Exploring 4G/5G Networks Using SDRs

Andre Puschmann

SRS
SOFTWARE RADIO SYSTEMS

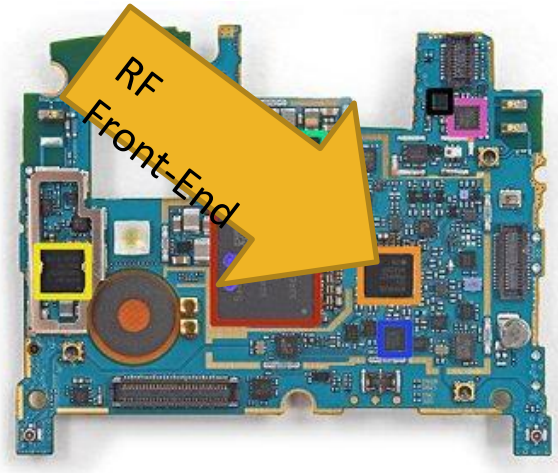
Bytespeicher Erfurt
Erfurt, August 6th 2019

Agenda

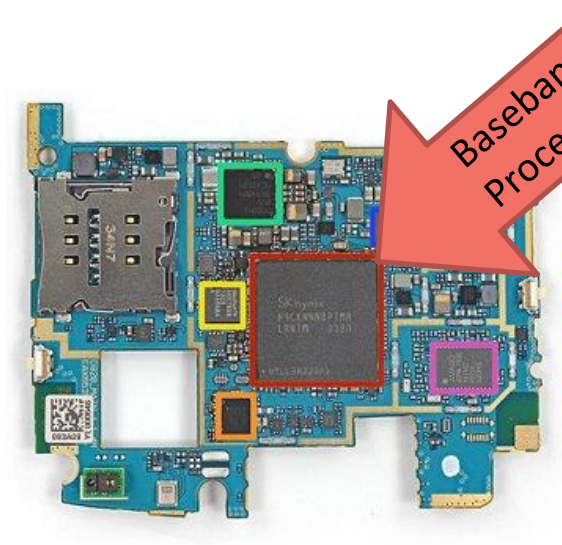
- What is a SDR?
- The Wireless Spectrum
- 4G/5G In a Nutshell
- srsLTE Introduction
- srsLTE Hands-on

What is a SDR?

A off-the-shelf Handset



- Sandisk SDIN8DE4 16 GB NAND flash
- Qualcomm WTR1605L LTE/HSPA+/CDMA2K/TDSCDMA/EDGE/GPS transceiver
- Qualcomm PM8841 power management IC
- Broadcom BCM4339 5G Wi-Fi combo chip with integrated power and low-noise amplifiers (the updated version of the BCM4335).
- Avago RFI335
- InvenSense MPU-6515 six-axis (gyro + accelerometer) MEMS MotionTracking device
- Asahi Kasei AK8963 3-axis electronic compass

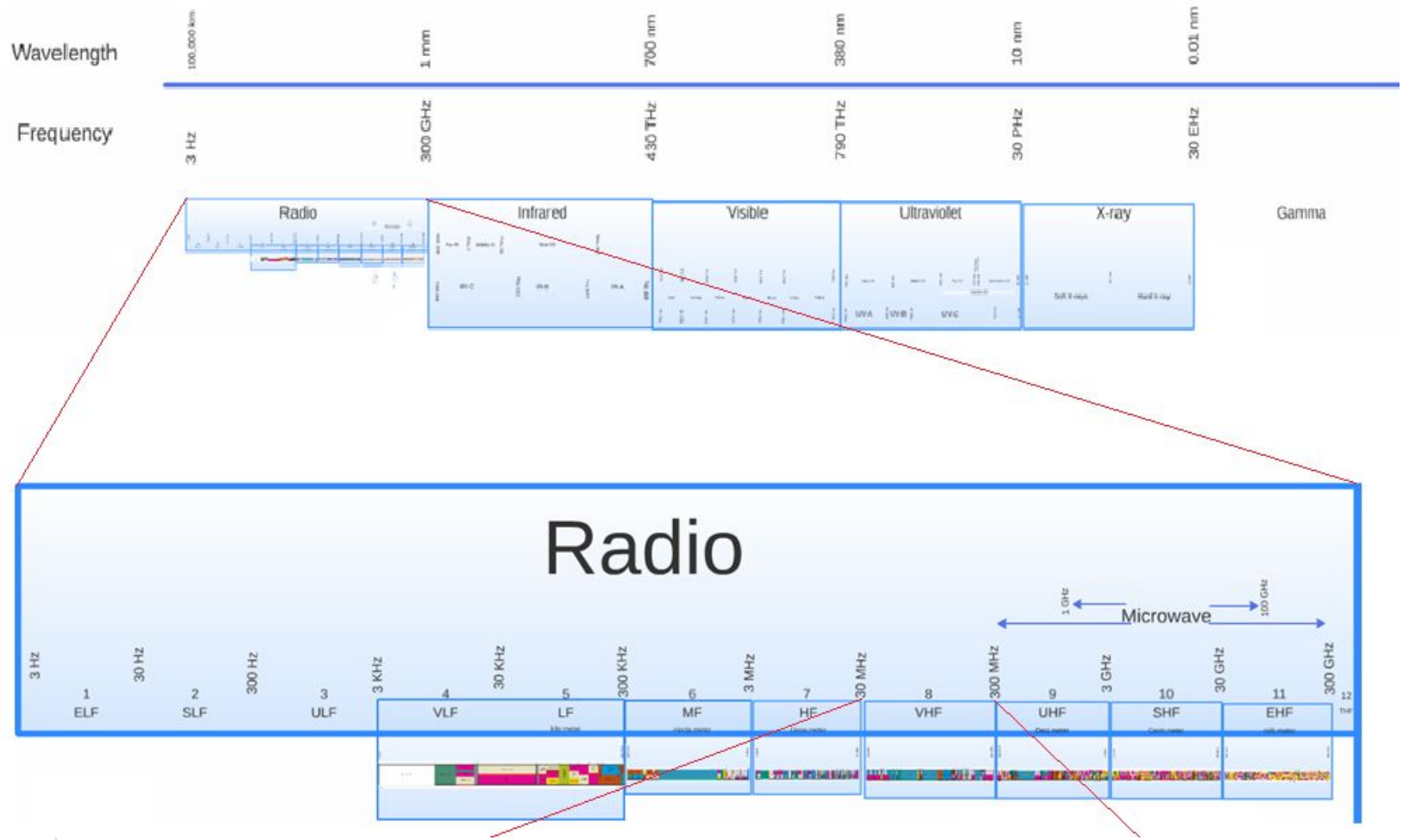


- SK Hynix H9CKNNN8PTMRLR-NTM 2 GB LPDDR3-1600 RAM
  - The Quad-core, 2.26 GHz Snapdragon 800 SoC is layered beneath the RAM
- Qualcomm WCD9320 audio codec
- Analogix ANX7808 SlimPort transmitter
- Qualcomm PM8941 power management IC
- Texas Instruments BQ24192 I2C controlled 4.5 A USB/adapter charger
- Avago ACPM-7600

SRS
SOFTWARE RADIO SYSTEMS

A Software-Defined-Radio (SDR)

The Wireless Spectrum

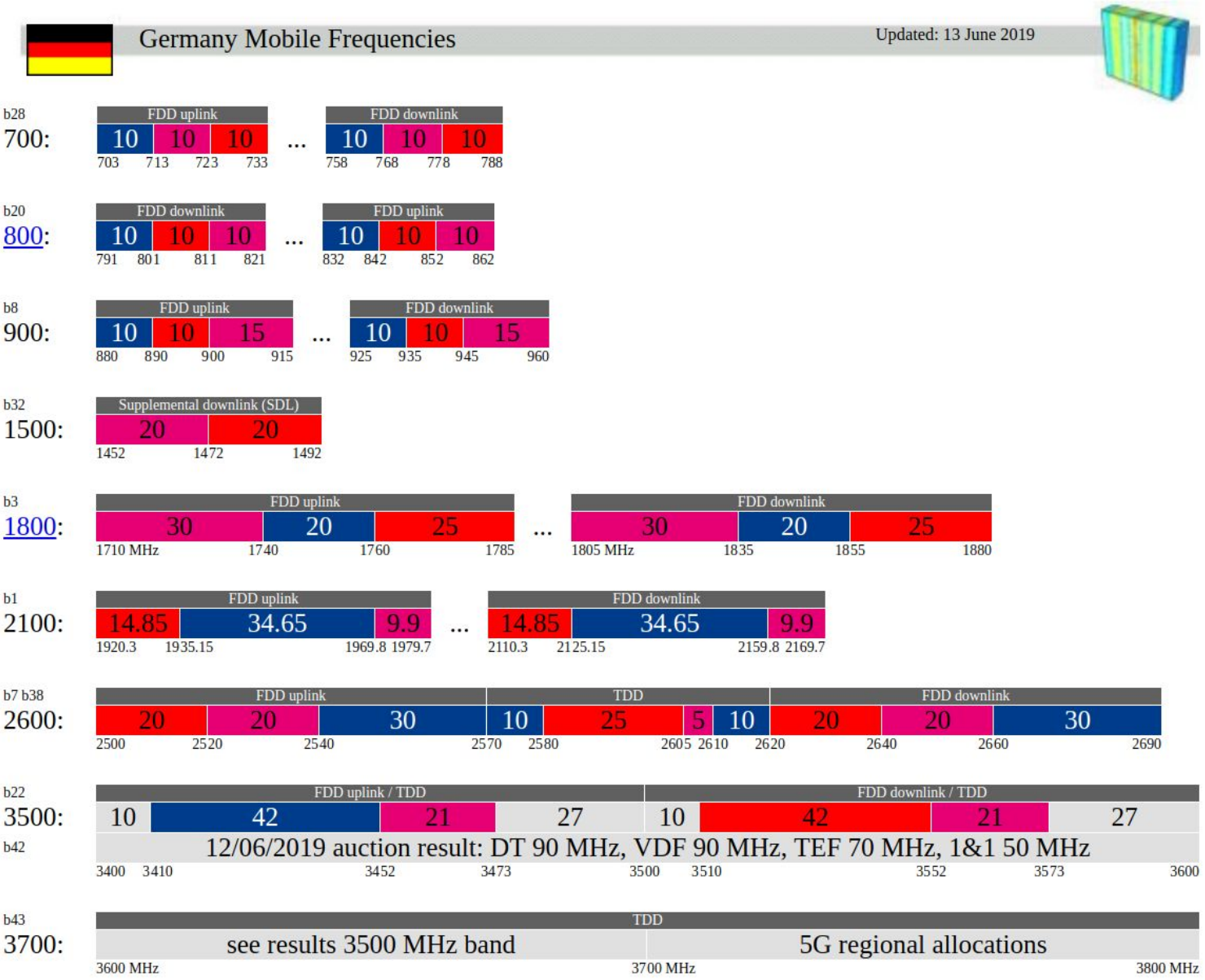


SRS
SOFTWARE RADIO SYSTEMS

Commercial Wireless Bands

- 88-108 MHz UKW FM
- 380-410 MHz TETRA (Europe)
- 500-650 MHz DVB-T2
- Cellular (up to 4G) 700 MHz - 2.6 GHz (countless bands and configuration depending on country)
- 5G at 3.7 GHz only in Germany
- …

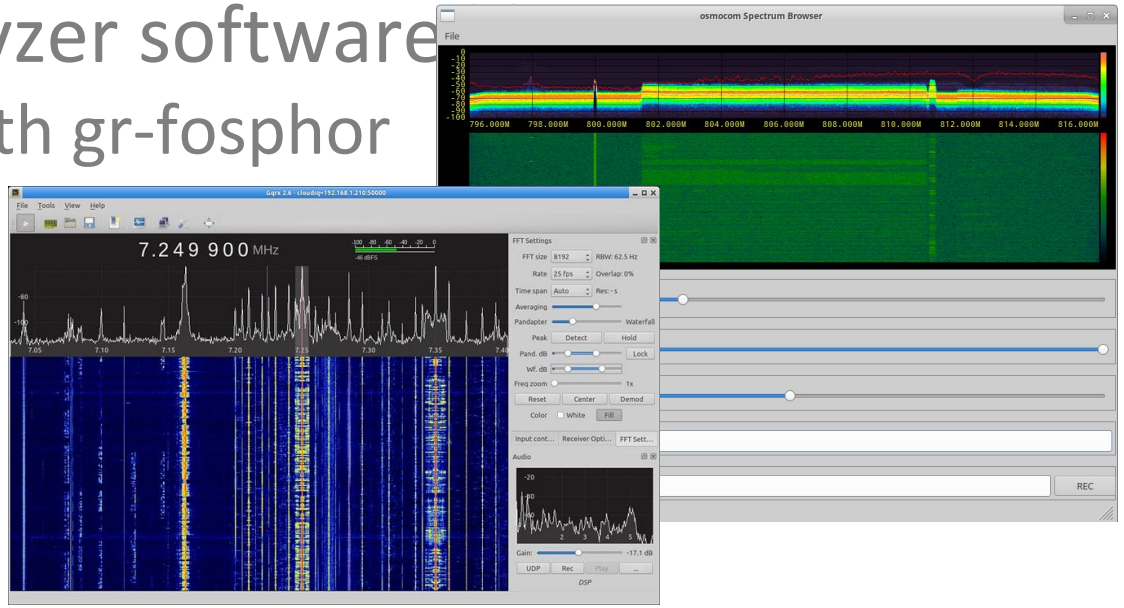
Cellular Bands in Germany



Source: https://www.spectrummonitoring.com

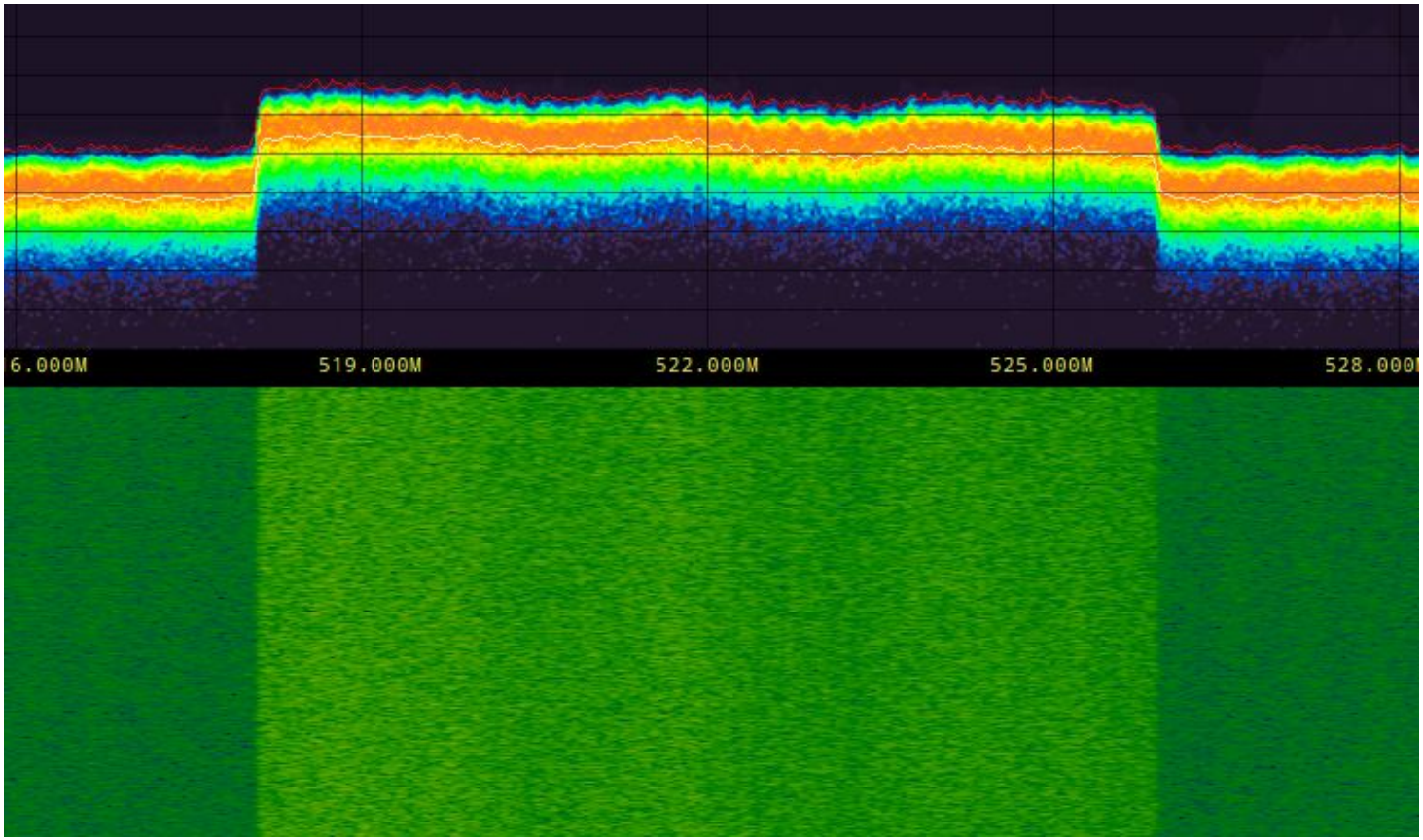
Exploring the Wireless Spectrum

- Conventional PC or Laptop
- RF front-end (RTL-SDR, USRP, LimeSDR, bladeRF)
- Linux OS, e.g. Ubuntu
- Spectrum analyzer software
  - GNU Radio with gr-fosphor
  - gqrx
  - sdrangel
  - etc.



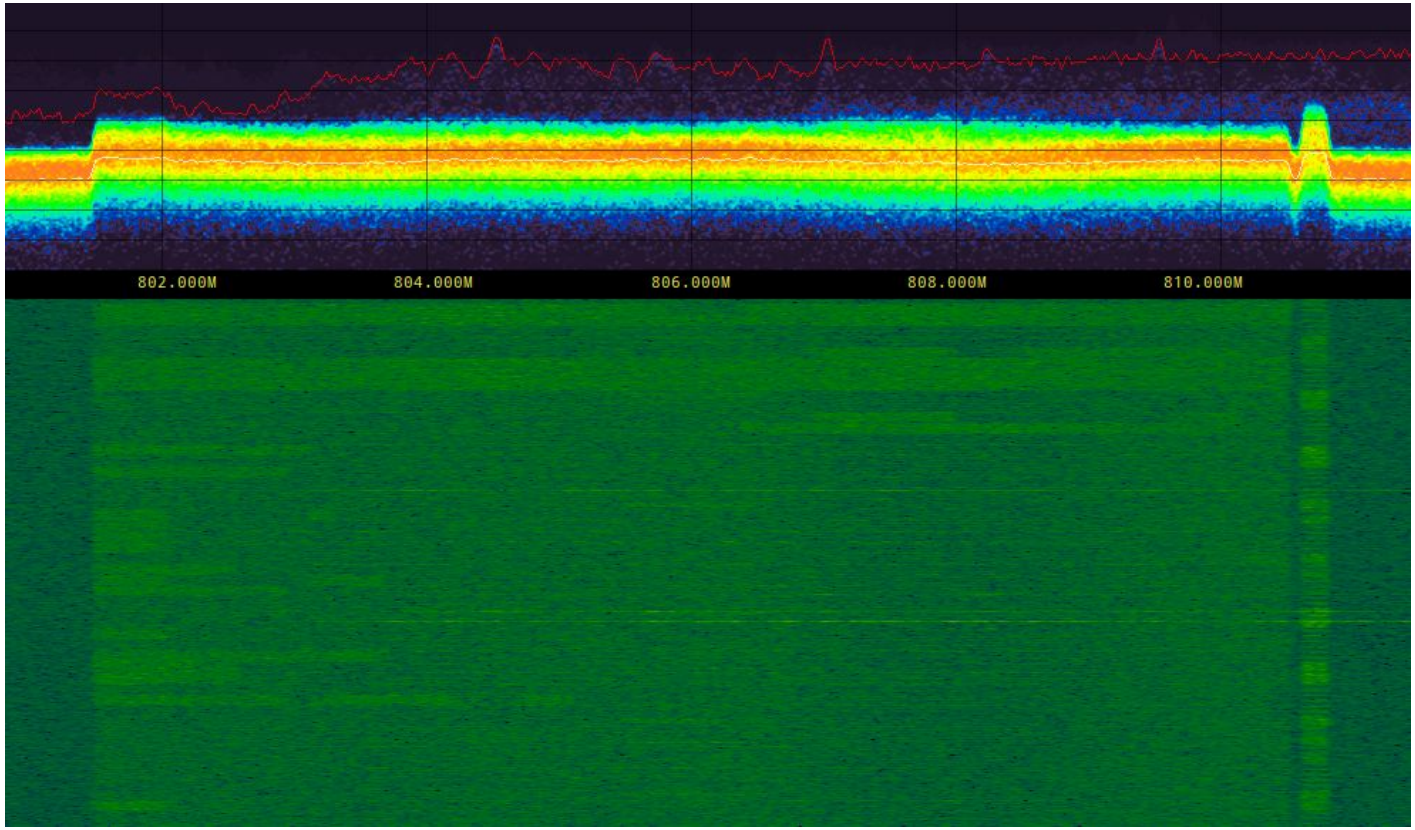
Local Examples (1)

- DVB-T2 from Inselsberg at 522 MHz



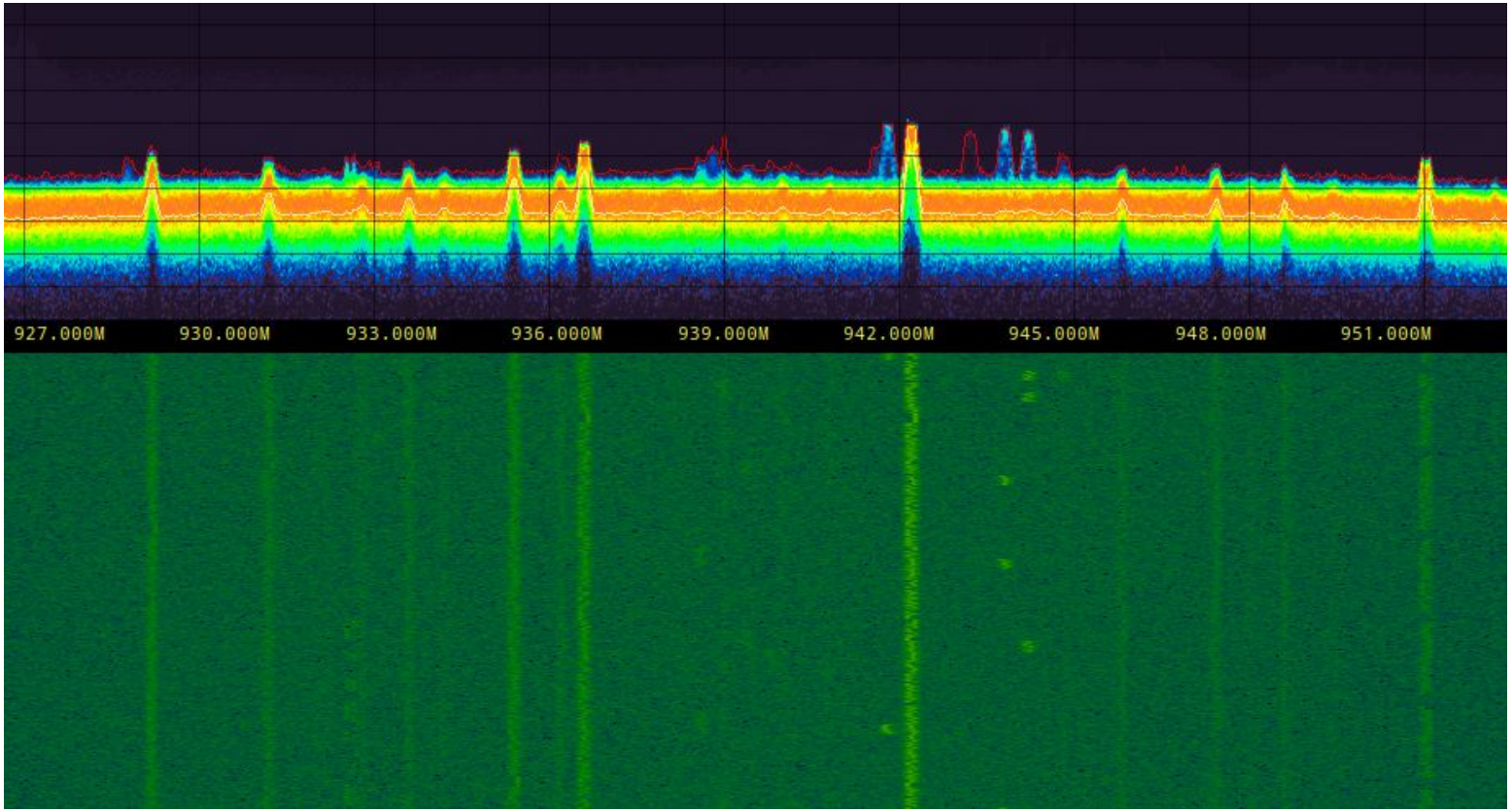
Local Examples (2)

- Vodafone LTE 10 MHz at 806 MHz with NB-IoT



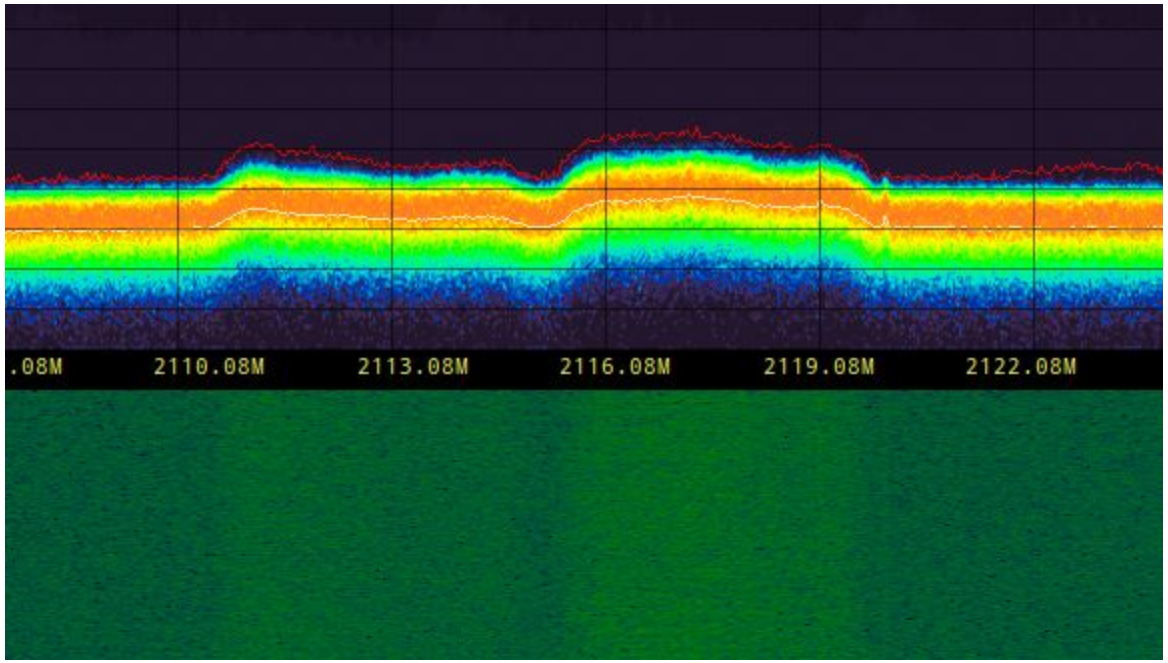
Local Examples (3)

- GSM at ~900 MHz



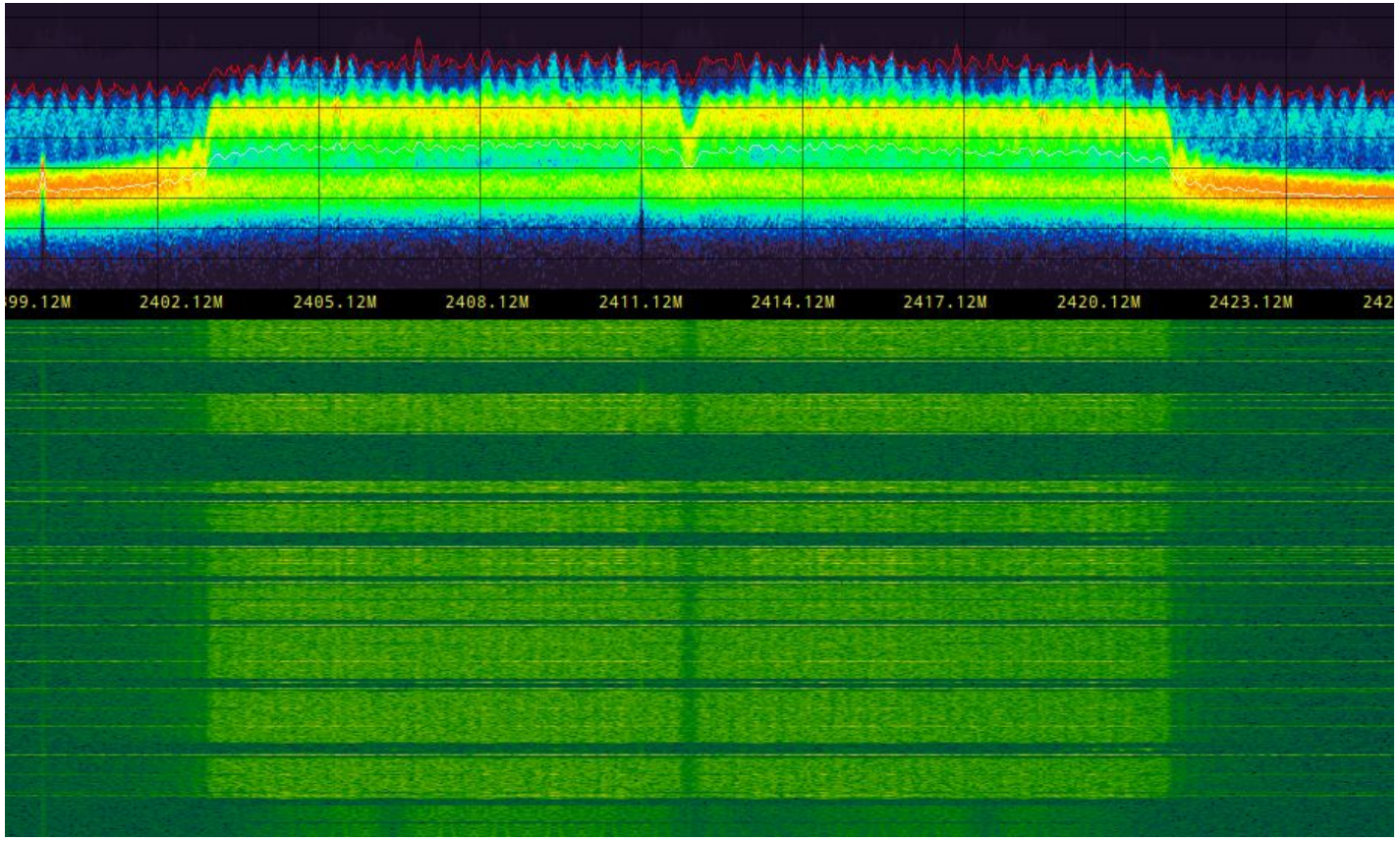
Local Examples (4)

- UMTS (3G) at 2100 MHz

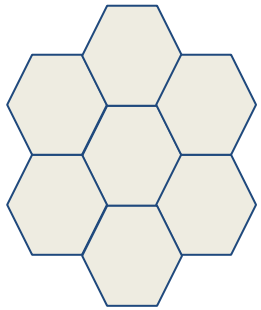


Local Examples (5)

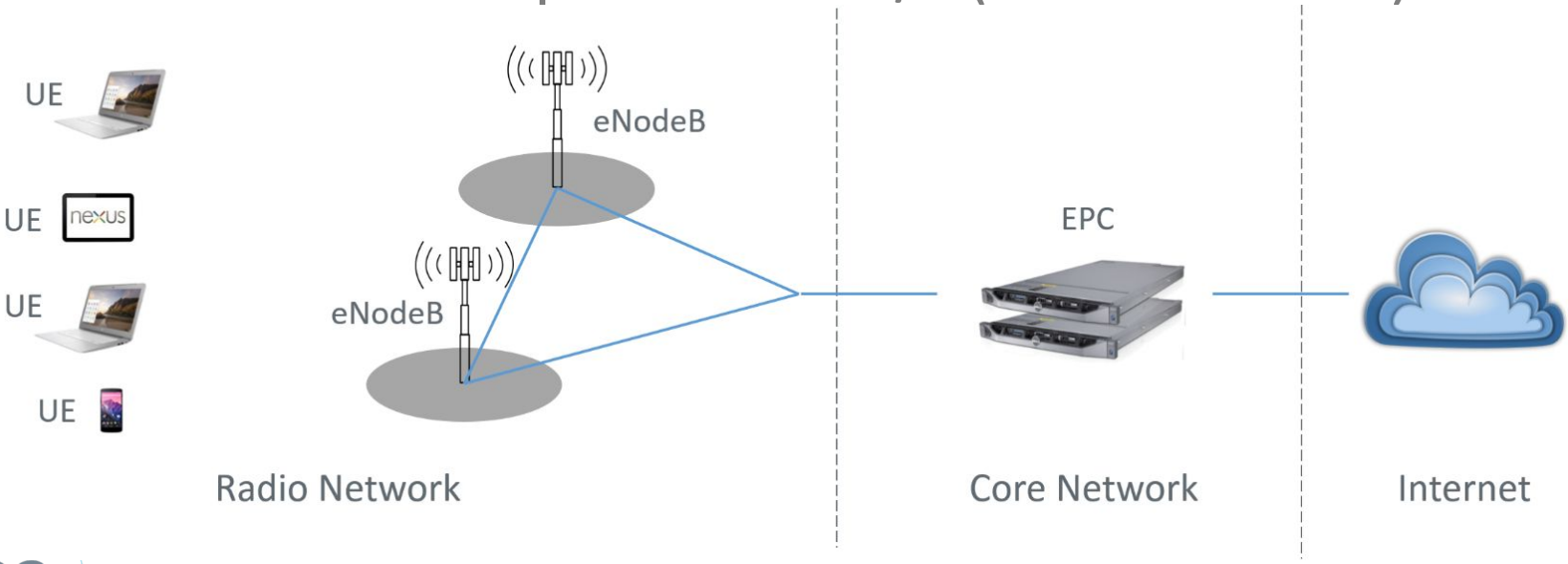
- Wifi at 2.4 GHz



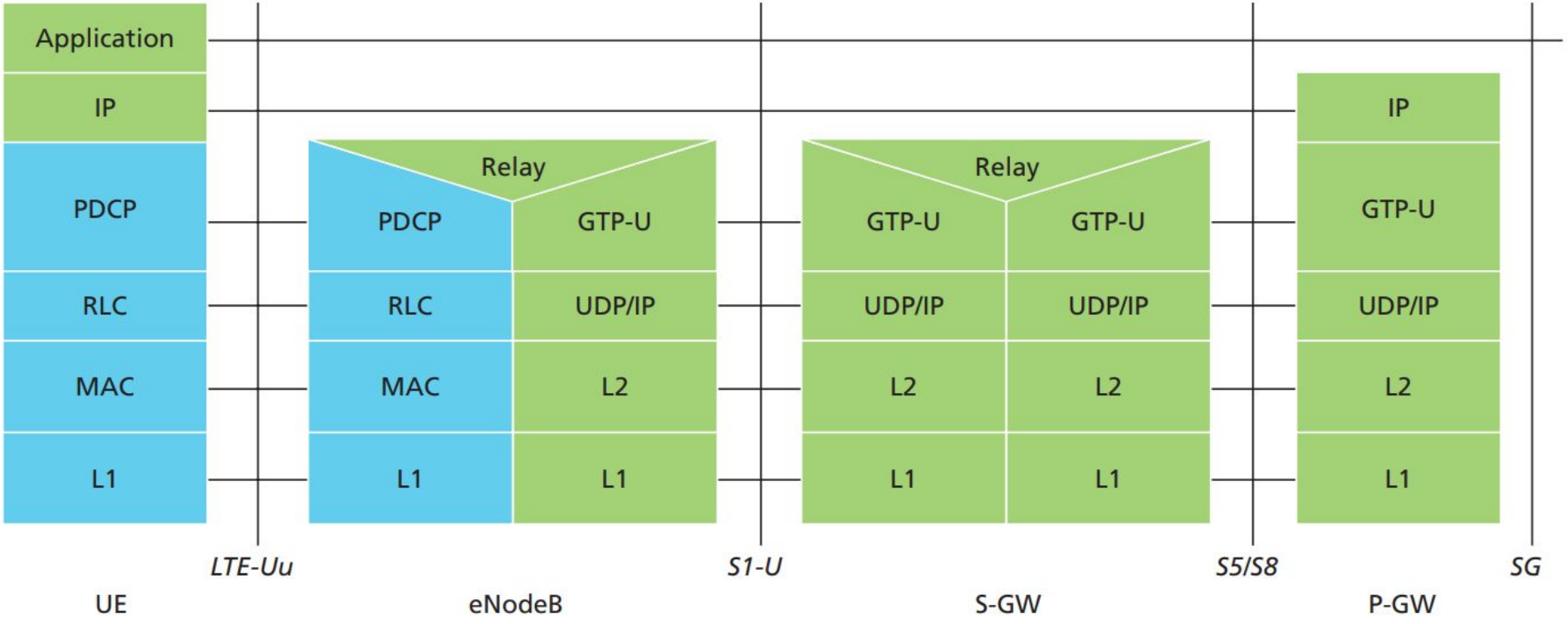
LTE (4G) In a Nutshell



- Cellular network architecture (like 2G/3G)
- Development in 3GPP in Releases (8-15)
- First tests in 2008, deployment 2010 (in D)
- Downlink rates up to 1.2 Gbit/s (5x 20 MHz CA)



User-plane Protocol Stack



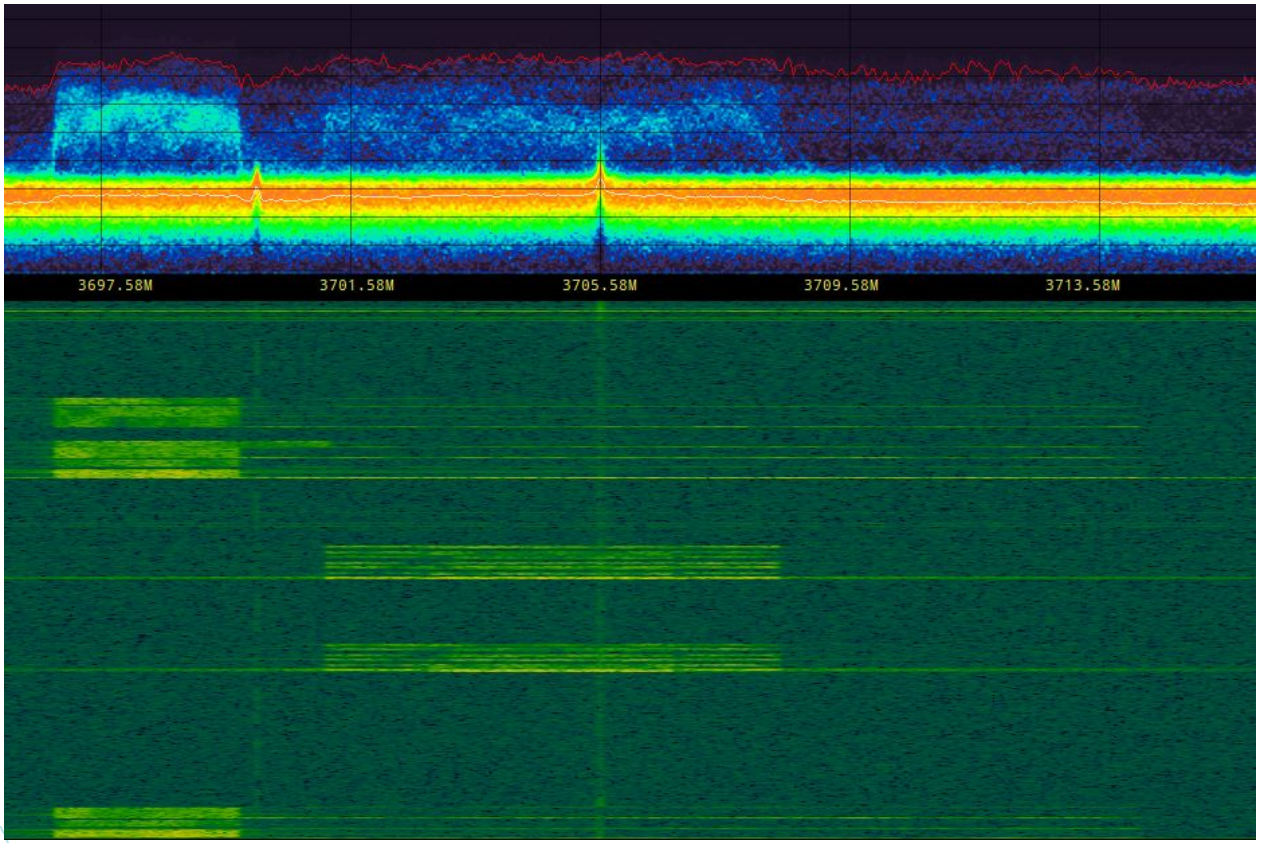
Source: http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf

5G New Radio (NR) In a Nutshell

- Mobile Broadband (eMBB), Machine-type (mMTC), Ultra-Reliable Low-Latency Comm (URLLC)
- Speed below 6 GHz (FR1) comparable to 4G, potentially much faster above 6 GHz (FR2)
- Latency target 1-4ms
- Non-standalone (NSA) and standalone (SA) deployment
- First (substantial) deployments in South Korea (SK Telecom)

First Commercial Deployments

Vodafone Spain, Placa Catalunya, BCN @ 3.7 GHz

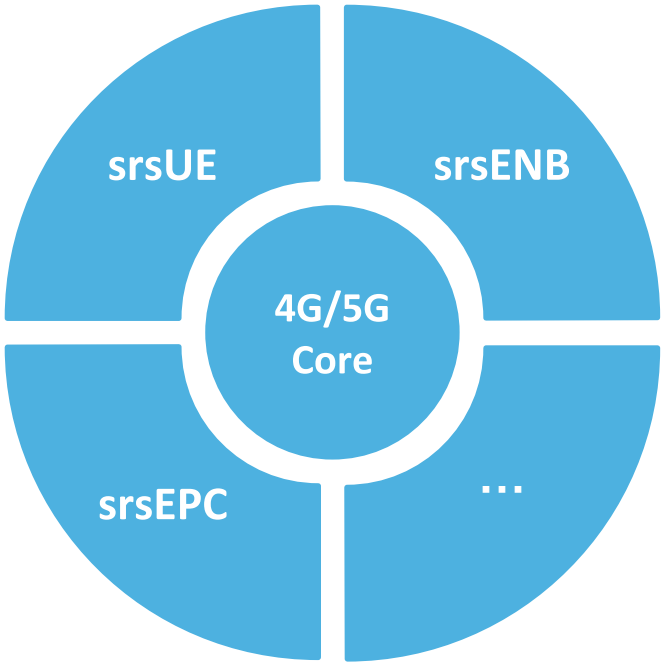


What is srsLTE?

The srsLTE Ecosystem

“Open-source 4G/5G software radio suite”

- Core 4G/5G library
  - Modular and portable, high-performance library for PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, NGAP, SDAP and GW
  - All bandwidths up to 20 MHz, TM1-4
  - Highly optimized Turbo decoder for Intel SSE4.1/AVX (+150Mbps in TM3/4)
- Applications
  - srsUE: First open-source SDR LTE UE
  - srsENB: A complete SDR LTE eNodeB application
  - srsEPC: A light-weight LTE core network
  - airScope: passive air-interface analyzer (commercial only)



New project webpage: www.srslte.com

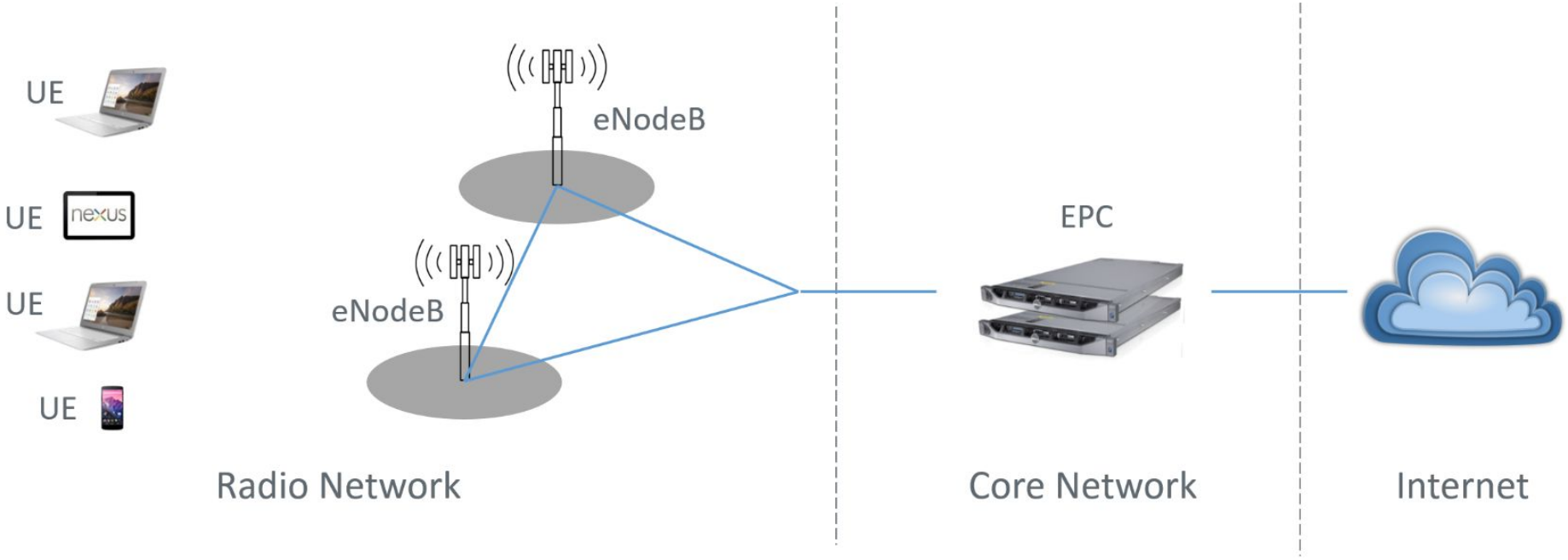
SRS
SOFTWARE RADIO SYSTEMS

A Full End-2-End Open LTE Solution

SRS UE

SRS ENB

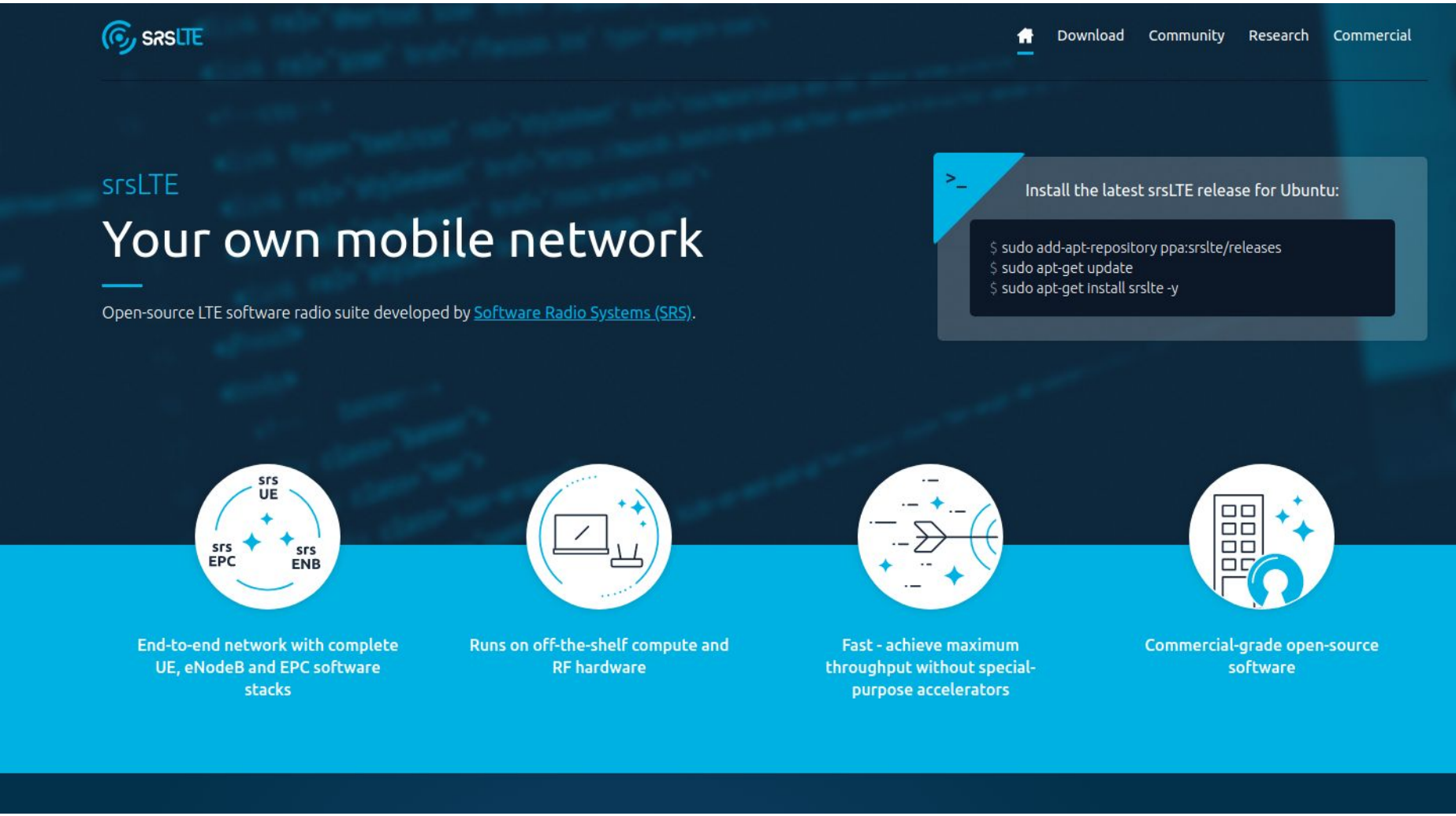
SRS EPC



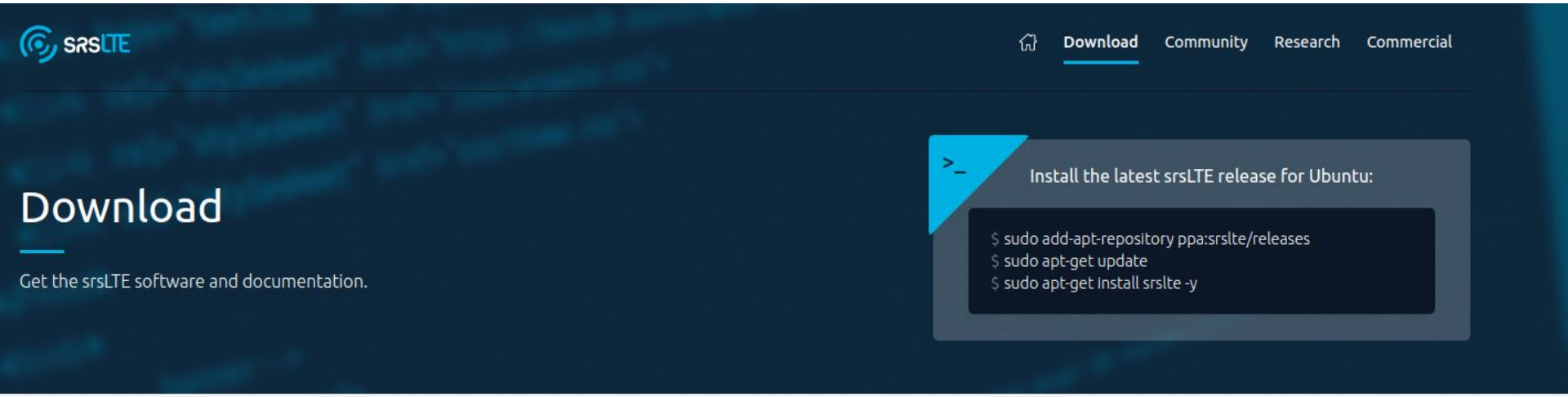
SRSLTE

SRS SOFTWARE RADIO SYSTEMS

www.srslte.com



www.srslte.com



Get Up and Running

Looking for the srsLTE docs?
See the user manuals

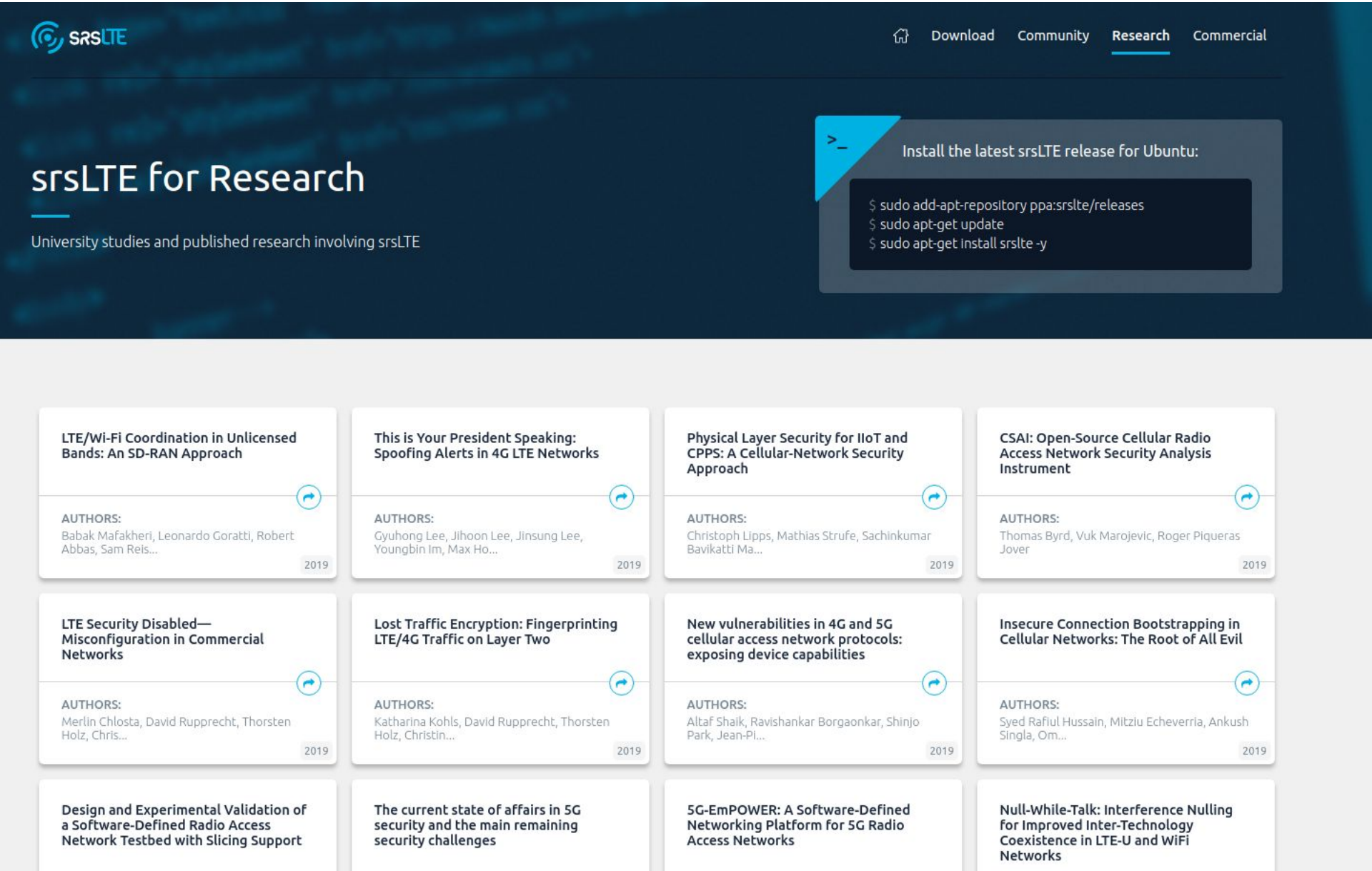
Get the Code

srsLTE on GitHub
Get the source code

What's New?
Read the release notes

Getting Started
Read the installation guide

www.srslte.com



Impact

Security

GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2018	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2018	0007	Ravishankar Borgaonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	0012	David Basin Jannik Dreier Lucca Hirschi Saša Radomirović Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omar Chowdhury	University of Iowa http://homepage.divms.uiowa.edu/~comarhaider/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/

Impact

Security

› Home › GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2018	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2018	0007	Ravishankar Borgaonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	0012	David Basin Jannik Dreier Lucca Hirschi Saša Radomirović Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omar Chowdhury	University of Iowa http://homepage.divms.uiowa.edu/~comarhaider/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/

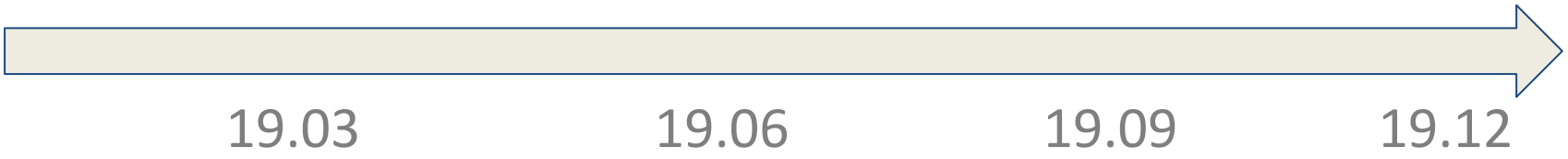
Binary Packaging

- Ubuntu packages
  - PPA: https://launchpad.net/~srslte
  - Maintained by SRS (added in 18.06)
- (Open-)SUSE packages
  - https://build.opensuse.org/package/show/home:mnhauke:sdr-devel/srsLTE
  - Maintained by Martin Hauke
- Debian packages
  - https://packages.debian.org/sid/srslte
  - Maintained by Ruben Undheim
- ?

Latest srsLTE Features

- srsLTE 19.03
  - TDD and Carrier Aggregation (CA) in srsUE
  - Paging support for srsENB and srsEPC
  - User-plane encryption for srsENB
  - Channel simulator for EPA, EVA, and ETU 3GPP channels
- srsLTE 19.06
  - Add QAM256 support in srsUE
  - Add QoS support in srsUE
  - User documentation

srsLTE Roadmap 2019



- NB-IoT physical layer
- Sidelink (D2D/V2X) in srsUE
- Developer documentation

Supported RF Hardware

- Native support:
  - Ettus Research USRP B2xx, X3x0
  - Nuand bladeRF x40/x115, 2.0 micro
  - Epiq Solutions Sidekiq
- Through SoapySDR (tested):
  - RTL-SDR
  - LimeSDR
  - IIO
- Soon: ZMQ No-RF

srsLTE Hands-On

Thanks

- to Stephan Jauch for the amazing orga
- to Bytespeicher for hosting the event

Thanks!

SRS

SOFTWARE RADIO SYSTEMS