Peeeeeow Klonk

Having fun with crane remotes

brian@security-bits.de ~~ www.security-bits.de ~~ @BadgeWizard

About Me

- Brian Butterly
- Hacker / Security Researcher
    - Hardware, Embedded, Telco/Cellular
- Currently Lead Security Architect
    - Day job, Fibre / Telco
- Sometimes get into fights concerning quality of security measures
    - And have the urge to motivate people to look into new topics

Why Cranes?

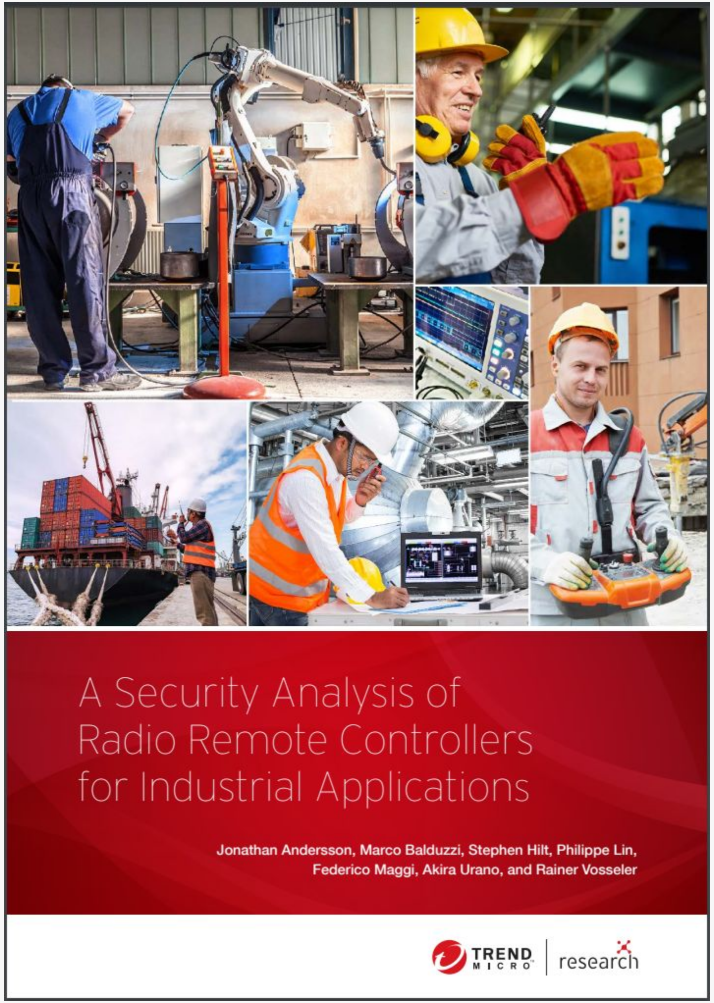
- A while back I had a larger discussion on Security
    - With an RF focus
- My big example was a set of portable traffic lights next to roadworks
- Simple, exposed but with a significant potential impact
- Needing to prove a point I bought a set on eBay and…

Portable Traffic Lights

- “Old”
  - Simple, audible FM transmission
  - Does the job
- No signal, lights go to flashing yellow
  - Typical error state
- Technically speaking an industrial RF remote control system
- Cranes simply have a more controllable impact
  - And I was curious

Industrial RF Remotes

- Not a new topic to be honest
- A Security Analysis of Radio Remote Controllers for Industrial Applications
  - TrendMicro 2019
- Honestly think it’s worth a reminder
  - And necessary to share some details



A Security Analysis of Radio Remote Controllers for Industrial Applications

Jonathan Andersson, Marco Balduzzi, Stephen Hilt, Philippe Lin, Federico Maggi, Akira Urano, and Rainer Vosseler

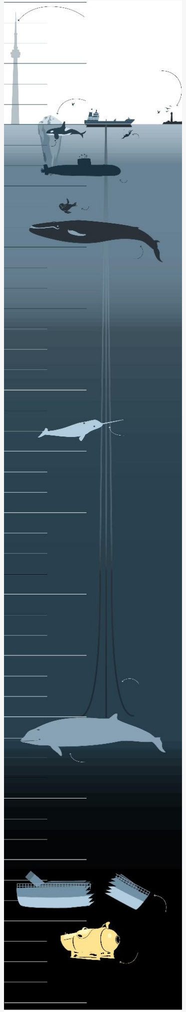
TREND MICRO | research

Case Study 0: Logitech F710

- Sadly famous
- Establishes connection using Logitech Unifying dongle
- First pwned 2016
  - BastilleResearch, MouseJack
- Further vulns published in 2019
  - Marcus Mengs
- Issues including key press injection, forced pairing and session key extraction
  - Game over…

Case Study 0: Logitech F710

- Vulnerable, easy to pwn
    - At least if you can get close enough and depending on the version
- The likelihood of somebody diving down to 3000m to attack the controller … well
    - Maybe a submarine heist? FlipperZero to hijack the sub from the inside?
        - Sounds potentially deadly



Case Study 0: Logitech F710

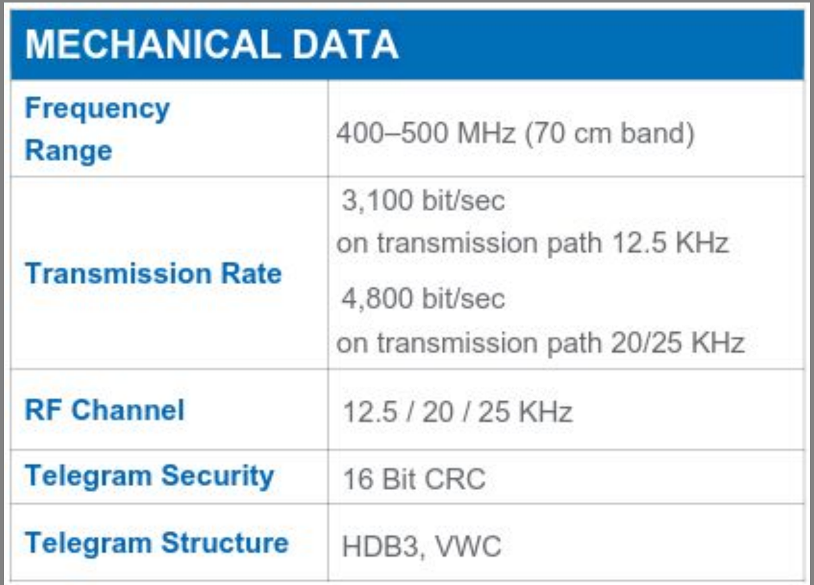
- To be fair, most criticism concerning the controller was probably safety and reliability based

Case Study 0: Logitech F710

- To be fair, most criticism concerning the controller was probably safety and reliability based
- Buuuut...
    - Let’s be honest, the potential shit storm caused by players concerning connection losses during tournaments or even casual gaming would be ginormous
- Maybe it was actually a good choice?
    - Does the gaming industry have higher requirements than the industrial world?

Approaches & Measures

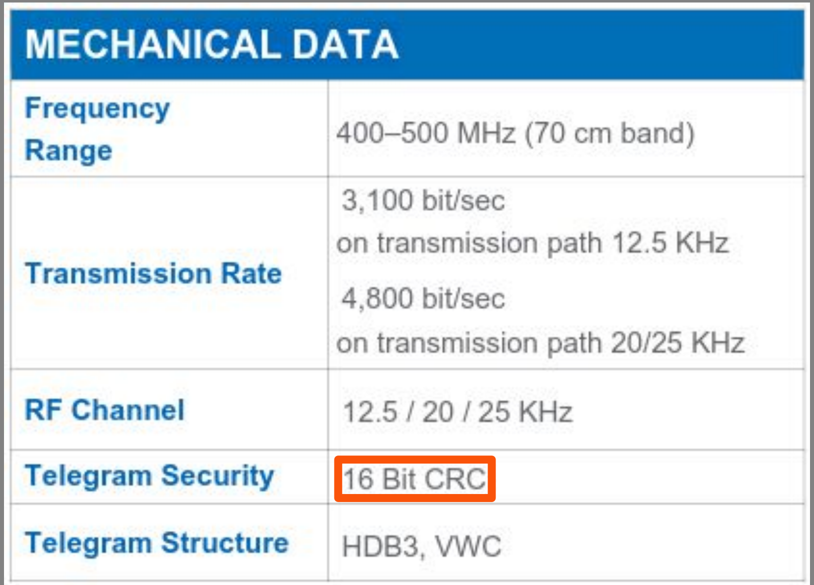
Security, Safety,
“works as designed”



MECHANICAL DATA	
Frequency Range	400–500 MHz (70 cm band)
Transmission Rate	3,100 bit/sec on transmission path 12.5 KHz 4,800 bit/sec on transmission path 20/25 KHz
RF Channel	12.5 / 20 / 25 KHz
Telegram Security	16 Bit CRC
Telegram Structure	HDB3, VWC

Approaches & Measures

Security, Safety,
“works as designed”



MECHANICAL DATA	
Frequency Range	400–500 MHz (70 cm band)
Transmission Rate	3,100 bit/sec on transmission path 12.5 KHz 4,800 bit/sec on transmission path 20/25 KHz
RF Channel	12.5 / 20 / 25 KHz
Telegram Security	16 Bit CRC
Telegram Structure	HDB3, VWC

Jamming

- Works as designed
- RF sucks
- Jamming is super trivial
  - Louder signal, nothing specific
- Connection drops
- Should be covered by basic safety measures
  - I.e. a moving system stops
  - In return stopping a system can still cause issues

Measures & Approaches

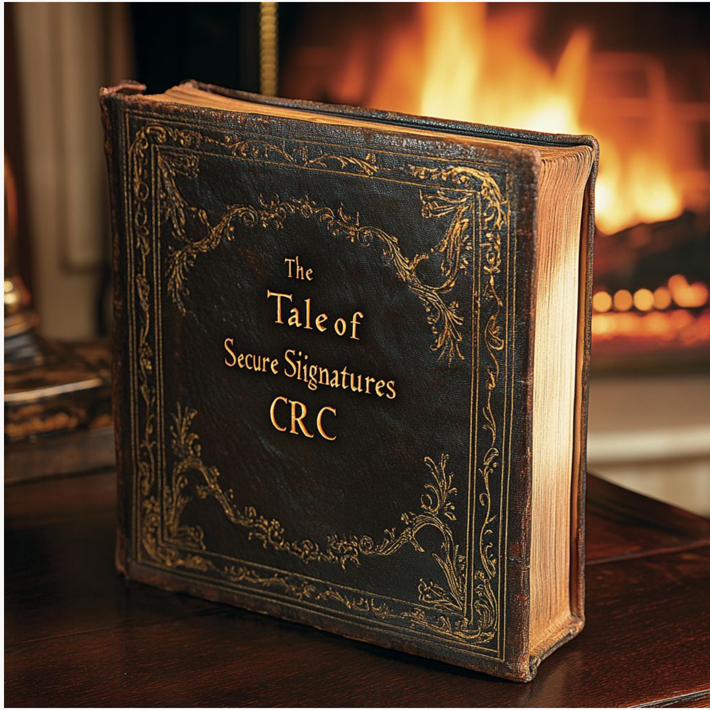
Periodic Transmission

- Periodic Transmission
- Allows receiver to detect loss of signal
- Usually safety feature
    - If something happens to the operator the system goes into a power-down state
- Practically also makes attacks by far harder
    - Injection can cause contradicting signals
    - Which may be detected

Measures & Approaches

Integrity & Error Detection

- RF is prone to transmission faults
  - Random or interferences
- It should obviously be ensured that commands are not misinterpreted
  - Down instead of up
- CRC or Hamming codes



Totally not a fake image!

Measures & Approaches

Emergency Stop

- Big Red Button
- When pressed the remote bursts a specific signal
    - Or packet
- System will stop or systematically go into a safe state
- Usually needs a few manual steps to re-enable
    - That’s where safety lies
- Classic base for DoS attacks
    - A necessary evil

Measures & Approaches
The A-Hole Factor

- Safety risk analysis
  - How likely is a certain event?
  - What are environmental factors like?
  - How likely is event + environmental factors?
- The A-Hole factor counters typical likely hoods by adding malicious intent
  - When a system is attacked, the event >>will<< occour in the worst possible situation
- Sadly malicious intent is usually not part of safety risk analysis

Transmission

- Many different protocols and RF modulations
- Some remotes may be 10..15..20 years old
  - Or even older
  - Especially when having a flexible fleet and insisting on backwards compatibility
  - Or because the used crane is very expensive
- Certain parallels to the world of model planes and vehicles can be seen
  - Well, same basis

Costs

- While OpenSource drone remotes cost <$100 OR $200
- Professional industrial remotes can cost more than $10k
  - Partially due to certification and a small market

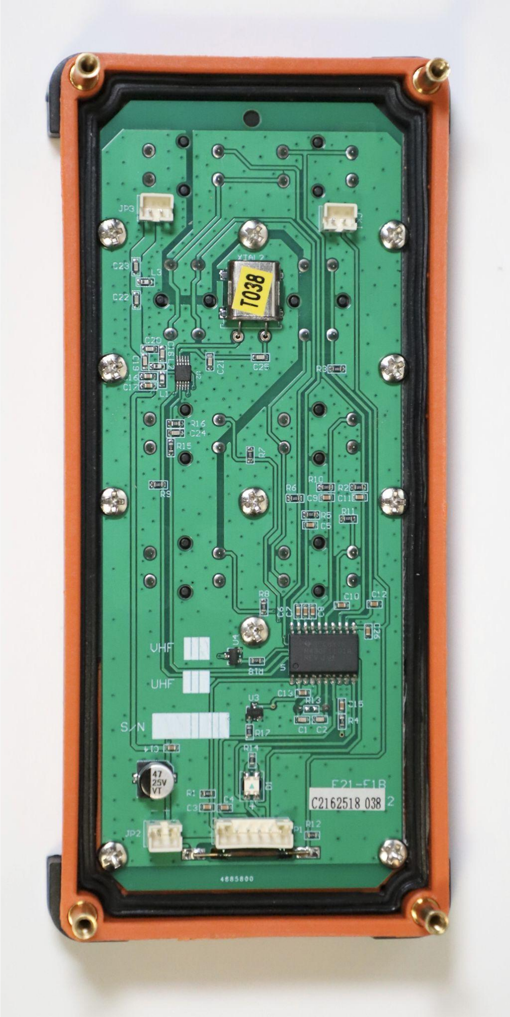
The Real Thing

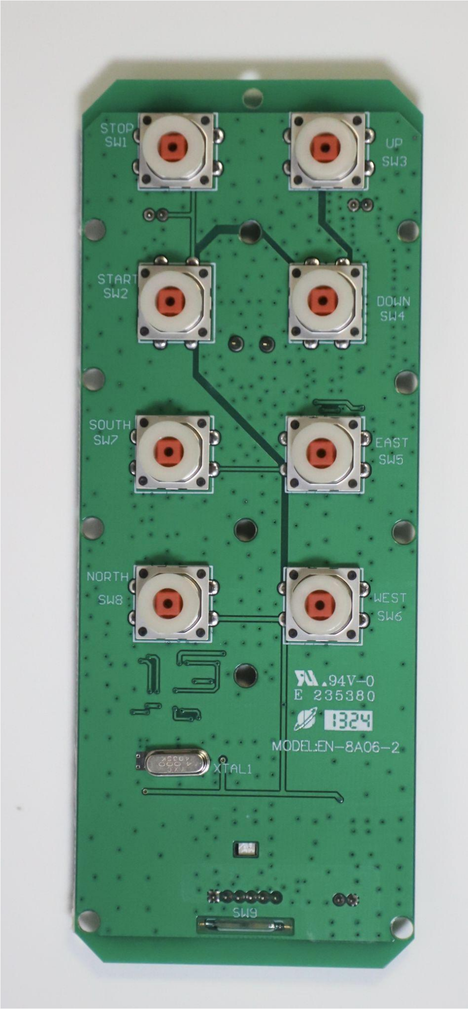
My current collection

Case Study 1:
F21-E1B TX

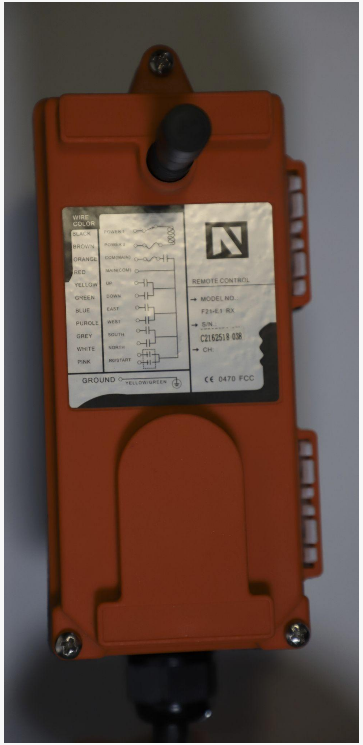
- Frequency: 319.925MHz
- Modulation FSK
- Cheap solution from the far east
- Just a reference
- Based on a MSP430F1101A
  - TDK5101F for the RF, in FSK Mode

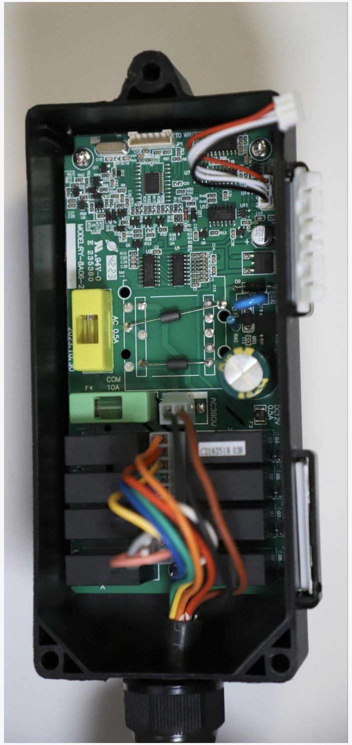
PCB

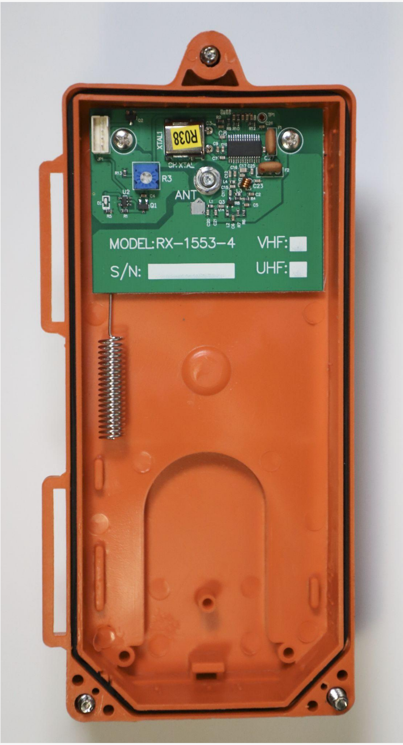

T038
XTAL2
JP3
C23
C22
C20
C25
C21
R3
R16
C24
R15
R9
R6
R10
R2
C9
C11
R11
R8
C5
C10
C12
VHF
UHF
S/N
47
25V
VT
U3
C13
R13
R17
C1
C2
R14
R1
C3
C4
JP2
P1
R12
F21-E1B
C2162518 038
4885800


STOP
SW1
UP
SW3
START
SW2
DOWN
SW4
SOUTH
SW7
EAST
SW5
NORTH
SW8
WEST
SW6
15
.94V-0
E 235380
1324
MODEL:EN-8A06-2
XTAL1
SW9

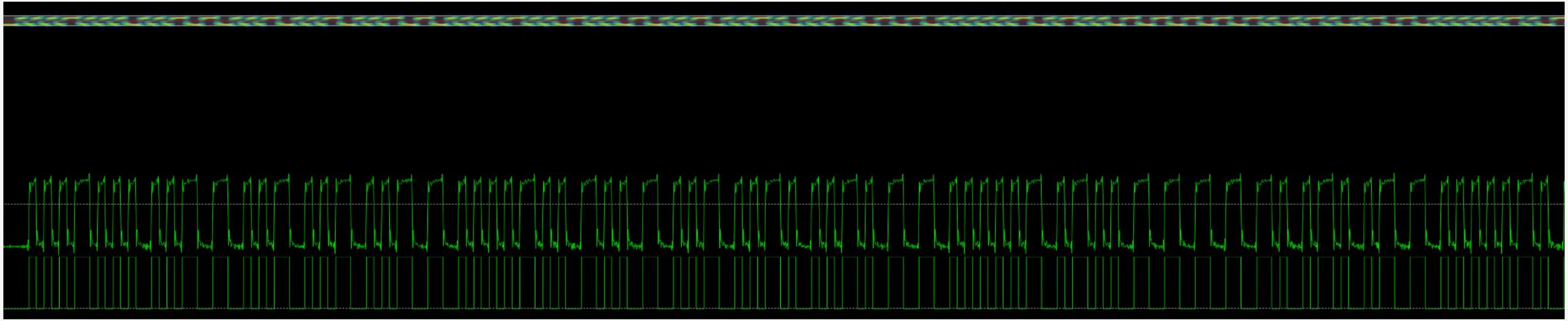
Receiver


WIRE COLOR
BLACK
BROWN
ORANGE
RED
YELLOW
GREEN
BLUE
PUROLE
GREY
WHITE
PINK
POWER 1
POWER 2
COM(MAIN)
MAIN(COM)
UP
DOWN
EAST
WEST
SOUTH
NORTH
R0/START
GROUND
YELLOW/GREEN
REMOTE CONTROL
MODEL NO.:
F21-E1 RX
S/N.:
C2162518 038
CH:
CE 0470 FCC


AC 0.5A
COM 10A
F4
AC380V
DC12V 0.5A
C2162518 038


R038
XTAL
R3
ANT
MODEL:RX-1553-4
VHF:
UHF:
S/N:

Data Transmission

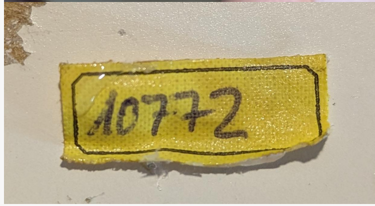


Data Transmission

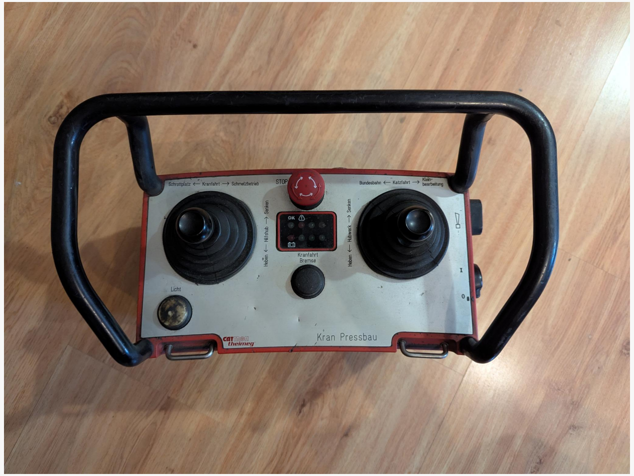
- Decoding results in repeating patterns
  - 101010101010101011001100101010110101010010101011010101001010110011001010110010101100101011001100101010101101010011010100110010101100101011010010101101001100110010101010101100101101010011001100110011001100110011001100110011001100
  - Which make up most of the transmission
- And nicely inverted patterns
  - 1a:10101011010101001010110011001010110010101100101011001100101010101101010011010100110010
    2a:01010100101010110101001100110101001101010011010100110011010101010010101100101011001101
  - 1b:1011001010110100101011010011001100101010101011001011010100110011001100110011001100110011
    2b:0100110101001011010100101100110011010101010100110100101011010011001100101010101010101100
  - Which is the beginning of a new transmission
- Thus next to no randomness → No encryption or signatures

Case Study 2: Cattron TH-EC/40

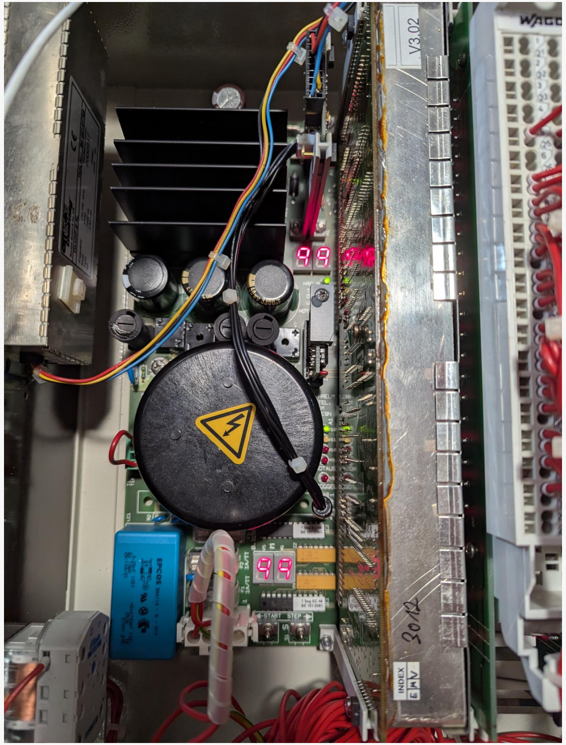
- Frequency: 170.730Mhz
- Modulation: FM using PPM
- Hamming Distance >=6
  - According to manual
- External address module
  - Address is 10772

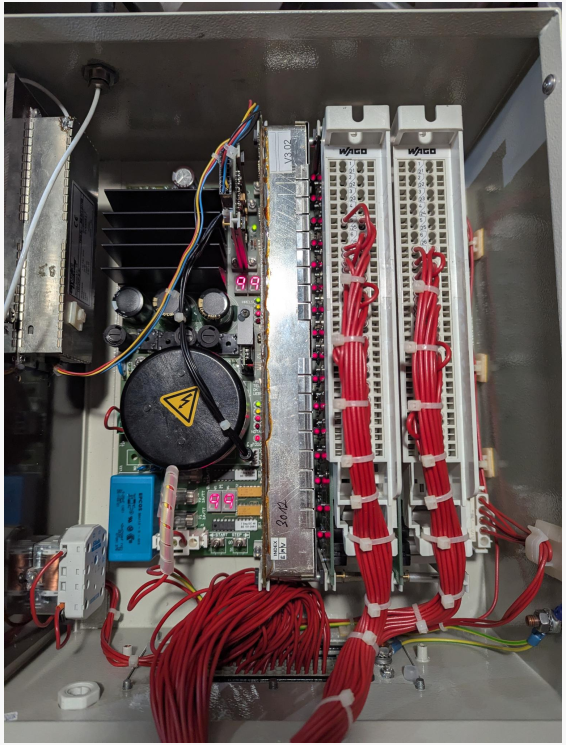


Remote


Schrottplatz ← Kranfahrt → Schmelzbetrieb
STOP
Bundesbahn ← Katzfahrt → Klein-bearbeitung
Heben ← Hilfshub → Senken
OK
Heben ← Hubwerk → Senken
Kranfahrt Bremse
Licht
I
0
CATTRON theimeg
Kran Pressbau

Receiver

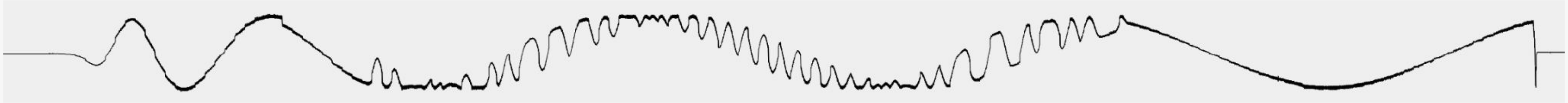

V3.02
WAGO
3012
INDEX
EMV
99


V3.02
WAGO
WAGO
3012

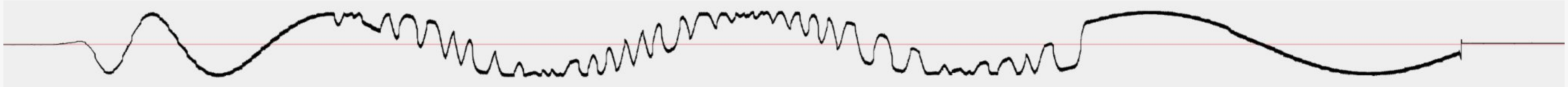
WAGO
WAGO
INDEX

Data Transmission

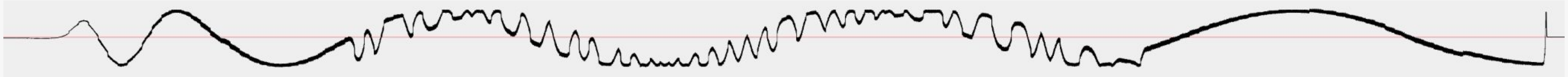
On



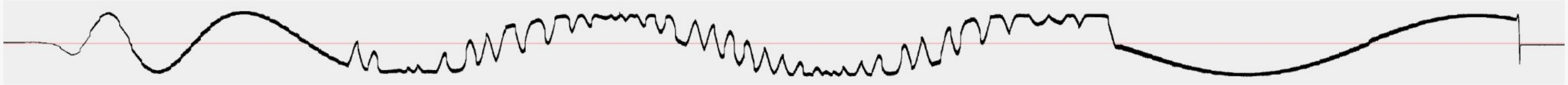
Left Joystick Full Forward



Right Joystick Full Forward

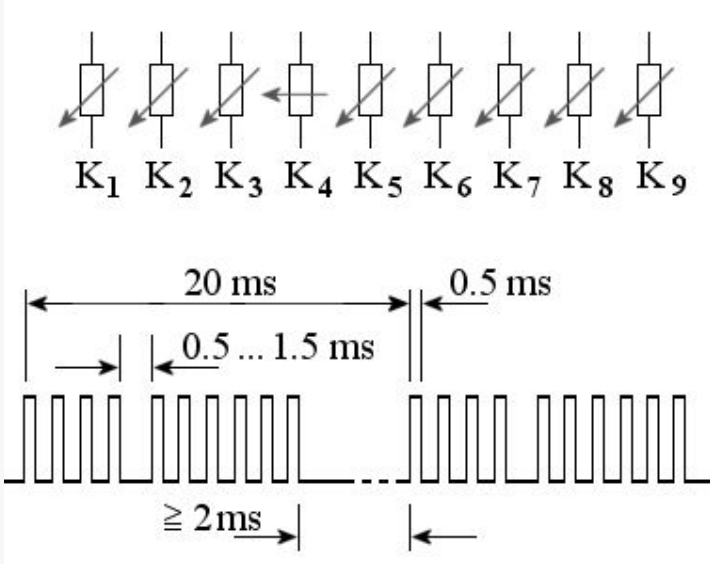


Light Button



Data Transmission

- PPM → Pulse Position Modulation
  - Each pulse is a channel
  - The position of an input/switch is transmitted by the length of the pulse
  - As such a packet with no inputs set is shorter than a packet with all inputs set
- Visualizing the changes is a little bit of a brain fuck due to the underlying carrier wave



Security

- PPM isn’t quite made to transmit large datasets
- In addition the packets are very similar
  - → No randomness, no encryption
- The complexity is small
  - → No cryptographic signatures

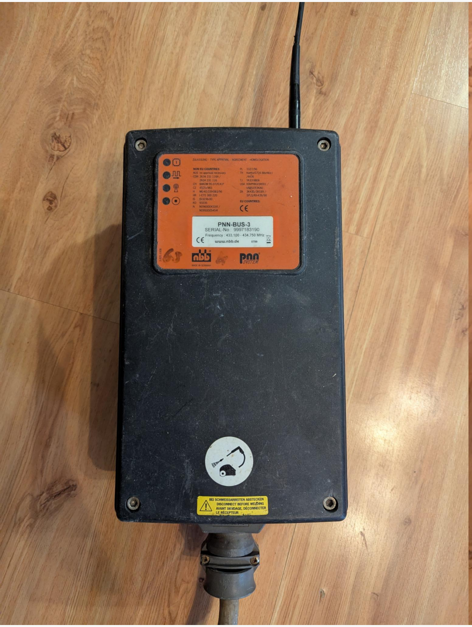
Case Study 3: nbb nano

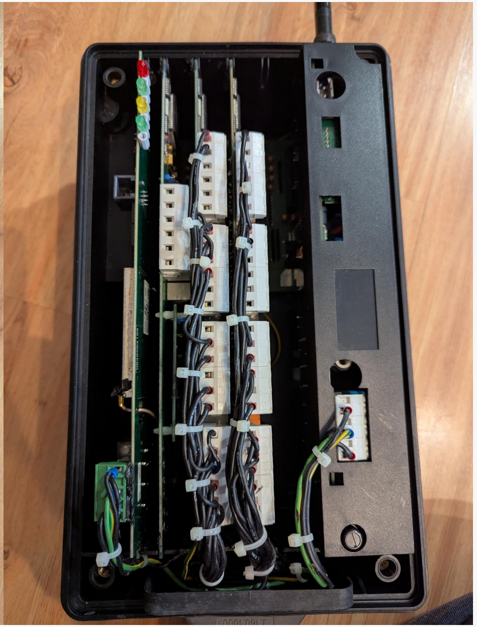
- Frequency: 433.475MHz
- Modulation AFSK
  - CCITT V.23 based
  - Modem style!
- “Security” is in the manual
  - Individual pair of addresses in a 16Bit range

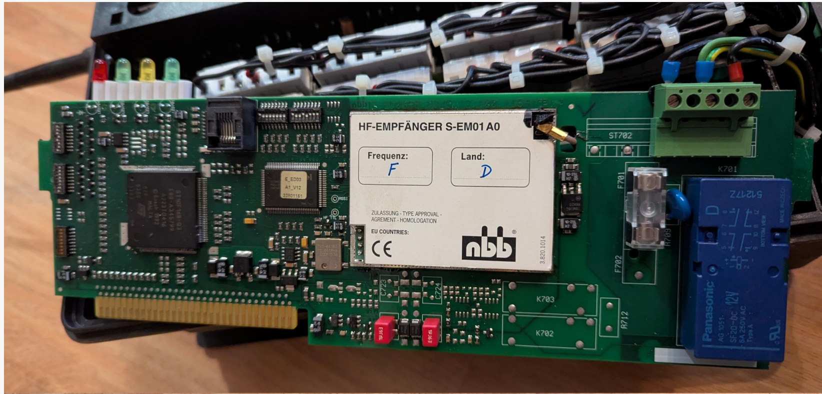
Closed Communication System

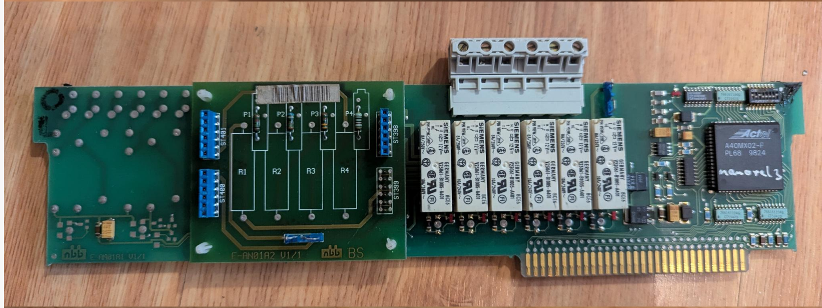
- Seen it, and heard it before
- Some companies treat RF communication between remote and receiver as a closed communication system
  - They have dedicated addresses so no third component can interfere
- Practically all addresses are transmitted as part of the packets
  - And are as such exposed

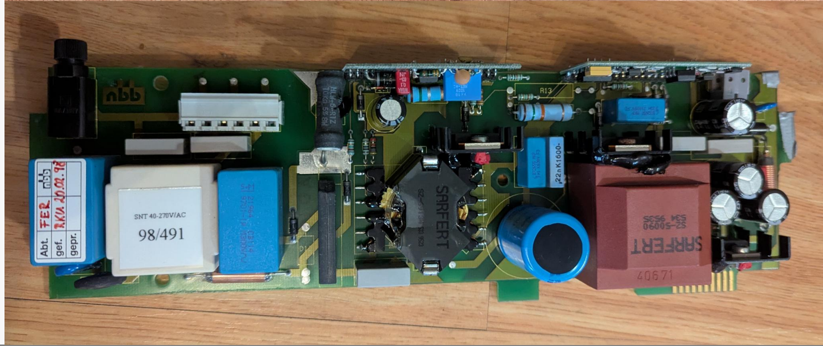
Receiver


PNN-BUS-3
SERIAL-No.: 9997183190
nbb
pnn



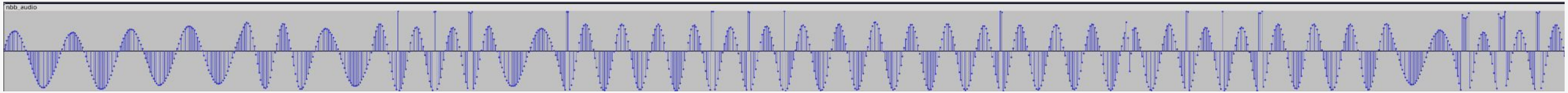

HF-EMPFÄNGER S-EM01 A0
Frequenz:
F
Land:
D
ZULASSUNG - TYPE APPROVAL - AGREMENT - HOMOLOGATION
EU COUNTRIES:
CE
nbb
ST702
K701
K702
K703
Panasonic


P1
P2
P3
P4
R1
R2
R3
R4
SIEMENS
Actel
E-AN01A2 V1/1
nbb BS


nbb
Abt. FER
gef.
gepr.
SNT 40-270V/AC
98/491
SARFERT
R13

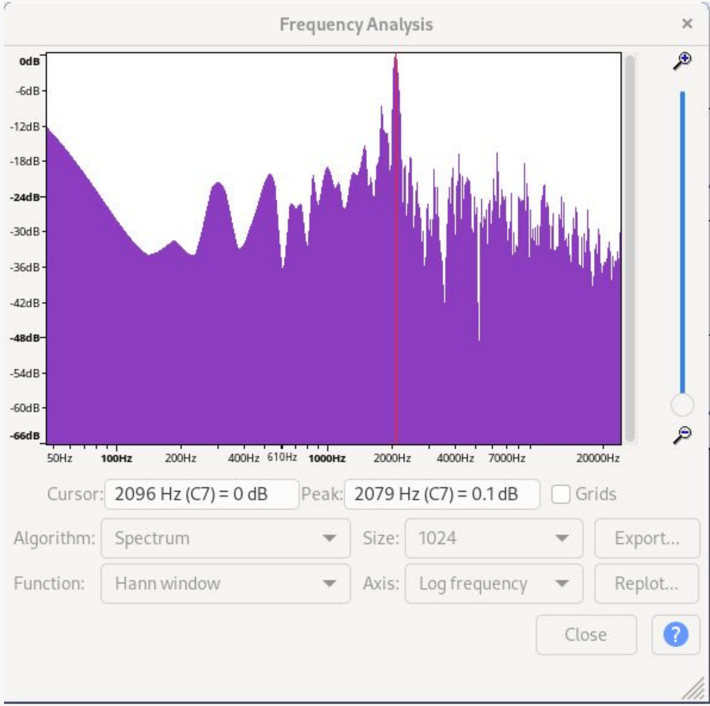
Do we have audio?

Beautiful view in Audacity



Data Transmission

- The frequency analysis gives us further insight into the used transmission mode
  - The peak at 2079Hz, close to 2100Hz
  - And the one hat 1780Hz, close to 1700Hz
  - Make it look like ITU-T V.23 Mode 2
    - Using 1300Hz (typically 1) and 2100Hz (typically 0) as symbols and 1700Hz as center frequency
- Only having a small peak 1300MHz might just show, that there isn’t much balance between the transmissions of the symbols
  - →Again no random, probably no security



Cursor: 2096 Hz (C7) = 0 dB
Peak: 2079 Hz (C7) = 0.1 dB
Algorithm: Spectrum
Size: 1024
Function: Hann window
Axis: Log frequency

Recommendations

- Old remotes, especially if safety critical should be replaced
  - Probably still a lack of Security in newer ones
- New, modern remote controls must implement some kind of integrity protection
  - I.e. cryptographic signatures based on cryptographic hashes
- Do more research on industrial remotes
  - They’re fun

Summary

- None of the remotes contain notable Security measures
  - Which is still pretty normal for industrial components, especially older ones
- They’re vulnerable to trivial attacks
  - Even though spoofing and being louder than the original remote can be challenging

- There seems to be a lot of room for improvement
- It’s a fun topic to look into

Summary

- That said
  - Peeeeeow Klonk
- Cranes usually don't have a quick release button to drop the load
  - For a very very good reason

Logitech F710

- Why?
- Because sometimes consumer equipment can be awesome inspiration
- It’s attacked by far more often than industrial components
- And as such as evolved by far quicker and further

One Last Note

- All passive analysis was performed with an RTL-SDR dongle from nooelec for less than $50
  - Not affiliated with them in any way, but the dongles have worked fine so far
- Everybody can afford the necessary equipment

Questions?

Brian Butterly

brian@security-bits.de

@BadgeWizard

Details, Sniffs, Traces

- Have already been posted on
- https://security-bits.de/research/various/crane_remotes

References

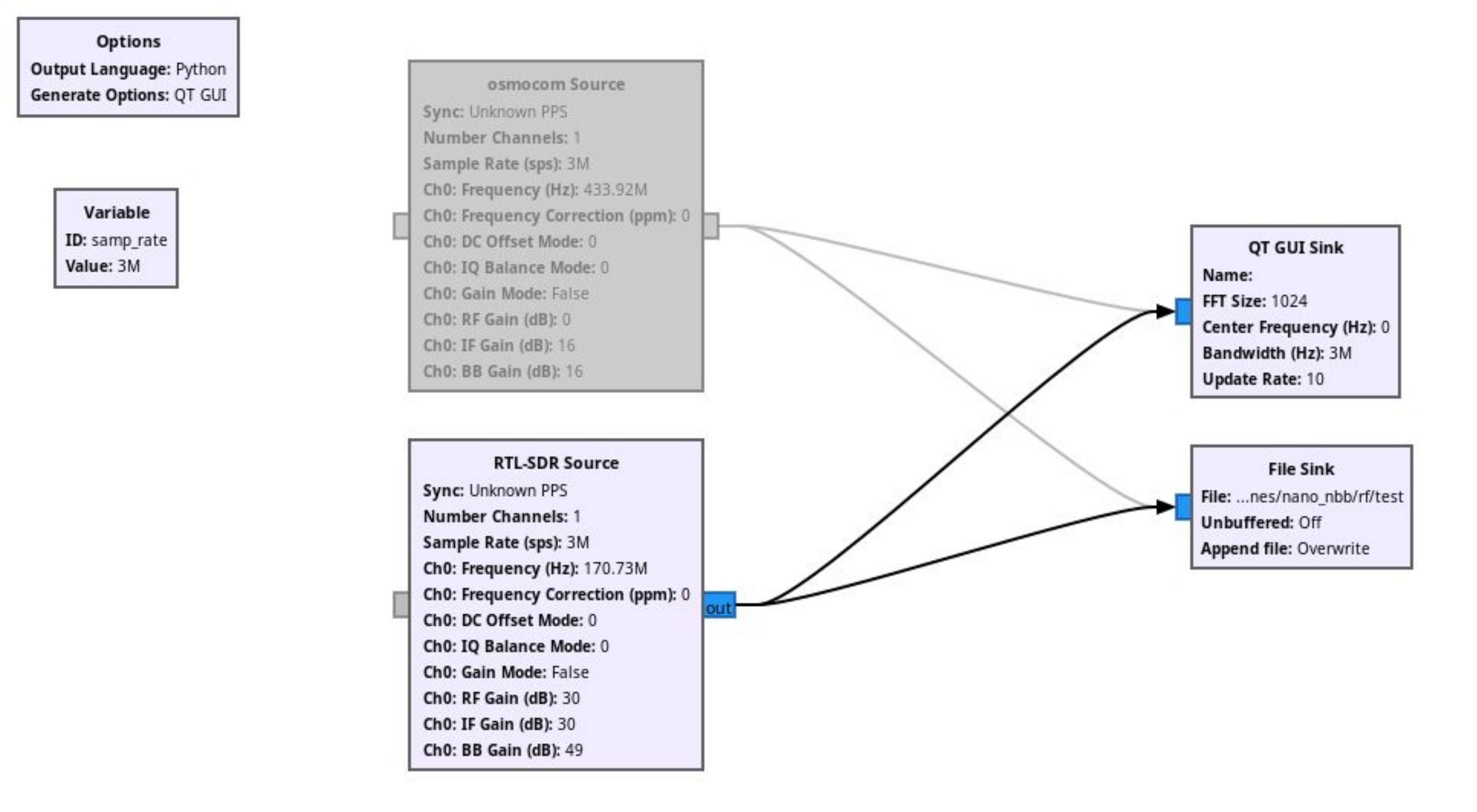
- https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
- https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations
-

Sources

- 2: My Own
- 5: Screenshot https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
- 6: https://en.wikipedia.org/wiki/Titan_submersible_implosion#/media/File:Titan_submersible_on_the_ocean_floor.jpg
- 7: https://www.cbc.ca/news/canada/missing-submersible-how-deep-1.6882739
- 10/11: Random Datasheet
- 12: Generated with https://www.midjourney.com
- 14: Generated with https://www.midjourney.com
- 20/21/22: My Own
- 23: Inspectrum Screenshot
- 25/26/27: My Own
- 28: URH Screenshot
- 28: https://de.wikipedia.org/wiki/Puls-Pausen-Modulation#/media/Datei:Fernsteuerungsmodulation.gif
- 31/33: My Own
- 34/35: Audacity Screenshot

Used Tools

- Underlying OS: Current Debian
- https://www.gqrx.dk/
- https://github.com/miek/inspectrum
- https://github.com/jopohl/urh
- https://www.audacityteam.org/
- https://www.gnuradio.org/
- RTL-SDR Dongle: https://www.nooelec.com/store/sdr/sdr-receivers/smart.html



Options
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 3M

osmocom Source
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 3M
Ch0: Frequency (Hz): 433.92M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 16
Ch0: BB Gain (dB): 16

RTL-SDR Source
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 3M
Ch0: Frequency (Hz): 170.73M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 30
Ch0: IF Gain (dB): 30
Ch0: BB Gain (dB): 49

QT GUI Sink
Name:
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 3M
Update Rate: 10

File Sink
File: ...nes/nano_nbb/rf/test
Unbuffered: Off
Append file: Overwrite

Recording with GRC