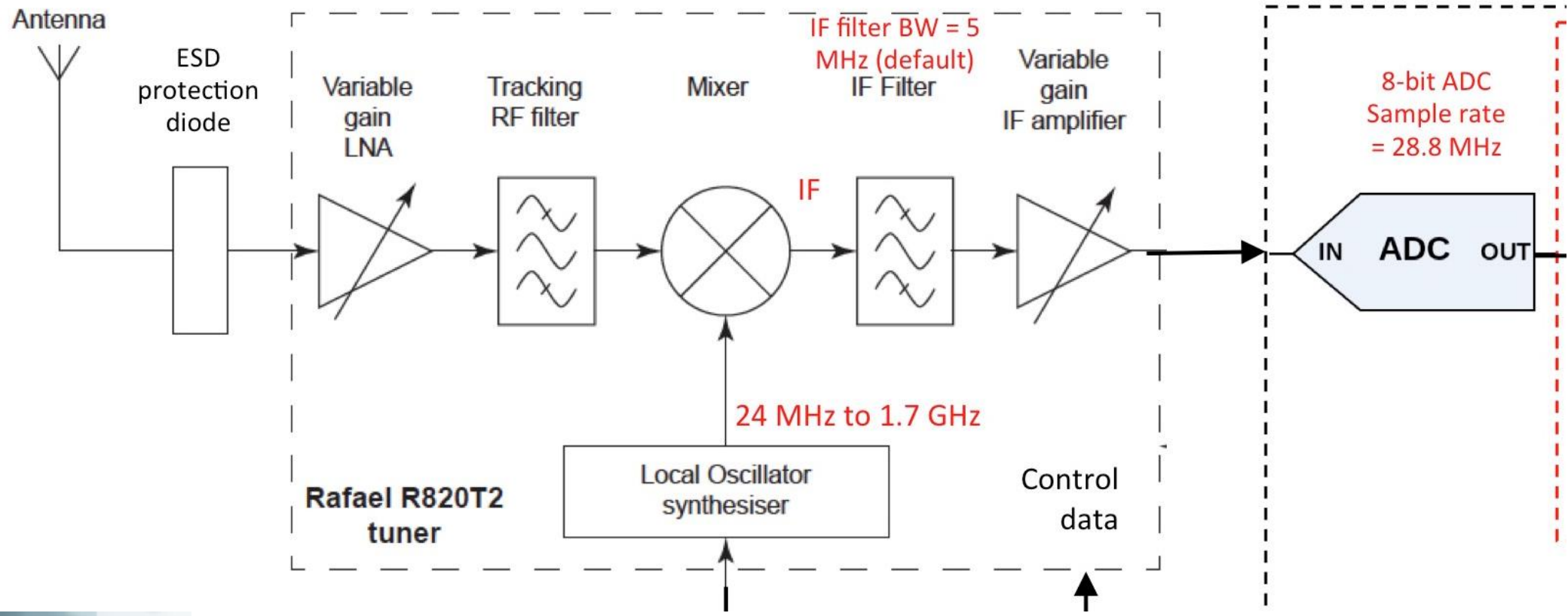
Blockdiagramm SDR

RTL-SDR - Überlagerungsempfänger



Blockdiagramm SDR

Mischer

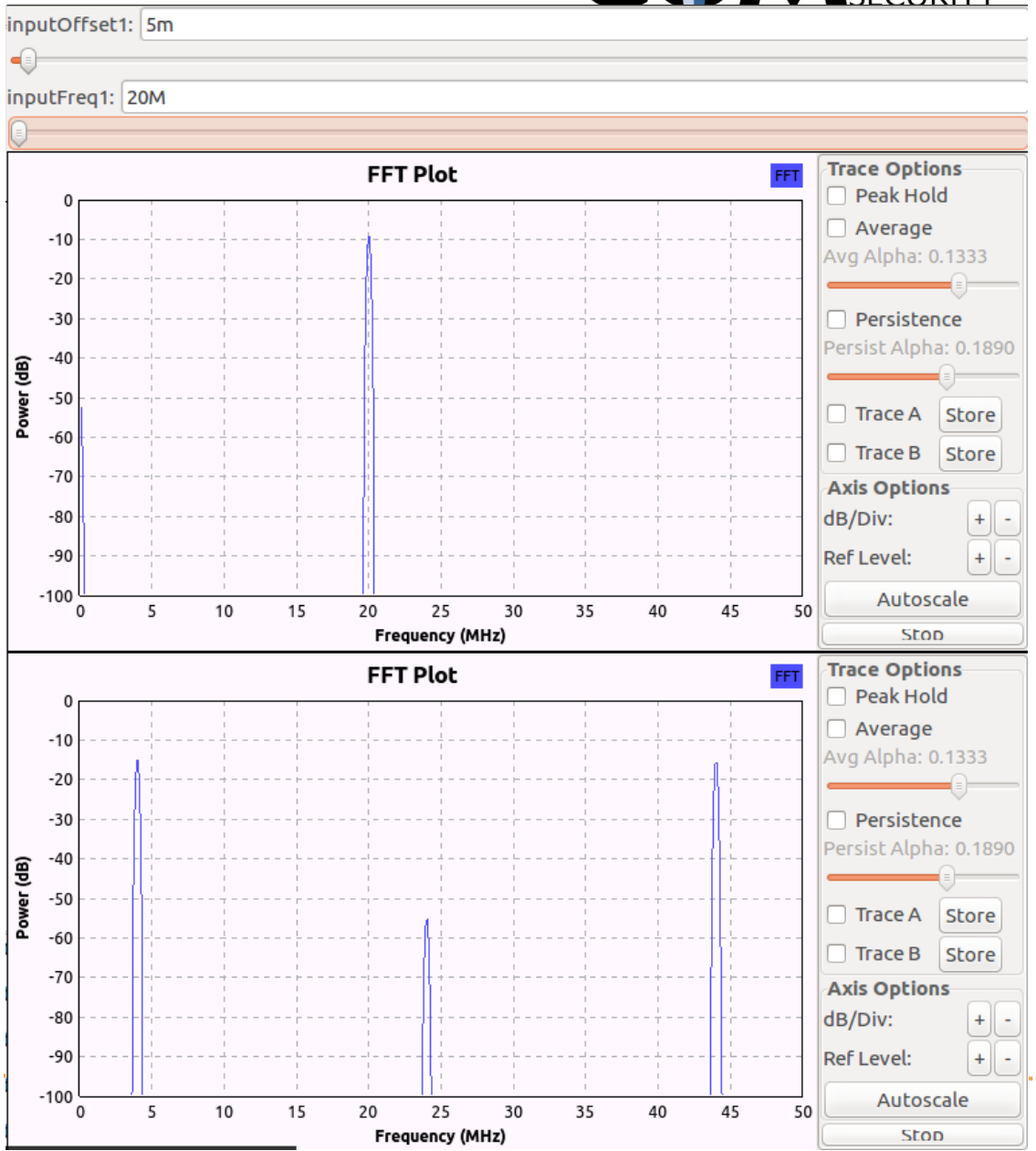


Zwischenfrequenz

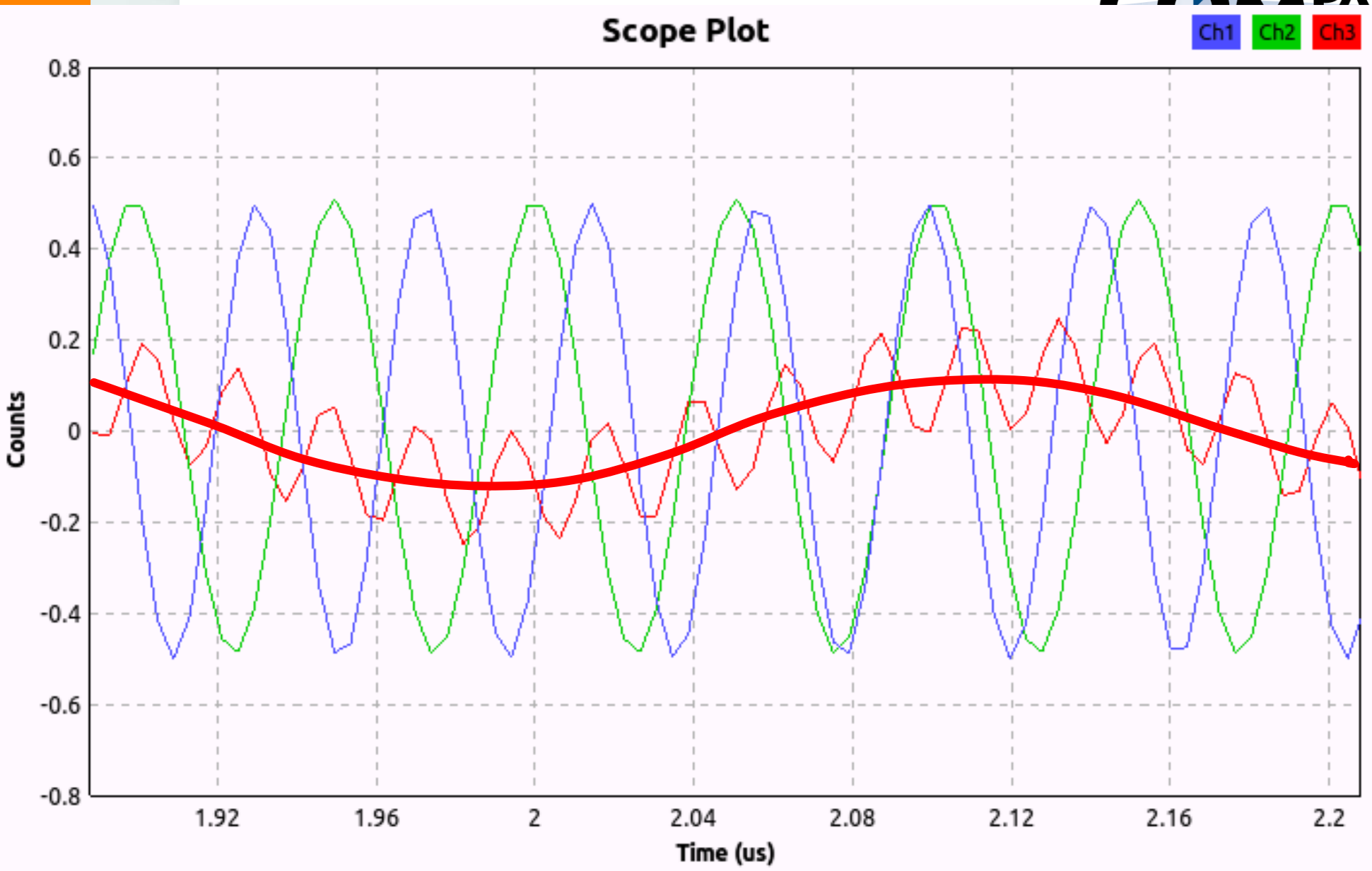
$$f_{ZF} = f_{LO} - f_e \text{ oder } f_{ZF} = f_{LO} + f_e.$$

f_{LO}=24MHz
f_e=20MHz

DC-Offset durch nicht Linearitäten



Mixer


Scope Plot
Ch1
Ch2
Ch3
Counts
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
1.92
1.96
2
2.04
2.08
2.12
2.16
2.2
Time (us)

Replay Attacken

- Die einfachste Attacke, keine Kenntnisse von der Modulation nötig.

Replay Attacken

- Funk aufzeichnen:

```
hackrf_transfer -r doorBell.wav -f 433500000 -l 32 -g 28 -b 1000000 -s
    10000000
```

- Aufzeichnung senden:

```
hackrf_transfer -t doorBell.wav -f 433500000 -x 40 -b 1000000 -s
    10000000
```

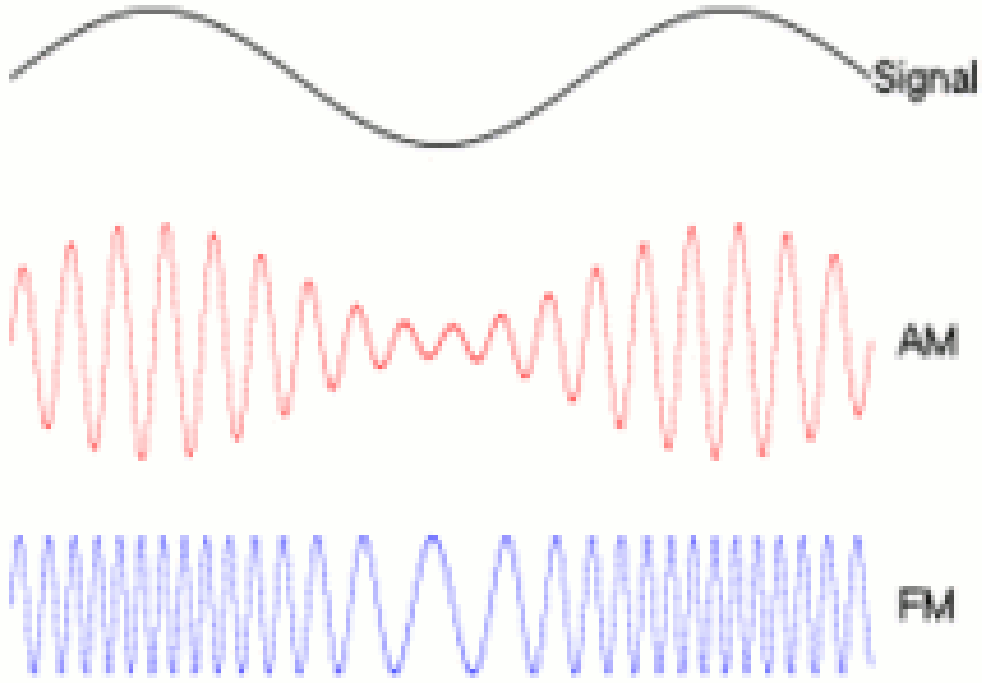
Modulationen

- Theorie zu den Modulationen

Analoge Modulationen

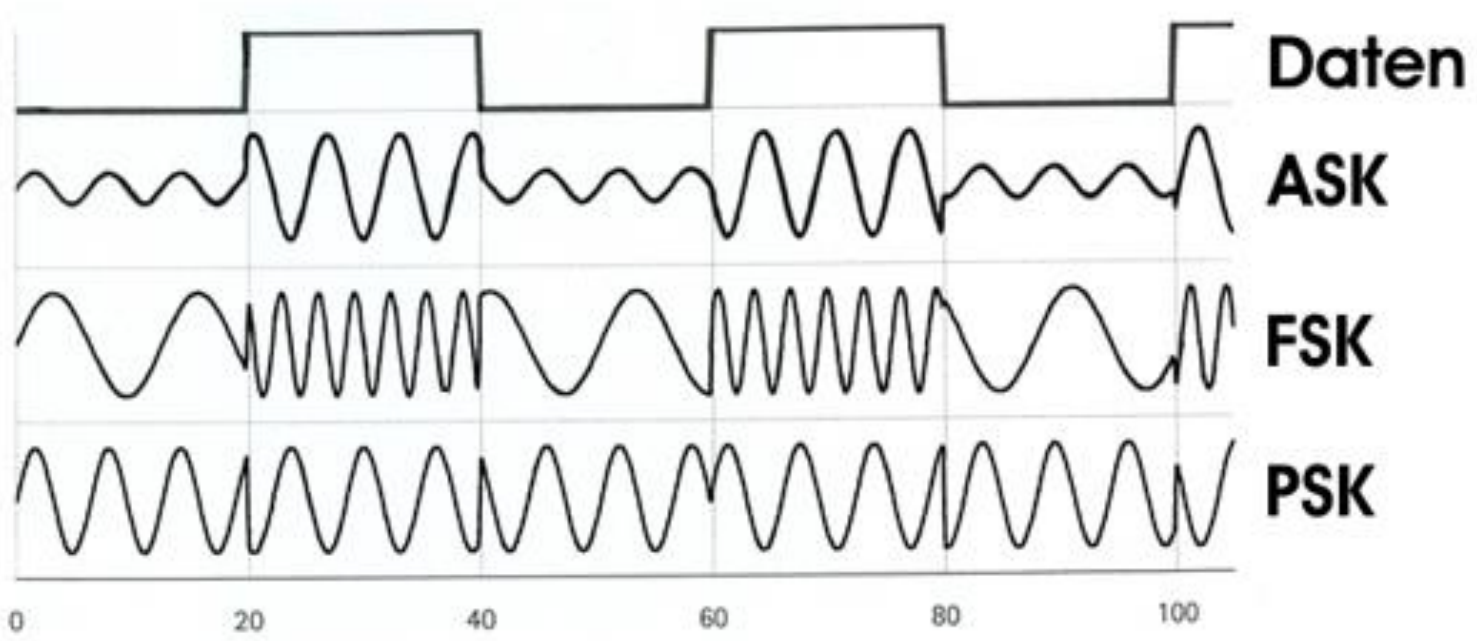
AM: Amplituden Modulation

FM: Frequenz Modulation



Digitale Modulationen

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)

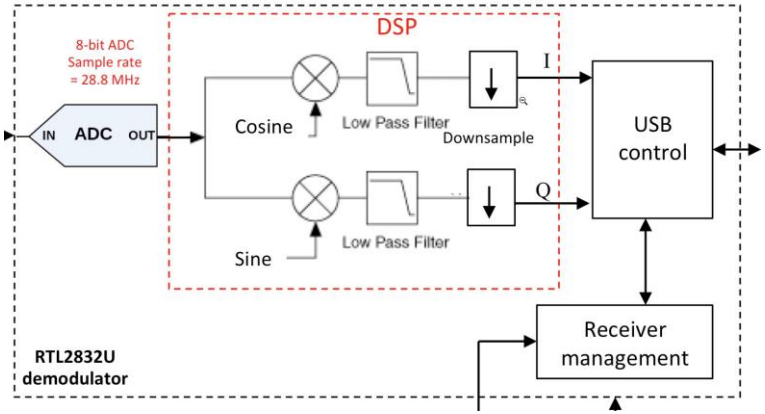


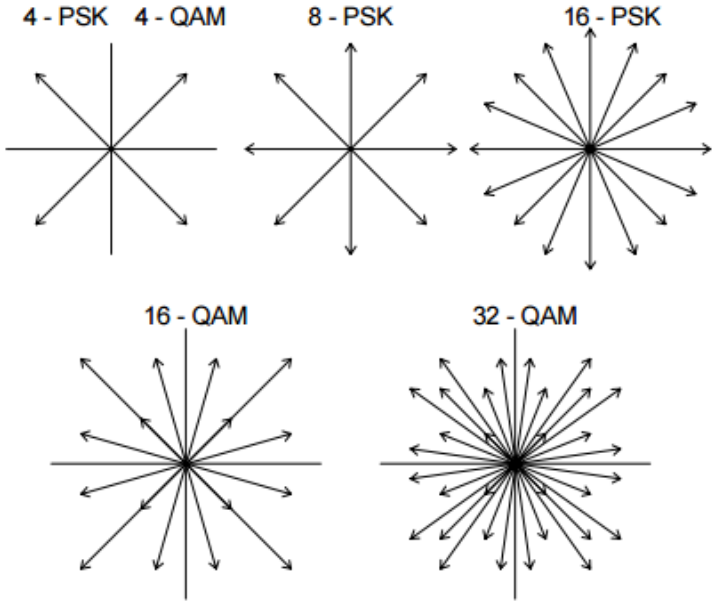
Phase Shift Keying (PSK)

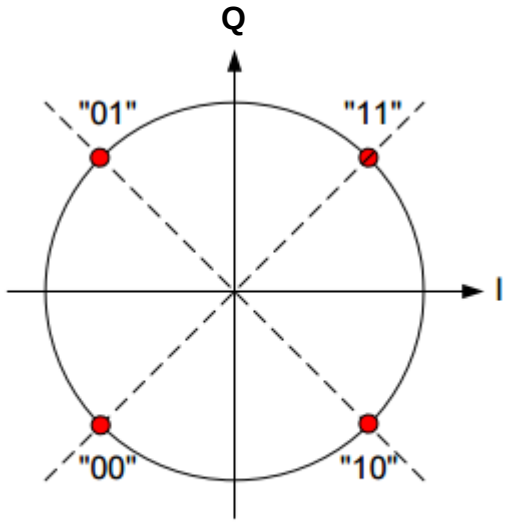
Phase Shift Keying PSK

Quadratur Amplituden Modulation QAM

Phasen Diagramm:

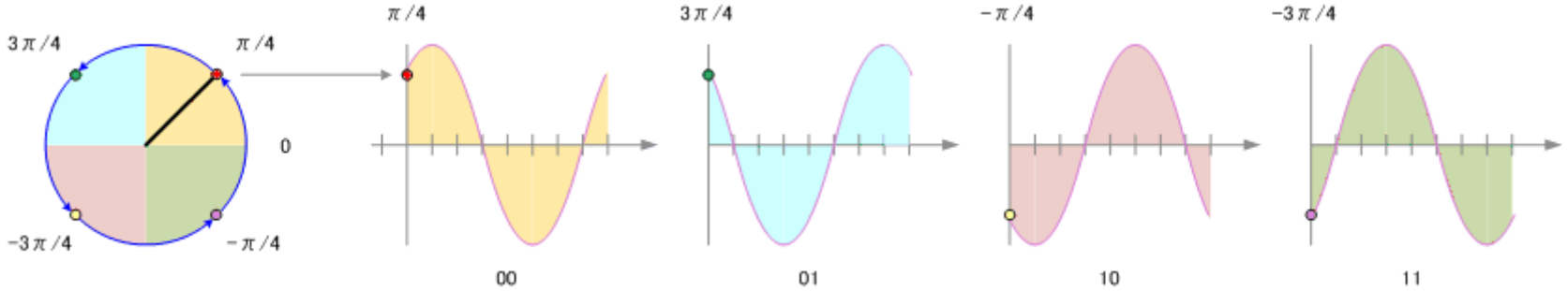


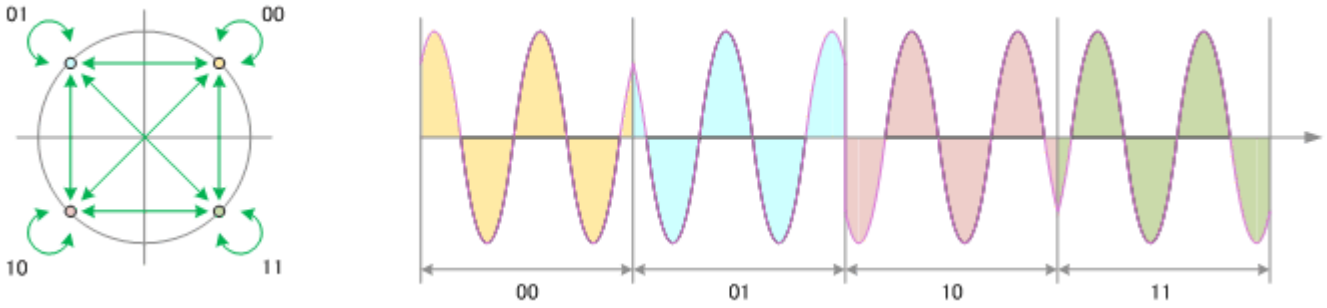




Gray-codiert

PSK Modulation



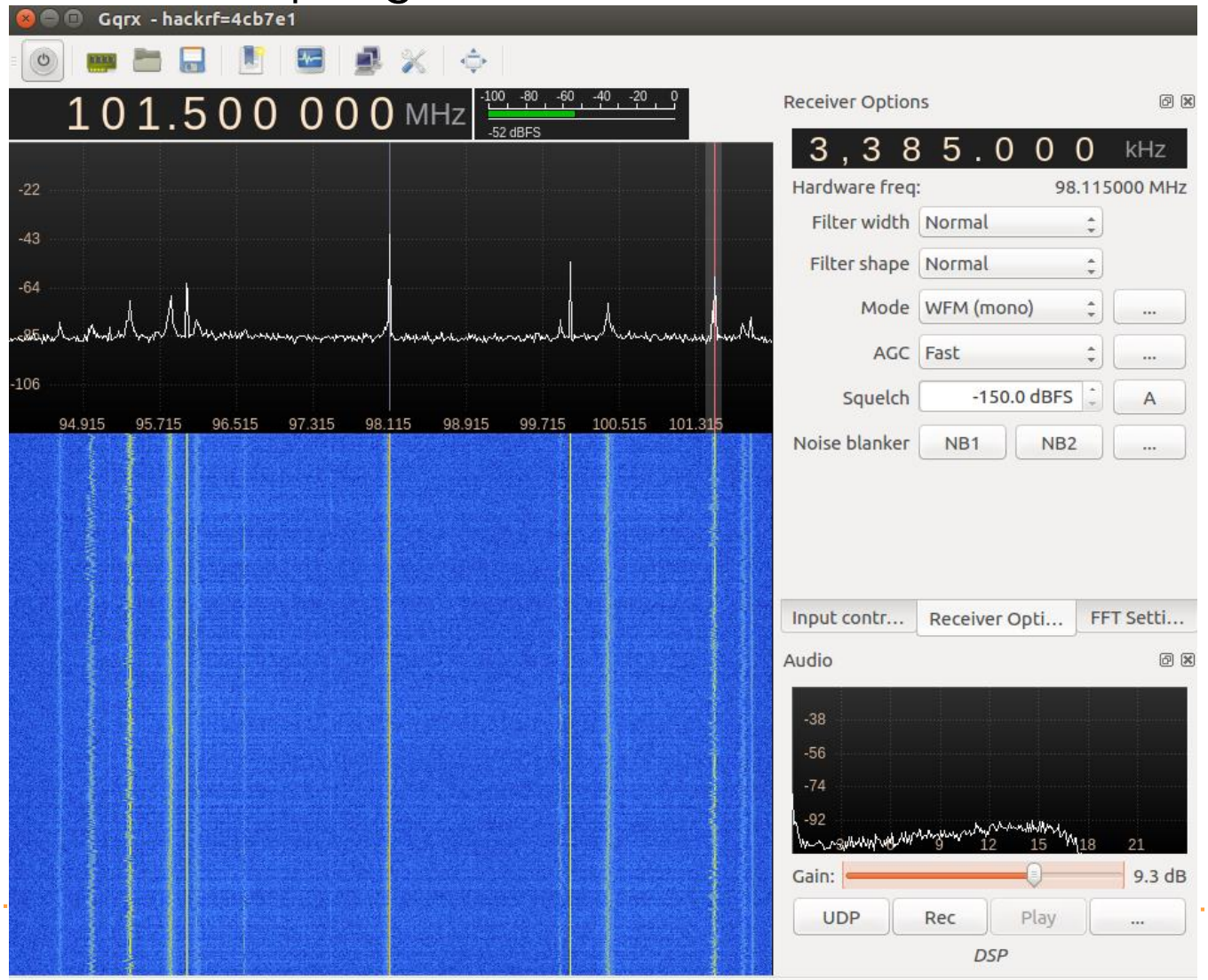


Signale identifizieren mit GQRX und Inspectrum

- Hilfsmittel um die Signale aufzuspüren

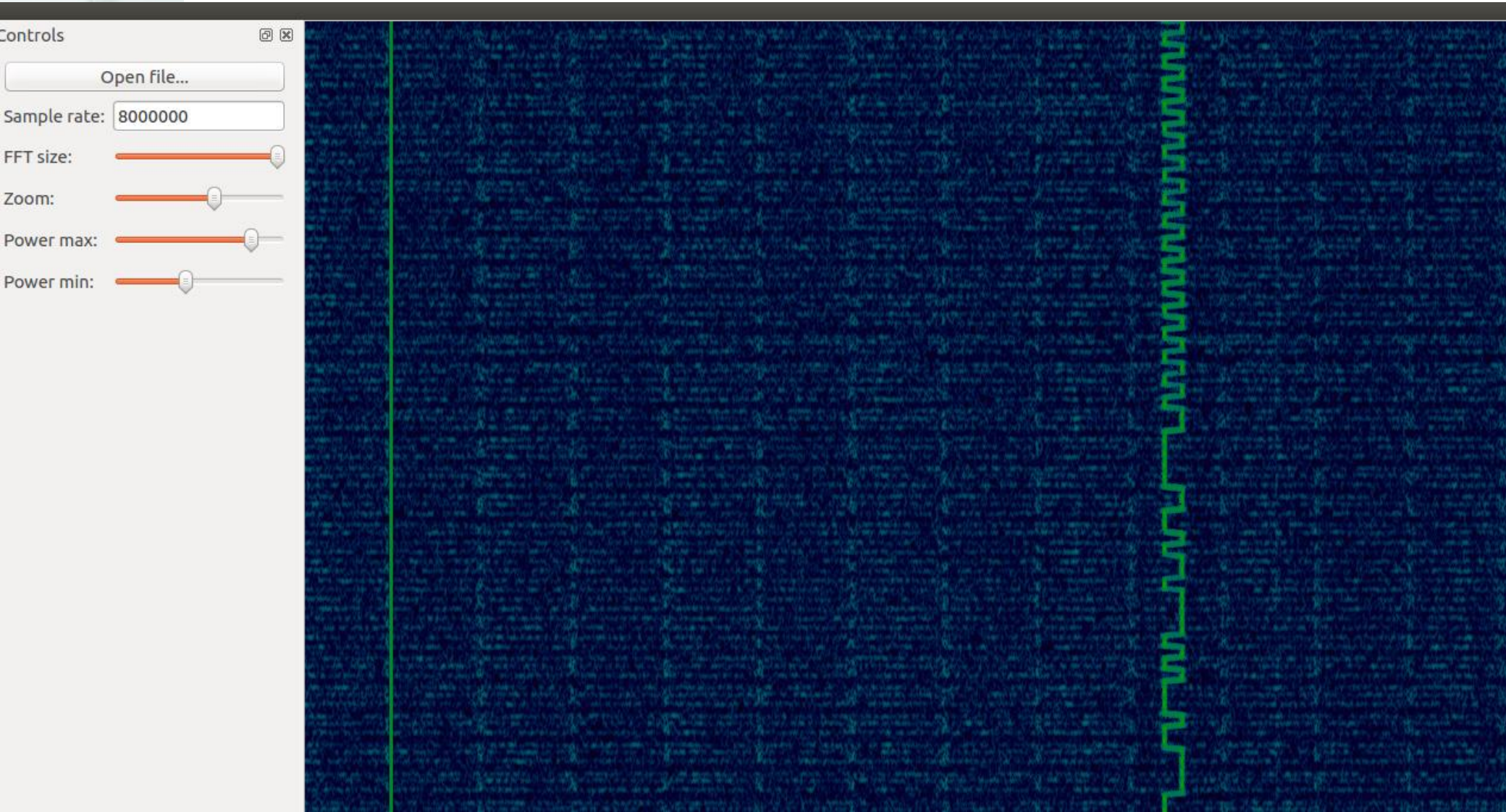
GQRX Software

Breitbandempfänger (z.B. FM-Radio)

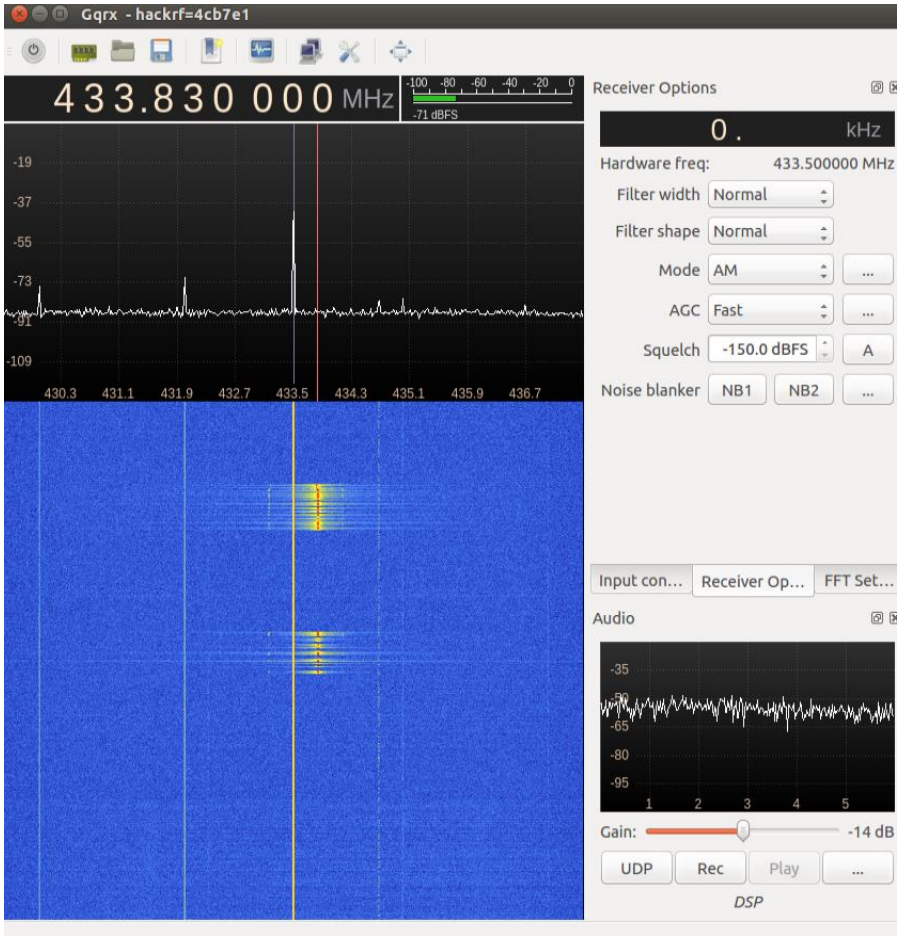


Inspectrum

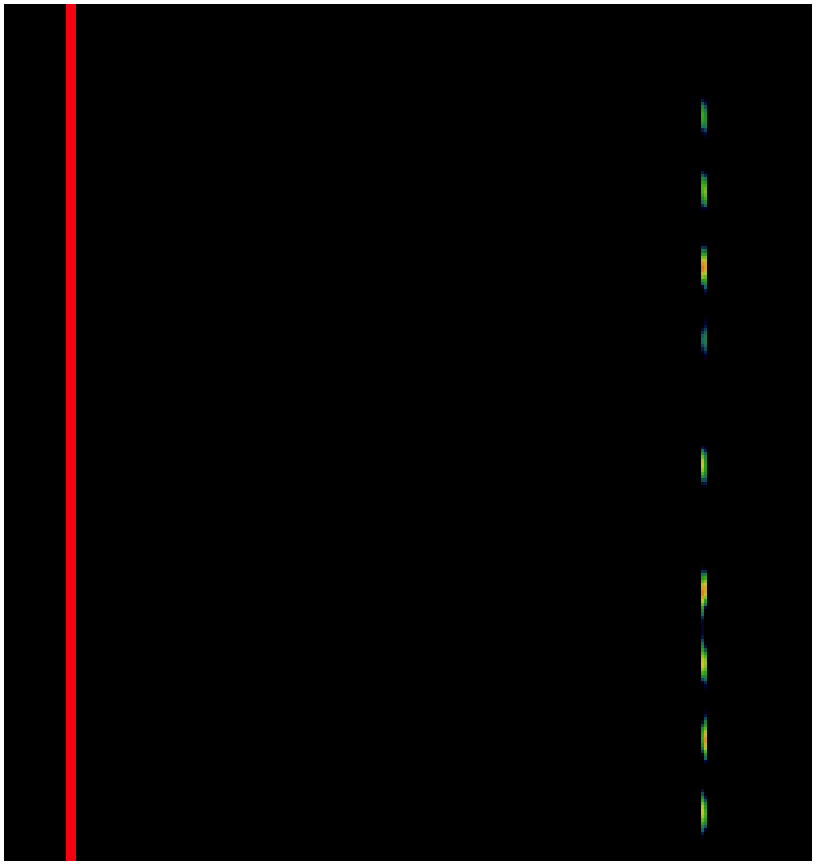
Pager FSK Signal 1.2kBit/s – mit Inspectrum zoomen



Türgong 433.92MHz, 2kBit/s



Inspectrum



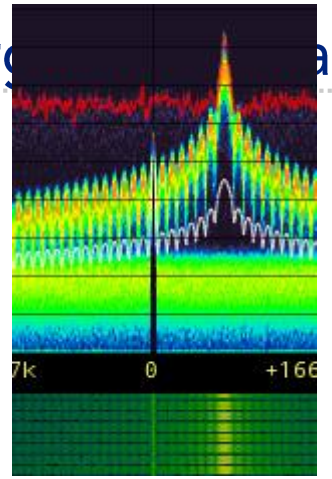
Türgong

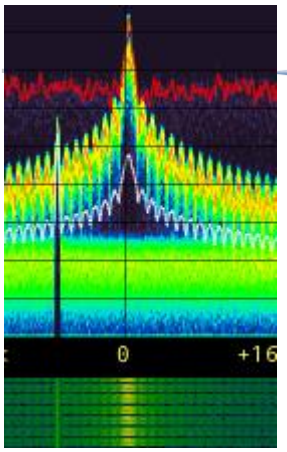
- ASK 2kbit/s, 433.92MHz

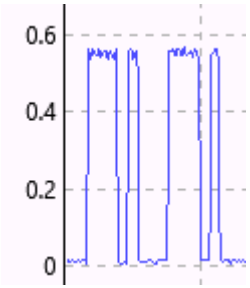
Türgong: Signal Analyse mit GNU-Radio

- Gnuradio erlaubt mit Funktionsblöcken die Signalverarbeitung

Türöffner Datenstream







Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 320k

File Source
File: ...doorbell\rawDump.wav
Repeat: No

Throttle
Sample Rate: 320k

Frequency Xlating FIR Filter
Decimation: 1
Taps: 1
Center Frequency: 20k
Sample Rate: 320k

Complex to Mag

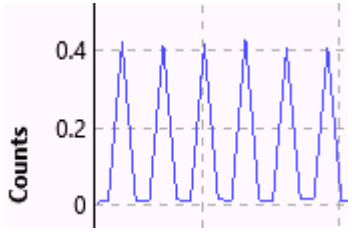
Clock Recovery MM
Omega: 160
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

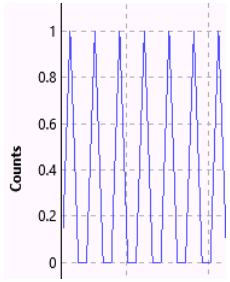
Threshold
Low: 100m
High: 200m
Initial State: 0

Add Const
Constant: -250m

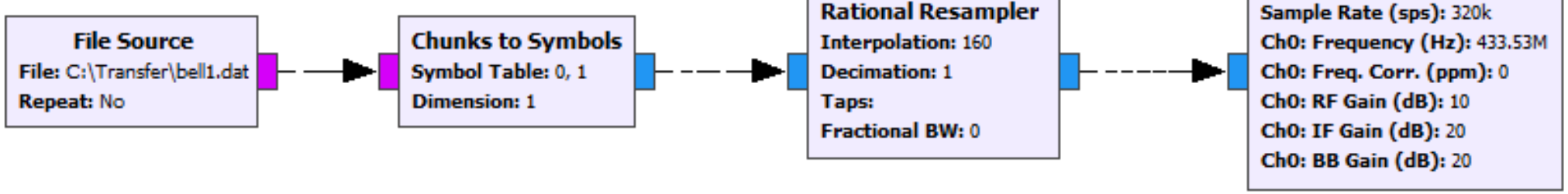
Binary Slicer

File Sink
File: C:\Transfer\bell1.dat
Unbuffered: Off
Append file: Overwrite

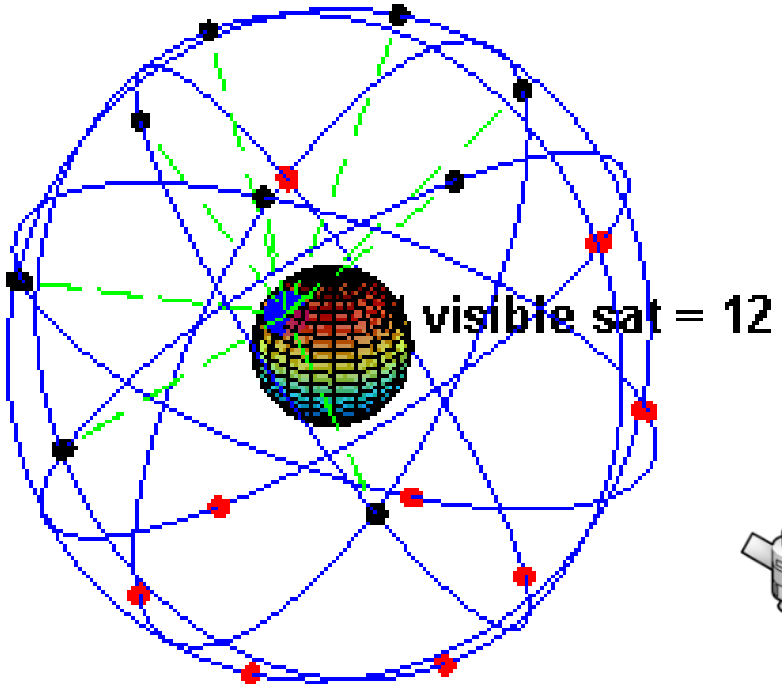


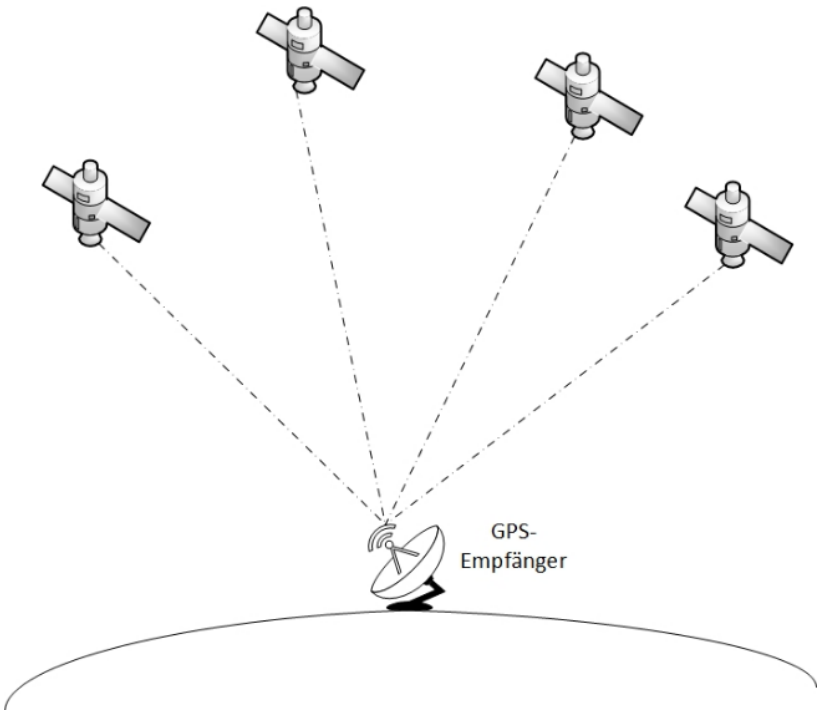


Datenstream senden



GPS

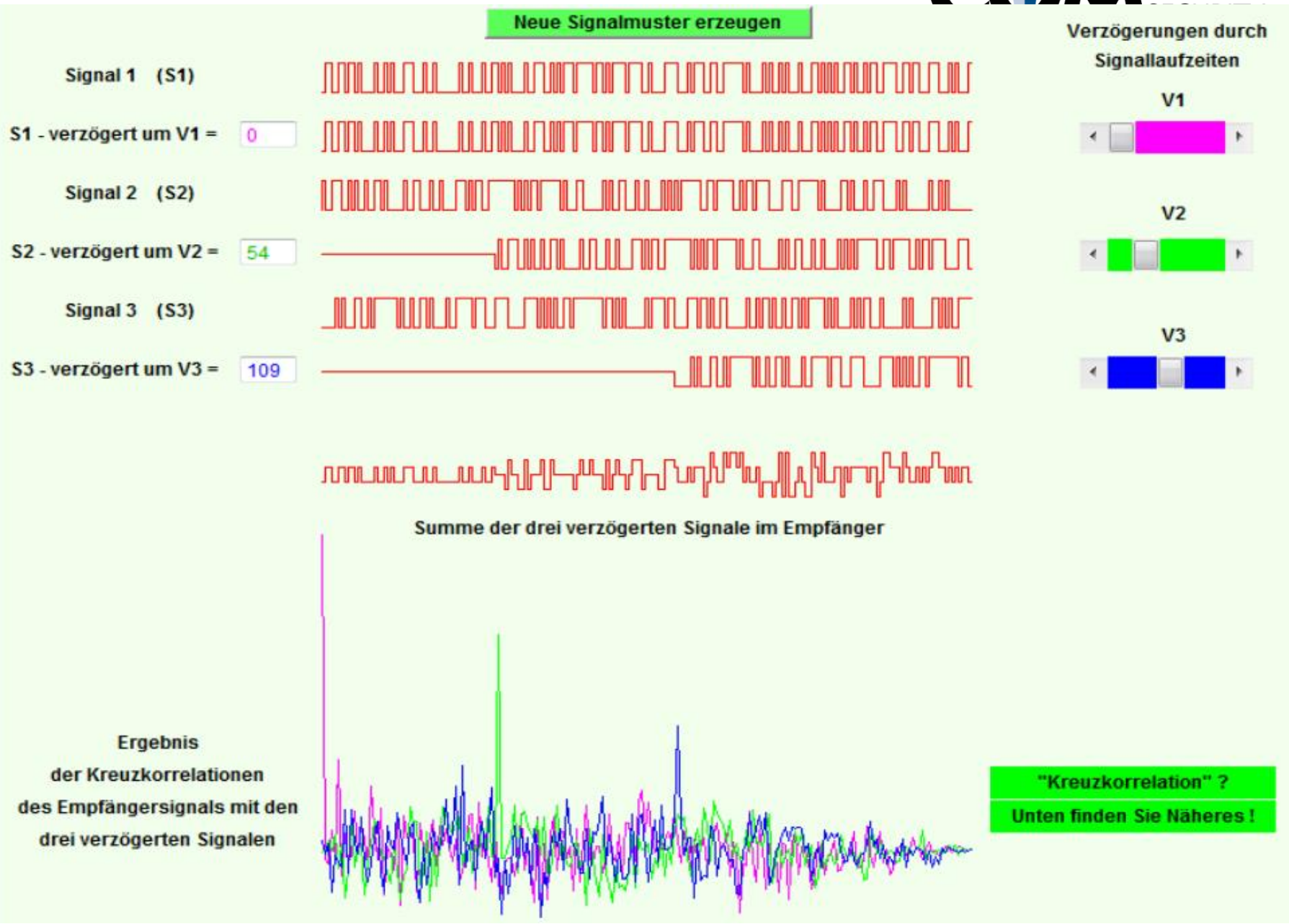




GPS

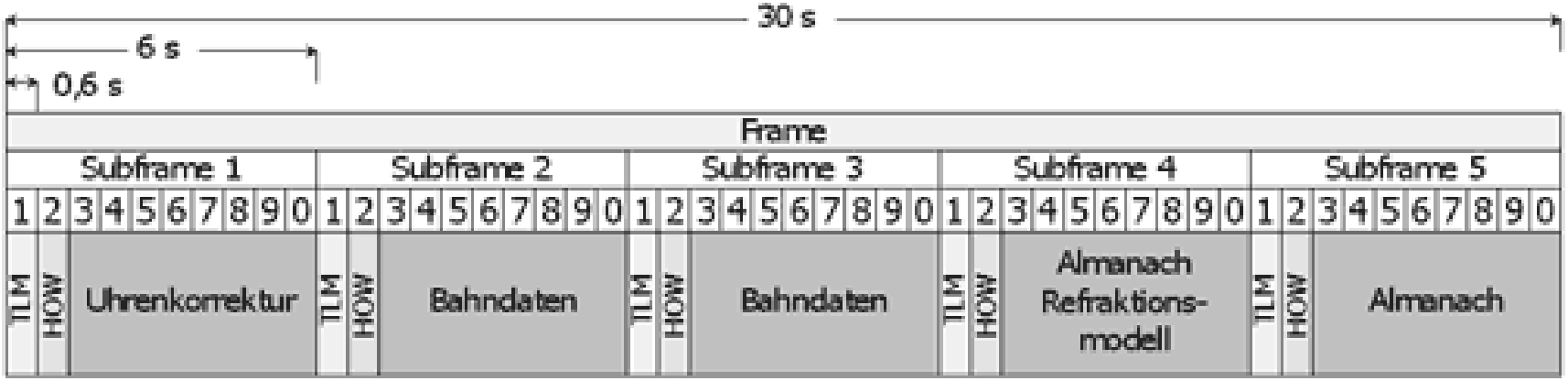
- Alle Satelliten senden auf derselben Frequenz (Codemultiplexverfahren).
- Alle Satelliten besitzen einen festgelegten „Pseudo Random Noise Code“(PRN-Code). Dieser besteht aus 1023 Bits.
- Der PRN-Code und die Daten werden mit einer unterschiedlichen Frequenz in das Trägersignal hinein moduliert.
- Die Kreuzkorrelation wird benutzt um die Signallaufzeiten der einzelnen Satelliten zu ermitteln.

GPS


Neue Signalmuster erzeugen
Verzögerungen durch Signallaufzeiten
Signal 1 (S1)
S1 - verzögert um V1 =
0
V1
Signal 2 (S2)
S2 - verzögert um V2 =
54
V2
Signal 3 (S3)
S3 - verzögert um V3 =
109
V3
Summe der drei verzögerten Signale im Empfänger
Ergebnis der Kreuzkorrelationen des Empfängersignals mit den drei verzögerten Signalen
"Kreuzkorrelation" ?
Unten finden Sie Näheres !

GPS Datensignal

- Zusätzlich zum C/A-Code wird mit 50 bit/s die Navigationsnachricht in das L1-Signal mit hineinmoduliert.
- Darin enthalten sind die Satellitenbahnen, Uhrenkorrekturen und andere Systemparameter
- Die vollständige Übertragung dauert 12.5 Minuten



Struktur der GPS-Navigationsdaten eines "frames"

GPS Spoofing

- GPS Korrektur-Daten sind erforderlich (im Internet verfügbar)
- Generiertes Signal wird zuerst in eine Datei geschrieben, um danach zu senden

Schlussfolgerung

- Gefahr - Jeder kann empfangen und senden:
  - Jamming
  - Garagentor
  - GSM
  - Autonome Autos
- Kein Physicher Zugang zu einem Kabel nötig
- Funkprotokolle müssen sicher sein (Rolling-Code / Encryption)
- SDR: Keine fremden Geräte stören/manipulieren!

Fragen?

Links

RTL-SDR Hardware bei Aliexpress:

https://www.aliexpress.com/item/New-TV-stick-RTL-SDR-USB-2-0-Software-FM-Radio-DVB-T-RTL2832U-R820T2-SDR/32813168086.html

GPS Spoofing Software und GPS Daten:

https://github.com/osqzss/gps-sdr-sim#generating-the-gps-signal-file

ftp://cddis.gsfc.nasa.gov/gnss/data/daily/2017/brdc/