Software Defined Radio

Davide "rainbow" Gerhard
rainbow@irh.it

16 Novembre 2013
RadioAmatore 2 (Pordenone)

Sommario

Chi sono

- laureato in Sicurezza Informatica a Milano
- master in Computer Science all'università di Trento
- free-software enthusiastic ($> 10 anni$)
- freelance in network-security & free-system
- per anni attivista del pnlug 1.0
- Gentoo&Debian maintainer/evangelist

Disclaimer

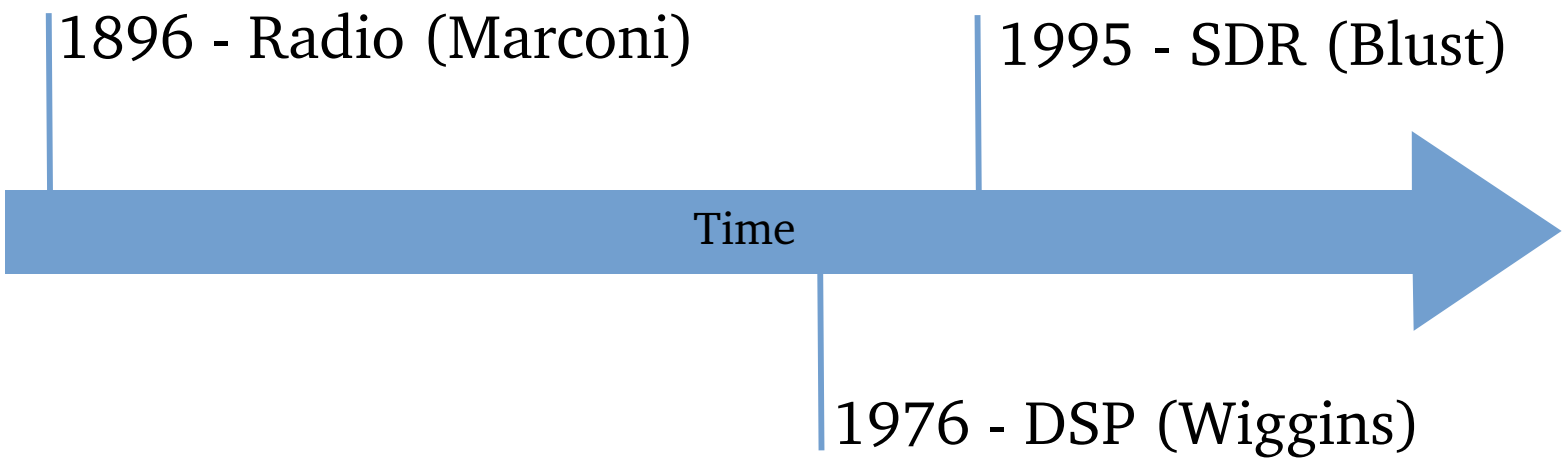
oggi NON parleremo di come:

- intercettare le forze dell'ordine
- catturare e decriptare il protocollo GSM
- implementare un'architettura GSM
- ...

ma di come la fantasia e l'ingegno possano aprire nuove strade creative...

Architettura

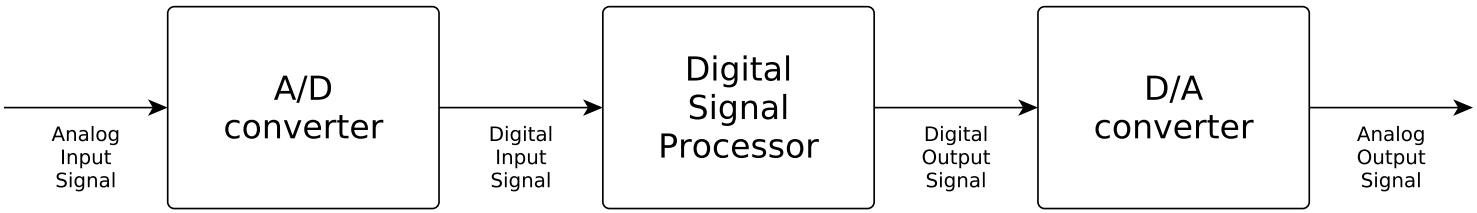
Evoluzione



Radio tradizionali

- la parte di ricezione e di demodulazione è implementata in hardware
- i filtri sono analogici e pre-configurati per il tipo di applicazione
- l'architettura è rimasta pressochè identica negli ultimi 100 anni

Digital Signal Processor (DSP)



- uno dei passi più importanti nella storia delle telecomunicazioni;
- la parte di de/modulazione e di analisi del segnale viene effettuato in ambiente digitale (tempo/frequenza discreto);
- hardware dedicato o basato su core DSP multipli;
- uso di tecniche di Digital Signaling Processing.

Software Defined Radio (SDR) - Idee

Software Defined Radio (SDR) - Idee

Radio in which some or all of the physical layer functions are software defined. (IEEE P19001 group)

Software Defined Radio (SDR) - Idee

Radio in which some or all of the physical layer functions are software defined. (IEEE P19001 group)

The main aim of SDR is "to turn hardware problems into software problems". (E. Blossom)

Software Defined Radio (SDR) - Idee

Radio in which some or all of the physical layer functions are software defined. (IEEE P19001 group)

The main aim of SDR is "to turn hardware problems into software problems". (E. Blossom)

The objective of SDR is to provide a reconfigurable radio platform that is capable of accommodating both current and future communication standards. (J. Mitola)

Software Defined Radio (SDR) - Idee

Radio in which some or all of the physical layer functions are software defined. (IEEE P19001 group)

The main aim of SDR is "to turn hardware problems into software problems". (E. Blossom)

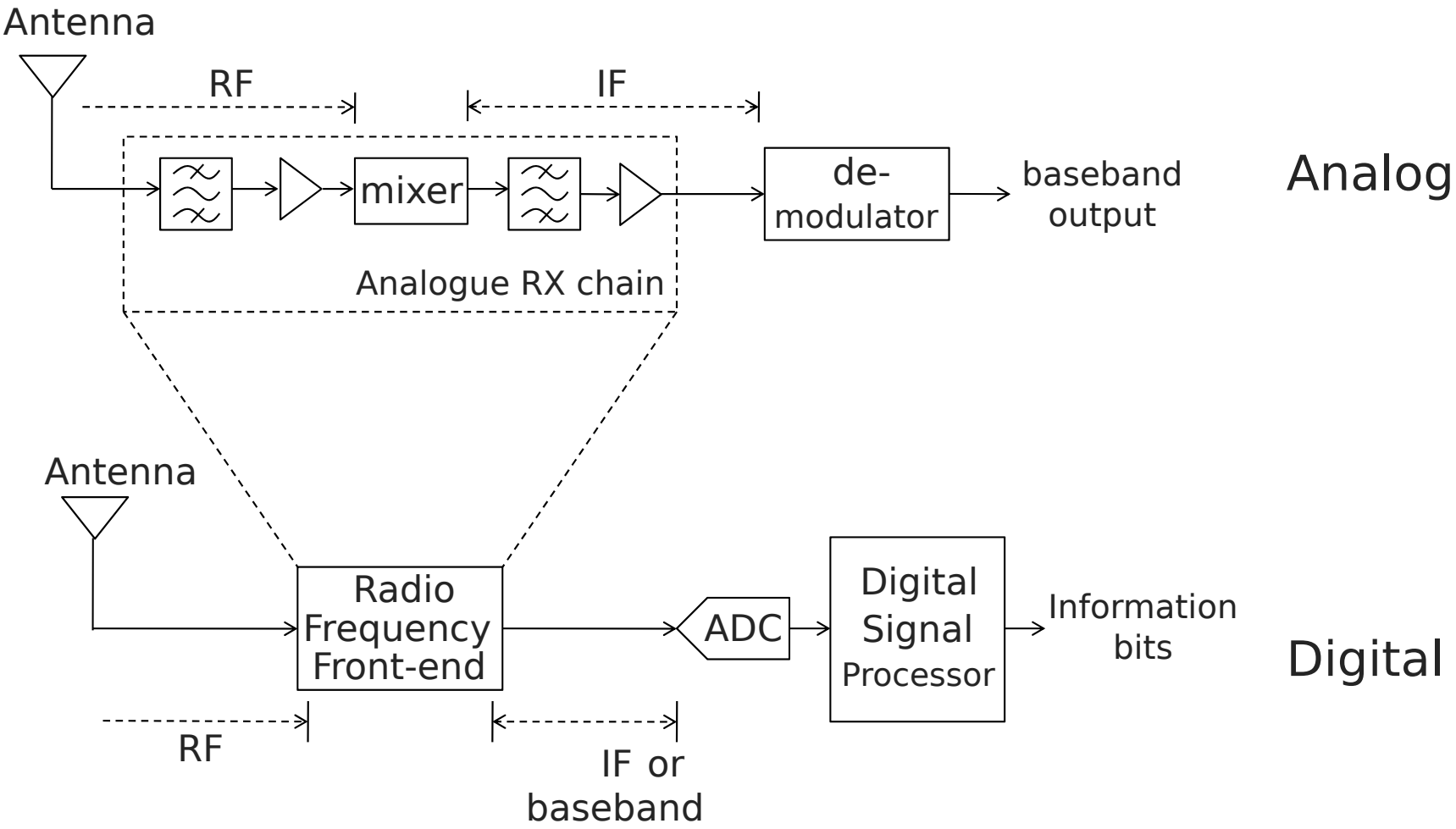
The objective of SDR is to provide a reconfigurable radio platform that is capable of accommodating both current and future communication standards. (J. Mitola)

Software ~~Defined~~ Radio

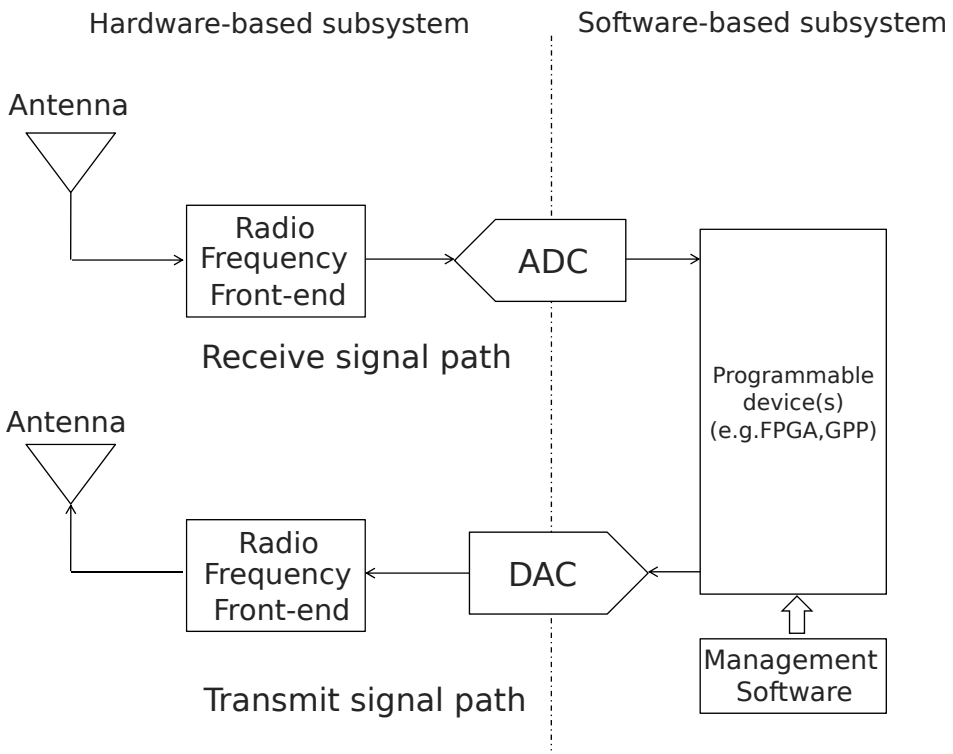
Software Defined Radio (SDR)

- inizia a diffondersi in ambito militare, accademico e amatoriale circa 15/20 anni fa;
- usa più o meno lo stesso frond-end delle radio classiche; un tuner che trasla la frequenza sintonizzata (quadrature mixing) a IF (intermediate-frequency) o a baseband;
- usa un ADC (Analog-Digital converter) per digitalizzare l'IF o la baseband; o DAC in caso di trasmissione;
- usa algoritmi software per il filtraggio, l'equalizzazione, la de/modulazione e la decodifica.

Architettura Radio Analogico/Digitale

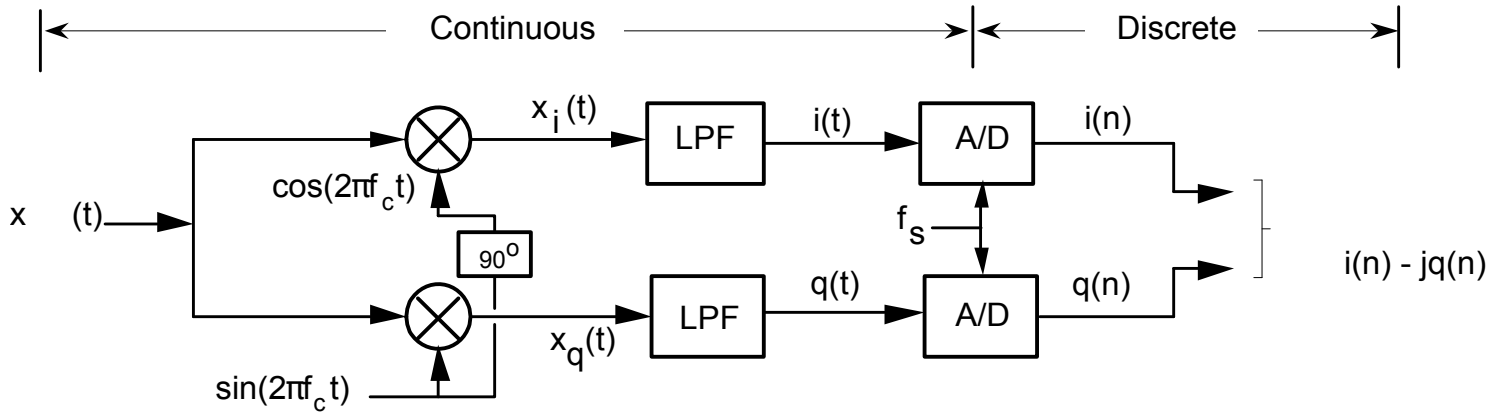


Transceiver SDR



- DSP: usa una porzione ristretta (narrowband) dello spettro e HW dedicato;
- SDR: usa una porzione larga (wideband) dello spettro e il filtraggio è effettuato via software.

Quadrature-sampling (I/Q)



- ogni convertitore A/D opera a metà della frequenza di campionamento di un normale sampler;
- ci permette di catturare un segnale analogico wideband;
- migliora l'efficienza della FFT (Fast Fourier Transform);
- la conoscenza della fase permette un'analisi coerente del segnale;
- permette di conoscere "istantaneamente" il valore del modulo e della fase del segnale durante la demodulazione.

Vantaggi

- essendo il ricevitore implementato via software non ci sono limiti se non quelli imposti dal tuner, dall'A/DC e dalla potenza computazionale disponibile;
- maggiore flessibilità nello sviluppo di sistemi di comunicazione;
- tale architettura è già usata in ambito militare (JTRS, SCA) e in infrastrutture commerciali (es. UMTS NodeB / LTE eNodeB)
- efficienza nei costi di sviluppo e di ricerca;
- maggiore propensione all'innovazione e all'aggiornamento.

Svantaggi

Potenza Computazionale

SDR nei prodotti di consumo

- molti dispositivo di largo consumo implementano già SDR:
  - il processore della baseband nei telefoni GSM/UMTS/LTE
  - Wifi, Bluetooth e GPS
- la flessibilità presente nell'hardware è il più delle volte ristretta via software; l'accesso a basso livello delle API DSP o ai campioni grezzi è limitato / non documentato o non attivo;
- l'utente è bloccato nello sfruttare i veri benefici disponibili con l'uso della tecnologia SDR.

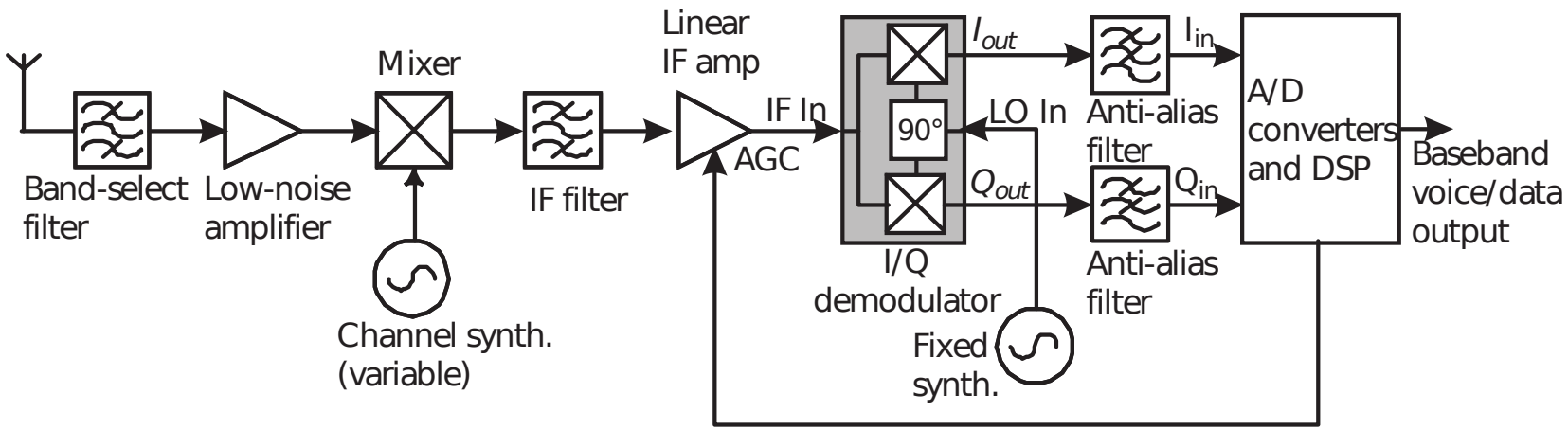
Hardware

Hardware necessario

In genere sono necessarie le seguenti parti:

- Antenna
- LNA (Low noise amplifier)
- (Quadrature sampling) mixer
- RF power amplifier
- A/D Converter

Down-Converter a due stadi



Antenne

a volte basta un semplice dipolo auto-costruito...

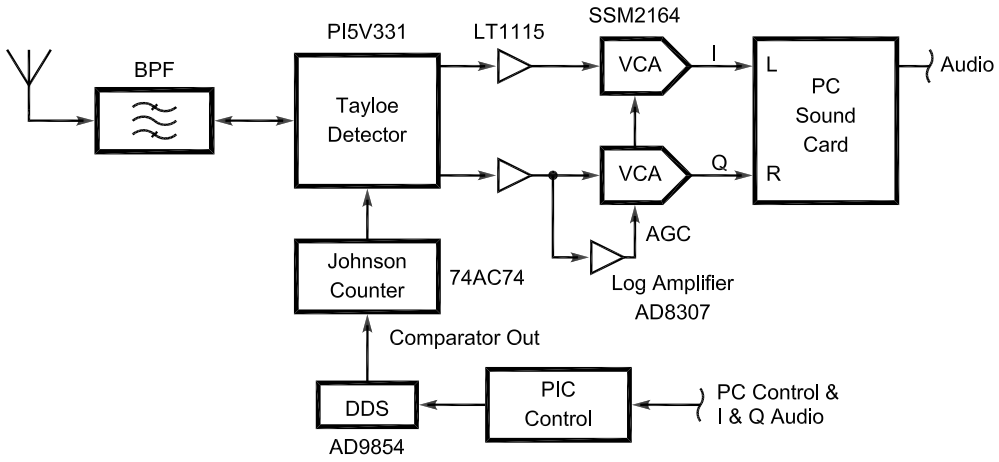
ma si tenga sempre presente che l'antenna è l'aspetto più importante di un sistema radio

Architetture programmabili

- Field Programmable Gate Array (FPGA)
- General Purpose Processor (GPP)
- Programmable System on Chip (SoC)
- Digital Signal Processor (DSP)

possono anche essere implementate soluzione miste come vedremo in seguito.

Dal mondo radioamatoriale

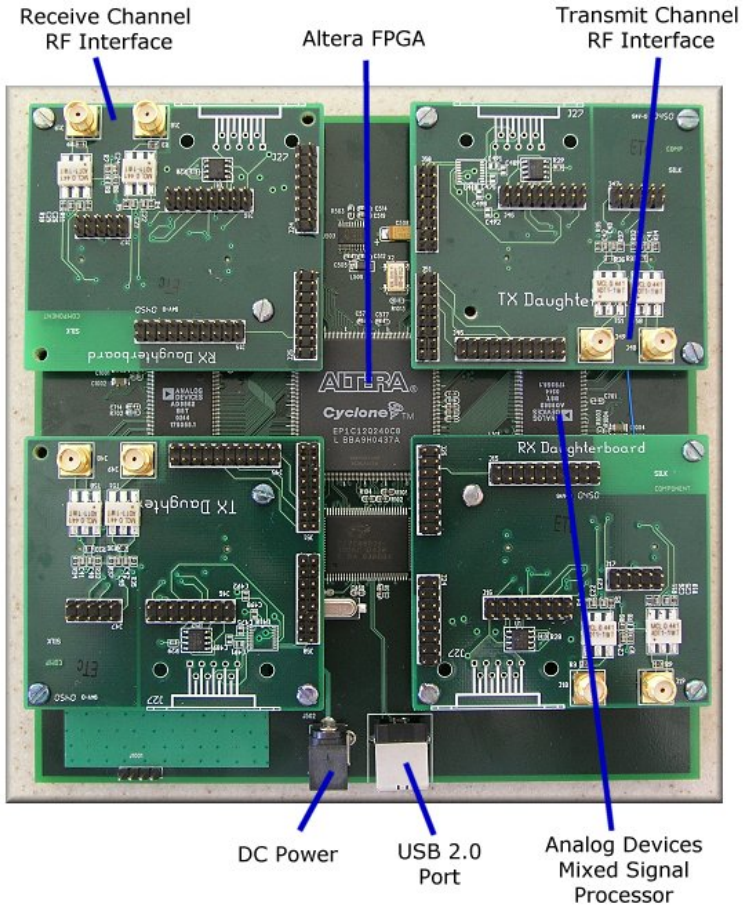


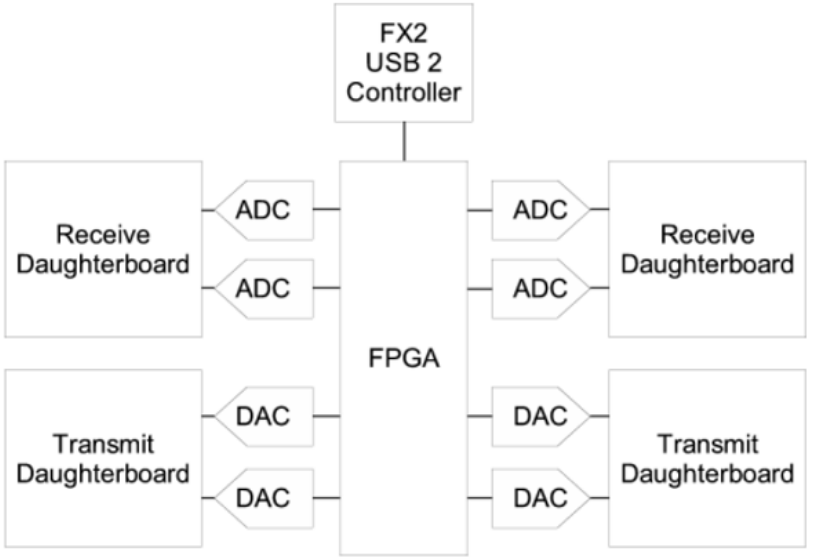
- uso della scheda audio per l'A/DC del segnale I/Q proveniente dal mixer;
- PREGIO: facile da costruire in casa;
- PROBLEMA: banda campionata limitata;
- esempi di transceiver: Softrock RT/TX, SDR Cube, FlexRadio, Elecraft KX3;

Universal Software Radio Peripheral (2006)

- general-purpose open-source hardware (gli schemi sono di pubblico dominio)
- concetto modulare:
  - la motherboard contiene l'interfaccia per il PC, il baseband processor (FPGA) e i D/A converter
  - le daughterboards contengono la radio e gli RF up/down-converter
- particolare attenzione è stato dato al prezzo finale che si aggira intorno ai 700-1000 euro; ben distante dai prodotti professionali allora presenti ma non ancora alla portata di tutti.

Universal Software Radio Peripheral (USRP)

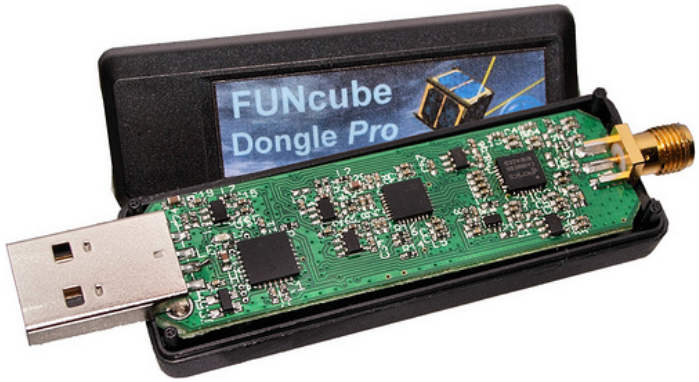




Universal Software Radio Peripheral 2

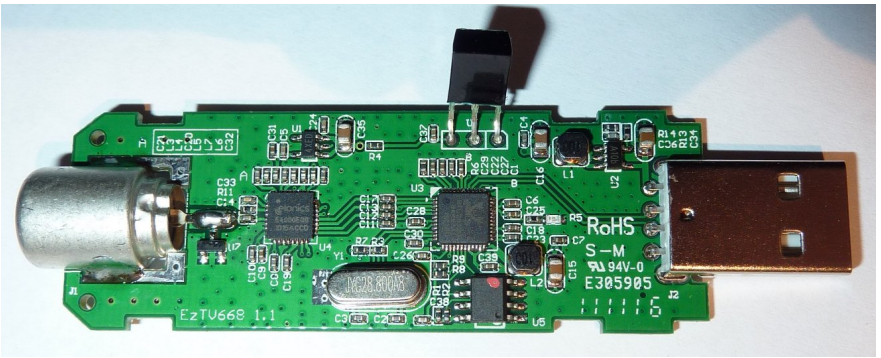
- evoluzione della prima versione per ovviare al problema più stringente: l'USB aveva solo 32MB/s half-duplex di banda;
- la nuova interfaccia e' Gigabit Ethernet (full-duplex);
- 25 MHz di banda RF;
- uso dello Xilinx Spartan 3-2000 (FPGA);
- 2×100 MHz 14 bit ADC;
- 2×400 MHz 16 bit DAC;
- il clock può essere collegato ad una sorgente esterna (GPS);
- modalità stand-alone;
- può essere collegata ad altre URSP2 ed implementare il MIMO;
- le Daughterboards sono compatibili con la prima versione;
- l'FPGA si occupa del down/up-conversion e interpolazione; la CPU del PC si occupa della de/modulazione.

FunCube Dongle Pro (2010)



- capace di ricevere le frequenze da 64 MHz a 1700 MHz;
- banda limitata a 96 kHz;
- 193$, prezzo ancora alto;
- nata per la ricezione dei satelliti radioamatoriali e NOAA;
- ottima per radioamatori e TETRA ma non ancora sufficiente per applicazioni wideband;
- gli schemi hardware e il firmware sono proprietari.

Realtek RTL2832U (ricevitore DVB-T)



- essendo un chip SoC per la ricezione del DVB-T il prezzo di mercato è molto basso ($\sim$ 20 euro);
- implementa un ADC, un demodulatore DVB-T ed un'interfaccia USB2;
- nella modalità DVB-T il chip riceve il segnale dal tuner, lo de-modula ed invia il video e l'audio MPEG2-TS via USB;
- le implementazioni dei produttori seguono sostanzialmente lo stesso schema;
- il reverse engineering del protocollo USB e l'uso di alcuni comandi ha permesso la ricezione dei raw sample.

Realtek RTL2832U - Caratteristiche

- i migliori tuner presenti sono l'Elonics E4000 (high frequency range) e il Rafael Micro R820T;
- in base al tuner possiamo ricevere un range diverso di frequenze:
  - Elonics E4000 : 52 - 2200 MHz con un gap da 1100 MHz a 1250 MHz;
  - Rafael Micro R820T : 24 - 1766 MHz;
- i sample sono di 8-bit I/Q;
- il sample-rate teorico è di 3.2 MS/s ma si consiglia di non superare il valore di 2.4 MS/s per non avere problemi di perdite o di aliasing;
- maggiori informazioni le trovate sul sito `http://sdr.osmocom.org/trac/wiki/rtl-sdr`

Nuove board

l'interesse sull'argomento a fatto nascere diversi progetti atti a creare nuovo hardware; tra questi troviamo:

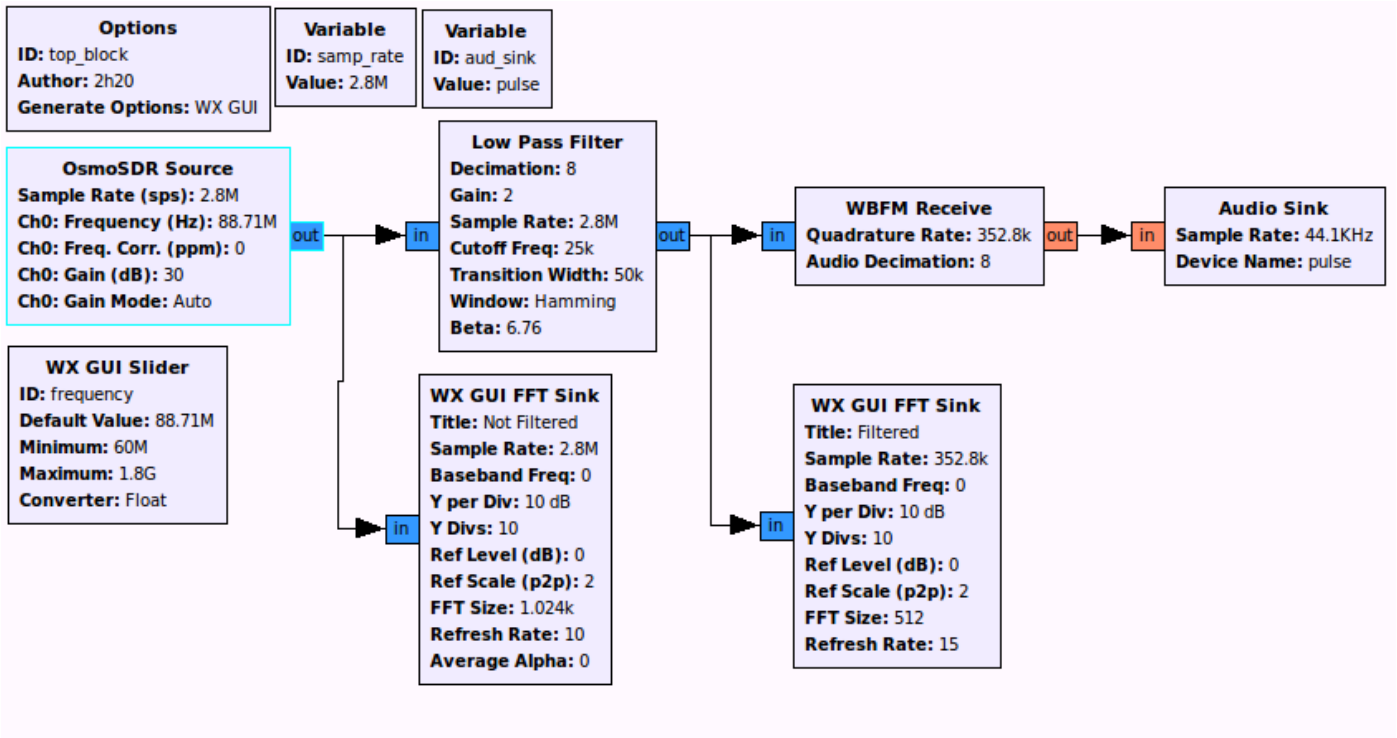
- OsmoSDR
- HackRF
- bladeRF
- HPSDR (High Performance Software Defined Radio)

Software

Gnuradio

- Idea: implementare SDR nella maniera più generica possibile e in un PC general-purpose;
- i moderni calcolatori multi-core x86_64 hanno sufficiente potenza per eseguire calcoli complessi ed intensivi come quelli richiesti dagli algoritmi DSP;
- tale architettura è ovviamente troppo dispendiosa per integrarli nei prodotti di massa ma perfettamente funzionale per il mondo amatoriale, di ricerca e di insegnamento;
- implementa le varie funzioni di signal processing in C++;
- uso di librerie in assembly per operazioni low-level;
- uso di python per i grafici, per l'iterazione e per il signal routing tra i blocchi.

Gnuradio - demodulatore wideband FM



- un transceiver è rappresentato da un grafo dove i vertici sono i blocchi della funzione applicata e gli archi sono i flussi dei dati.

rtl-sdr e gr-osmosdr

- rtl-sdr: libreria e tool standalone che permettono l'uso delle chiavette DVB-T basate su RTL2832U in modalità raw; tra i tool troviamo:
  - rtl_test: tool di benchmark per RTL2832;
  - rtl_sdr: registra i sample in modalità raw (I/Q);
  - rtl_tcp: permette di inviare i sample via rete (per esempio usando la raspberry);
  - rtl_fm: permette di de-modulare il segnale FM;
- gr-osmosdr: source block per gnuradio e supporta diversi hardware SDR (OsmoSDR, rtlsdr, hackrf).

Software SDR

- rtl_*
- multimode
- gqrx
- dump1090
- linrad
- QtRadio
- SDR#
- gr-air-modes
- tetra_demod_fft (TETRA radio)
- airprobe (GSM receiver)
- ...

Esempi

Esempi d'uso

- ricezione APRS
- ricezione frequenze radioamatoriali (LSB/USB/AM/FM)
- ricezione frequenze radio commerciali
- ricezione NOAA
- trasmettitore DVB-T
- infrastruttura GSM (OpenBTS)
- intercettazione GSM (OsmocomBB)
- analisi delle frequenze provenienti dallo spazio
- ...
- **immaginazione**

IMPORTANTE: kalibrate-rtl

Kalibrate è un software per GNU/Linux che permette, sfruttando le celle GSM, di determinare l'offset del tuner.
Ogni chiavetta RTL-SDR ha un piccolo errore nel posizionamento della frequenza centrale dovuto alla produzione a basso costo dei componenti e alla mancata taratura iniziale. Questo errore, definito in parti per milione (PPM), si presenta linearmente al crescere della frequenza e quindi può essere facilmente definito in ogni programma SDR.

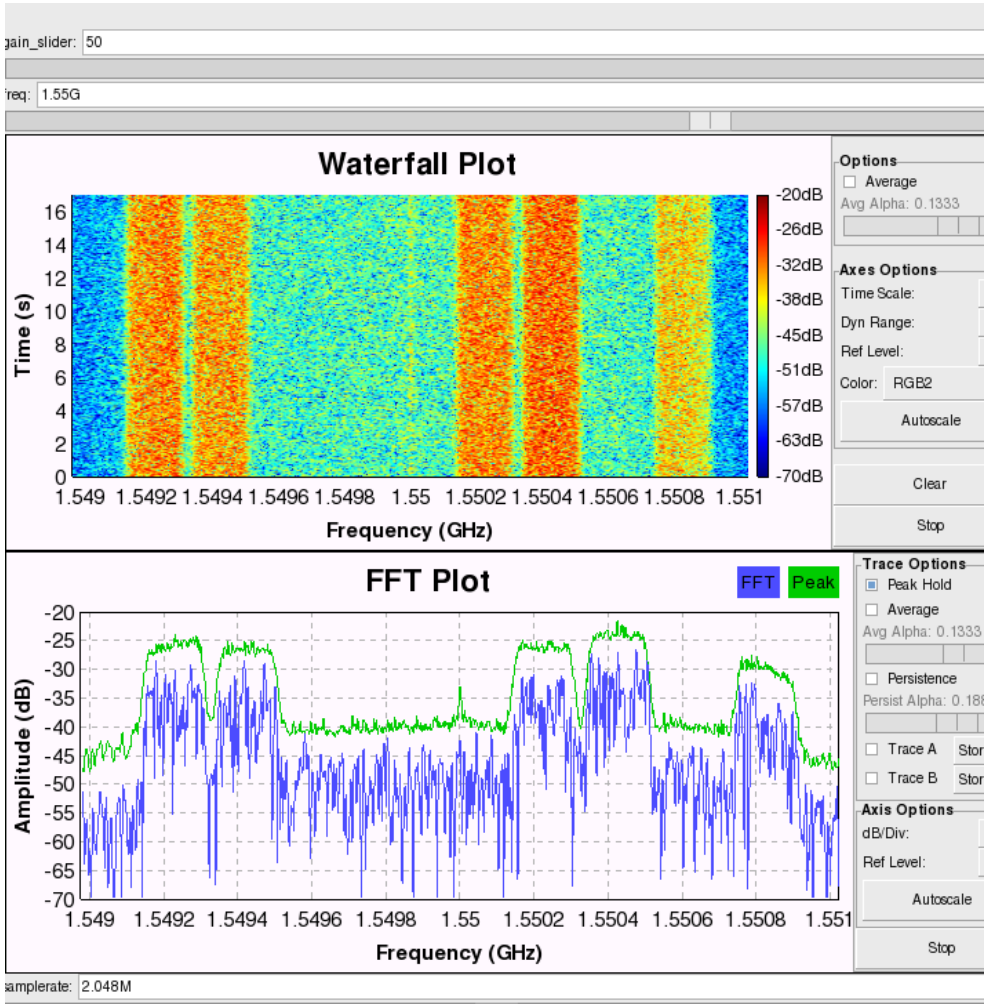
`https://github.com/steve-m/kalibrate-rtl`

Demo time

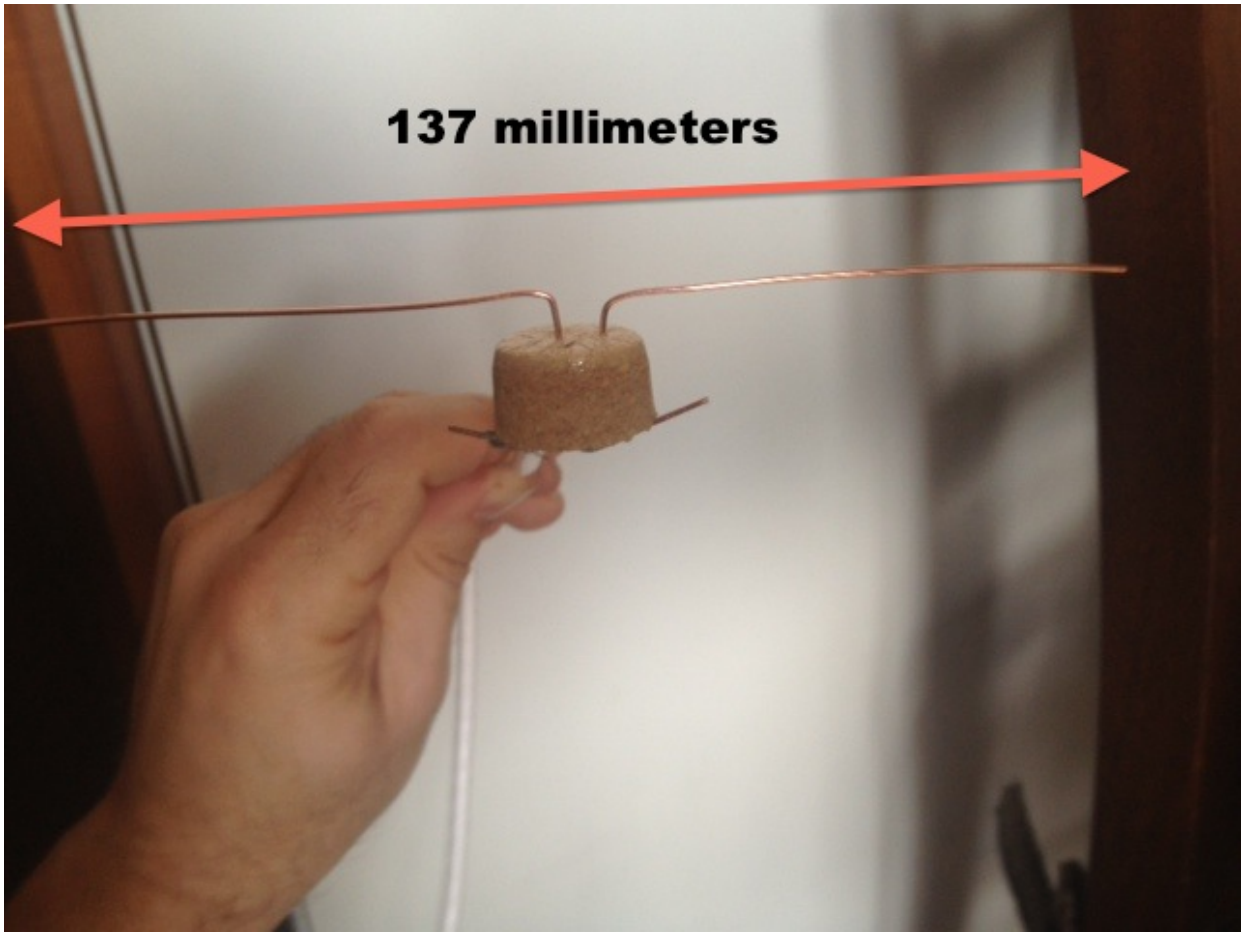
Ricezione Radio Commerciali

con gqrx

inmarsat (con LNA)



Antenna 1090 MHz (dipolo)



Demo time

Ricezione Automatic Dependent Surveillance - Broadcast (ADS-B)

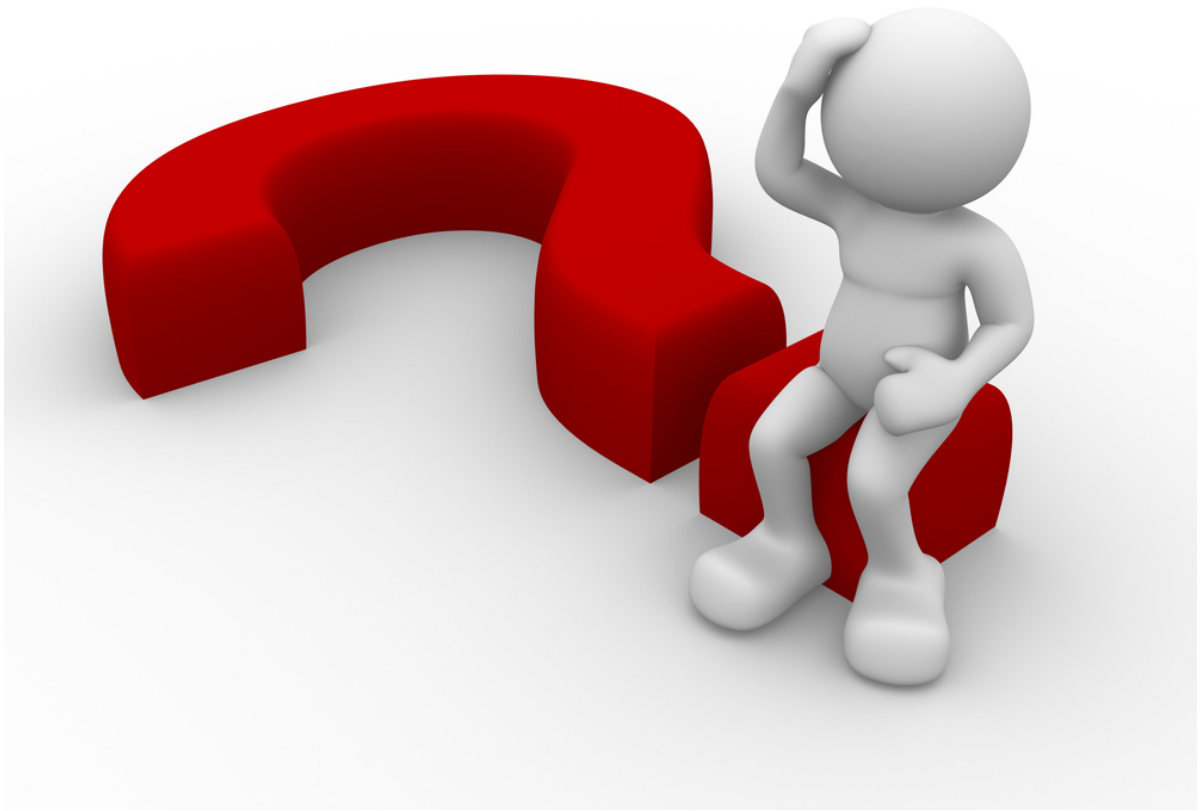
con dump1090 by antirez

Ricapitolando

- una bella opportunità per avvicinarsi al mondo radioamatoriale;
- una bella opportunità per investigare l'etere, le mille modulazioni e codifiche presenti;
- una bella opportunità per sviluppare e testare nuovi sistemi radio;
- ed una bella opportunità per dare sfogo alla propria immaginazione . . .

per gli interessati esiste anche un'architettura analoga nel mondo delle reti: Software Defined Networking

?? Domande ??



Bibliografia

- J. Proakis, Digital Signal Processing (4th Edition)
- E. Grayver, Implementing Software Defined Radio
- P. Kenington, Rf And Baseband Techniques for Software Defined Radio
- R. Lyons, Quadrature Signals: Complex, but not complicated
- G. Youngblood, A Software-Defined Radio for the Masses
- H. Welte, rtl-sdr: Turning 20$ Realtek DVB-T receiver into a SDR
- D. Valerio, Open Source Software-Defined Radio: A survey on GNUradio and its applications

Grazie per la cortese attenzione

le slide le potete trovare su
`http://rainbow.irh.it`

Licenza