433 MHz in tcpdump
wireless sniffing malo drugače

Tomaž Šolc
tomaz.solc@tablix.org

Pipini odprti termini

10 januar 2012

Kako delujejo?

vir: Amazon.com

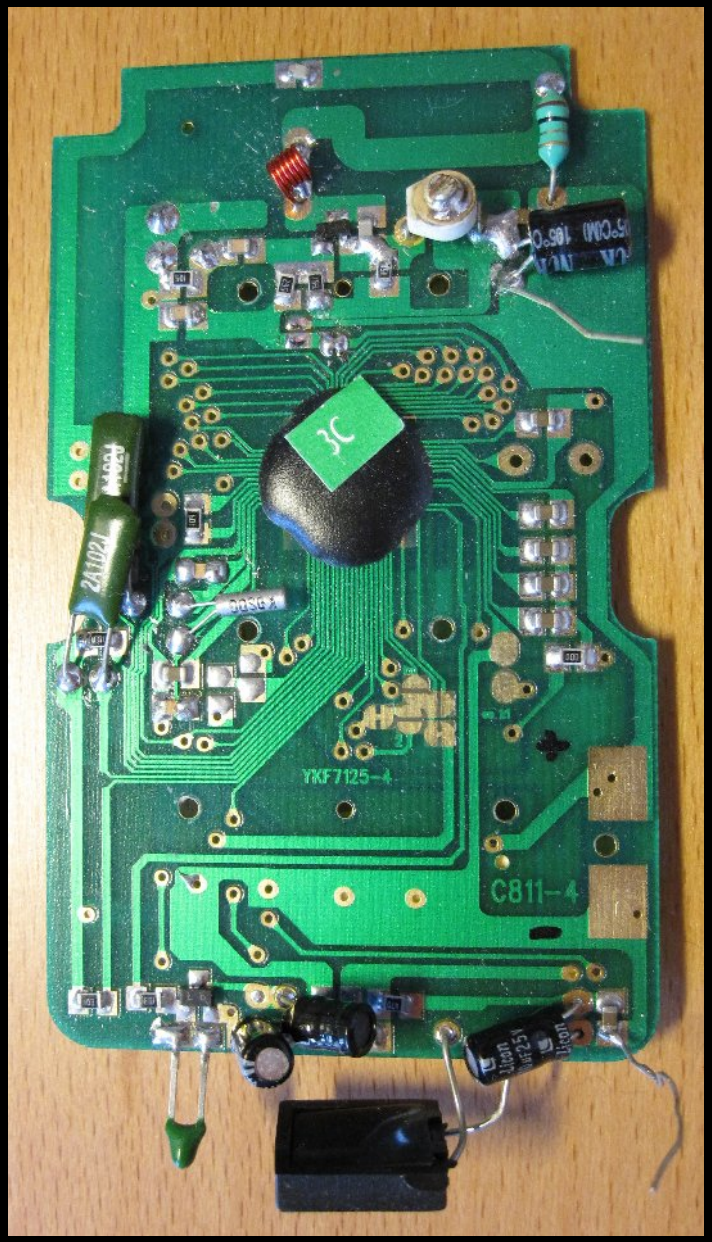
vir: Conrad.si

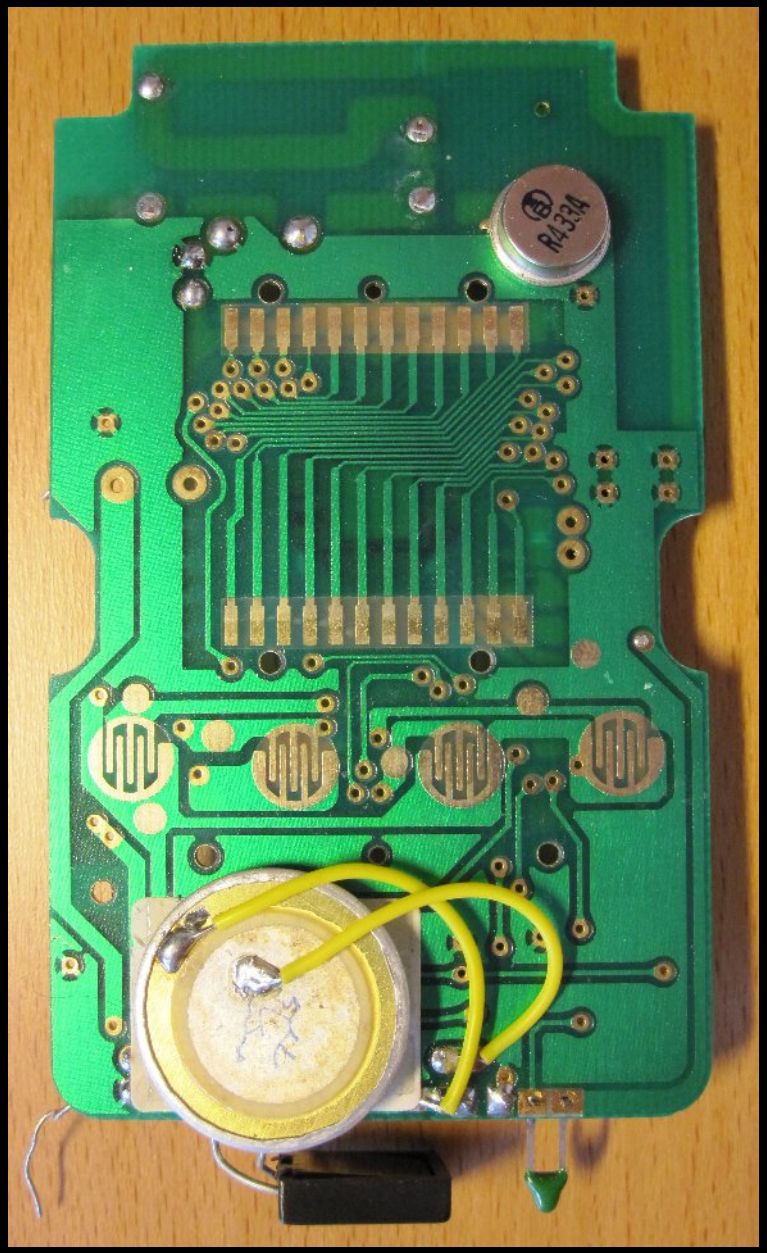
vir: Conrad.si

Lastnosti

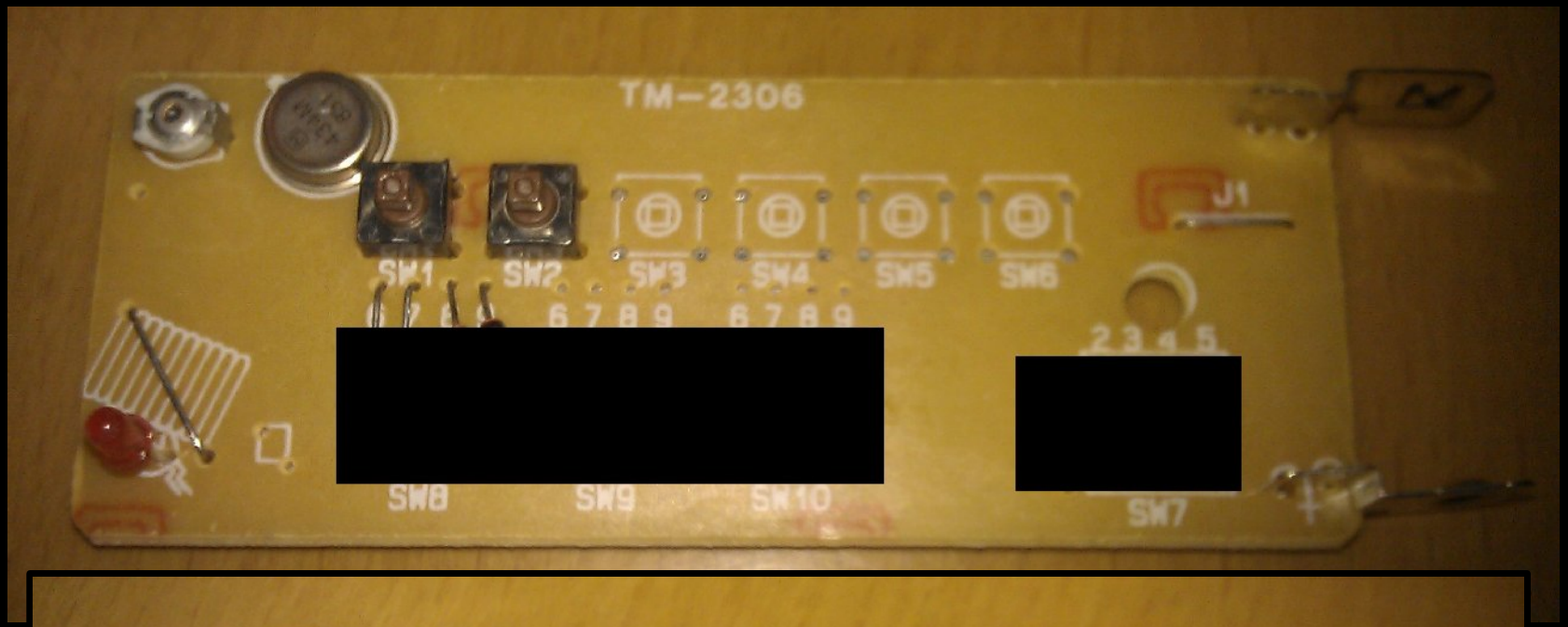
- Nizka bitna hitrost,
- majhna količina podatkov,
- nizke zahteve po zanesljivosti,
- paketni prenos,
- enosmerna zveza,
- eden ali oba konca radijske zveze baterijsko napajana,
- nizka cena

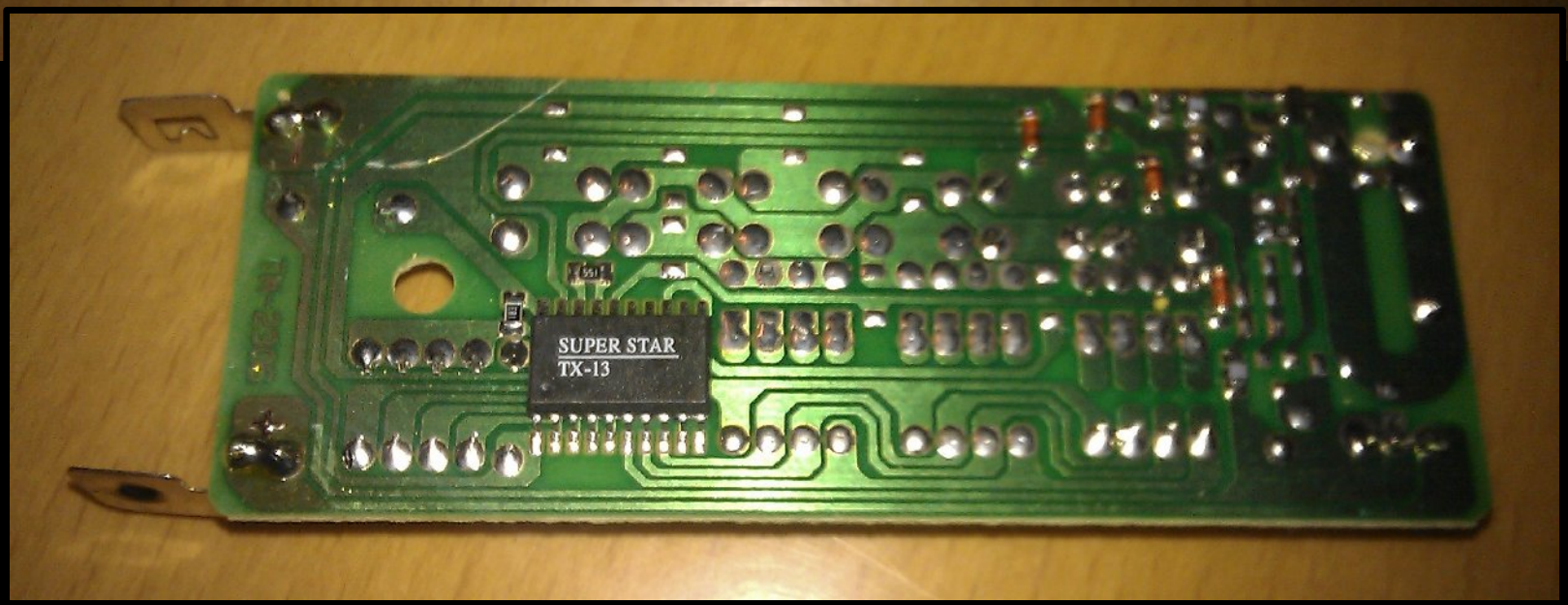
Pogled v notranjost



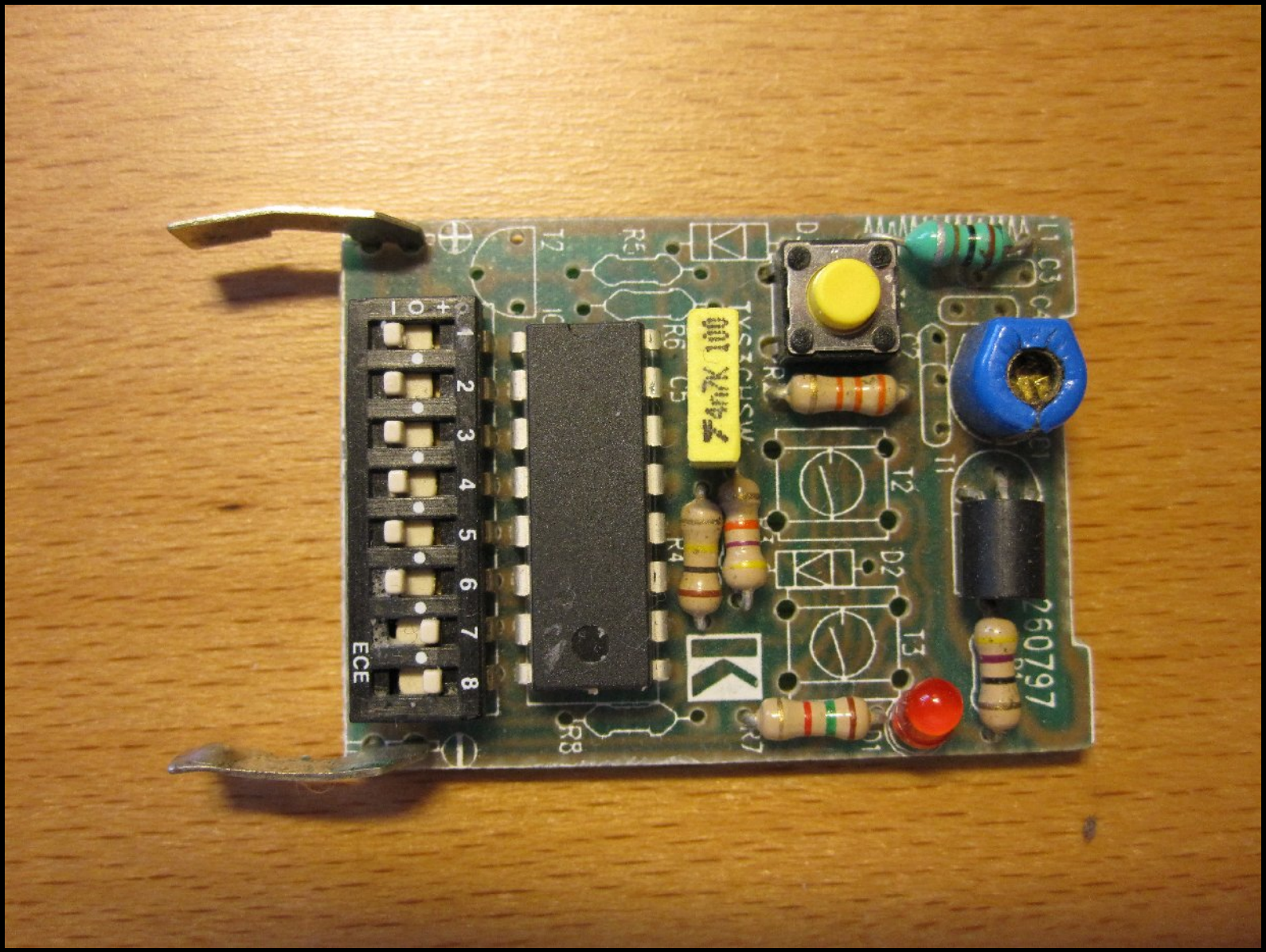


Pogled v notranjost

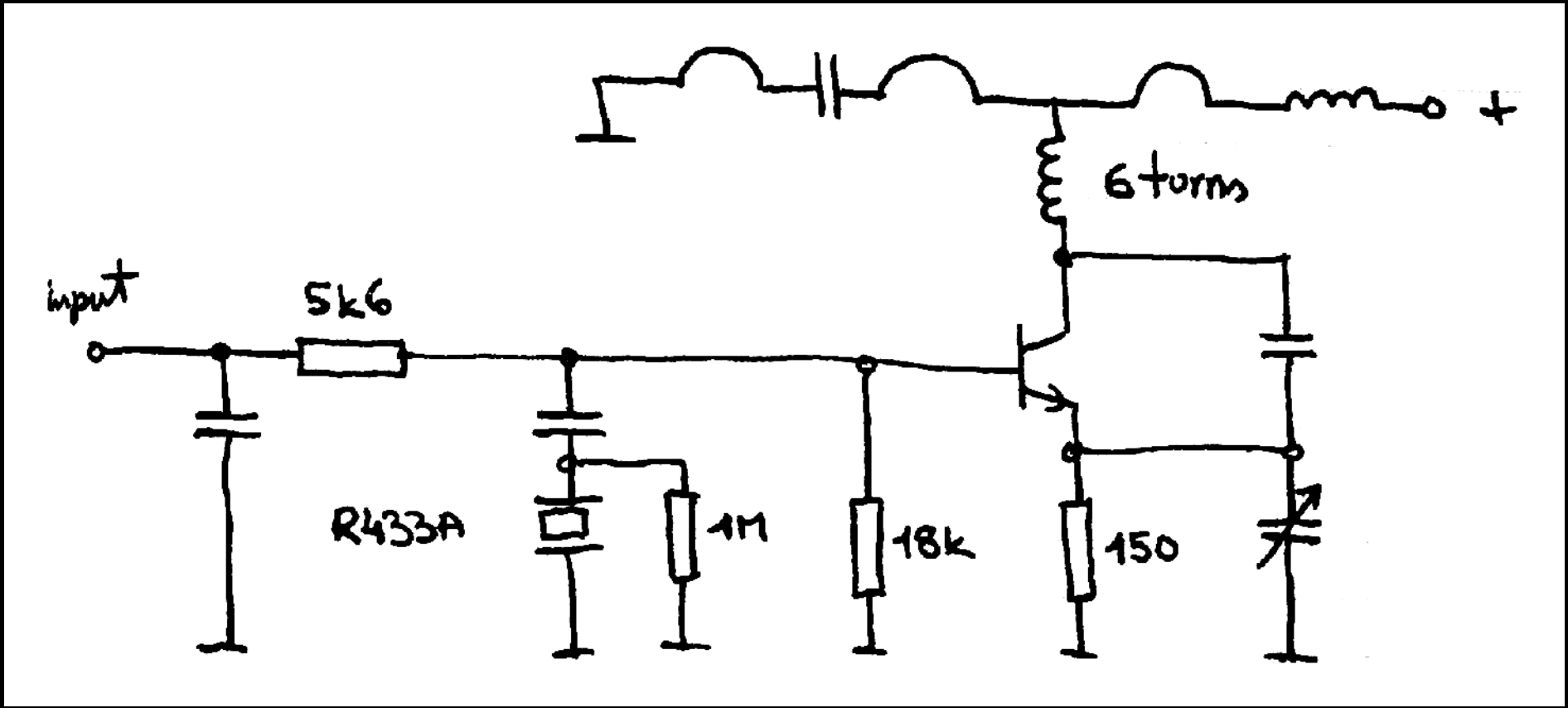




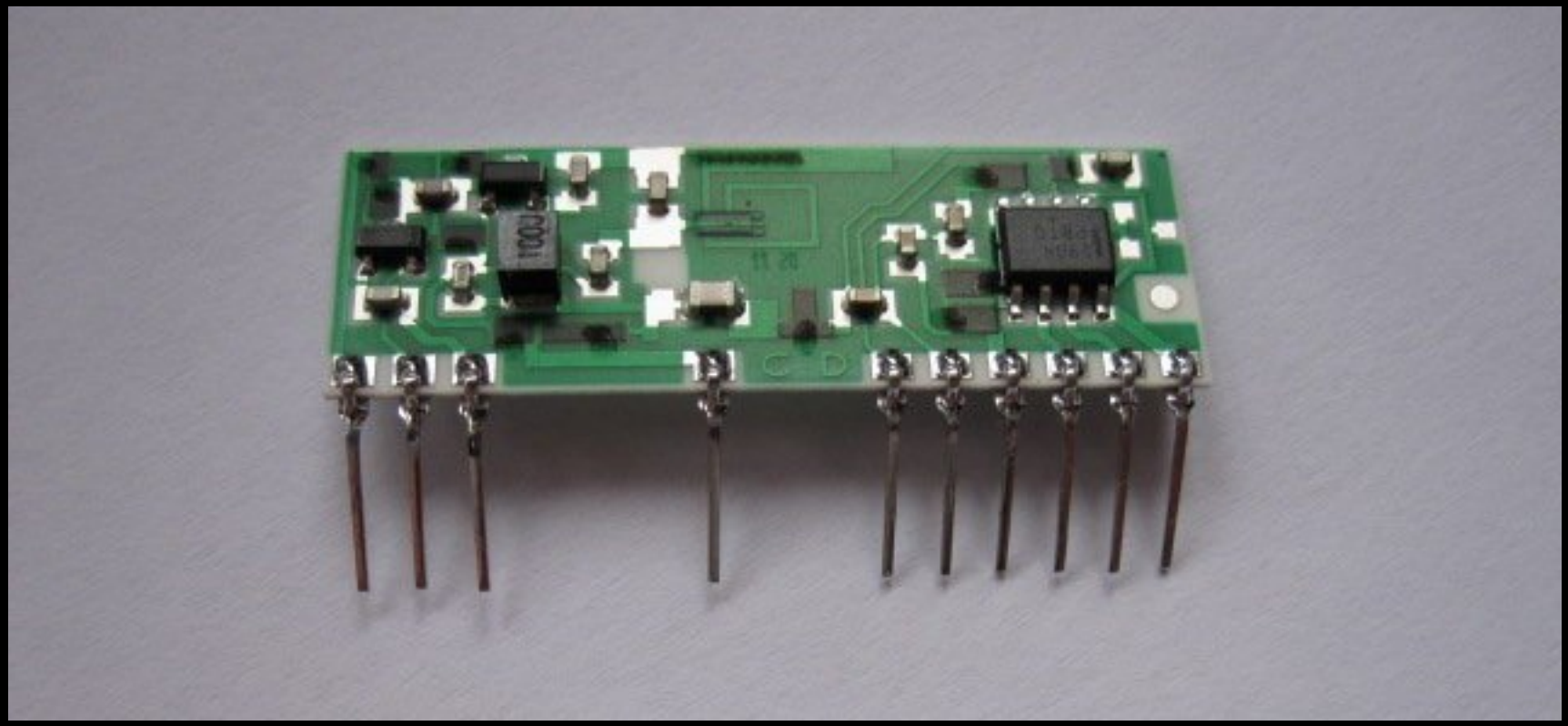
Pogled v notranjost



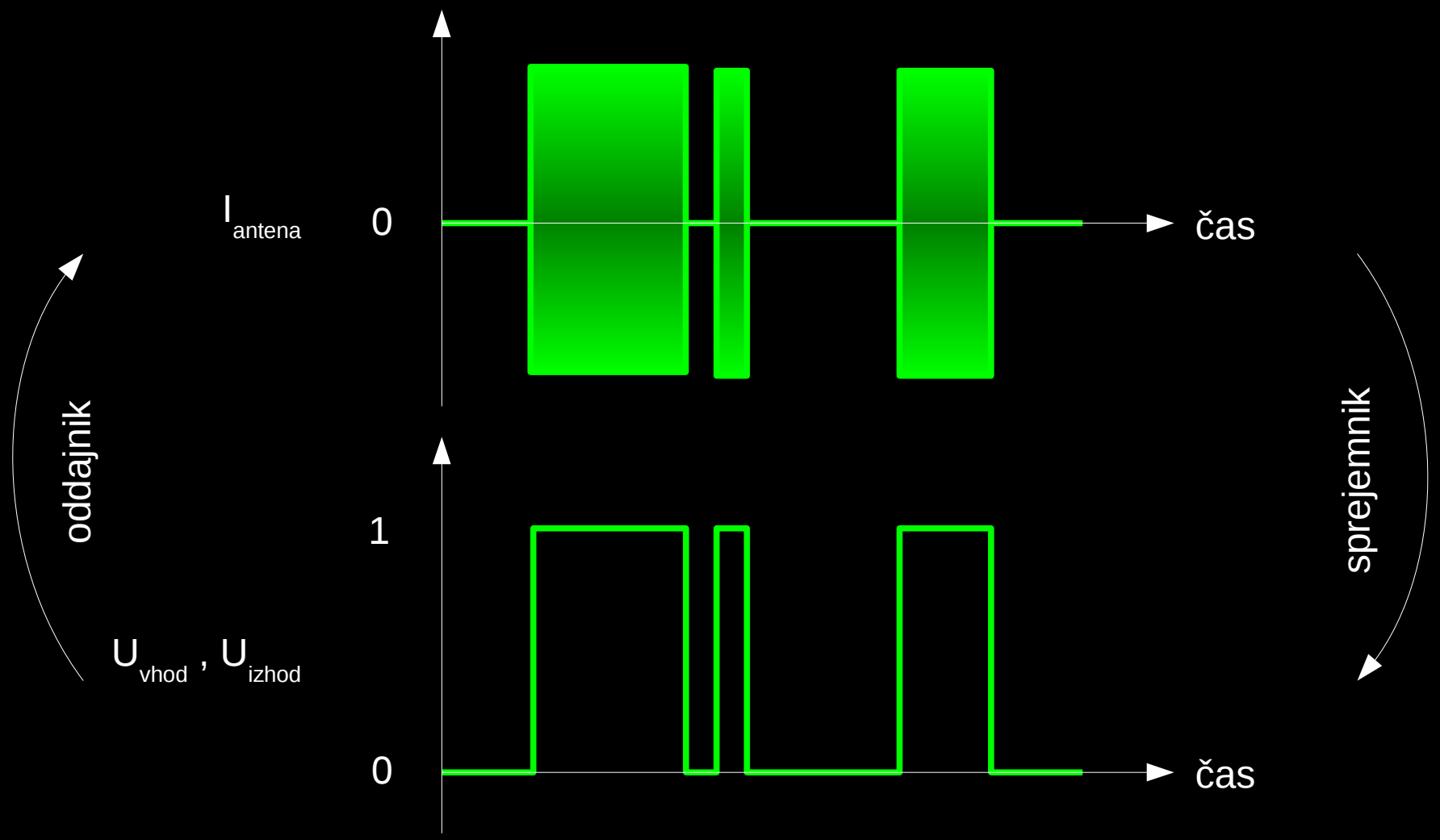
Oddajnik



Sprejemnik

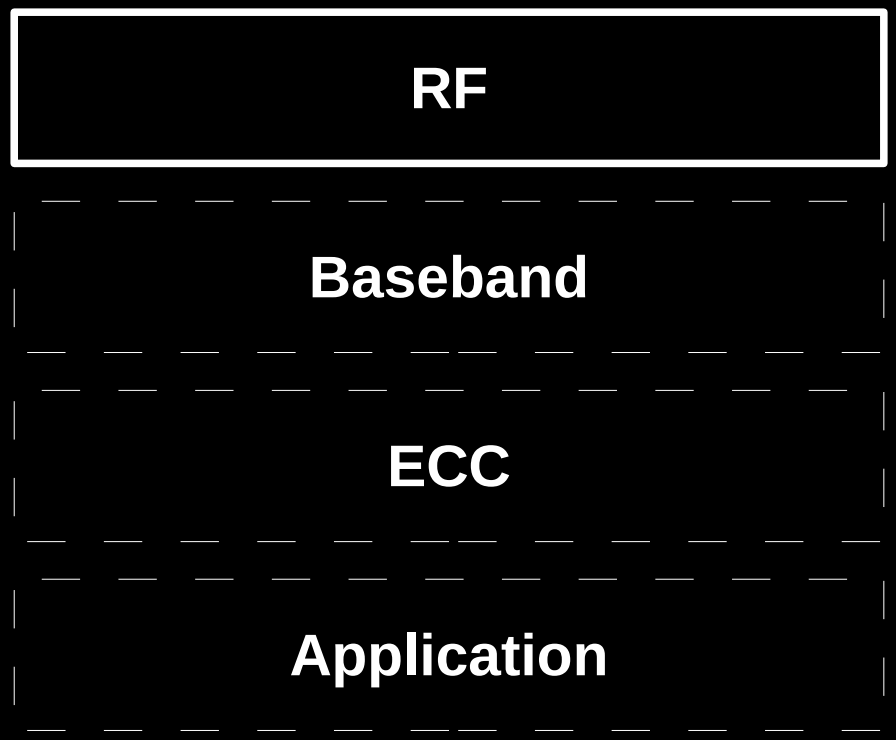


Radiofrekvenčni del



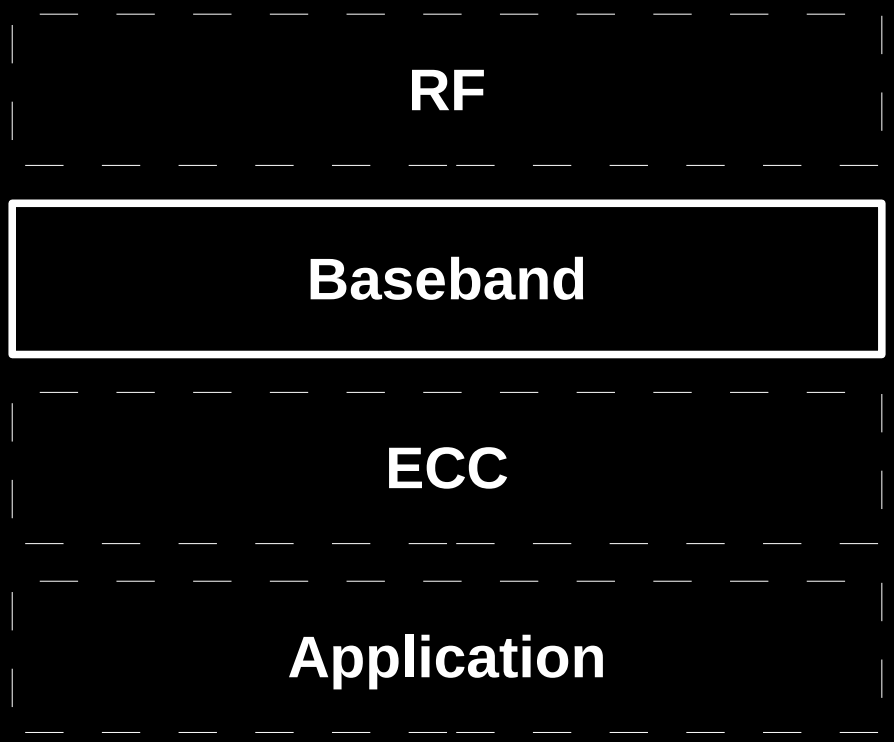
Radiofrekvenčni del

- 100% amplitudna modulacija, OOK, ASK
- ISM frekvenčni pas 433 ali 868 MHz
- souporaba enega kanala
- zasedenost <1%

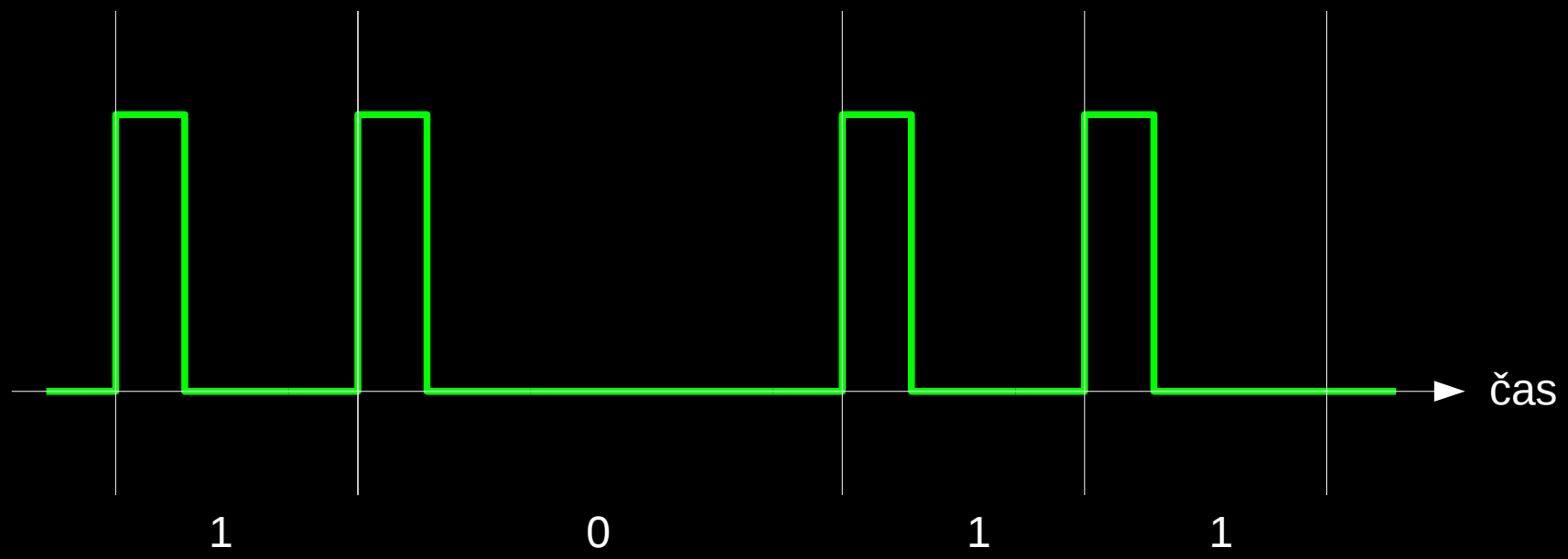


Nizkofrekvenčni del

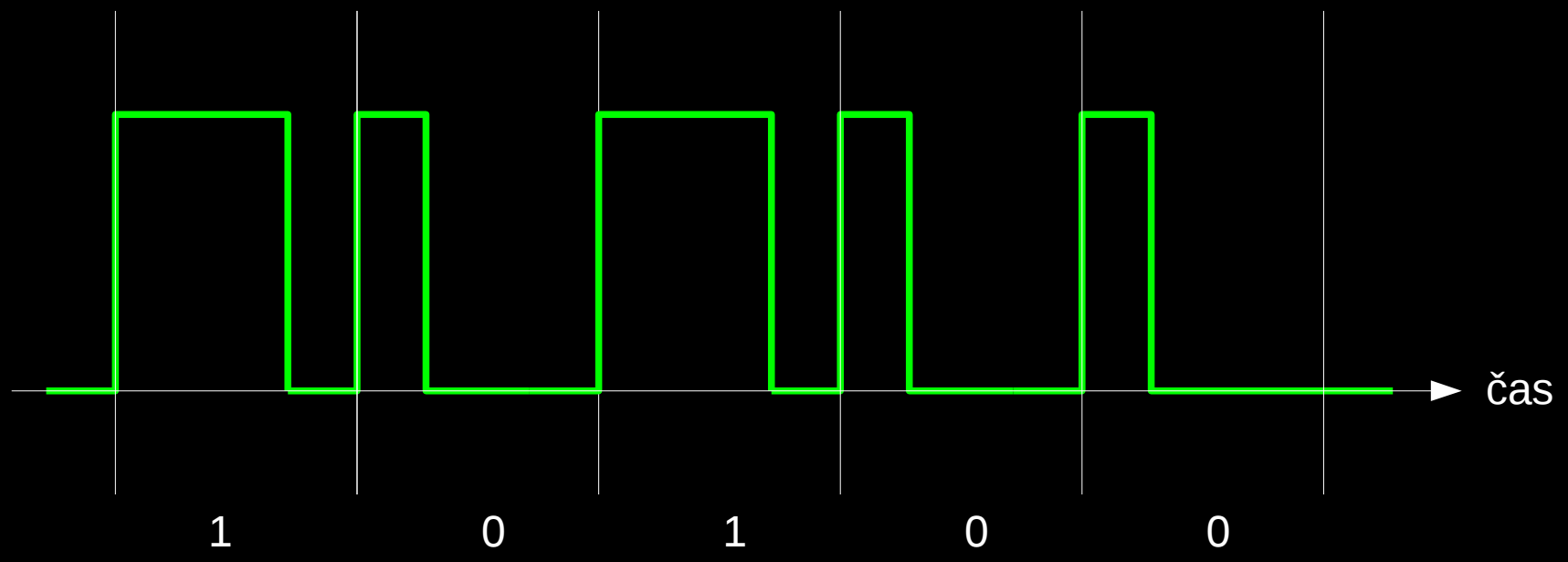
- FSK, PWM, PPM, Manchester in različna lastniška kodiranja
- frekvenca urinega impulza med 100 Hz in 10 kHz
- glava, rep za sinhronizacijo



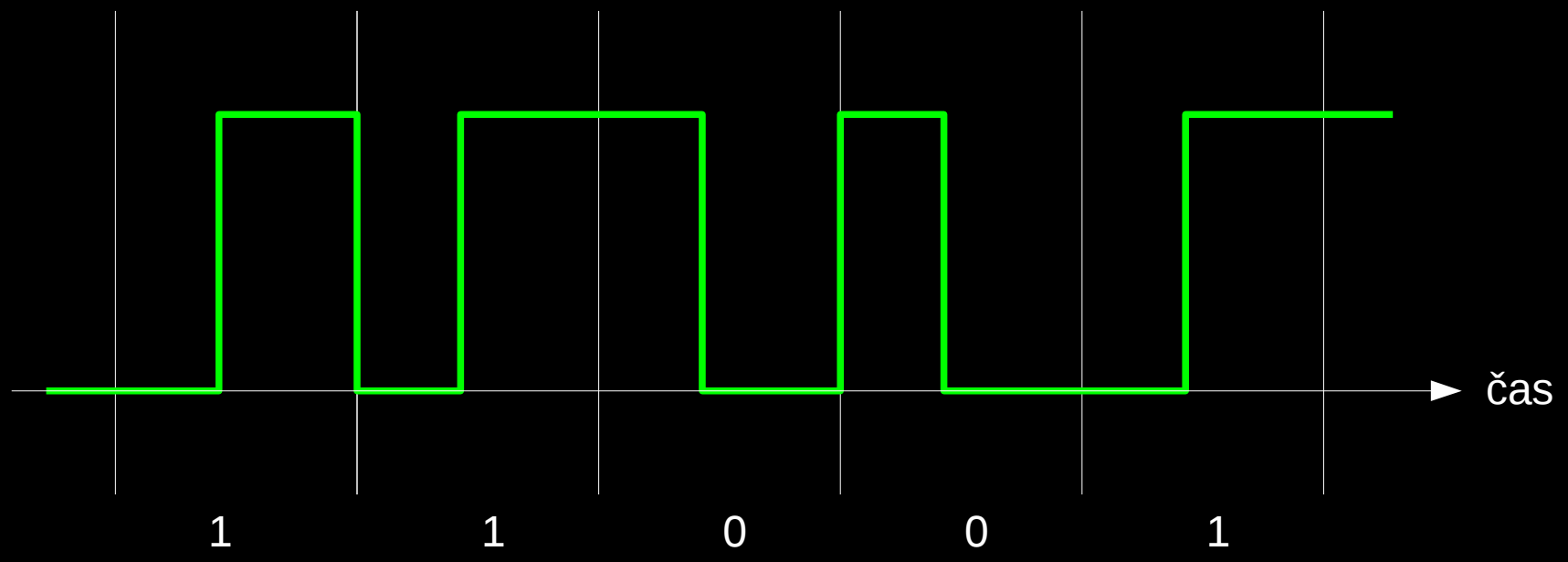
frekvenčna modulacija (FSK)



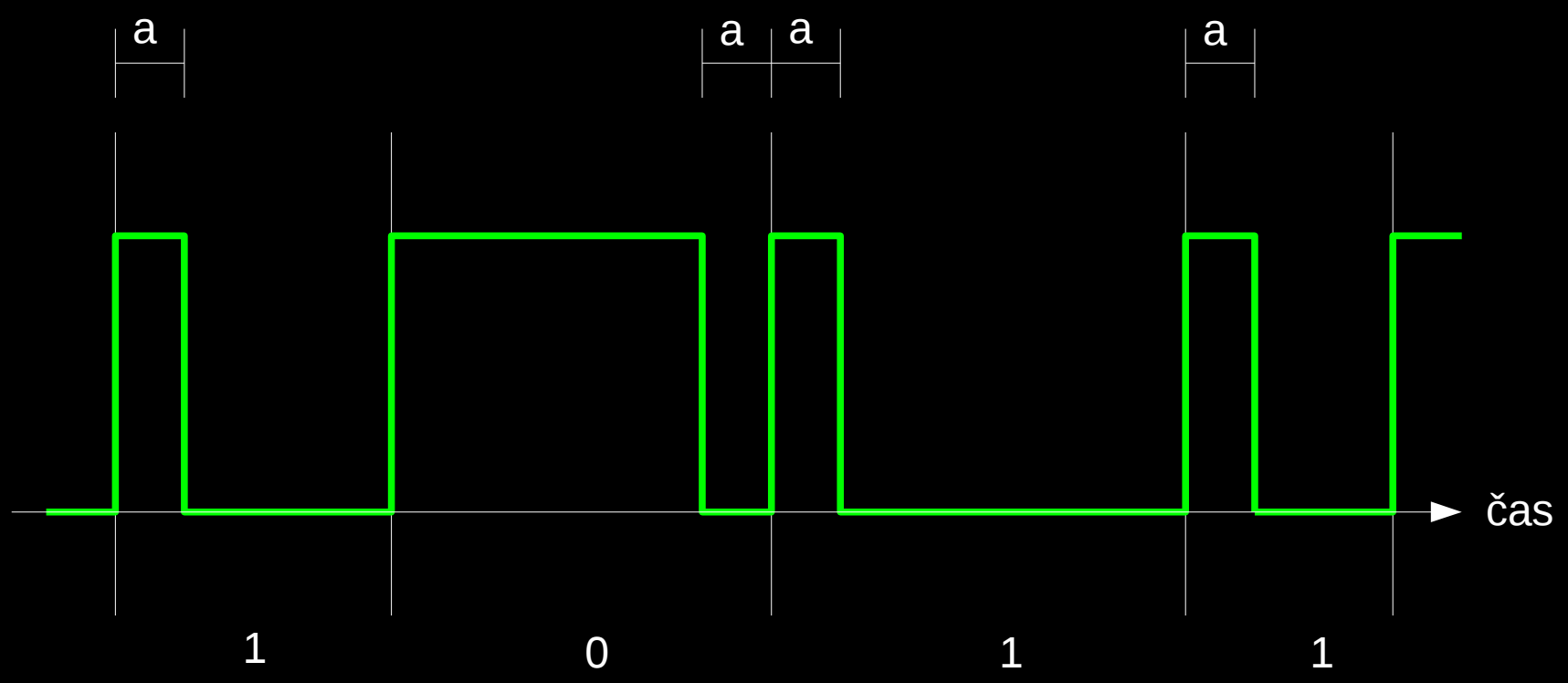
pulzno-širinska modulacija (PWM)



Manchester kodiranje



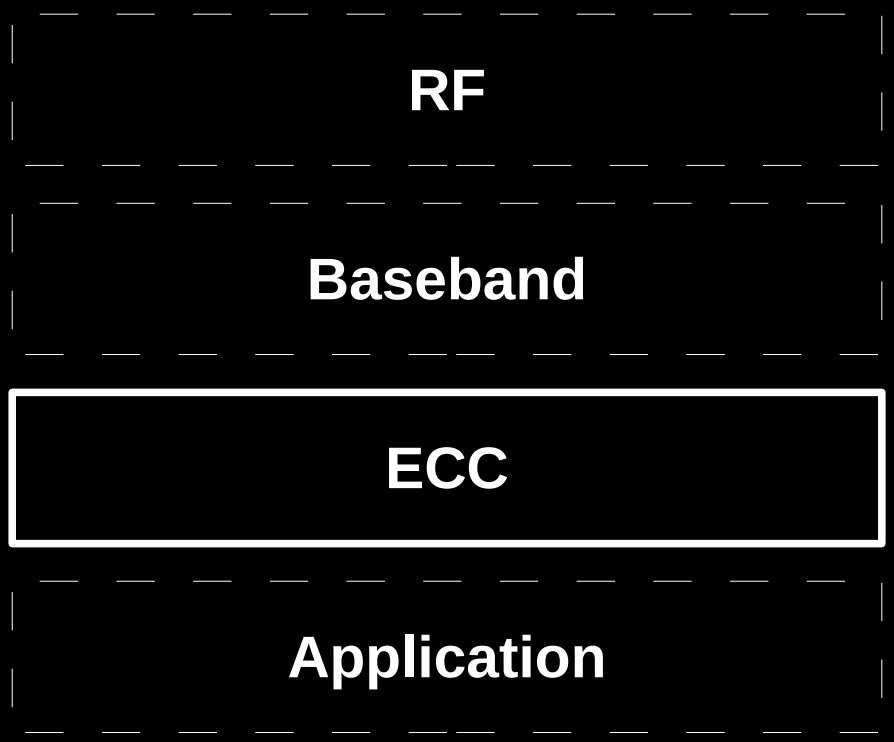
Primer lastniškega kodiranja



Robustnost

- nekatere naprave posamezne bite dodatno kodirajo v vzorce, ki se težje pojavijo po naključju
- *„The words are transmitted twice per encoding sequence to increase security.“*

(MC145026 datasheet)



Robustnost

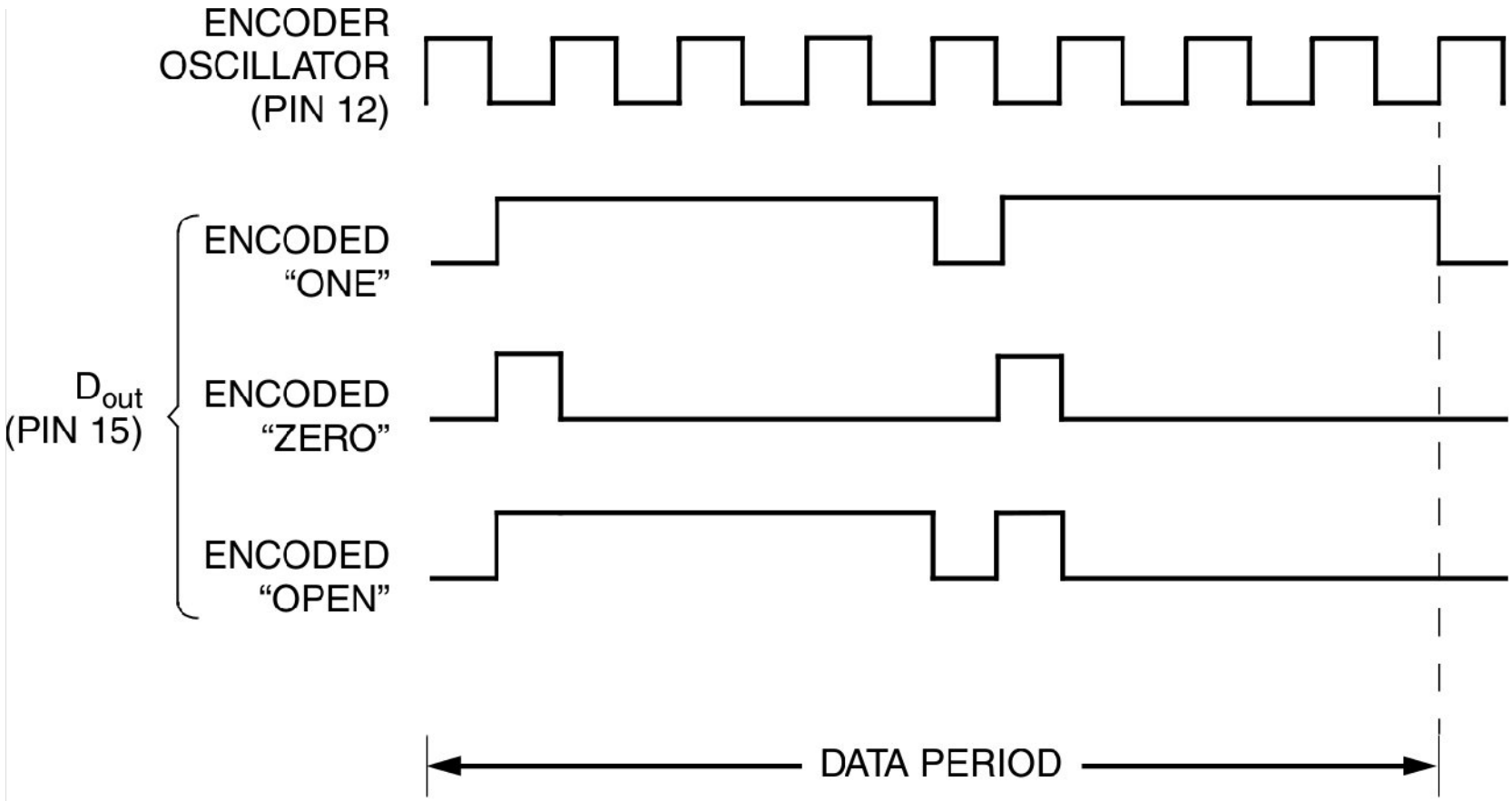
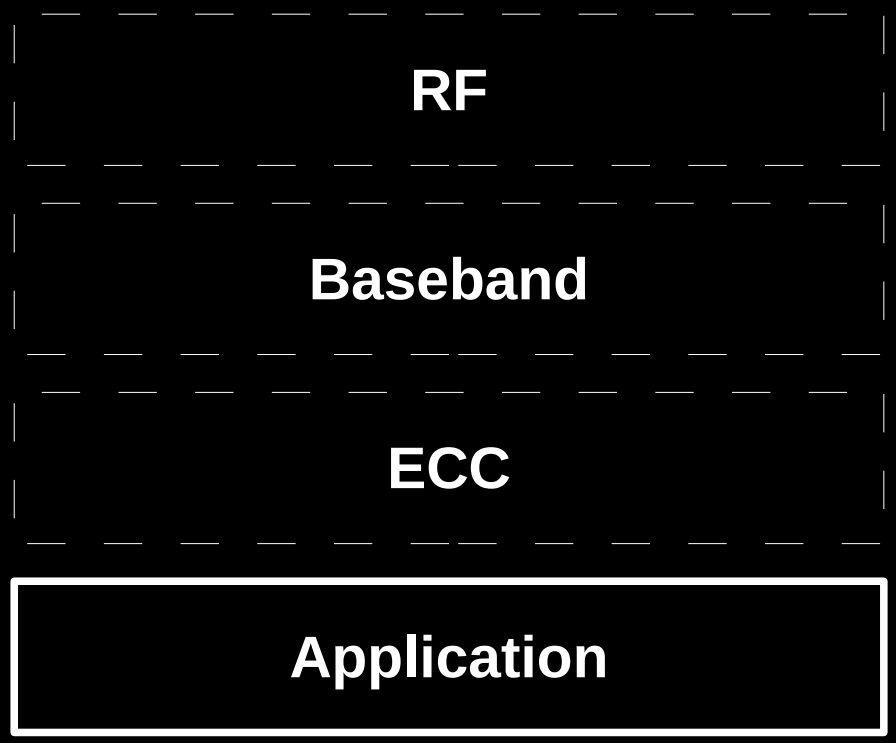


Figure 12. Encoder Data Waveforms

Aplikacijski nivo

- Različni lastniški protokoli



Vremenski senzor

```
0 0 0 0 0 0 0 0 1 1 1 0 1 1 0 0 0 1 0 0 0 1 1 1 0 0 1 1

a b   c       d       e       f       g       h       i


a - BATT FAIL      [FALSE]

b – DEV ID             [0]

c - RH % BCD DIGIT 1   [0]
d - RH % BCD DIGIT 2   [7]
e - RH % BCD DIGIT 3   [6]

f - TEMP C BCD DIGIT 1 [2]
g - TEMP C BCD DIGIT 2 [3]
h - TEMP C BCD DIGIT 3 [9]
i - TEMP C BCD SIGN    [+]
```

Daljinski upravljalnik

XX XX XX XX XX XX XX XX XX

d1 d2 d3 d4 d5 d6 d7 d8 d9

00 – pin high

01 – pin open

11 – pin low

Ključ

```
00 .. 00 XX XX XX XX YY YY YY YY YY YY YY YY ZZ

a        b           c                        d

a – 26 bytes zero
b – 4  bytes device ID
c – 8  bytes pseudorandom authentication code
d – 1  byte  function ID
```

Ključ

oddajnik	f6	62	d2	99	fe	74
sprejemnik	f6	62	d2	99	fe	74

Ključ

Ključ

oddajnik ~~f6~~ 62 d2 99 fe 74

sprejemnik ~~f6~~ 62 d2 99 fe 74

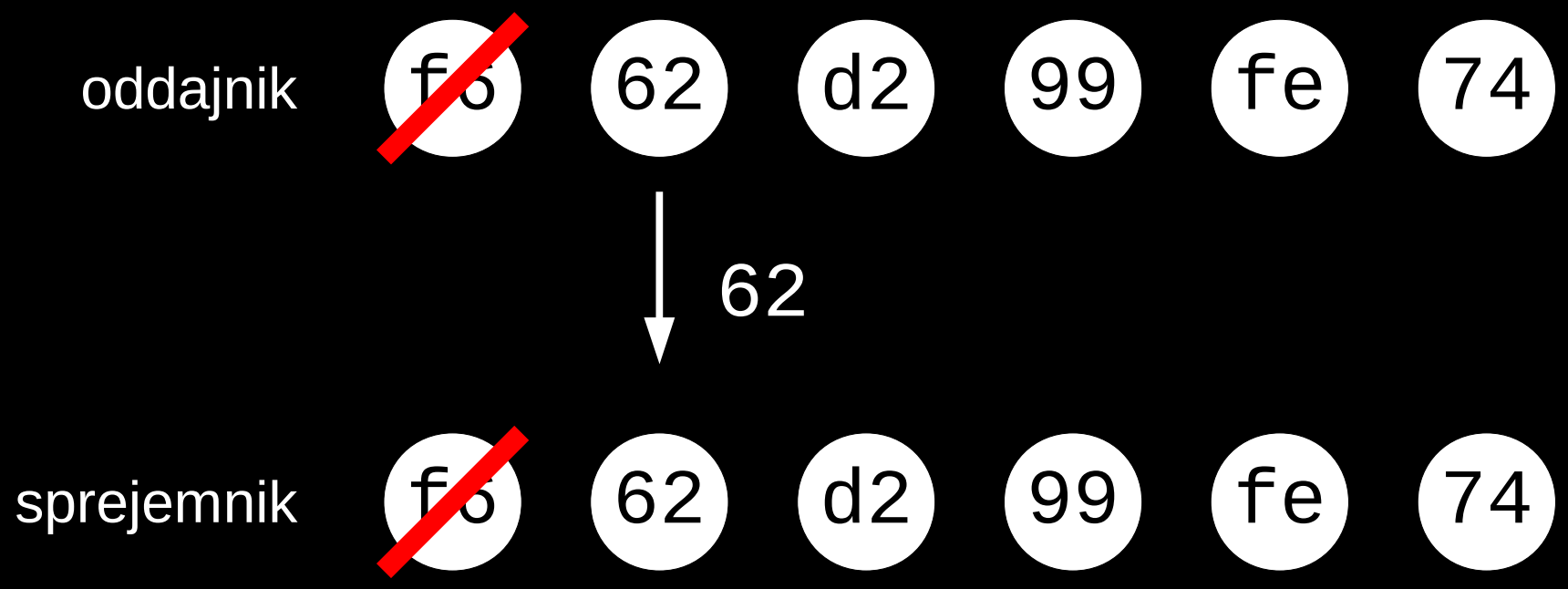
Ključ

oddajnik ~~f6~~ 62 d2 99 fe 74

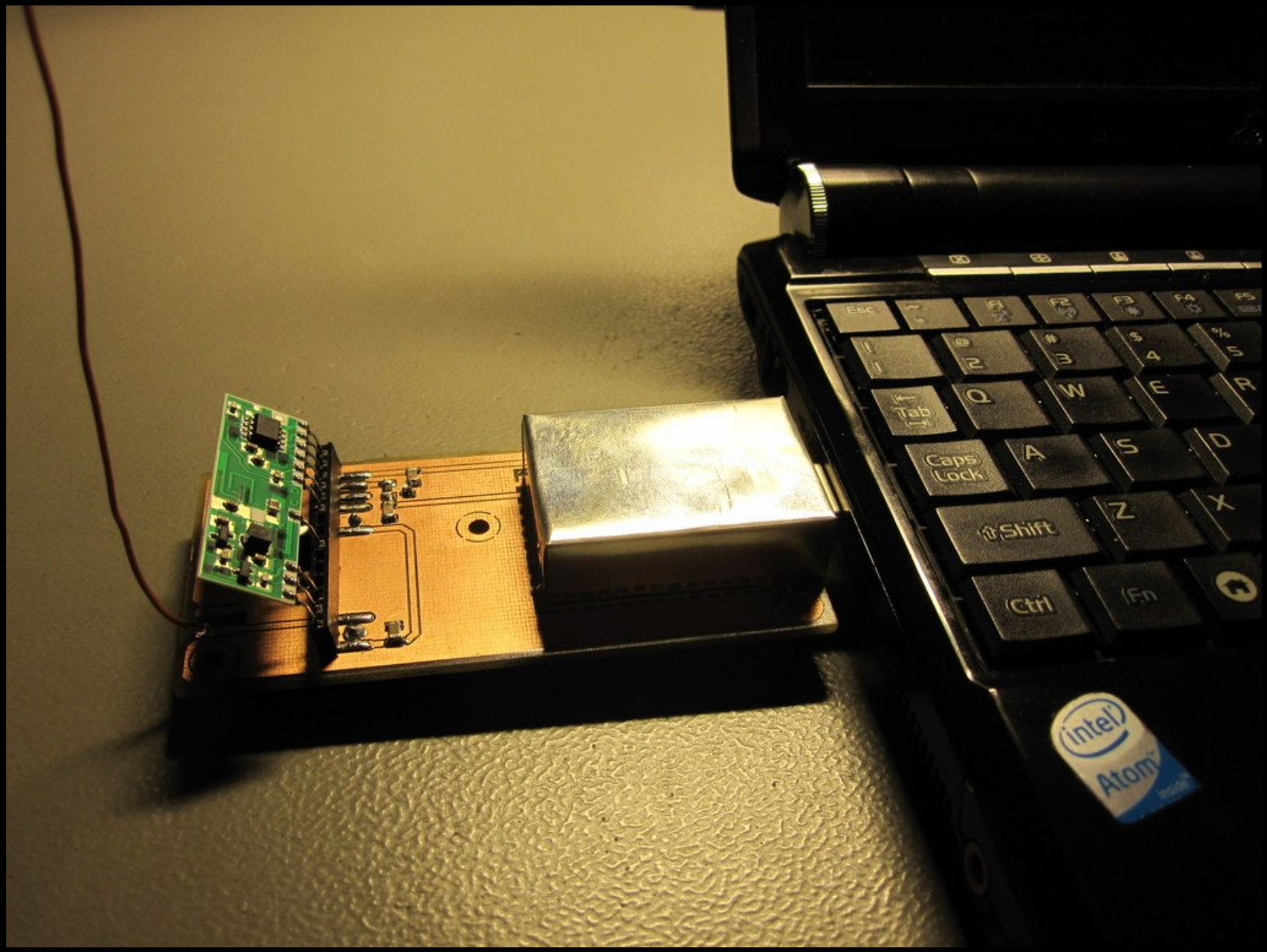
sprejemnik ~~f6~~ 62 d2 99 fe 74

f6

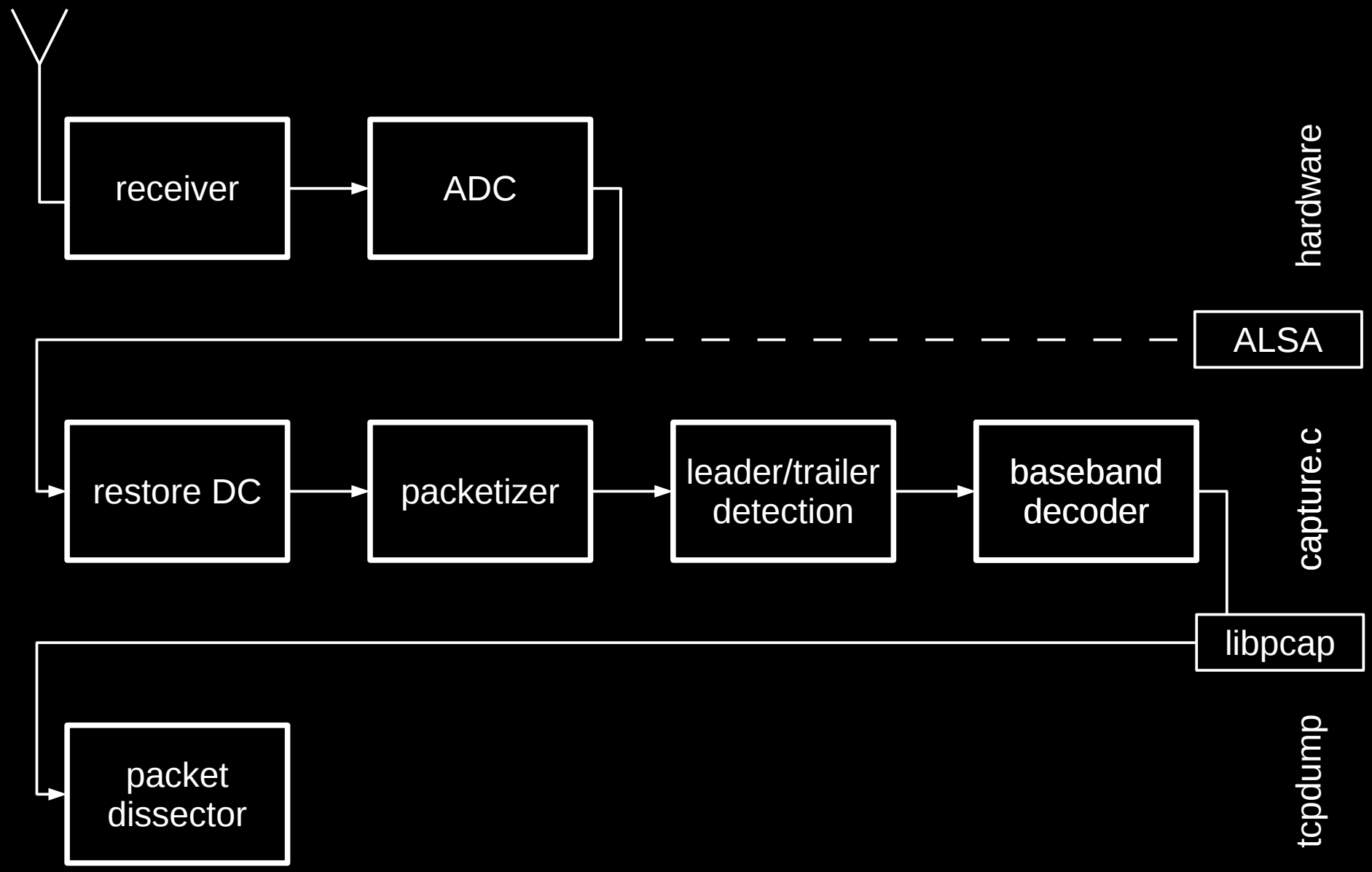
Ključ



Sniffer



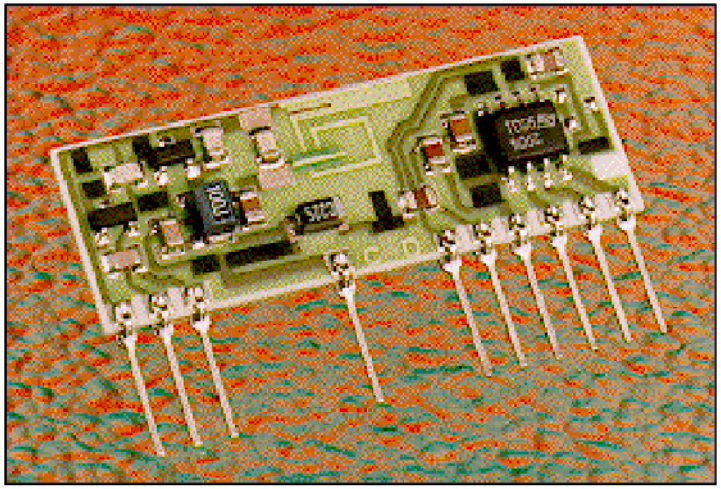
Blok shema


receiver
ADC
hardware
ALSA
restore DC
packetizer
leader/trailer detection
baseband decoder
capture.c
libpcap
packet dissector
tcpdump

Sprejemnik

AM SUPER REGENERATIVE RECEIVERS. AM-HRRN-XXX

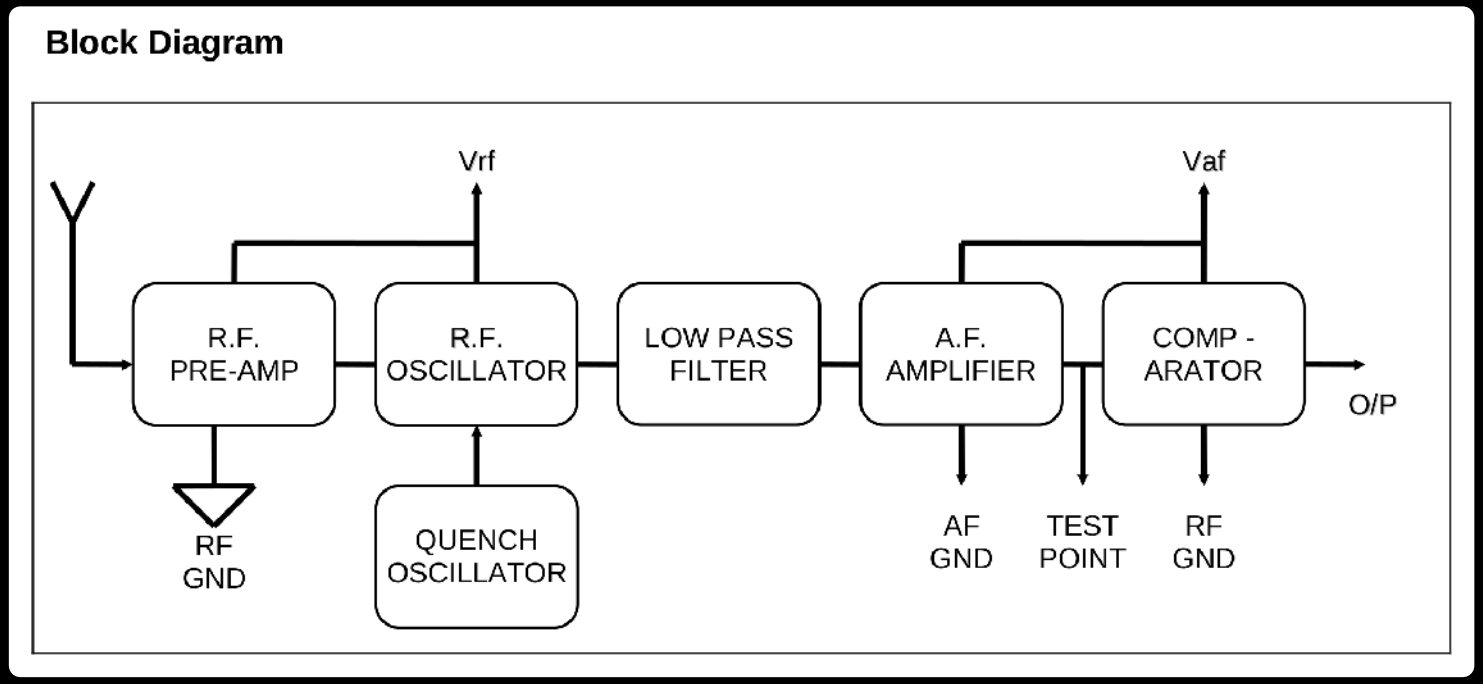
- Compact Hybrid Modules.
- Standard Frequencies; 315, 433, 868MHz
- Frequencies Available: 250-450MHz
- Very High Frequency Stability (With No Adjustable Components).
- Receiving Range Up To 50 Metres.
- CMOS/TTL Compatible Output.
- Low Current Consumption;
  - ⇒ HRR3 Typ 2.5mA.
  - ⇒ HRR18 Typ 70uA.
- Single Supply Voltage 3V or 5V.
- Compatible With R.F. Solutions AM Transmitters.
- Patented Laser Trimmed Inductor.
- Compliant To ETSI300-220.
- Requires No Radio Licence To Operate.



vir: RF Solutions

Sprejemnik

- -105 dBm tipična občutljivost
- 2 kHz pasovna širina
- 12 EUR



vir: RF Solutions

Analogno digitalni pretvornik

Zunanja zvočna kartica SPEEDlink SL-8850, USB

9 od 9 priporoča nakup tega artikla.
Napiši mnenje. | Preberi mnenja

SL-8850 je zvočna kartica, ki jo lahko priklopite na USB vrata in tako hitro in udobno na vaš prenosnik ali namizni računalnik priklopite slušalke in mikrofon.
Vse podrobnosti | Tehnične podrobnosti

Redna cena:	~~13,62 €~~
Spletna cena:	12,94 €
Prihranek:	0,68 € (4,99%)

V košarico

Na zalogi

V centralnem skladišču. Običajno pošljemo še isti dan, prevzameš pa lahko naslednji dan.

- Kakšen je strošek dostave?
- Je možen osebni prevzem naročila?
- Kako plačam, lahko ob prevzemu?
- Kaj je Spletna cena?

+1 0

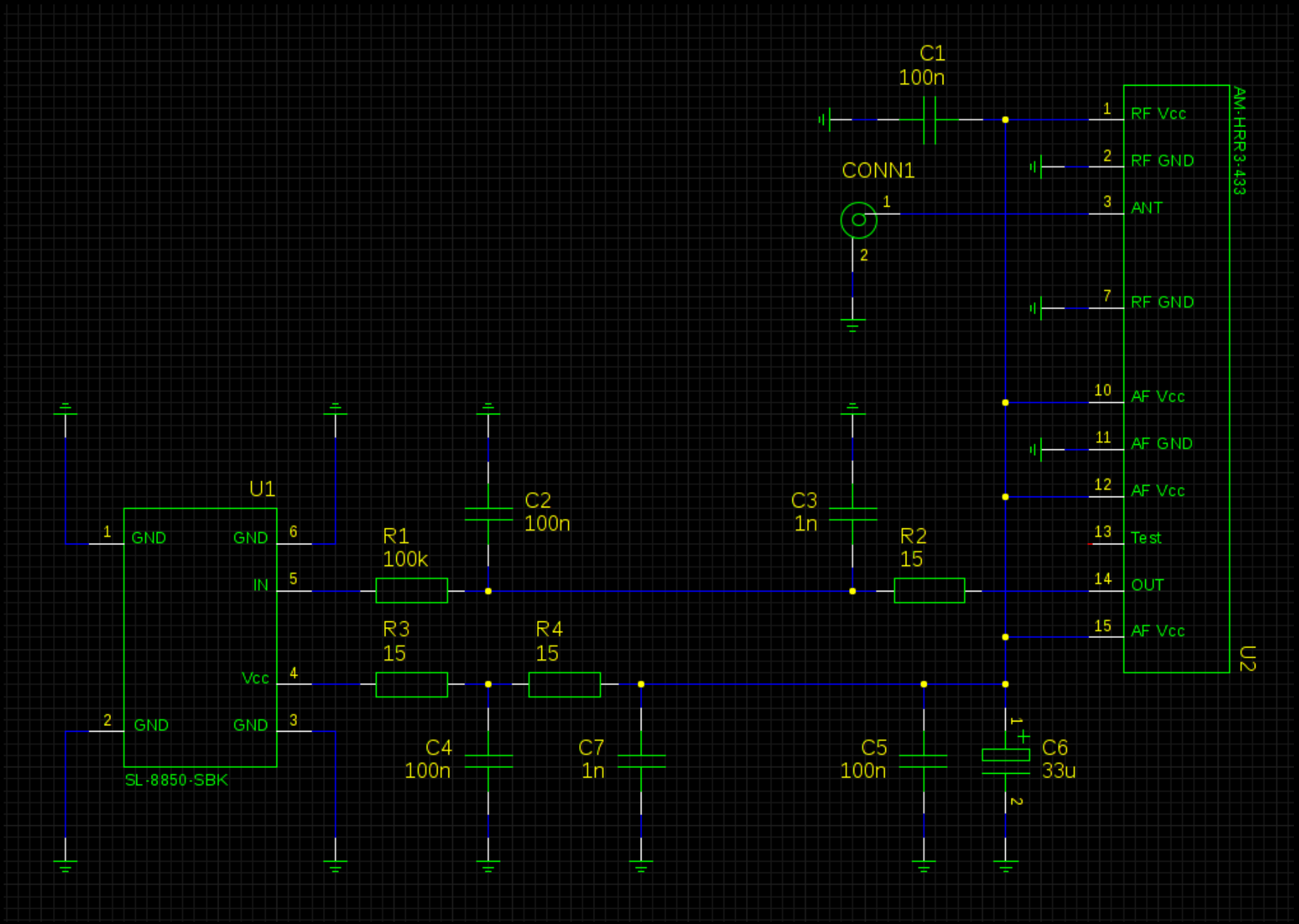
Predstavitev | Mnenja (9) | Slike izdelka | Tehnične podrobnosti | Podobni artikli

- Uradna stran artikla
- Več od SPEEDLINK
- Več iz oddelka Zvočne kartice
- Priporočila
- Kratka povezava na to stran: http://mv.rs/t/2880017026

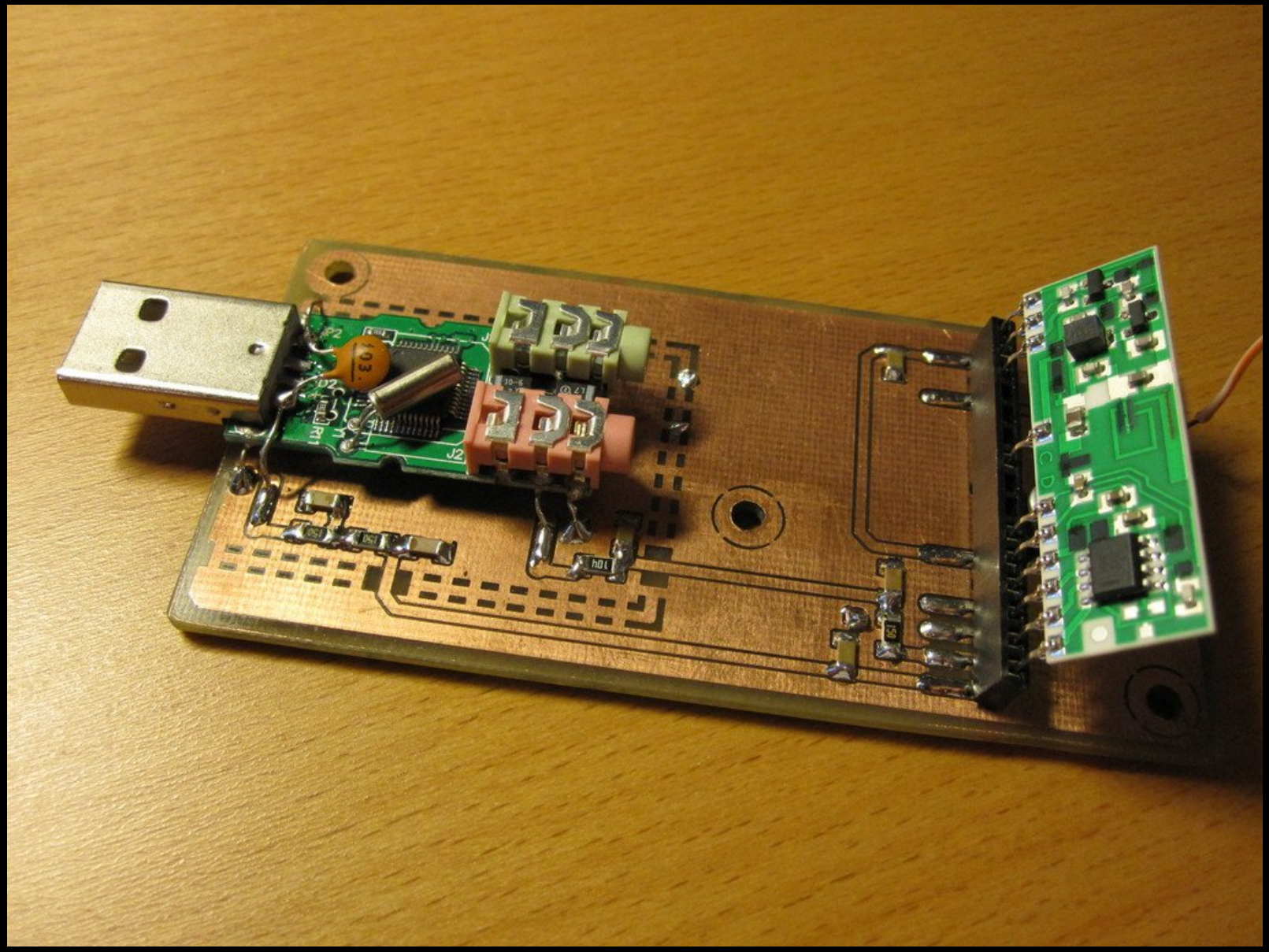
C-Media CM108

- 2 x DAC, 1 x ADC
- 28 kHz vzorčevanje
- I^2S vmesnik
- 4 x GPIO, 4 x vhod za tipko
- USB audio device, USB HID
  nastavljiva product, vendor ID preko zunanjega EEPROMa
- max. 24 h neprekinjenega snemanja

Shema


C1
100n
CONN1
1
2
RF Vcc
RF GND
ANT
RF GND
AF Vcc
AF GND
AF Vcc
Test
OUT
AF Vcc
AM-HRR3-433
U2
U1
GND
GND
IN
Vcc
GND
GND
SL-8850-SBK
R1
100k
C2
100n
C3
1n
R2
15
R3
15
R4
15
C4
100n
C7
1n
C5
100n
C6
33u

Izdelek



Capture

- libasound za dostop do naprave
- packetizer
  - premor za več kot 5 povprečnih urinih ciklov označuje nov paket
- dekoder
  - poiskuša od bolj zapletenih do bolj preprostih shem
- filtriranje šuma
  - paket s samimi ničlami ali enicami je najverjetneje šum

libpcap

- fake RFMON device with pipe to forked capture.c process
- new link type DLT_AM433
- link-level header

```
struct am433_capture_hdr {
        uint64_t timestamp_us;
        uint32_t bitcount;
        uint32_t clock_hz;
        uint8_t modulation;
        uint8_t leader_edges;
        uint8_t trailer_edges;
} __attribute__((__packed__));
```

tcpdump

Terminal

```
avian@orion:~/dev/manchester/tcpdump$ ./tcpdump -i am433_2_0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on am433_2_0, link-type 254, capture size 65535 bytes
07:22:38.366780 fsk clk 888 Hz l 2 t 1 unknown  9 bits [40 00]
07:22:38.452759 mod unknown 37 ms
07:22:42.521364 mod unknown 184 ms
07:22:42.975405 mod unknown 36 ms
07:22:46.569197 mod unknown 42 ms
07:22:47.866134 mod unknown 23 ms
07:22:47.921155 mod unknown 28 ms
07:22:49.261259 mod unknown 28 ms
07:22:50.053468 mod unknown 20 ms
07:22:51.591780 pwm clk 510 Hz l 0 t 0 unknown 12 bits [7d 90]
07:22:51.641301 pwm clk 500 Hz l 0 t 0 unknown  9 bits [7d 80]
07:22:51.839364 pwm clk 489 Hz l 0 t 0 unknown 11 bits [7d 80]
07:22:51.886697 pwm clk 494 Hz l 1 t 2 unknown  9 bits [7d 80]
07:22:51.982697 mod unknown 30 ms
07:22:52.087093 pwm clk 475 Hz l 0 t 0 unknown 12 bits [7d 80]
07:22:52.186197 pwm clk 494 Hz l 0 t 0 unknown 10 bits [7d 80]
07:22:52.235739 pwm clk 484 Hz l 0 t 0 unknown 12 bits [7d b0]
07:22:52.285301 pwm clk 489 Hz l 1 t 0 unknown 11 bits [fb 60]
07:22:52.540968 mod unknown 31 ms
07:22:52.809134 mod unknown 27 ms
07:22:54.174322 ppk clk 1297 Hz l 0 t 0 unknown 10 bits [5f c0]
```

tcpdump

Terminal

```
07:22:52.186197 pwm clk 494 Hz l 0 t 0 unknown 10 bits [7d 80]
07:22:52.235739 pwm clk 484 Hz l 0 t 0 unknown 12 bits [7d b0]
07:22:52.285301 pwm clk 489 Hz l 1 t 0 unknown 11 bits [fb 60]
07:22:52.540968 mod unknown 31 ms
07:22:52.809134 mod unknown 27 ms
07:22:54.174322 ppk clk 1297 Hz l 0 t 0 unknown 10 bits [5f c0]
07:22:54.270364 mod unknown 20 ms
07:22:54.522051 mod unknown 187 ms
07:22:57.139697 ppk clk 1371 Hz l 0 t 0 unknown 11 bits [7f c0]
07:23:00.649114 mod unknown 27 ms
07:23:00.984864 mod unknown 28 ms
07:23:01.182280 mod unknown 48 ms
07:23:02.975239 mod unknown 35 ms
07:23:04.756614 mod unknown 11 ms
07:23:05.182947 mod unknown 51 ms
07:23:05.420280 mod unknown 35 ms
07:23:06.152884 ppk clk 1297 Hz l 0 t 0 unknown 10 bits [7e c0]
07:23:06.415780 ppk clk 1714 Hz l 0 t 0 unknown 12 bits [17 f0]
07:23:06.530009 weather monitor [+21.0 C 058 % RH] batt ok 0 0
07:23:06.985801 mod unknown 29 ms
07:23:08.404134 mod unknown 43 ms
07:23:08.636030 mod unknown 65 ms
07:23:09.412197 mod unknown 137 ms
07:23:10.205343 mod unknown 43 ms
```

Demo

Wish list

- Večja odpornost na USB motnje,
- oddajnik + libpcap injection support,
- wireshark support,
- zmogljivejši radijski del (FM, ...)
- ...?

Vprašanja?

tomaz.solc@tablix.org

http://www.tablix.org/~avian/blog/articles/am433
(hardware design, source)