Univerza *v Ljubljani*
Fakulteta *za elektrotehniko*

Analiza spektra z RTL-SDR

Seminarska naloga pri predmetu
Digitalne komunikacije

Natalija Nadbath, Tomaž Dežman, Andrej Vrabič

Maj 2015

Povzetek. V sklopu seminarske naloge smo hoteli pokazati kaj vse lahko sprejemamo z uporabo nizkocenovnih RTL-SDR naprav. Bolj smo se posvetili nižjemu delu spektra (50 MHz - 500 MHz) in na njem našli par zanimivih reprezentativnih signalov katere smo ujeli, demodulirali in interpretirali. Prav tako smo se poglobili v samo delovanje RTL-SDR naprav in opazovali različne pojave na napravah z Rafael Micro R820T tunerjem.

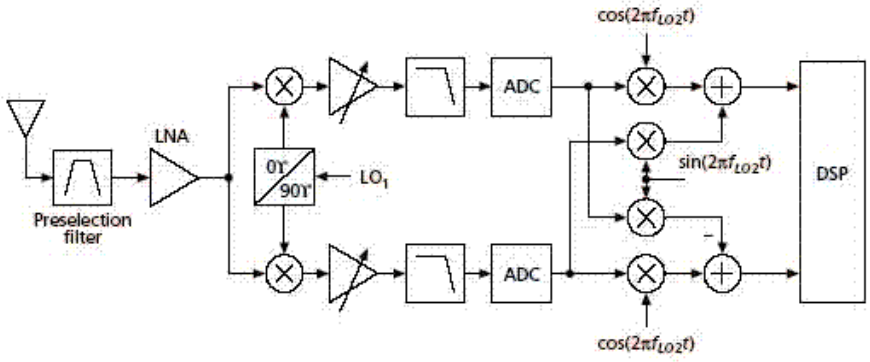
Kazalo

1 Uvod

Pri meritvah smo uporabili DVB-T+DAB+FM ključek neznanega kitajskega proizvajalca z Rafael Micro R820T tunerjem, kateri ima frekvenčno območje od 24 MHz do 1766 MHz, dalo pa bi se ga še razširiti z eksperimentalnimi gonilniki. Uporabili smo tudi programsko orodje SDR#, ki deluje na Windows platformi in je za prikaz spektra od vseh možnih programskih okolij tudi najprijaznejši uporabniku. Spisek programskih orodij, ki so kompatibilni z RTL-SDR ključki pa lahko najdete na spletni strani RTL-SDR[5].
Naša RTL-SDR naprava ima dva osnovna čipa: Raphael Micro R820T radio tuner in Realtek RTL2832U, ki ima 8 bitni ADP(analogno digitalni pretvornik) in USB za črpanje podatkov. Informacije za Realtek RTL2832U niso prosto dostopne.

Slika 1: Strojna oprema.

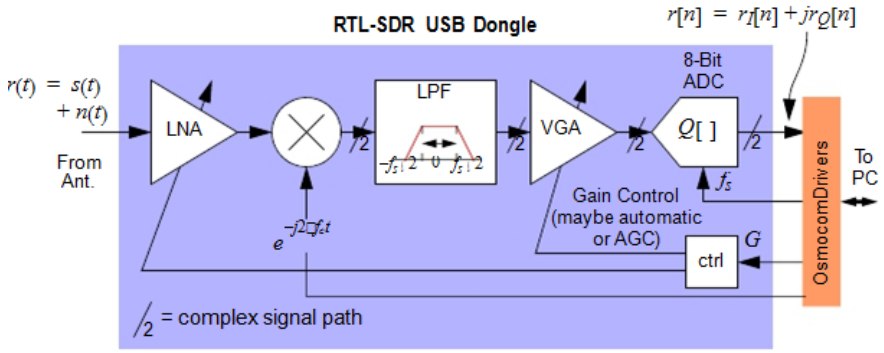
Osnovna konfiguracija je prikazana na sliki 1. Tuner služi kot RF *front-end* za SDR. Miniaturnemu koaksialnemu konektorju za anteno sledi nizko šumni ojačevalnik LNA s šumom okoli 3,5 dB (*noise figure*). Na sliki nista prikazana vhod za nastavitev frekvence vzorčenja f_s in ojačanje tunerja.



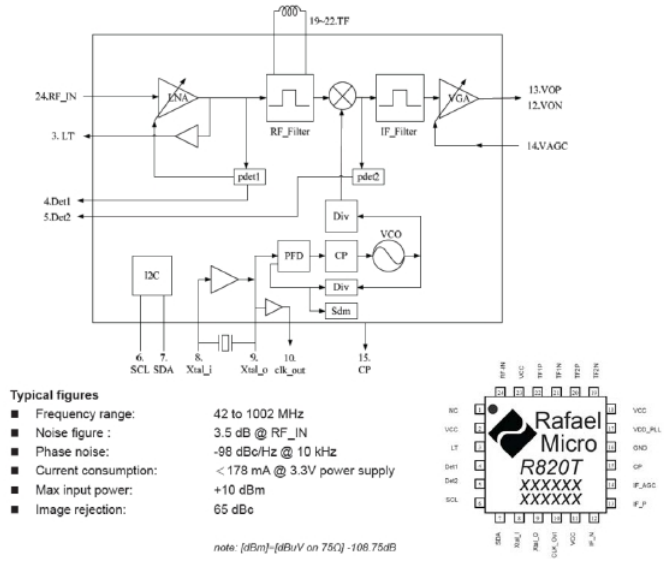
Slika 2: Blokovna shema heterodinskega sprejemnika.

Frekvenčni sintetizator znotraj čipa R820T generira signal lokalnega oscilatorja (f_{LO}), ki skrbi za mešanje frekvence prejetega RF signala (f_{RF}) navzdol na vmesno frekvenco f_{IF}. Kontrola ojačanja je tako na vhodu LNA kot tudi na izhodu s spremenljivim ojačevalnikom (VGA-*variable gain amplifier*). Izraz AGC (*Automatic gain control*) na sliki 3 se nanaša na algoritem/vezje za zaznavanje moči signala, ki vrača kontrolni signal v vezje za kontrolo ojačanja na RF sprejemniku. V tem primeru je to lahko VGA in/ali LNA.

Vhodni signal r(t) je sestavljen iz želenega radijskega signala s(t) in šuma n(t), ki je posledica RF sprejemnika z anteno. Ker ima sprejemnik široko frekvenčno območje so prisotni številni signali. Nadzor ojačanja služi, da ostaja signalno procesiranje linearno, vendar pa na račun dinamičnega območja. Dodajanje pasovnega filtra pred LNA lahko razumemo kot zavračanje možnih neželenih signalov, ki ležijo izven frekvenčnega pasu.[4]

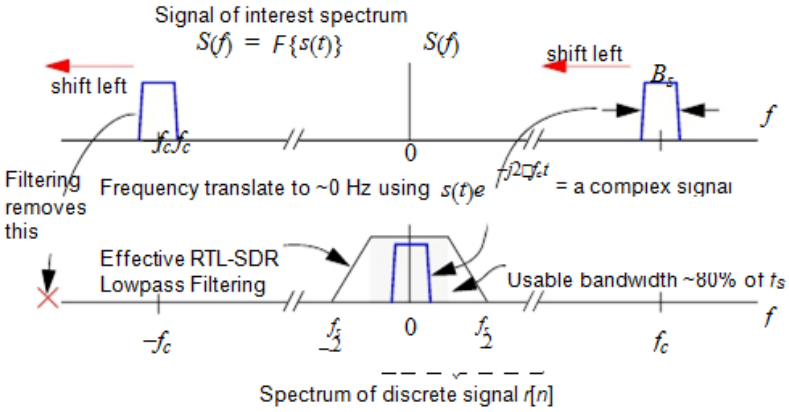


Slika 3: Preprost model vezja.



Slika 4: Blokovna shema Rafael micro R820T.

Za LNA je množilnik, ki ima vhod z lokalnega oscilatorja $e^{-j2\pi f_c t}$. To pomeni mešanje navzdol za f_c. Zaradi teorema o frekvenčni translaciji se premakne vhodni spekter levo za f_c Hz. Signal, ki nas zanima s centrom pri f_c, bo sedaj premaknjen na f_{IM} (*intermediate frequency* - vmesna frekvenca).



Slika 5: Primer mešanja v *baseband*. Velja analogija za mešanje na vmesno frekvenco.

Kompleksni signal gre skozi nizkopasovno sito, ki je funkcija vzorčne frekvence v RTL-SDR. Po teoremu vzorčenja mora biti $f_{VZ} = 2f_S$ Hz. Uporabna pasovna širina je 80% f_s, ker realno sito rabi prehodni pas iz območja prepuščanja v zaporo. Vso procesiranje po

množilniku je kompleksno. V realni strojni opremi je filtriranje realnega in imaginarnega dela z nizkopasovnim sitom izvedeno deloma v R820T, kjer je to enopasovni realni filter in v RTL2382U, kjer je filtriranje I/Q.

Zadnji del je kvantizator. Ker samo osem bitov predstavlja tako realni kot tudi imaginarni del, pomeni, da se generira velik kvantzacijski šum.[3]

2 Moteči pojavi

Pri uporabi ključka se moramo zavedati, da niso vsi signali, ki jih vidimo v SDR# tisti, ki jih nekdo oddaja. Določene 'špice' lahko pripišemo strojni opremi ključka, druge pa klasificiramo kot možne stranske pojave zaradi napačne vzorčne frekvence, filtriranja, ipd.

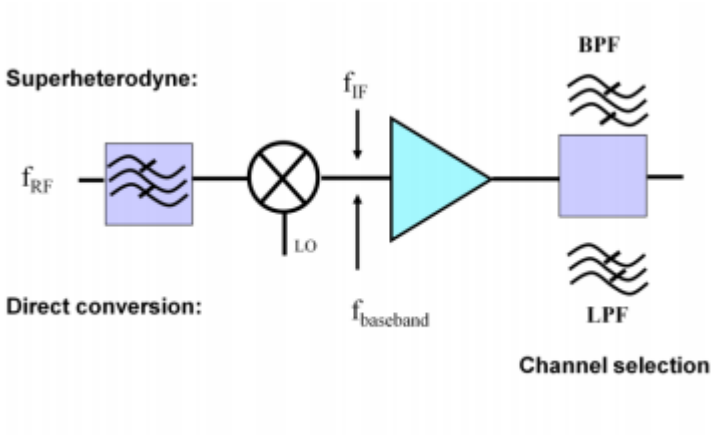
2.1 Vpliv strojne opreme

2.1.1 Odmik od prave frekvence

Pri prvi uporabi je priporočljivo, da naš RTL - SDR najprej umerimo. Ker gre za poceni kitajski izdelek (množična proizvodnja), se zgodi da kristal v oscilatorju ni rezan dovolj natančno in tako dobimo nenatančno tunanje. V programu SDR# lahko to popravimo v nastavitvah s korigiranjem ppm [12], vendar pa pri korekciji potrebujemo referenčno frekvenco s pomočjo katere umerimo tuner. Ta odmik je linearen pojav tekom celotnega spektra, zato je potrebno le eno umerjanje na začetku. Je pa tudi močno odvisno od ambientne temperature zaradi določenih lastnosti kristalov. [12] [13]

2.1.2 DC bias

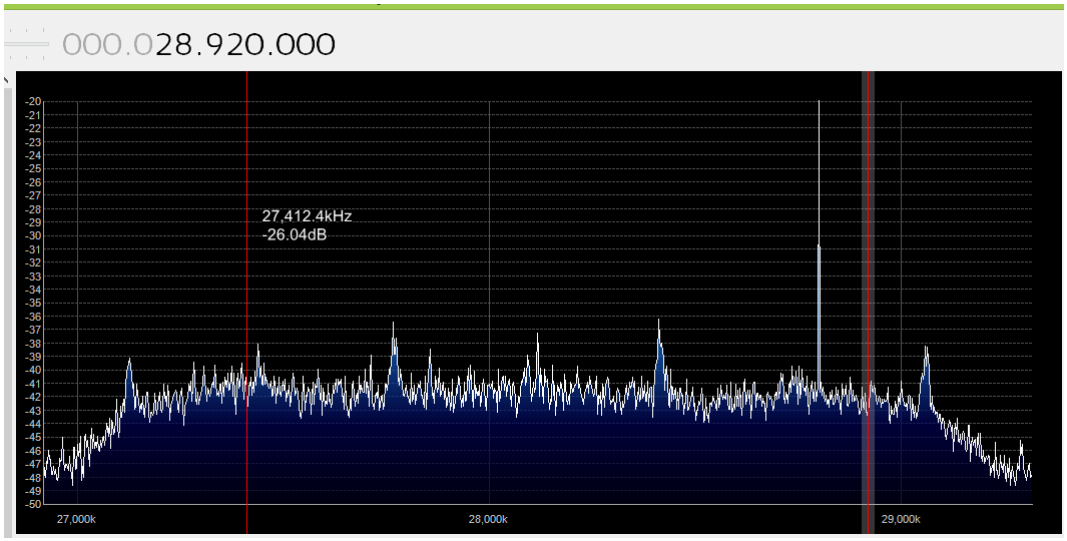
DC bias je bolj izrazit pojav v homodinskih sprejemnikih kot v heterodinskih. Razlika med homodinskim in heterodinskim sprejemnikom je, da homodinski preslika signal f_{RF} v osnovni pas(*baseband*), medtem ko ga heterodinski preslika na neko vmesno frekvenco f_{IF} (*intermediate frequency*). *DC bias* je prispevek strojne opreme in se ga da v programu SDR# navidezno odstraniti oziroma zmanjšati. Pri homodinskih sprejemnikih pride ta pojav od nenatančnosti faze lokalnega oscilatorja in tako dobimo signala I in Q, ki nista zamaknjena za točno $\frac{\Pi}{2}$. V heterodinskih sprejemnikih pa pripisujemo ta pojav ne le nenatančnosti faze lokalnega oscilatorja ampak tudi prispevku A/D pretvornika.



Slika 6: Heterodinski vs. homodinski sprejemnik - blokovna shema.

2.1.3 Notranja ura

Oscilator, ki daje takt celotnemu vezju (ni isti lokalnemu oscilatorju, ki ga najdemo v tunerju) deluje s frekvenco 28.8 MHz. V programu SDR# ga vidimo kot signal na tej frekvenci in na njenih večkratnikih. Zavedati se moramo, da to ni realen signal, ki ga nekdo oddaja, ampak je prispevek naše strojne opreme in v resnici ni prisoten v radijskem spektru. Take signale imenujemo tudi *birdies* in jih najdemo v vseh heterodinskih sprejemnikih. *Birdies* so torej v nekem smislu naši fantomski signali, ki pa niso nujno samo harmoniki frekvence notranje ure. Najdemo jih tudi na frekvencah, ki so vsote ali razlike prispevka notranjega oscilatorja.



Slika 7: Prispevek notranje ure.

2.2 Ostali pojavi

Nekaj meritev smo izvedli s pomočjo signalnega generetorja, ki je oddajal na frekvenci 200 MHz. Namen testiranja je bilo potrditi ali ovreči par pojavov, ki so bili opaženi pri meritvah opravljenih z USRP-jem (Universal software defined radio)[9] v laboratoriju LAiT.

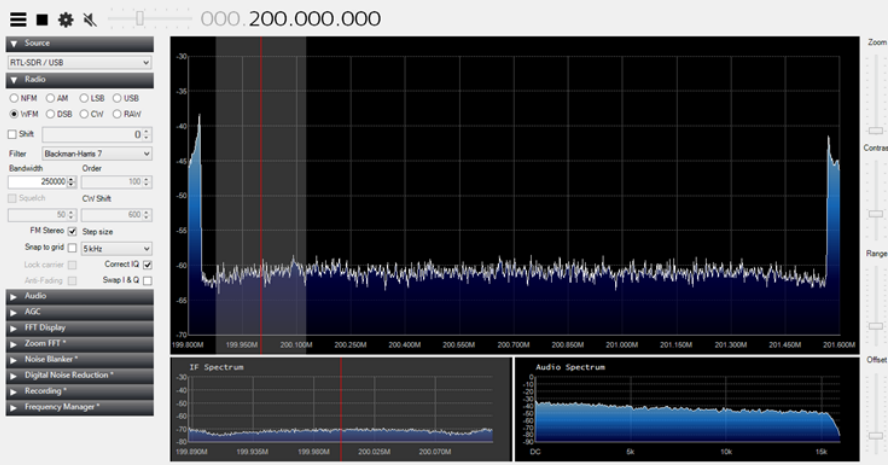
2.2.1 Fantomski signali in image rejection

Pri heterodinskem sprejemniku nam povzročajo težave fantomski signali. Če si predstavljate signal na vhodu f_1, ki se množi s signalom f_{LO} (lokalnega generatorja) dobimo v okolici f_{IF} želen signal f_{RF} in neželen signal f_{IM} (*image frequency*). V teoriji ta pojav razložimo tako, da lahko dobimo na izhodu mešalnika f_1,f_2,$f_1 + f_2$ ali $|f_1 - f_2|$. Težavo rešimo tako, da dodamo filter že pred množilnikom, zato da zajamemo le ozek pas okoli želenega signala. Ker pa realna sita niso idealna, ne zadušimo vseh neželenih prispevkov. Tako se v množilniku upoštevajo tudi prispevki neželenih komponent f_{IM} in se preslikajo v okolico f_{IF} skupaj z želenim signalom f_{RF}. IF filter je ponavadi *passband* filter saj poskuša zajeti le želene signale. Signal na njegovem izhodu ojačamo in pošljemo še skozi en filter preden vstopi v ADP. Vendar velikokrat tudi to ne pomaga. V našem primeru (RTL-SDR z Rafaelo Micro R820T) v programskem okolju SDR# nismo videli fantomskega signala poleg signala generiranega s signalnim generatorjem, saj nimamo dovolj velikega dinamičnega območja. Vendar ti signali obstajajo, saj nam jih potrjuje že

sama teorija.[11]
Image rejection je mera kako dobro naša strojna oprema odfiltrira fantomske signale. Podana je kot razmerje želenega signala f_{RF} z fantomskim f_{IM}, izraženo v dB.[18]

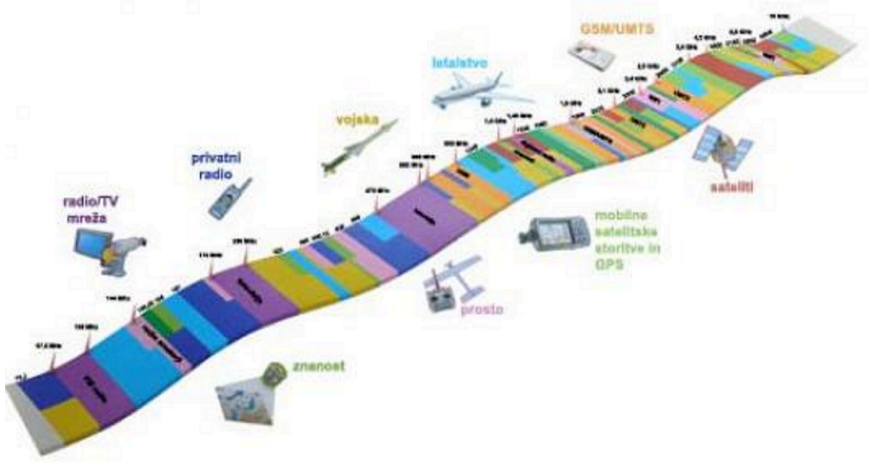
2.2.2 Preslikanje spektra (Aliasing)

Pri meritvah pa smo opazili še eno pomanjkljivost. Če se premikamo po spektru stran od močnega signala (v tem primeru generiranega s signalnim generatorjem) do te mere, da f_{RF} 'pade' napol iz vidnega prikaza, se pojavi njegov *alias* z druge strani prikaza. Bolj kot se premikamo stran pa ta drugi prispevek počasi pade nazaj v šum. V tem primeru lahko predpostavimo, da pas, ki ga vidimo v SDR# ni verodostojen in da bi morali upoštevati prikazan pas minus cca. 10% z leve in desne strani. Do pojava pride zaradi neprimerne vzorčne frekvence, ki jo določimo s pomočjo Nyquistovega teorema $f_{vzorcna} \geq 2f_{signala}$, ki pravi, da mora biti vzorčna frekvenca vsaj dvakrat večja od najvišje frekvence vzorčenega signala. Problem s preslikanjem spektra najdemo v veliko SDR napravah.[17]



Slika 8: Prikaz dobljene preslikave.

3 Pregled spektra in zanimivi signali



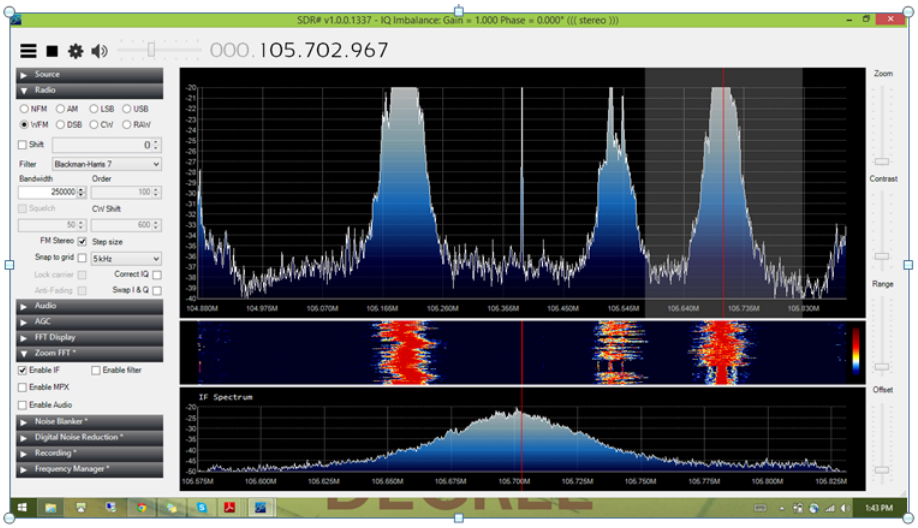
Slika 9: RF spekter.

Na sliki frekvenčnega spektra vidimo, da radijski spekter zavzema frekvence od 20 kHz do 30 GHz. Naš RTL-SDR pa lahko zajame spekter le na območju 24 MHz - 1766 MHz. Če pogledamo v evidenco AKOS-a (Agencija za komunikacijska omrežja in storitve Republike Slovenije)[14] [15] [16] lahko vidimo kateri pasovi radijskega spektra so rezervirani in/ali zakupljeni ter kateri so prosti za odprto komunikacijo. V sklopu naloge smo se 'sprehodili' po frekvenčnem pasu, ki ga naš sprejemnik lahko sprejema in opazovali v katerih pasovih so najmočnejši signali. Meritve so bile opravljene v Domžalah.
Prvi izraziti signali se pojavijo šele z FM radiom (87.6 MHz - 107.9 MHz). Naslednji sklop močno oddajanih signalov predstavlja digitalna televizija (cca 470 MHz - 862 MHz). Le-tej pa sledi GSM - mobilna telefonija (cca 790 MHz - 960 MHz .[6]). V vmesnem območju lahko opazujemo številne signale, ki nimajo tako velikega dinamičnega območja in so težje 'ulovljivi', saj je normalna komunikacija ponavadi odsekana in ne zvezna. Predno ulovimo uporaben signal, ki ga tudi lahko demoduliramo, se ponavadi komunikacija konča. Če bi si hoteli povečati verjetnost 'vidnih' signalov lahko zamenjamo anteno, ki smo jo dobili z RTL-SDR ključkom z neko drugo, močnejšo. S tem si izboljšamo možnosti lovljenja signalov tudi ob slabih pogojih (znotraj stavb, deževni dnevi, ipd.).

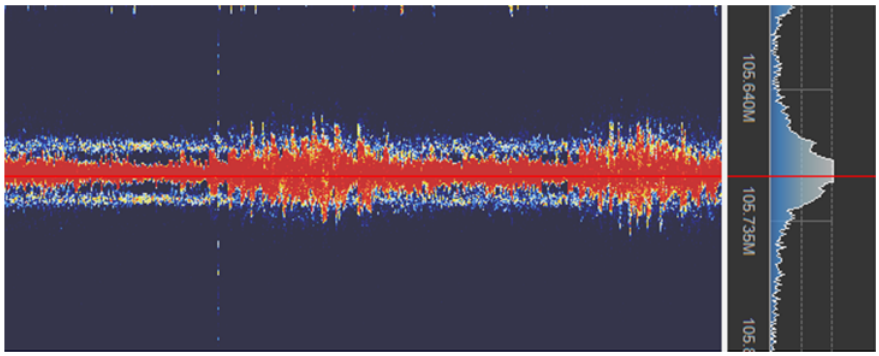
3.1 FM radio

Začeli smo z nečim preprostim, torej smo našli **FM radijsko postajo**, se postavili nanjo in demodulirali z širokopasovno frekvenčno demodulacijo (WFM - *wideband FM*). Prika-

zani signal je radijska postaja RTV Slo1 ARS na frekvenci 105.7 MHz, ki povečini predvaja klasično glasbo. Prikaz spektra in radijske postaje v časovnem prostoru (*waterfall*) je spodaj. Avdio posnetek demoduliranega signala je priložen posebej.



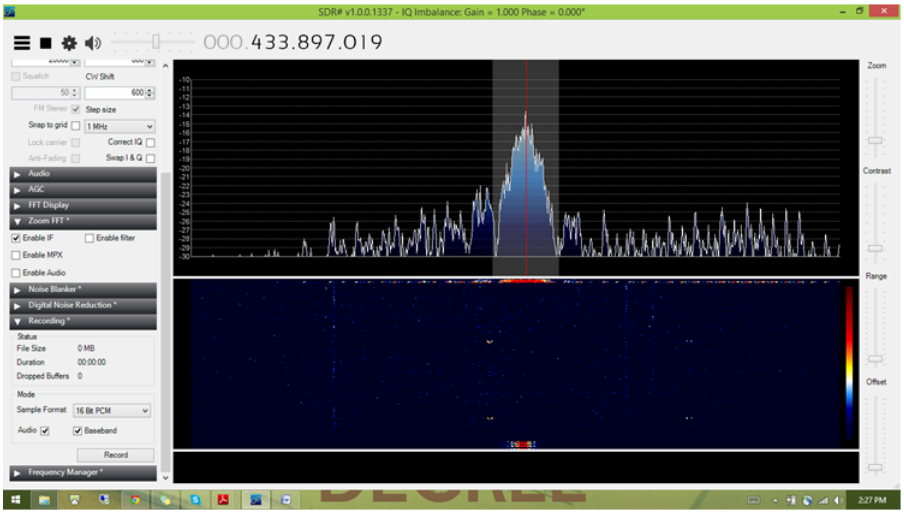
Slika 10: Prikaz FM radia v SDR#.



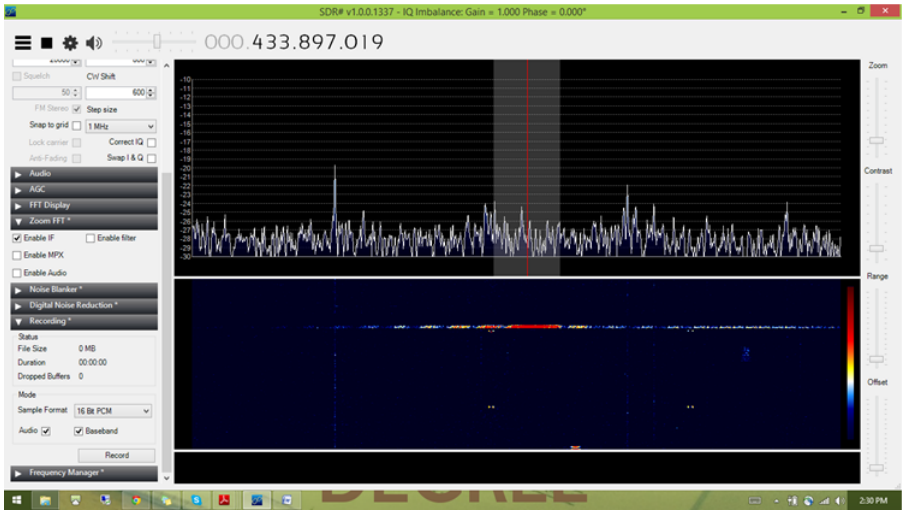
Slika 11: Prikaz FM radia v *waterfallu* - časovni domeni.

3.2 Avtomobilski ključi

Nato smo testirali ali lahko s SDR# zaznamo **avtomobilski ključ** znamke Reanault Clio druge serije. Ključi delujejo na 315 MHz za Severno Ameriko in 433.92 MHz za Evropo. Na sliki 12 vidimo kako se signal dvigne iz šuma ob pritisku na gumb, na naslednji sliki pa vidimo signal na *waterfallu*.

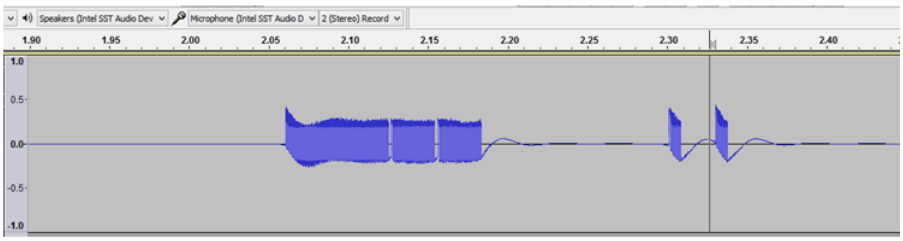


Slika 12: Prikaz spektra avtomobilskega ključa.

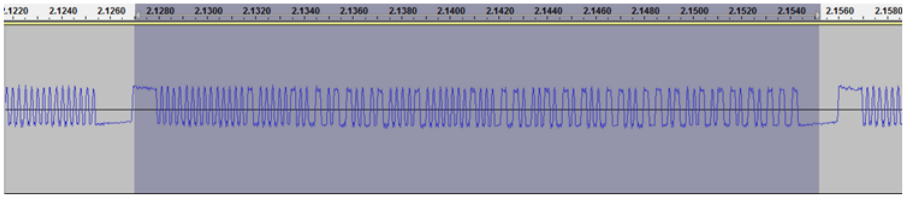


Slika 13: Prikaz v *waterfallu* - časovni domeni.

Testno meritev smo posneli znotraj SDR# pri amplitudni demodulaciji in ga nato uvozili v program Audacity. Na sliki 14 vidimo signal v Audacity-ju, sestavljen je iz sinhronizacijskega dela, dveh delov, ki sta namenjena komunikaciji in dveh zaključnih delov. Na sliki 15 smo prvi del ki je namenjen komunikaciji raztegnili in opazimo bite - ničle in enke. Če bi hoteli dekodirati komunikacijo bi jo morali še dekriptirati. V tem primeru gre za HITAG2 kripcijo katero zasledimo v starejših avtomobilih.[19]

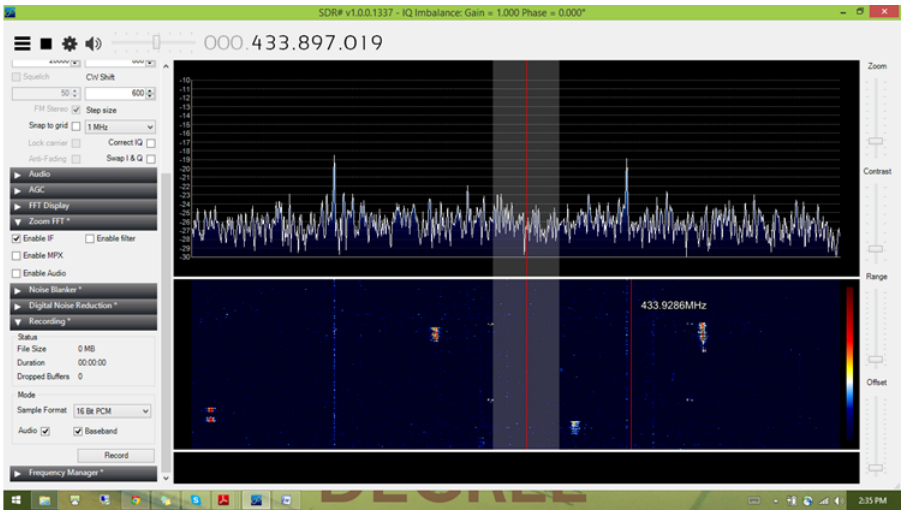


Slika 14: Prikaz avdio posnetka avtomobilskega ključa.



Slika 15: Prikaz bitov v Audacity-ju.

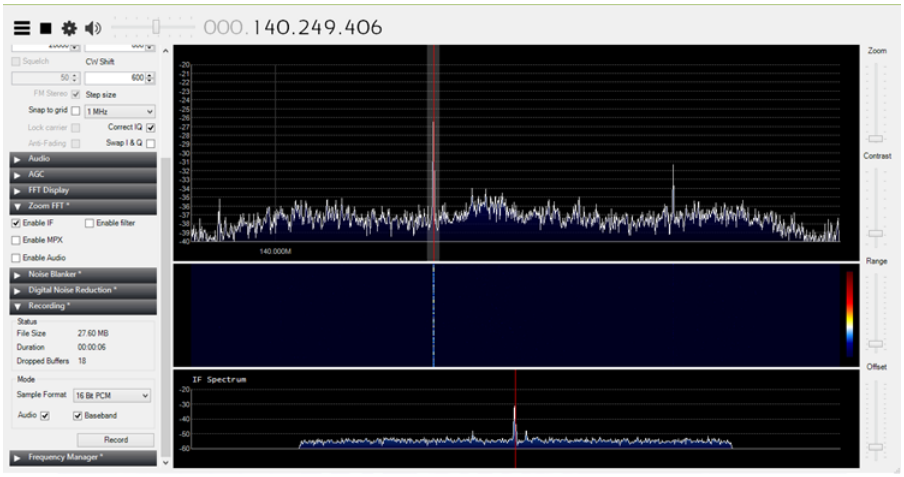
Pri opravljanju te meritve smo opazili zanimiv pojav, ki potrebuje dodatno interpretacijo. Na naslednji sliki vidimo na *waterfall* prikazu zanimive prispevke, kateri pa se ne poznajo na prikazu spektra. Gre za komunikacijo zunanjih senzorjev z vremensko postajo v hiši. Ker so ti signali zelo šibki se ne poznajo na frekvenčnem prikazu, saj so skriti v šumu.



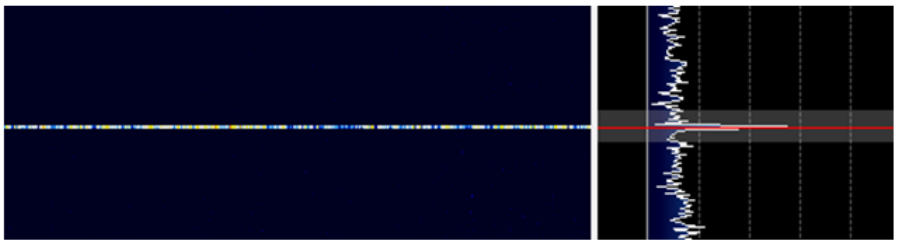
Slika 16: Senzorji temperature, vlage in pritiska.

3.3 Radioamaterji

Ujeli smo tudi radioamaterja, ki je oddajal na frekvenci 140.25 MHz. Signal smo demodulirali s CW (*continuous wave*) demodulacijo. Na *waterfall* prikazu prepoznamo Morsejevo abecedo.



Slika 17: Signal radioamaterja.



Slika 18: Prikaz Morsejeve abecede.

3.4 Gasilci in druge službe na področju varstva pred naravnimi in drugimi nesrečami

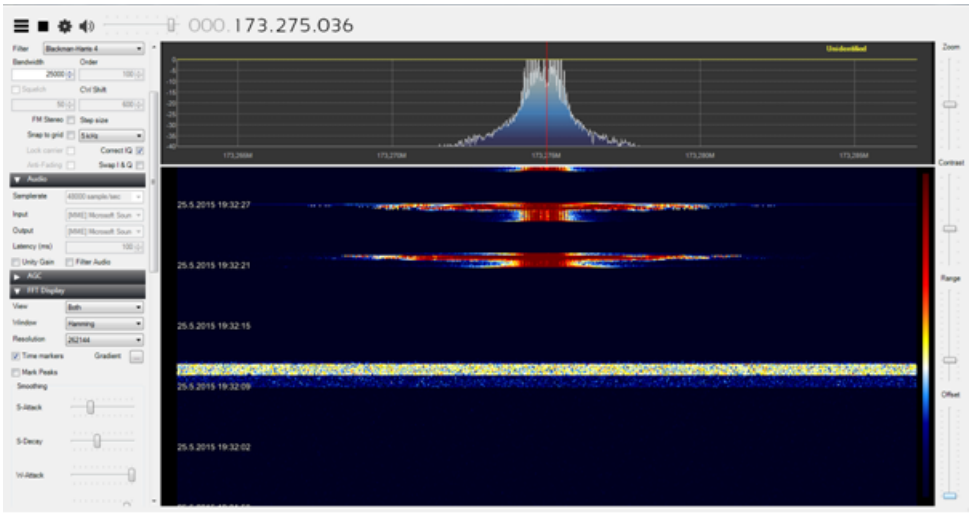
V Republiki Sloveniji uporabljamo na področju varstva pred naravnimi in drugimi nesrečami samostojen sistem radijskih zvez **ZARE**. Ta je od svojega začetka v letu 1994 počasi prerasel v največji klasični sistem radijskih zvez v državi.[21]
Funkcionalno gledano je sistem ZARE razdeljen na: podsistem radijskih zvez (radijske

postaje) in podsistem osebnega klica (pozivniki).

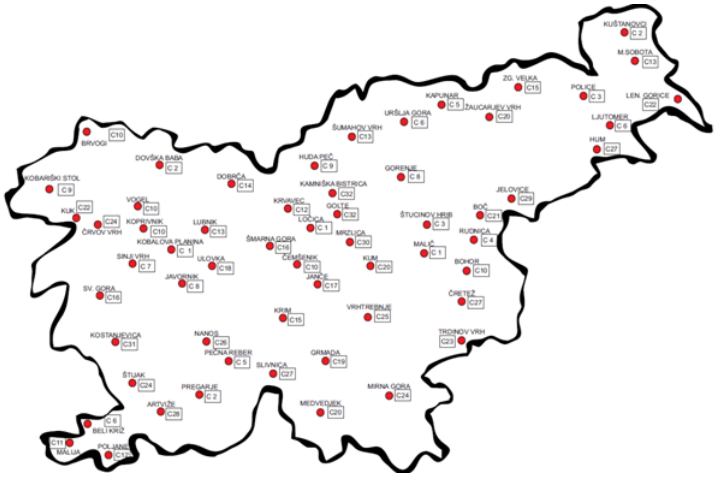
Tehnološko gledano je razdeljen na:

- ZARE - analogne radijske zveze, omogočajo zgolj govorne komunikacije
- ZARE PLUS - digitalne zveze, omogoča prenos govora in podatkov
- ZARE DMR - digitalne zveze, omogoča prenos govora in podatkov

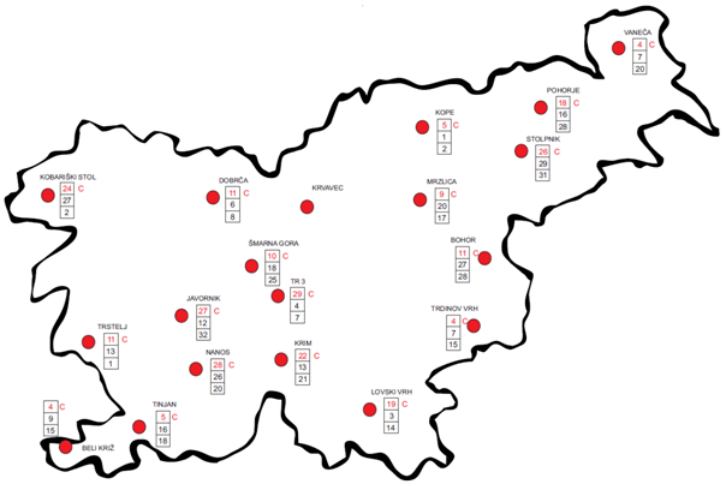
Gasilce smo ujeli na kanalu 41, gre pa za sistem osebnega klica – pozivniki. Pozivniki se prožijo na kanalu 40, frekvenca 173,2500MHz (velja za celotno Slovenijo). Uporablja se POCSAG kodiranje in FSK modulacija.[20]



Slika 19: Primer spektra za kanal 41 (173.275MHz).



Slika 20: Lokacije repetitorjev ZARE (oktober 2014).



Slika 21: Lokacije baznih postaj ZARE+.

4 Zaključek

V zaključku bi povzeli, da RTL-SDR ni spektralni analizator, vendar je zelo uporaben v učne namene in raziskovanje RF spektra. Njegove prednosti so predvsem dostopnost, cena in dobro podprta programska oprema. Njegove slabosti pa predvsem slabo dinamično območje, okornost pri lovljenju hitro spreminjajočih se signalov in omejitve elektronike.

RTL-SDR lahko uporabimo v mnogih domačih projektih in na spletu najdemo veliko primerov kaj vse so že naredili z njim.[10]

Literatura

[1] Tomažič, S. (2012). Digitalne komunikacije. Ljubljana: Fakulteta za elektrotehniko.

[2] http://www.lait.fe.uni-lj.si/gradiva/DK/LAB/RTL-SDR%20in%20GNU%20Radio.pdf

[3] Di Pu in Alexander M. Wyglinski. Digital Communication Systems Engineering with Software-Defined radio.

[4] http://www.eas.uccs.edu/wickert/ece4670/lecture_notes/Lab6.pdf

[5] http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/

[6] http://www.mobilna-telefonija.com/mobilni-informator/85-frekvence.html

[7] http://www.uradni-list.si/files/RS_-1998-007-00291-OB~P001-0001.PDF#!/pdf

[8] http://www.rtl-sdr.com/tag/ppm/

[9] http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral

[10] http://hackaday.com/tag/rtl-sdr/

[11] http://analog.intgckts.com/wireless-receiver-architectures/

[12] http://superkuh.com/gnuradio/live/ppmerror_751600000.png

[13] http://superkuh.com/rtlsdr.html

[14] http://www.uradni-list.si/1/content?id=292

[15] http://www.uradni-list.si/files/RS_-1998-007-00291-OB~P001-0002.PDF#!/pdf

[16] http://www.uradni-list.si/files/RS_-1998-007-00291-OB~P001-0001.PDF#!/pdf

[17] http://www.rtl-sdr.com/tag/aliasing/

[18] http://en.wikipedia.org/wiki/Superheterodyne_receiver#Image_frequency_.28fimg.29

[19] https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf

[20] http://en.wikipedia.org/wiki/POCSAG

[21] http://www.sos112.si/slo/tdocs/predstavitev_rz2007.pdf