Free and Open Source Software Defined Radio

Where Free and Open Source Software Meets Open Hardware

Alick Zhao

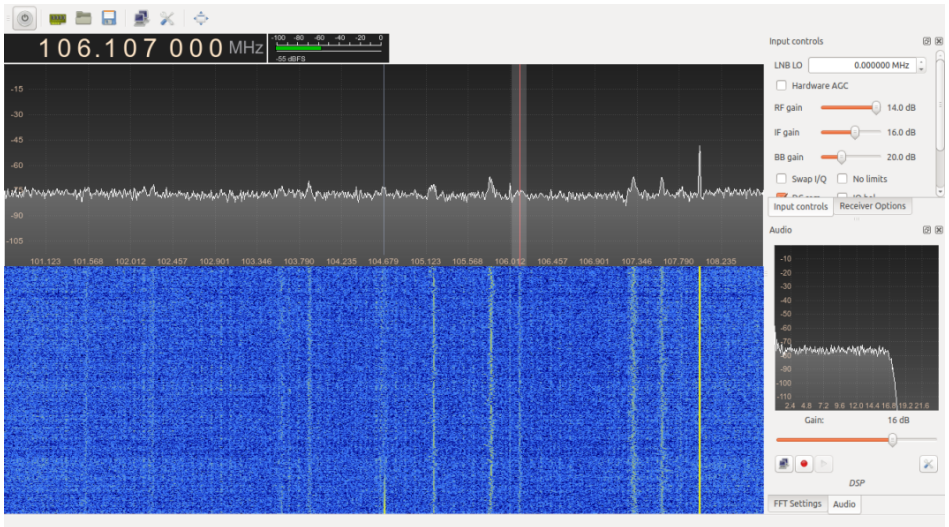
alick@fedoraproject.org

Fedora Project

Sep 20, 2014

FM Radio

- FM receiver
  - gqrx: `http://gqrx.dk/`
- FM transmitter



Record and Play

- GPS
- Remote control:
  - toy car
  - electric gate

OpenBTS

- GSM/GPRS base station (BS)
  - Phone calls
  - Short messages
  - Internet data service
- Run on laptop PCs
- UMTS: coming soon

Let's Define Software Defined Radio!

- Traditional (Hardware defined) radio:
  - Functions: embedded (coupled) in hardware
  - Inflexible, hard to update, long development cycle
- Software defined radio (SDR)
  - Hardware: universal, general purpose
  - Functions: programmable by software (on PC/DSP/FPGA)
  - Flexible, rapid development

Free and Open Source SDR

- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

Free and Open Source SDR

- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

Free and Open Source SDR

- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

Free and Open Source SDR

- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

Free and Open Source SDR

- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

Free and Open Source SDR

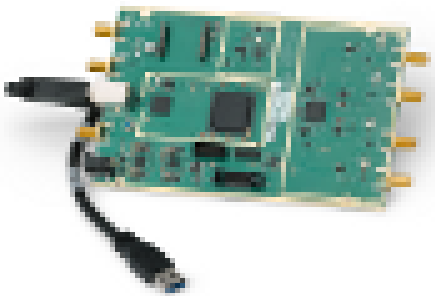
- Why?
  - Free: as in freedom, and free beer
  - Linus Law: give enough eyeballs, all bugs are shallow.
  - Community: friendship, knowledge sharing, collaboration
- Are there?
  - Yes!

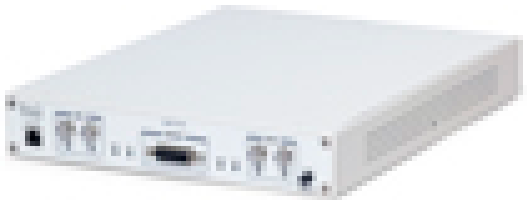
GNU Radio

- SDR software development platform
  - Many signal processing blocks
  - FOSS: GPL, © FSF
  - GUI development support: GRC
  - C++, Python

USRP

- Universl Software Radio Peripheral
  - Ettus Research, NI
  - High performance
  - Not that cheap

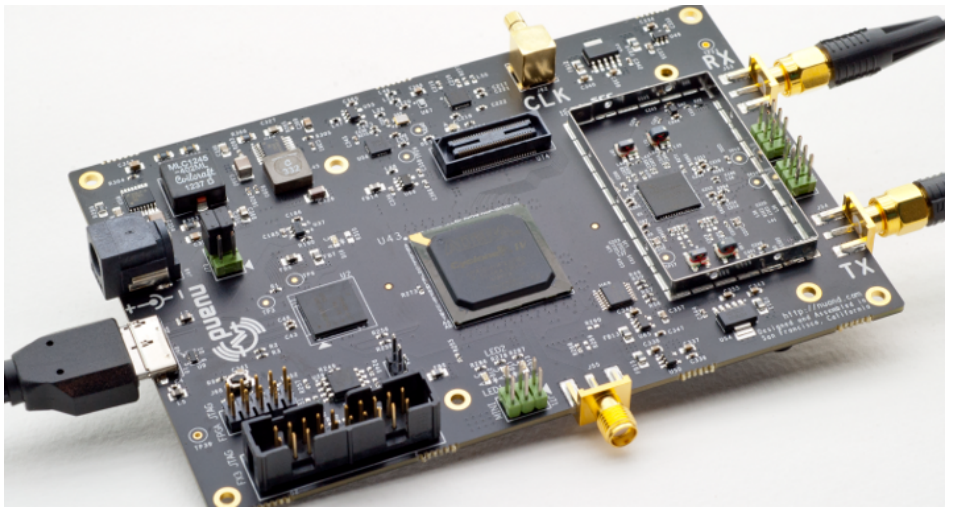




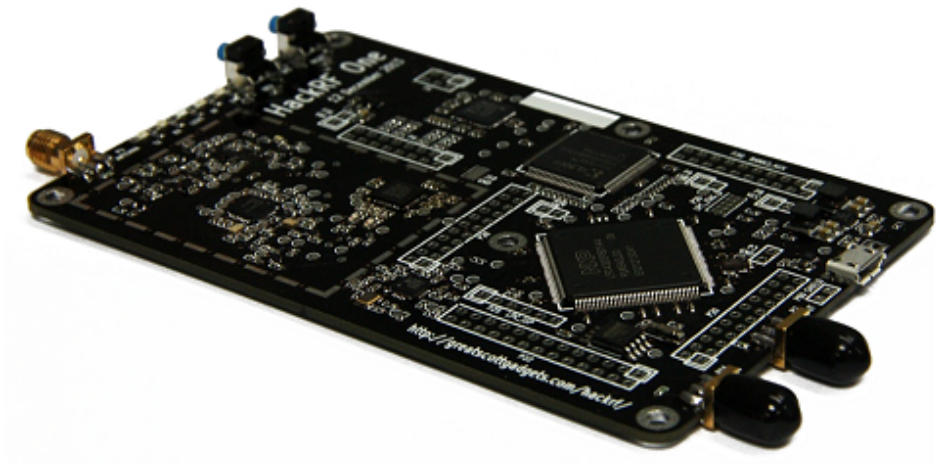
*RF

- bladeRF
  - Nuand:

    `http://www.nuand.com/`
  - USB 3.0
  - 300 MHz - 3.8 GHz
  - Headless mode



- HackRF
  - Michael Ossmann
  - Funded on Kickstarter
  - Cheap
  - Fully open source: layout



More Use Cases

- Test equipment
  - Spectrum analyzer
  - Signal generator
- Airplane
  - ADS-B
  - ACARS
- Ship
  - AIS
- Amateur Radio

LTE

- Cell scanner
- LTE receiver: gr-lte
- LTE eNodeB (BS)
  - openLTE
  - libLTE
  - OpenAirInterface

Detected Cells information list

	Duplex mode	Cell ID	Antenna ports	Frequency offset	Received power	CP type	Num. RB	PHICH duration	PHICH resource
1860MHz	FDD	142	2	-41.8006kHz	-0.90925	Normal	100	Normal	1
1860MHz	FDD	86	2	-41.7744kHz	-1.1267	Normal	100	Normal	1
1890MHz	TDD	253	2	-41.116kHz	11.1699	Normal	100	Normal	1 / 2
2565MHz	TDD	29	2	-36.1428kHz	34.8551	Normal	100	Normal	1
2565MHz	TDD	28	2	-86.9578kHz	33.9531	Normal	100	Normal	1
2565MHz	TDD	27	2	-86.9563kHz	31.5544	Normal	100	Normal	1
2585MHz	TDD	68	2	-87.975kHz	35.9489	Normal	100	Normal	1 / 6
2585MHz	TDD	66	2	-88.2294kHz	28.9758	Normal	100	Normal	1 / 6
2585MHz	TDD	67	2	-94.2675kHz	31.1485	Normal	100	Normal	1 / 6
2604.9MHz	TDD	355	2	4.905kHz	34.416	Normal	100	Normal	1
2645MHz	TDD	22	2	-89.3233kHz	29.8605	Normal	100	Normal	1
2645MHz	TDD	21	2	-89.3376kHz	27.2821	Normal	100	Normal	1

Note: Frequency offset is dongle specific.
Note: Received Power only has relative meaning.

WiFi

- gr-ieee802-11
  - An IEEE 802.11 a/g/p transceiver for GNU Radio
  - `https://github.com/bastibl/gr-ieee802-11`

Summary

- Radio frequency: a new dimension for hacking
- SDR: flexibility, progammability
- FOSS SDR: hacking in free and open source way

Happy hacking!