

# HACKING EINES FUNKTHERMOSTATS

SDRs und die wunderbare Welt der Funkverbindungen



# VORSTELLUNG



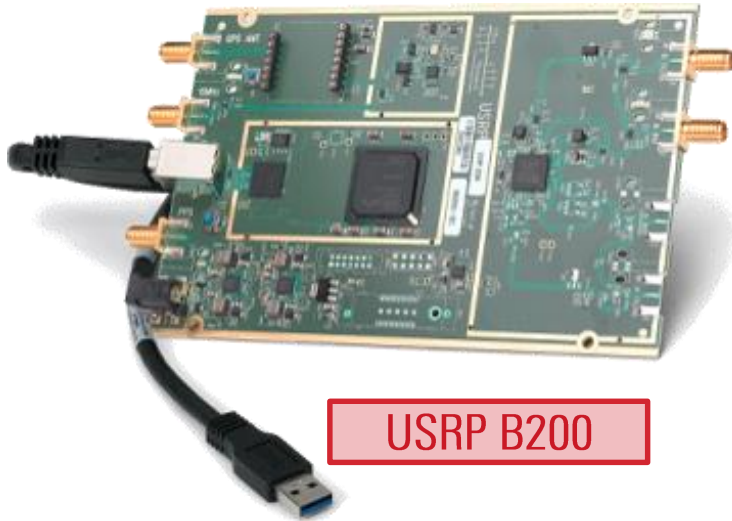
## Gerhard Klostermeier

- Pentester / Expert IT Security Consultant
- Seit 2014 bei SySS GmbH
- Teammanager „Embedded Security“
- Interessen: Hardware-Hacking, IoT, Automotive, Funktechnologien, NFC/RFID, Android usw.
- E-Mail-Adresse: [gerhard.klostermeier@syss.de](mailto:gerhard.klostermeier@syss.de)

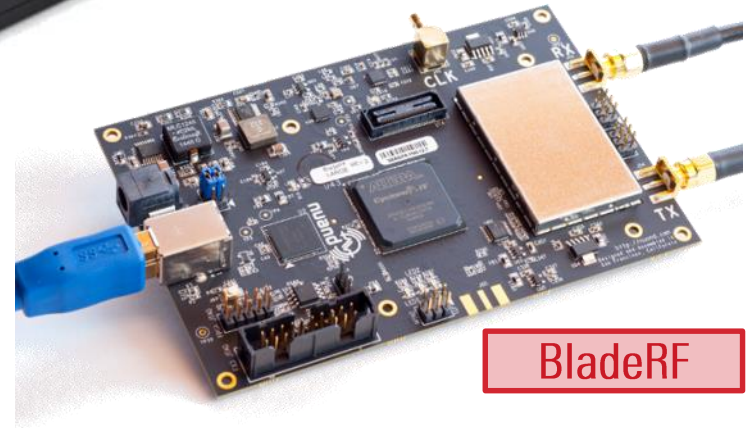
# Wireless-Hacking

# WERKZEUGE: HARDWARE

HackRF One



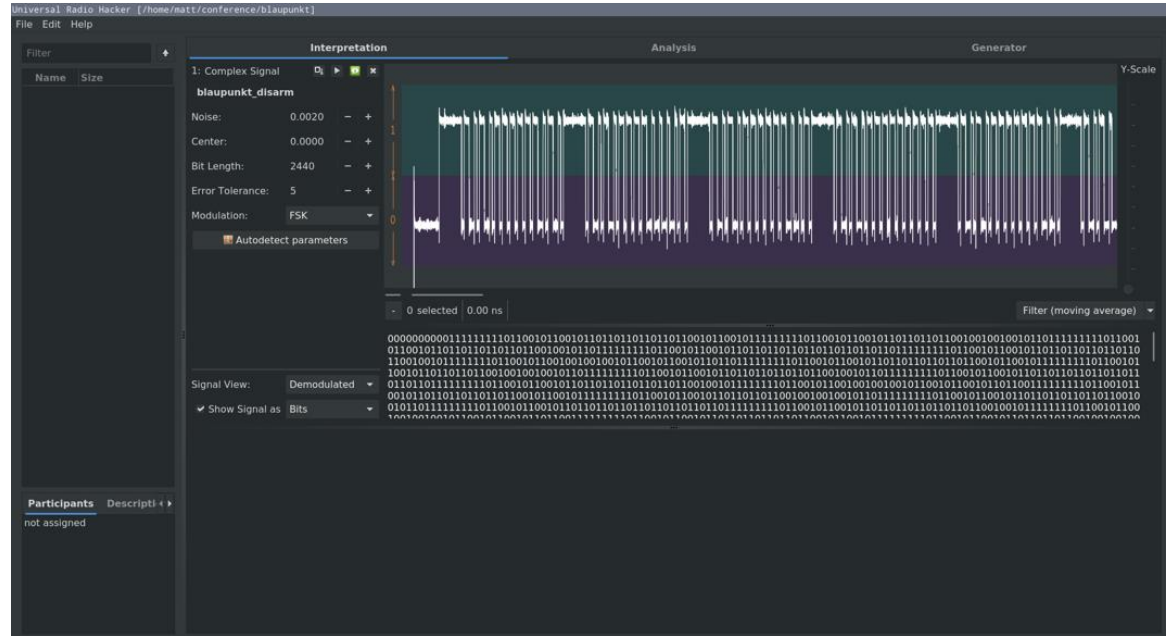
USRP B200



BladeRF

# WERKZEUGE: SOFTWARE

- GNU Radio
- Universal Radio Hacker
- GQRX
- SDRangel
- Inspectrum
- ...



# WERKZEUGE: GADGETS



## Sub-1 GHz Transceiver

### Sub-1 GHz Range

This is the operating range for a wide class of wireless devices and access control systems, such as garage door remotes, boom barriers, IoT sensors and remote keyless systems.

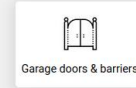
Flipper has an integrated 433MHz antenna, and a CC1101 chip, which makes it a powerful transceiver capable of **up to 50 meters range**.



Smart sockets & bulbs



IoT sensors & doorbells



Garage doors & barriers

### Customizable radio platform

CC1101 is a universal transceiver designed for very low-power wireless applications. It supports various types of digital modulations such as 2-FSK, 4-FSK, GFSK and MSK, as well as OOK and flexible ASK shaping. You can perform any digital communication in your applications such as connecting to IoT devices and access control systems.

Oh, and one more thing – Flipper uses 433 MHz to communicate with other Flippers out there, so you can make some cyber-dolphin friends :)

Sub-1 GHz antenna

TI CC1101 chip



# UNTERSUCHUNGSGEGENSTAND



# HERSTELLERANGABEN



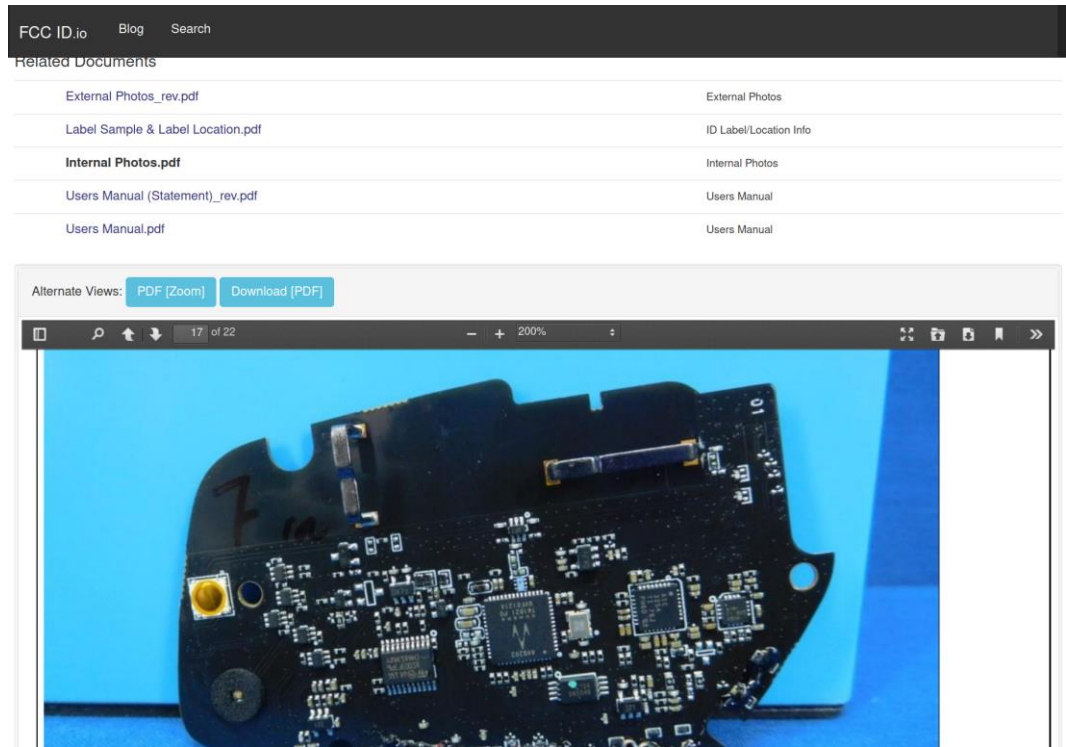
## Technical specification

Power supply	battery (2x1.5 AAA - not included)
Thermostat type	wireless
Type of control	hysteresis (0,2°C)
Accuracy	0,5 °C
Dimensions (LxWxD)	81x81x25 mm
Protection	IP20
Working temperature	0 °C to 40 °C
Temperature changes per day	6
Range of adjustable temperature	5 °C to 39 °C
Temperature setting by	0, 5 °C
Min. programming time	10 min
Min. indication step	0,1 °C
Frequency	433, 92 MHz
Vf power	16 mW
Battery life	heating season



# INFORMATIONSBESCHAFFUNG: FCC(ID)

- Funkende Geräte müssen in den USA durch die Federal Communications Commission (FCC) zugelassen werden
- Prüfberichte sind (meist) öffentlich und durch FCC-ID auffindbar
- Bei der Prüfung werden Fotos vom Testgegenstand gemacht – auch im zerlegten Zustand
- Manchmal sind sogar Chipbezeichnungen abzulesen



The screenshot shows the FCC ID.io website interface. At the top, there are navigation links for 'FCC ID.io', 'Blog', and 'Search'. Below this is a 'Related Documents' section with a table of links:

External Photos_rev.pdf	External Photos
Label Sample & Label Location.pdf	ID Label/Location Info
<b>Internal Photos.pdf</b>	Internal Photos
Users Manual (Statement)_rev.pdf	Users Manual
Users Manual.pdf	Users Manual

Below the table, there are 'Alternate Views' buttons for 'PDF [Zoom]' and 'Download [PDF]'. The main content area shows a PDF viewer displaying a photograph of a disassembled electronic device, likely a smart thermostat, with various components and chips visible on the printed circuit board (PCB). The PCB has some handwritten markings, including 'F' and '10'. The viewer interface includes a search icon, a page indicator '17 of 22', a zoom level of '200%', and navigation arrows.

# Praktische Analyse

# PRAKTISCHE ANALYSE



- Wo funkt das Gerät (Frequenz)?
  - gqrx, sdrangel, GNU Radio (gr-fosphor)
- Wie funkt das Gerät (Modulation)?
  - GNU Radio (gr-fosphor), Universal Radio Hacker
- Wie werden die Daten übertragen (Encoding)?
  - Universal Radio Hacker
- Was für Angriffsfläche ergibt sich daraus?
  - Verschlüsselung, Signaturen, etc.?

THE PENTEST EXPERTS

[WWW.SYSS.DE](http://WWW.SYSS.DE)