Softwarově definované rádio

InstallFest 2016

Jan Hrach

http://jenda.hrach.eu/
PGP: CD98 5440 4372 0C6D 164D A24D F019 2F8E 6527 282E

Obsah

- Proč je SDR tak skvělé
- Hardware pro SDR
- Signály kolem nás
- Demo: GnuRadio – knihovna pro SDR v Linuxu

- Zdroje:
- https://brmlab.cz/project/sdr

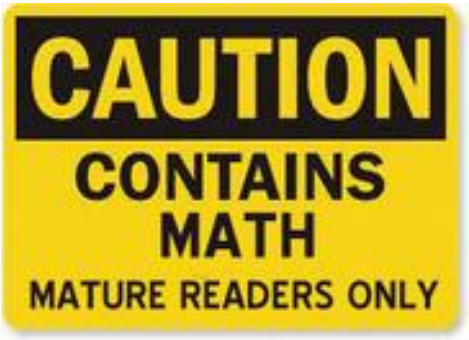
  je tam tolik odkazů, že máte do příštího IF co číst

SDR

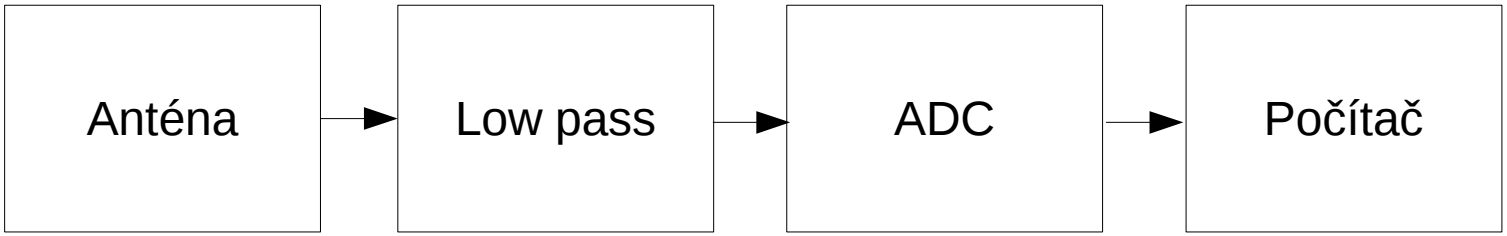
- Co nejdřív převést rádiové vlny do digitální podoby a pak už jen programovat

+ libovolný přijímač a vysílač na přání
+ ukládání signálu pro pozdější pokusy
+ programování analogově složitých/nemožných věcí
+ debugger
+ verzování software
+ síťování, „vzdálená anténa“
+ aktualizace přes Internet

- komplikovaná matematika
- velké nároky na výpočetní výkon

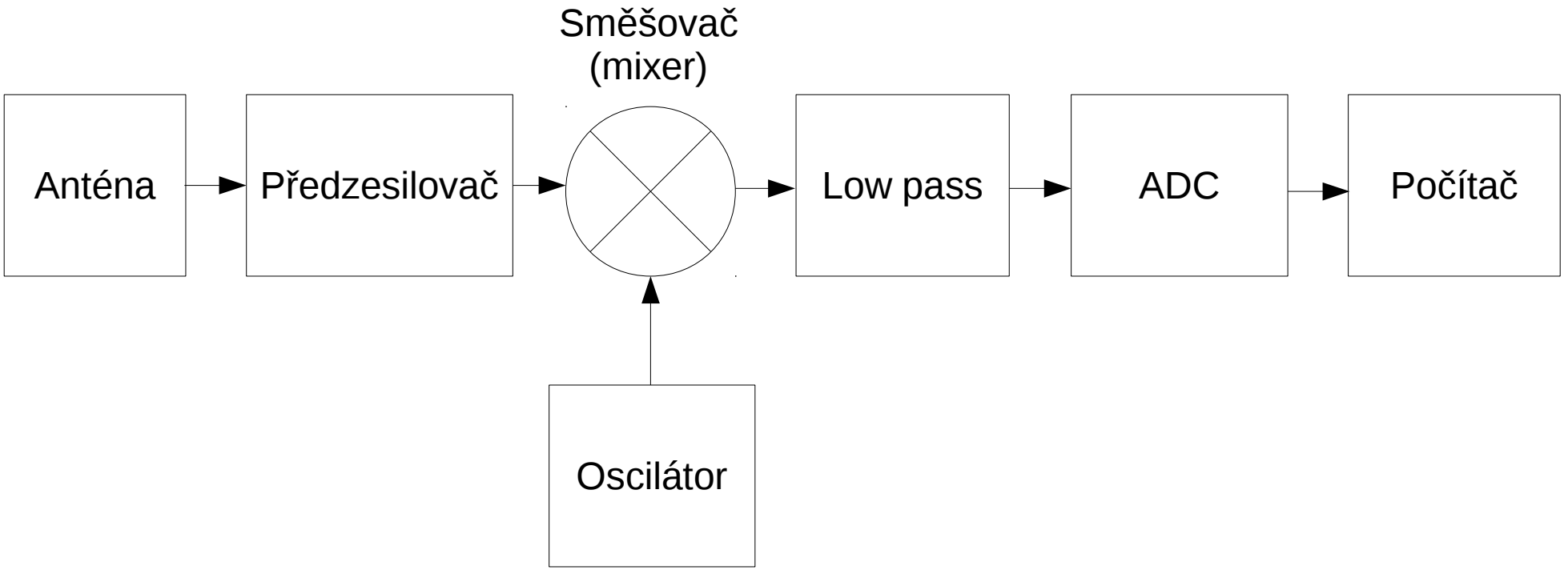


Triviální přístup



- Problém: Nyquist

Praktický přístup



- Problémy: interference, zahlcení, ...
  lze řešit precizním provedením vstupní části (důvod, proč SDR stojí od 200 Kč do 200 000 Kč)

Hardware pro SDR

- rtl-sdr (200 Kč)

- 2,4 MHz
- Kvalita strašná
- Ale pro spoustu věcí stačí
- Lze přidat filtr (vyrábí např. teroz.cz)

Hardware

- bladeRF (12 000 Kč)
- hackrf (CCC badge)
- SDR Play
- USRP (25 000 Kč)
- ...
- některá umí vysílat

Software

- rtl_*
- GQRX
- https://brmlab.cz/user/jenda/kukuruku
- GNU Radio

- kvalita velmi různorodá

Letem světem signály kolem nás

- Jak poznat signál? http://www.sigidwiki.com/

- FM hlas
  - 150-180, 440-480 MHz
  - taxi, messengeři, ochranky…
  - bezdrátové mikrofony (670-800 MHz)

Letem světem signály kolem nás

- GSM (900, 1800 MHz)
  - software: Airprobe, OsmocomBB
  - občas leakne IMSI, potom šifrované
  - …ale nekvalitní šifrou!
    - https://brmlab.cz/project/gsm/deka/start
  - GSM-R – vláčky
    - malý provoz, možná by to chtělo umět GPRS


Eee PC
/gpeshell.sh
FIXME: Watchdog sucks
FIXME: Pool support not implemented
FIXME: Session save/restore (at least bursts-to-be-cracked)
FIXME: Crack queue and offloading
Loading firmware
Turning off...dehilesqcfgjkutr OK
Init /dev/ttyUSB1 (C123, id 0)...OK
Init /dev/ttyUSB2 (C123, id 1)...OK
Init /dev/ttyUSB3 (C123, id 2)...OK
Init /dev/ttyUSB4 (C123, id 3)...OK
Init /dev/ttyUSB5 (C123, id 4)...OK
Init /dev/ttyUSB6 (C123, id 5)...OK
Init /dev/ttyUSB7 (C123, id 6)...OK
Init /dev/ttyUSB8 (C123, id 7)...OK
Armed.
[s]can BTSs, [l]oad previous scan, [e]nter ARFCNs

Tetra

- “Průmyslové GSM”, 420-440 MHz
- Městská policie, dopravní podnik…
- Šifrování: několik módů, nákladné
- Spousta sítí je “mode 0”, včetně Prahy
- Software: https://brmlab.cz/project/sdr/tetra
  - celou síť lze dekódovat paralelně na malém clusteru
    - kompletní dekódování (nešifrovaného) audia
  - dekódování vyšších vrstev (datové zprávy atd.) by si zasloužilo trochu péče

Mototrbo/DMR

- Další síť, hlas + data, zhruba 150-170 MHz
- software: DMRDecode, dsd
- Šifrování: vyberte si: žádné, tragické, mizerné
  - nově už je tedy i AES
  - ale žádná dostupná kryptoanalýza
- Městská policie, průmysl, SCADA

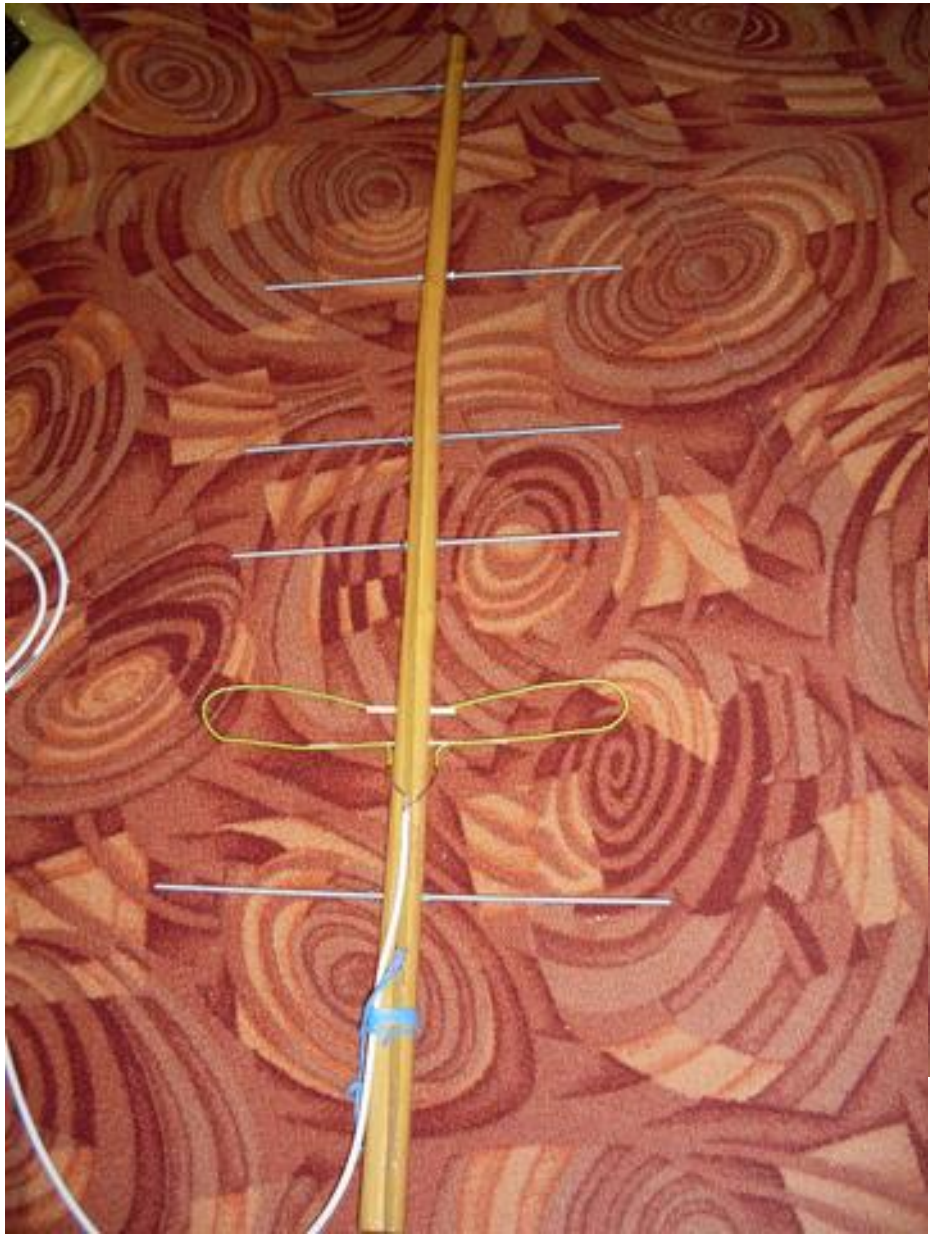
Tetrapol/Matra

- Další digitální síť, 390-395 MHz
- Policie, armáda
- 99,99 % provozu v ČR šifrováno
- Šifrování: neznámý algoritmus, indicie, že je slabý
- Experimentální dekodér nešifrovaných metadat a nešifrovanáho audia
  - https://brmlab.cz/project/sdr/tetrapol

FM(AFSK(Data))

- Všude možně (150-180, 400-550 MHz)
- Vláčky
- Sirény
- nechci, aby mě zavřeli, takže kvalitu zabezpečení jsem prostě nezkoušel
- Radiosondy
  - Zaměřování vysílače v terénu
  - https://www.brmlab.cz/project/sdr/fff
  - https://www.brmlab.cz/project/weathersonde/start

Find, fix and finish



http://petr-kubac.blog.cz/1301/radiokompas-1


SEARCHER

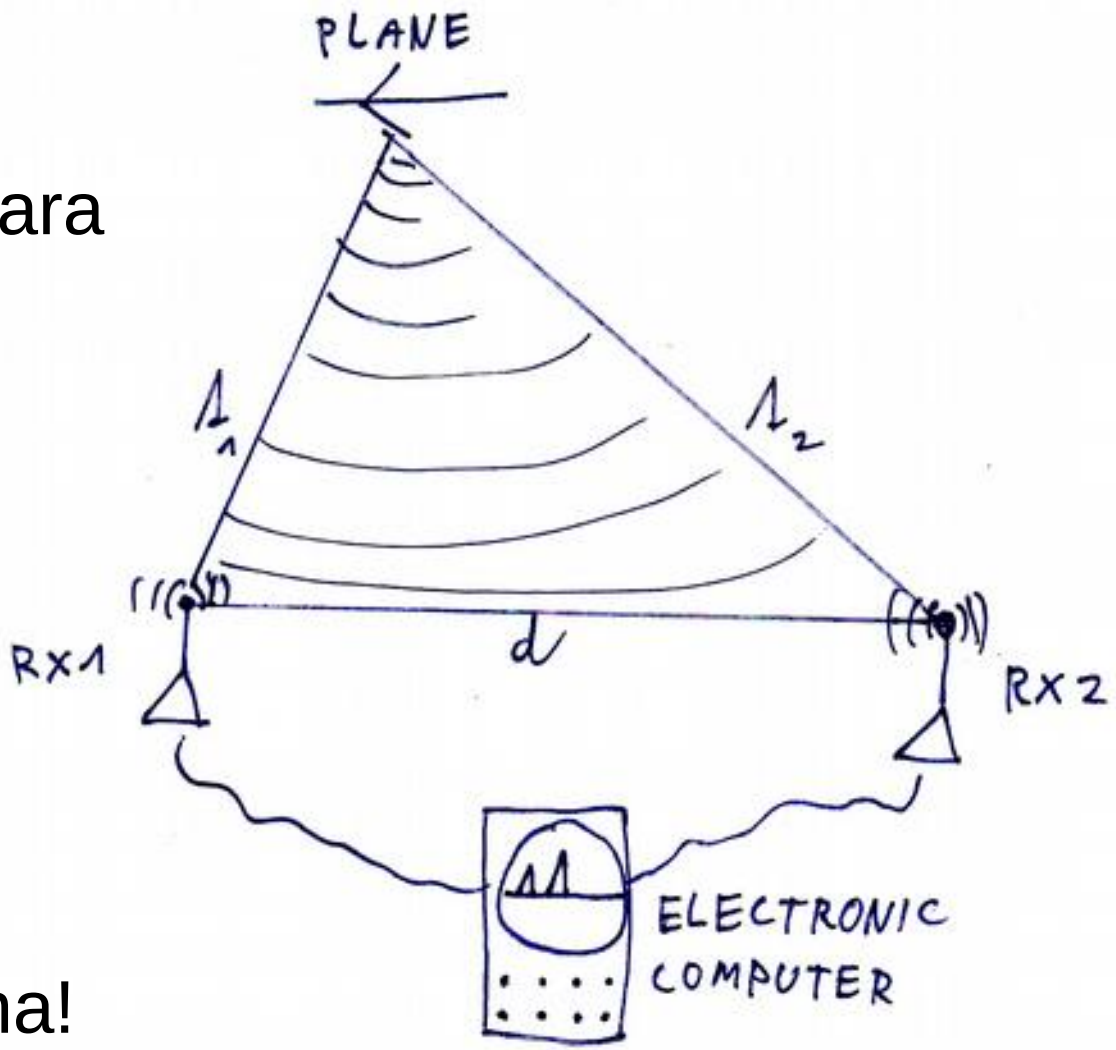
Letadla

- Aktivní: ACARS, ADS-B
  - znáte jako http://www.flightradar24.com/
- acarsdec, dump1090

- pasivní radar

Letadla

- Active-passive:
  - Kopáč/Ramona/Tamara
  - Flightradar24 MLAT



  - Open-source Ramona!

    https://github.com/mutability/mlat-server

Gnu Radio

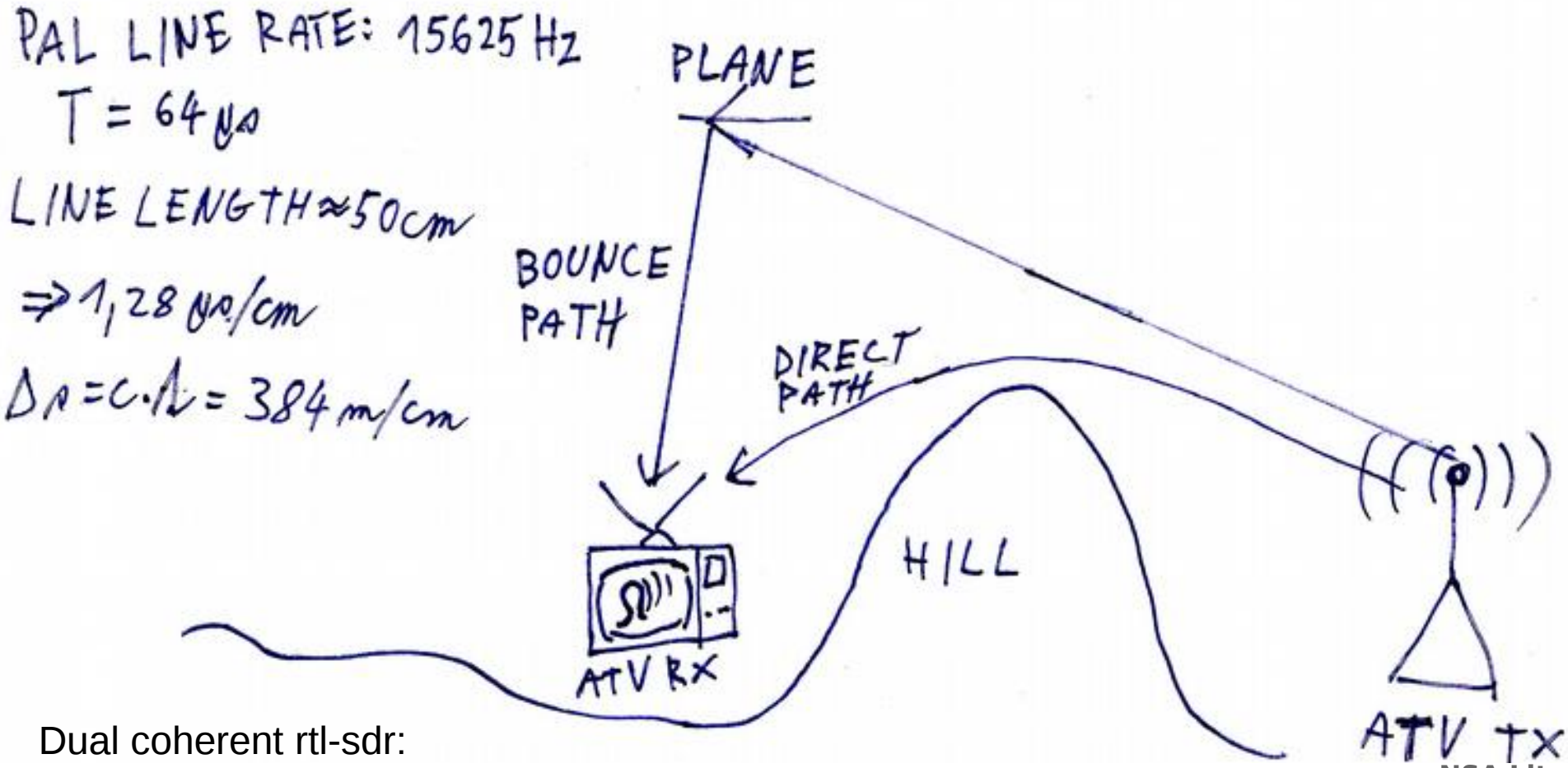
- dependency nightmare
- dynamický vývoj
- https://brmlab.cz/user/jenda/gnuradio

DEMO?

Duchy na analogové televizi

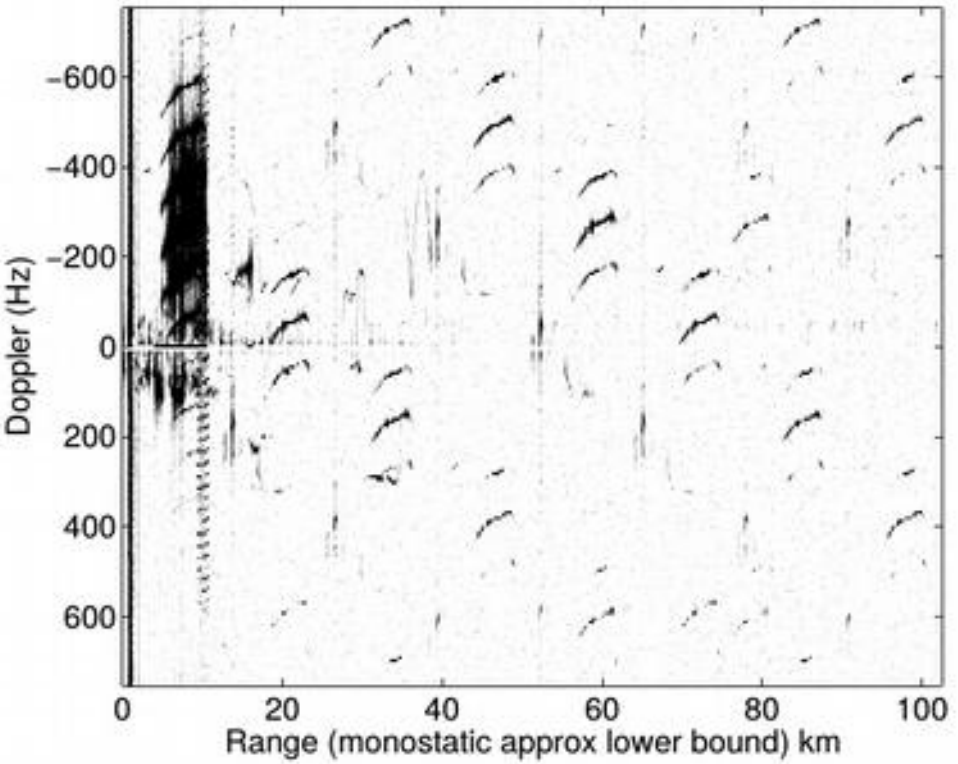
source: http://www.rsm.govt.nz/cms/consumers/reception-problems/what-does-interference-look-like

- Plně pasivní
  - VERA (Věra)
  - http://jenda.hrach.eu/f2/passive-radar-processing-preprint.pdf
    - dost složitá matematika



Dual coherent rtl-sdr:
https://www.youtube.com/watch?v=KRqtqtCVRR0

http://www.armadninoviny.cz/cesky-tichy-strazce-vidi-i-neviditelna-letadla-.html
http://clanekvera.sweb.cz/



NSA Litoměřice
the only company that actually listens to your needs

ASMKS

- ASMKS (Automatic system for frequency spectrum monitoring) by ČTÚ
- Coherent scanners + MLAT
- DYI: SDR + GPS, SDR + FM?
- Anyone?

UAG