ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

Stupid Pluto Tricks with the ADALM-PLUTO

FOSDEM 2018

ROBIN GETZ

MICHAEL HENNERICH

02/04/2018

Agenda

- Analog Devices and Education
- Introduction to the ADALM-PLUTO
- Software support
  - Libiio
  - Supported applications
- Building custom images
- Watching airplanes (via dump1090)
- Detecting cell phone jammers

Analog Devices Educational offering

Secondary Schools | First Year University: General Technology | Second/Third Year University: Electrical Engineering | Fourth Year/MSc University: Electrical Engineering | PhD Students: Practicing Electrical Engineers

Static Voltage/Current | **Time varying signals** | **Impedance Measurements** | **Frequency Domain** | **Mechatronics / Controls** | **Network Analysis** | **High Frequency & Specialized**

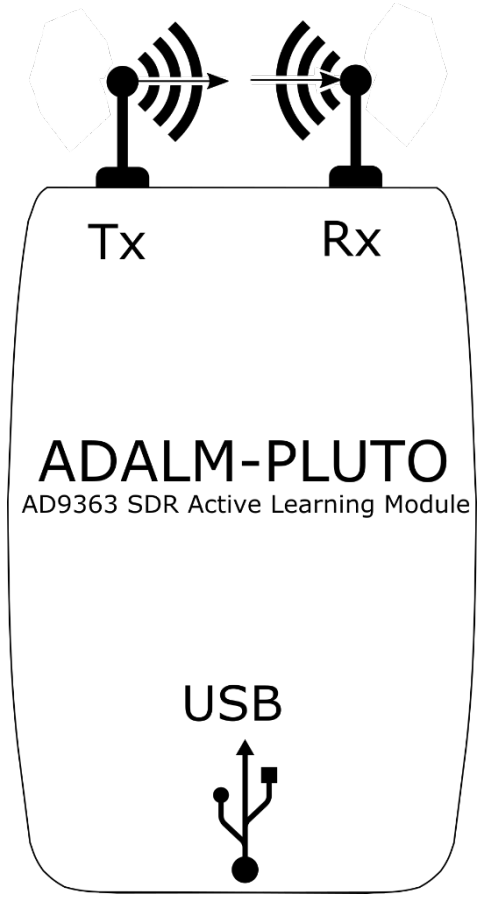
Tools for Explorations & Understanding

Introductory Instrumentation

Advanced PC Based Instrumentation

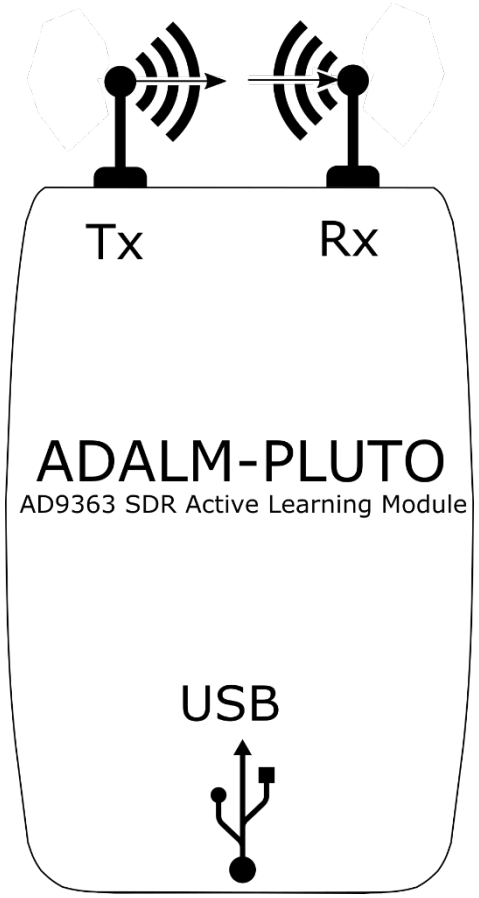
ADALM-PLUTO

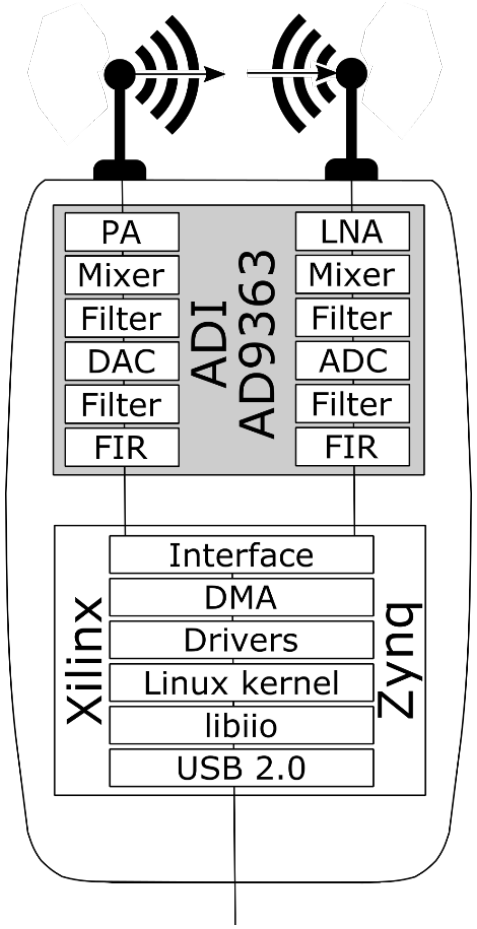
AD9363 Software Defined Radio Active Learning Module

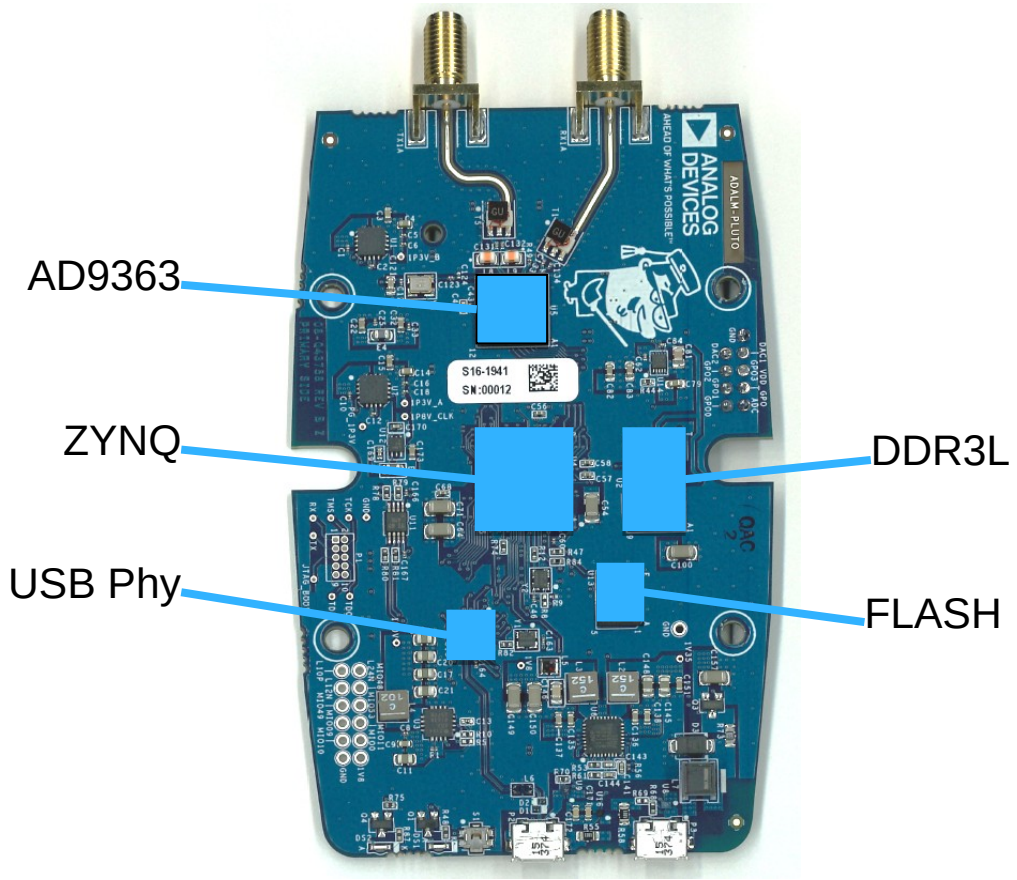


- Captures I/Q Samples
  - 12-bits
  - 65.1 kSPS to 61.44 MSPS
  - 200kHz to 20 MHz signal bandwidth
- Sends them to PC for processing over USB2
- $149
  - $99 introductory price
- Tuning range;
  - 325 MHz to 3.8 GHz

Inside the ADALM-PLUTO



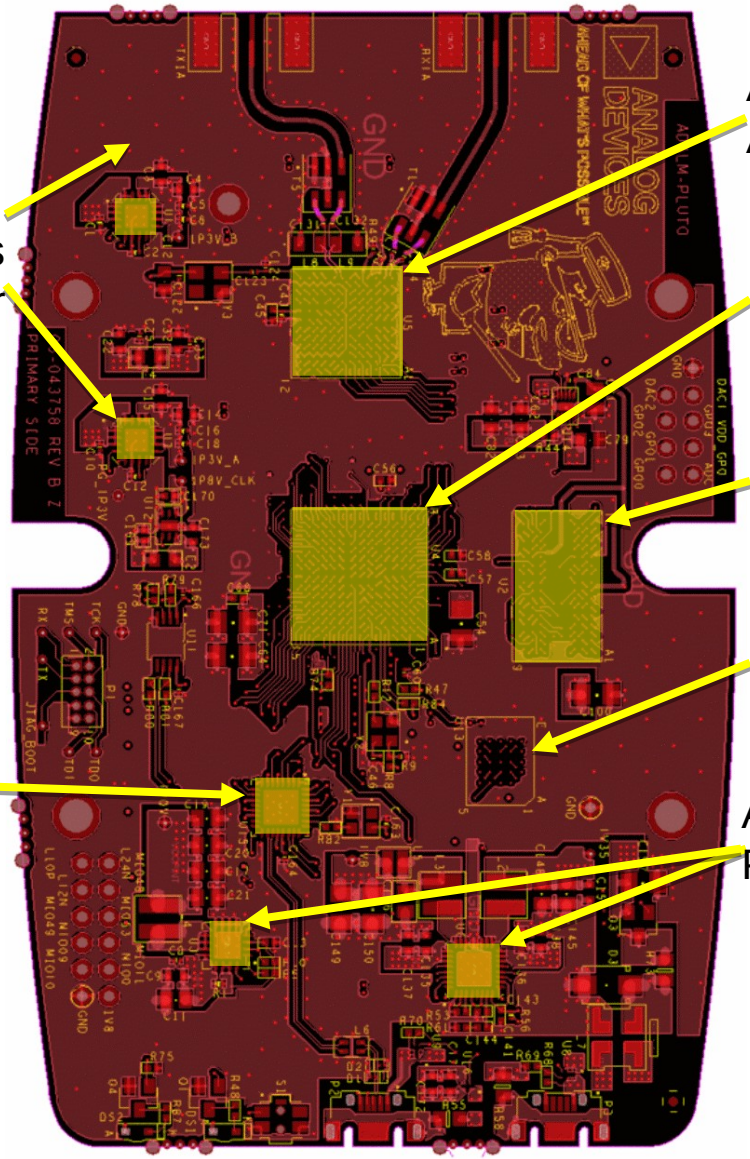




ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADALM-PLUTO Design

- Design is open, just like all other ADI designs
  - Shows a minimal full system design
    - From antenna to USB
    - RF to bits
  - Only 72 parts on the BOM
    - All IC, R, C, L, connectors, etc
  - Schematics, Gerbers, BOM, Allegro Files posted
    - https://wiki.analog.com/university/tools/pluto/hacking/hardware
  - Passes FCC and CE tests
  - Achieves better RF than AD9363 datasheet specs



Regulation? (FCC is local, but most countries have similar organizations)

- ADALM-PLUTO is not a “Radio”.
  - WiFi, BLE, transmitters
    - Waveform, dwell time, LO frequency, bandwidth, etc.
  - These require type ***certification***

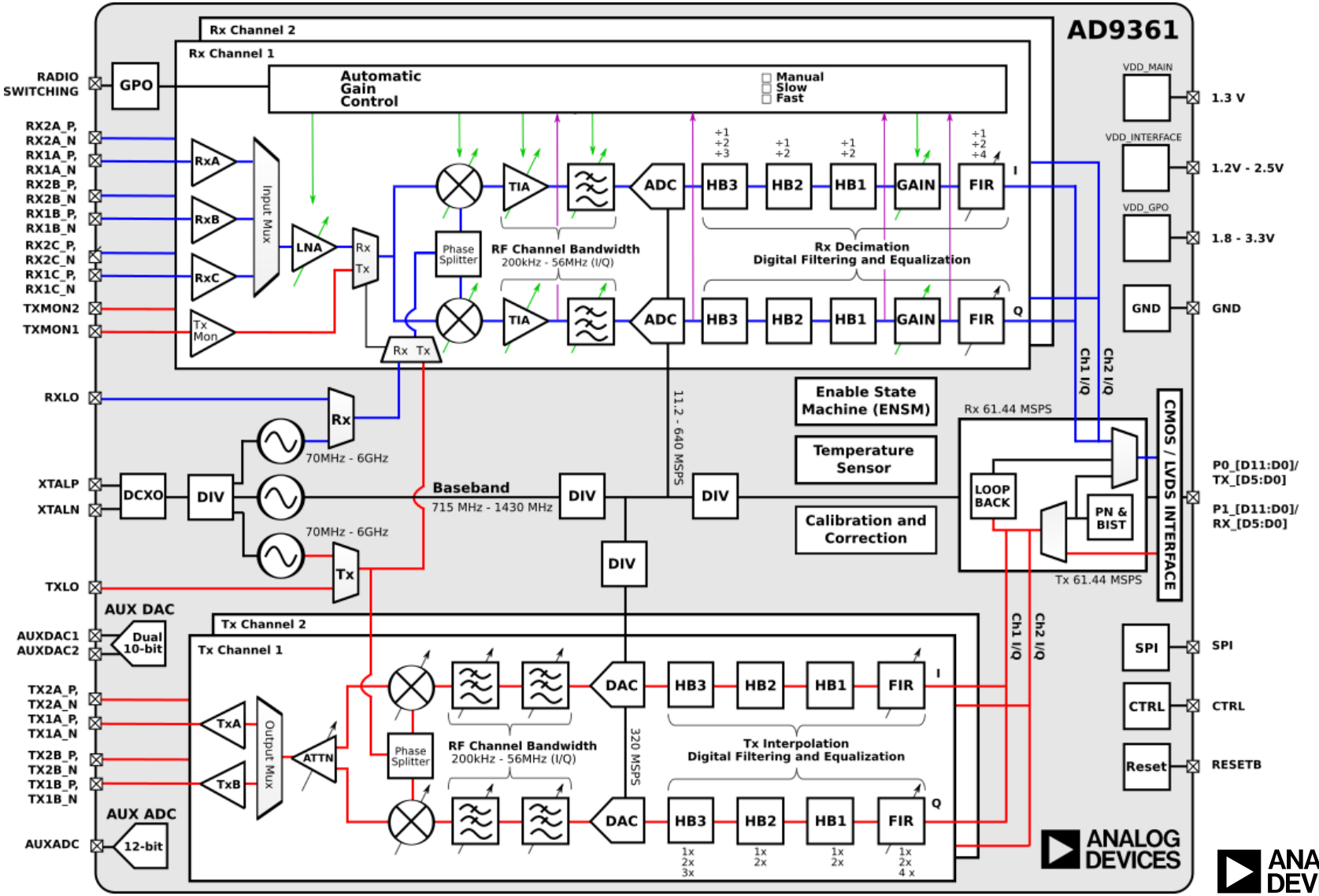
- ADALM-PLUTO is nothing more than:
  - RF arbitrary waveform generator
  - RF capture device
  - These sorts of devices are FCC ***verified***.
    - this device does not cause harmful interference.
    - this device must accept any interference received
  - We do this – we pass part 15 (Class A)
    - For use in business/industrial/commercial environments only.

- End users make it a radio.
  - End users may need certification
  - Highly encourage every user to get their HAM radio license
- The FCC allows a hobbyist to build up to five devices of a single design for personal use with no testing whatsoever.
- If you are contacted by the FCC (or anyone else) about a matter of spectrum interference, immediately stop using the device, don't use it again.
- Home-built transmitters, like all Part 15 transmitters, are not allowed to cause interference to licensed radio communications and must accept any interference that they receive.
- If the Commission determines that the operator of a transmitter has not attempted to ensure compliance by employing good engineering practices then that operator may be fined up to $10,000 for each violation and $75,000 for a repeat or continuing violation.

AD9363 Under the Hood

For more information:
- http://www.analog.com/ad9361
- http://www.analog.com/ad9364
- http://www.analog.com/ad9363

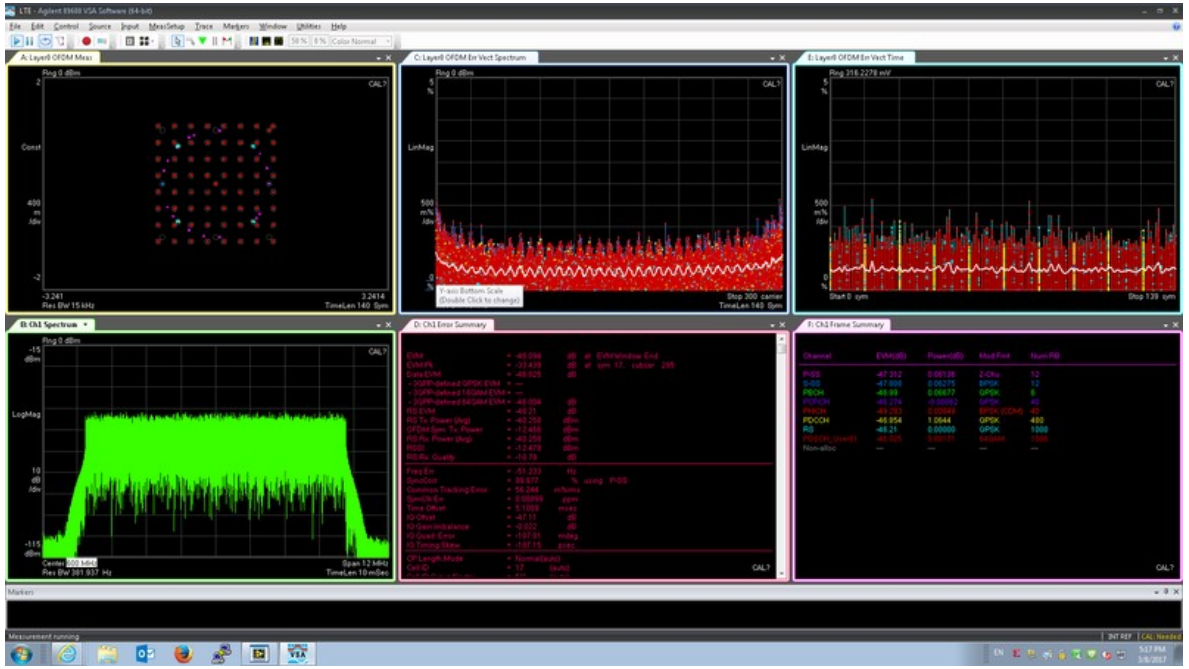
- AD9361: 2 Rx + 2 Tx
- AD9364: 1 Rx + 1 Tx
- AD9363: 2 Rx + 2 Tx
- Major sections:
  - RF input/output paths
  - RF PLL/LO
  - Clock generation
  - ADC/DAC
  - Digital filters
  - Digital interface
  - Enable state machine
  - RX Gain (AGC)
  - TX Attenuation
  - Aux DAC/ADC and GPOs
  - Analog and Digital Correction/Calibration



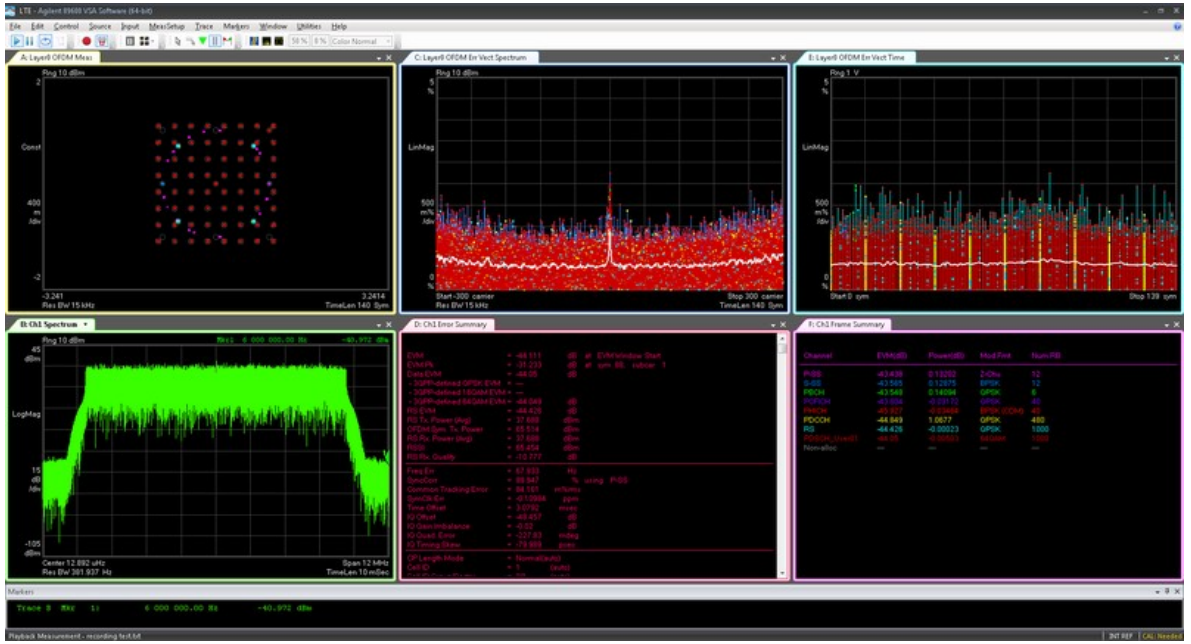
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Performance Data (meets or exceeds AD9363 specs)

- Tx:
  - EVM (64 QAM, LTE10) of -46dB @ 800MHz
    - Waveform created with MathWorks LTE Toolbox, played out the ADALM-PLUTO, connected to Keysight PXA 9030A via SMA cable, and analyzed with Keysight Signal Studio.



- Rx:
  - EVM (64 QAM, LTE10) of -43 dB @ 800MHz
    - Waveform created with MathWorks LTE Toolbox, played out Keysight Arbitrary waveform generator connected to the ADALM-PLUTO via SMA cable, and then analyzed with Keysight Signal Studio.



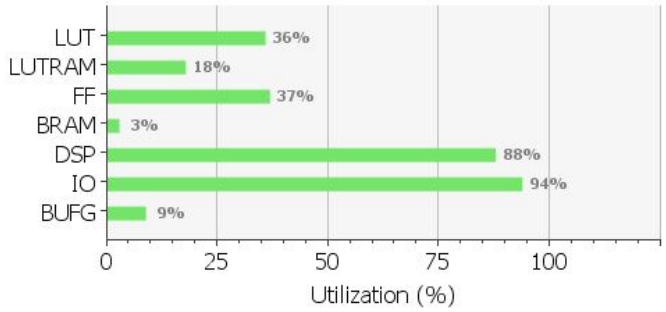
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

It’s a learning tool, for educational settings

Just like the dwarf planet, ADALM-PLUTO is the dwarf SDR

- Temp range : 10°C to 40°C
  - Easier to correct for oscillator we used
- USB 2.0
  - 7 – 12 MSPS, depending on the host, without loosing samples.
- FPGA Size : tiny

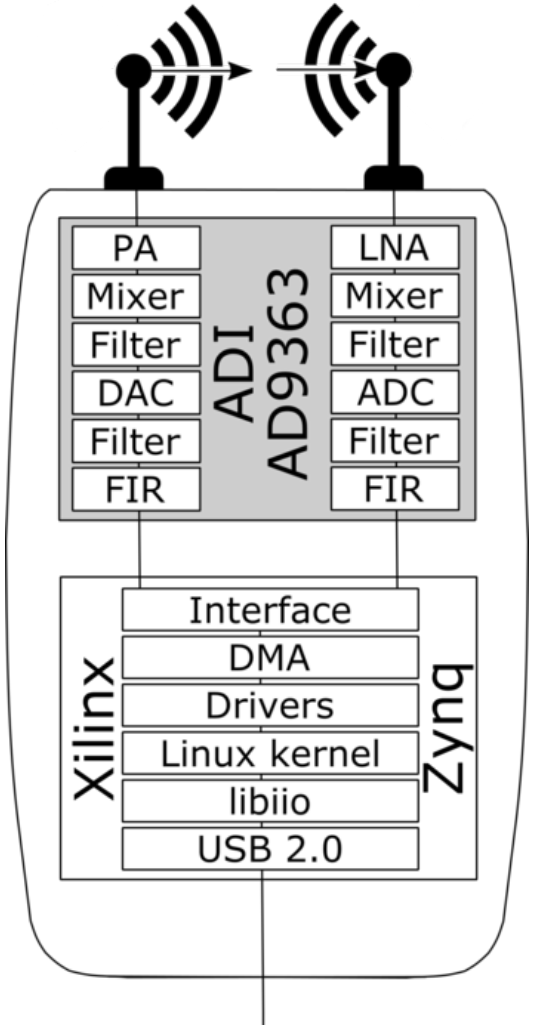
Resource	Utilization	Available	Utilization %
LUT	6422	17600	36.49
LUTRAM	1066	6000	17.77
FF	13162	35200	37.39
BRAM	2	60	3.33
DSP	70	80	87.50
IO	51	54	94.44
BUFG	3	32	9.38



- ARM : Single Core
- Oscillator
  - Rakon RXO3225M,
    - ±25ppm (uncorrected)
    - ±10ppm (factory calibrated)
    - ±1ppm (tuned for temperature)
- Tuning Range:
  - 300 – 3800 MHz (datasheet specs)
  - 70 – 6000 MHz (out of spec)
- RF Shielding
  - None
- RF Filtering
  - None
- Output power
  - 0dBm (CW), varies with frequency

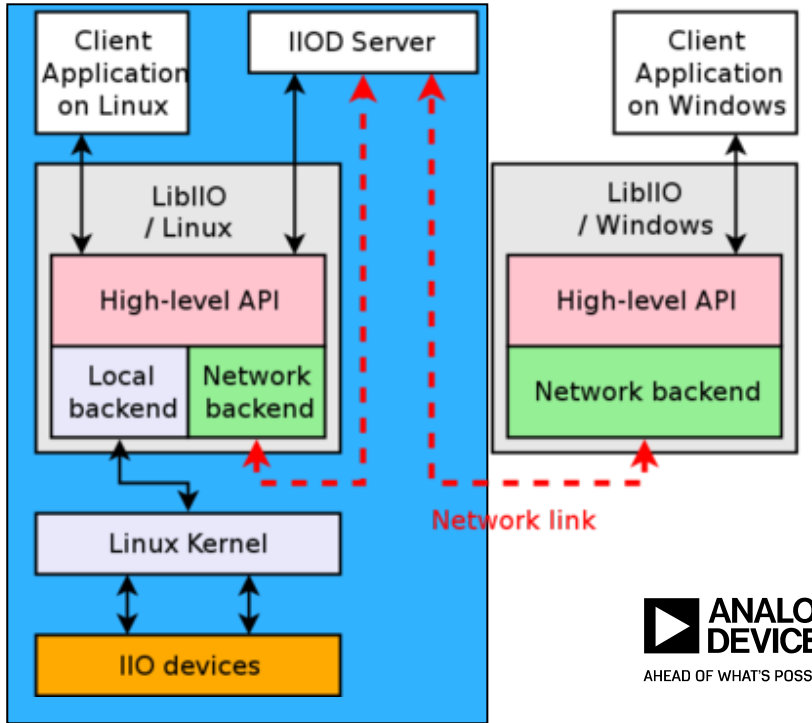
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADALM-PLUTO software stack



- Runs Linux inside the device
- Uses Linux's IIO framework to expose I/Q data and control
- Multi-Function Device
  - Native IIO over USB
  - Serial over USB
  - Ethernet over USB
  - Mass Storage
  - Device Firmware Update
- Host
  - USB dongles

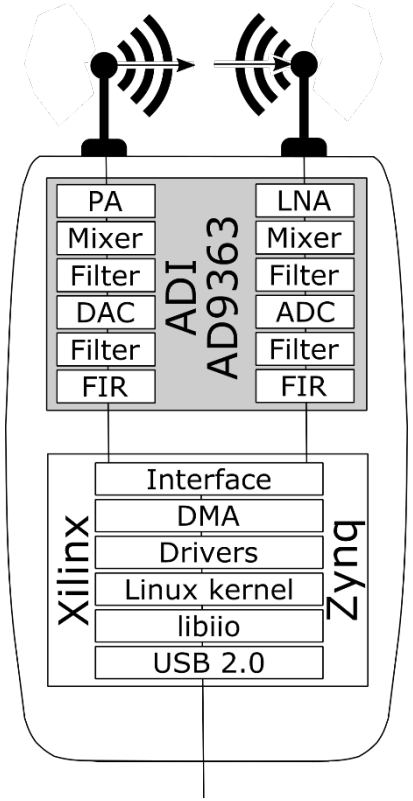
- Cross Platform
  - Windows
  - Linux
  - MAC
- Cross framework
  - Stacked libraries based on libiio



ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADALM-PLUTO possible use cases include IoT!

Connect to host



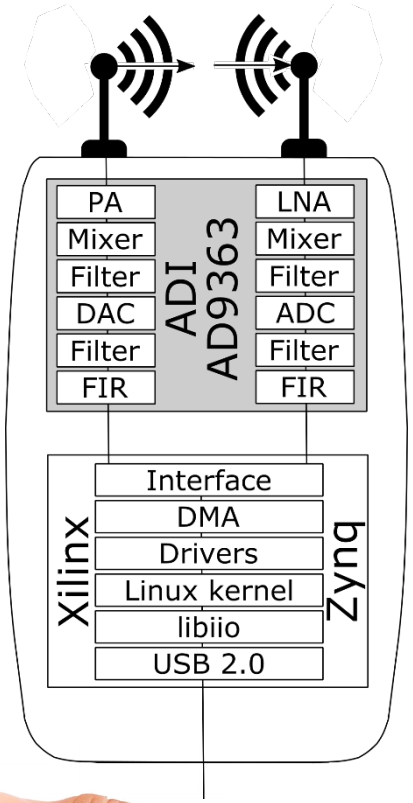
Linux

Mac

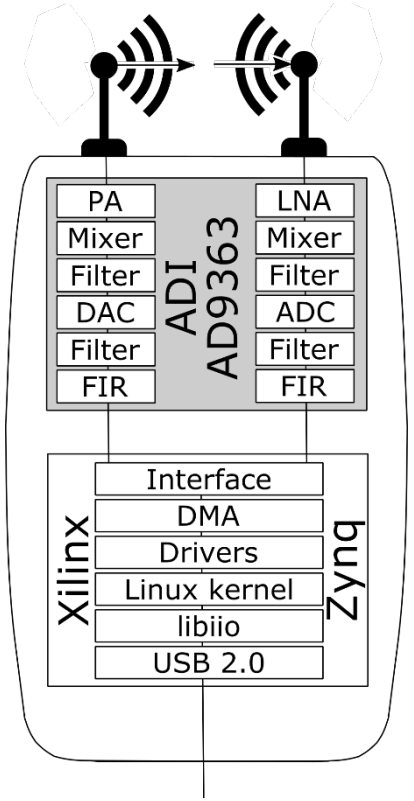
Windows

eLinux

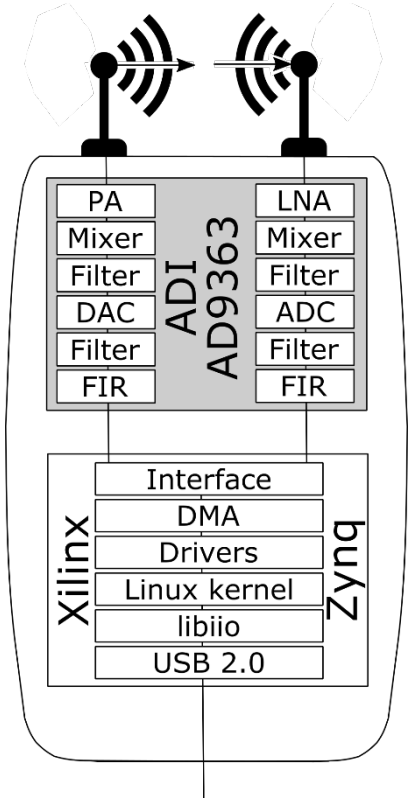
USB Thumb Drive



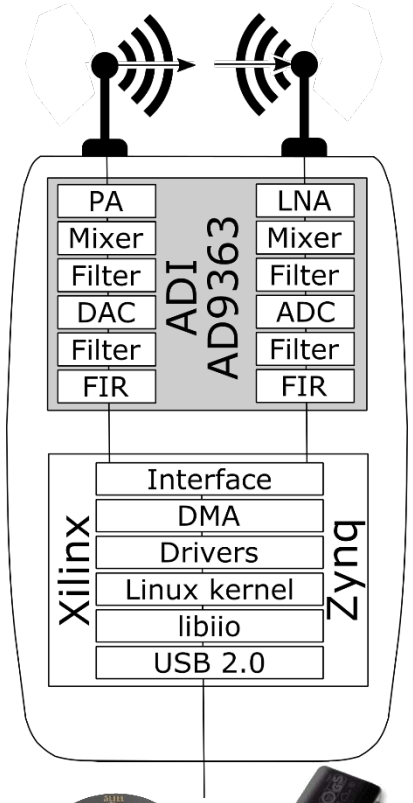
USB LAN



USB WiFi

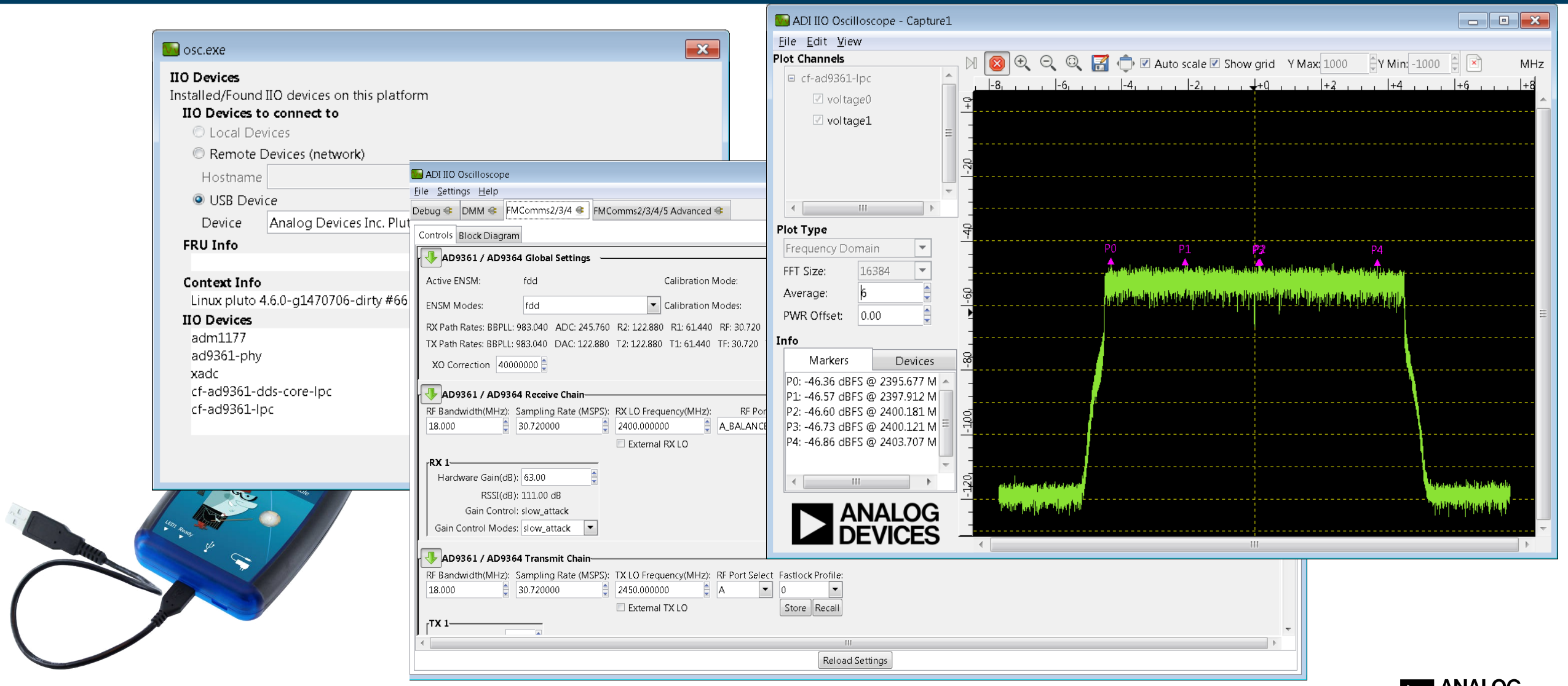


USB Audio



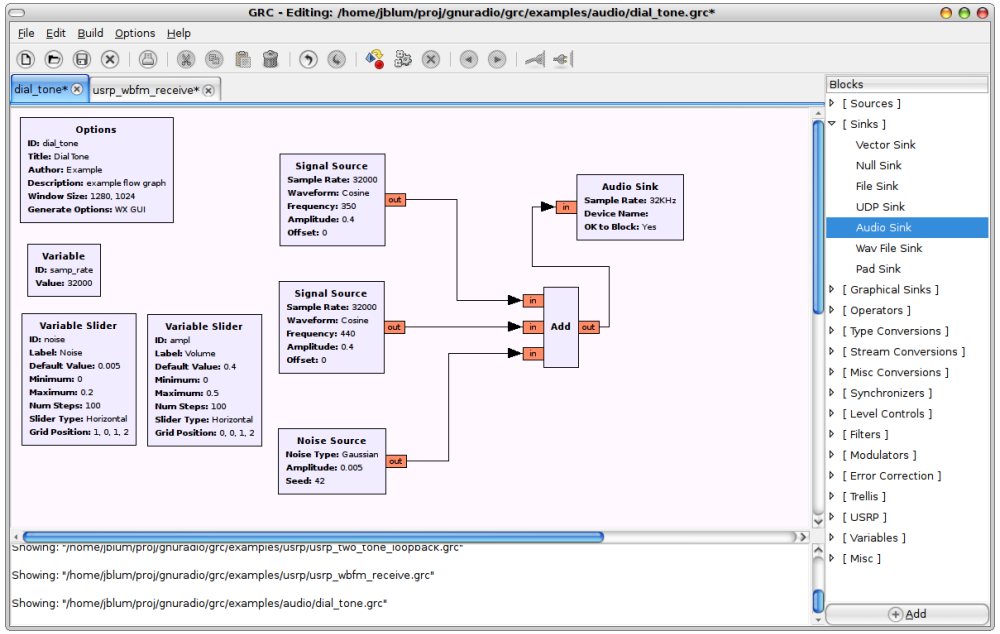
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADALM-PLUTO with IIO Oscilloscope

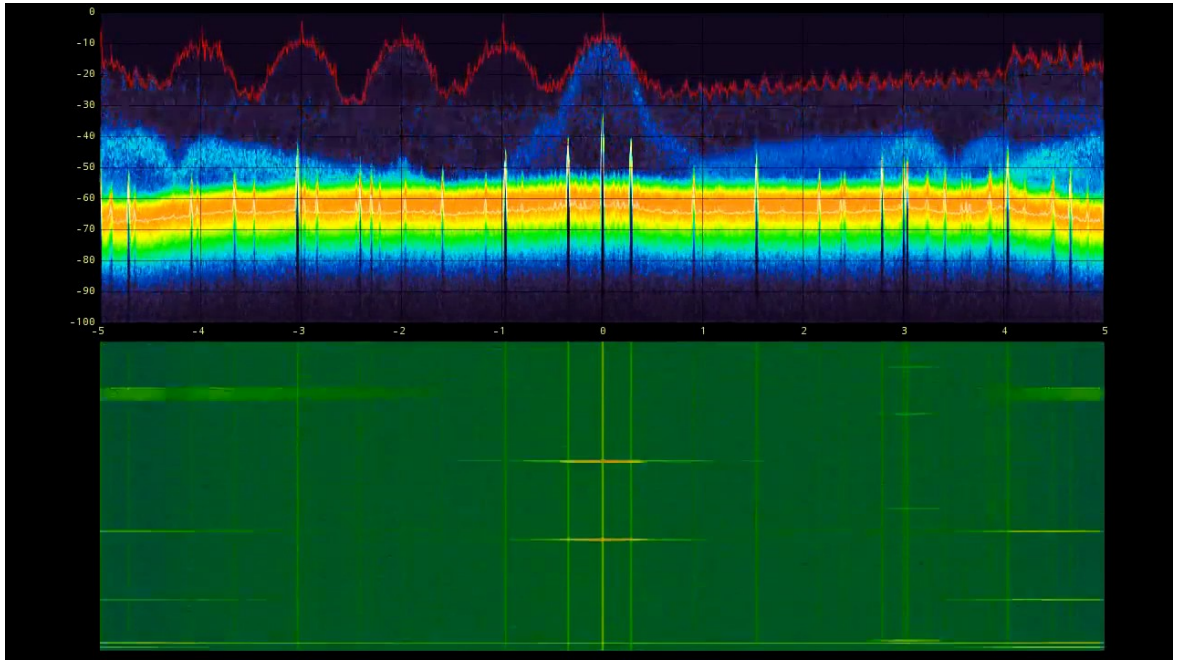


GNU Radio

- GNU Radio
  - Open-source software development toolkit that provides signal processing blocks to implement software radios.

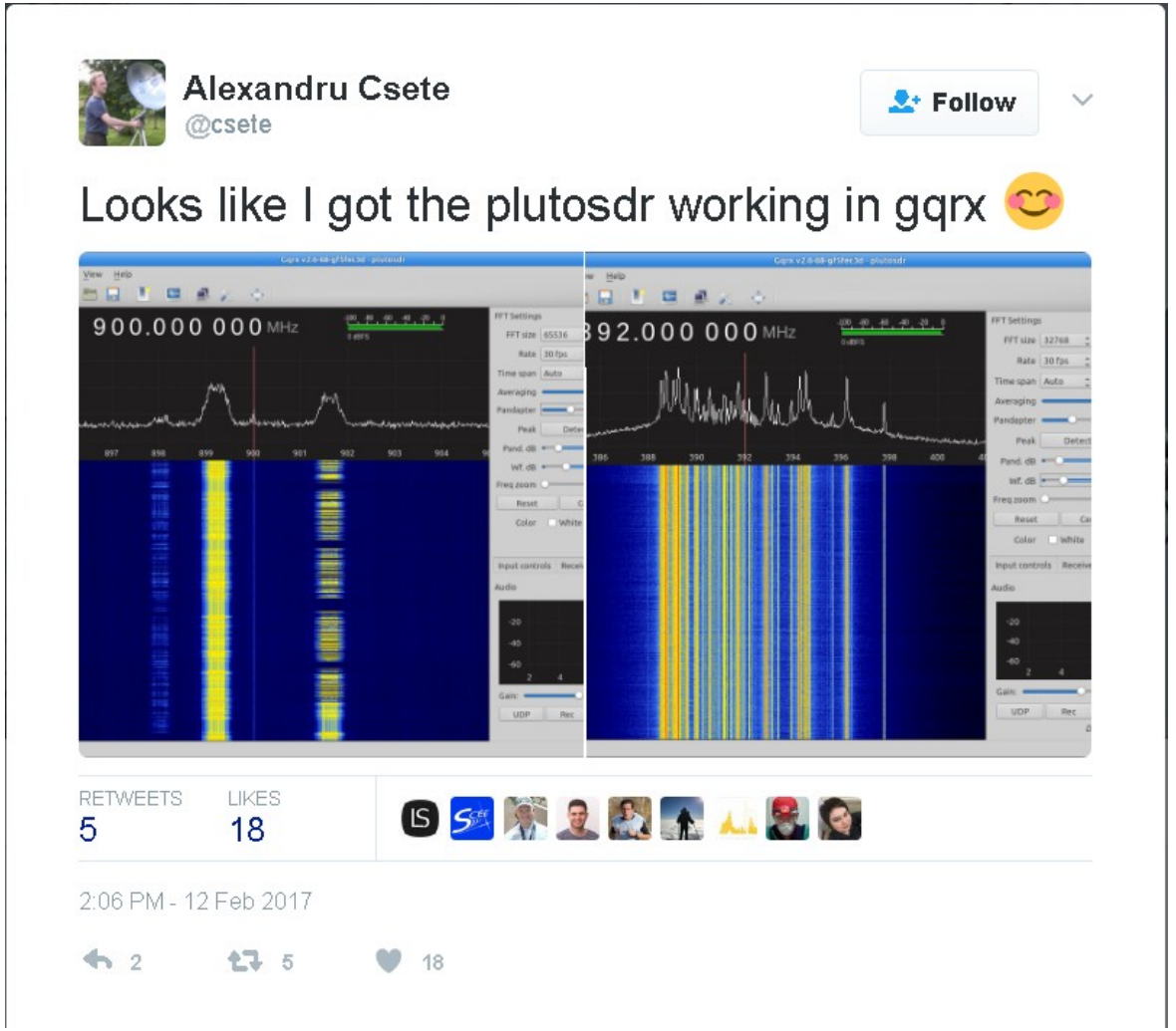


- GR fosphor
  - GNU Radio block for RTSA-like spectrum visualization using OpenCL and OpenGL acceleration



Gqrx SDR

- gqrx
  - Gqrx is an open source software defined radio receiver (SDR) powered by the GNU Radio and the Qt graphical toolkit.
  - Change frequency, gain and apply various corrections (frequency, I/Q balance).
  - AM, SSB, CW, FM-N and FM-W (mono and stereo) demodulators.
  - Special FM mode for NOAA APT.
  - Variable band pass filter.
  - AGC, squelch and noise blankers.
  - FFT plot and waterfall.
  - Record and playback audio to / from WAV file.
  - Record and playback raw baseband data.
  - Spectrum analyzer mode where all signal processing is disabled.

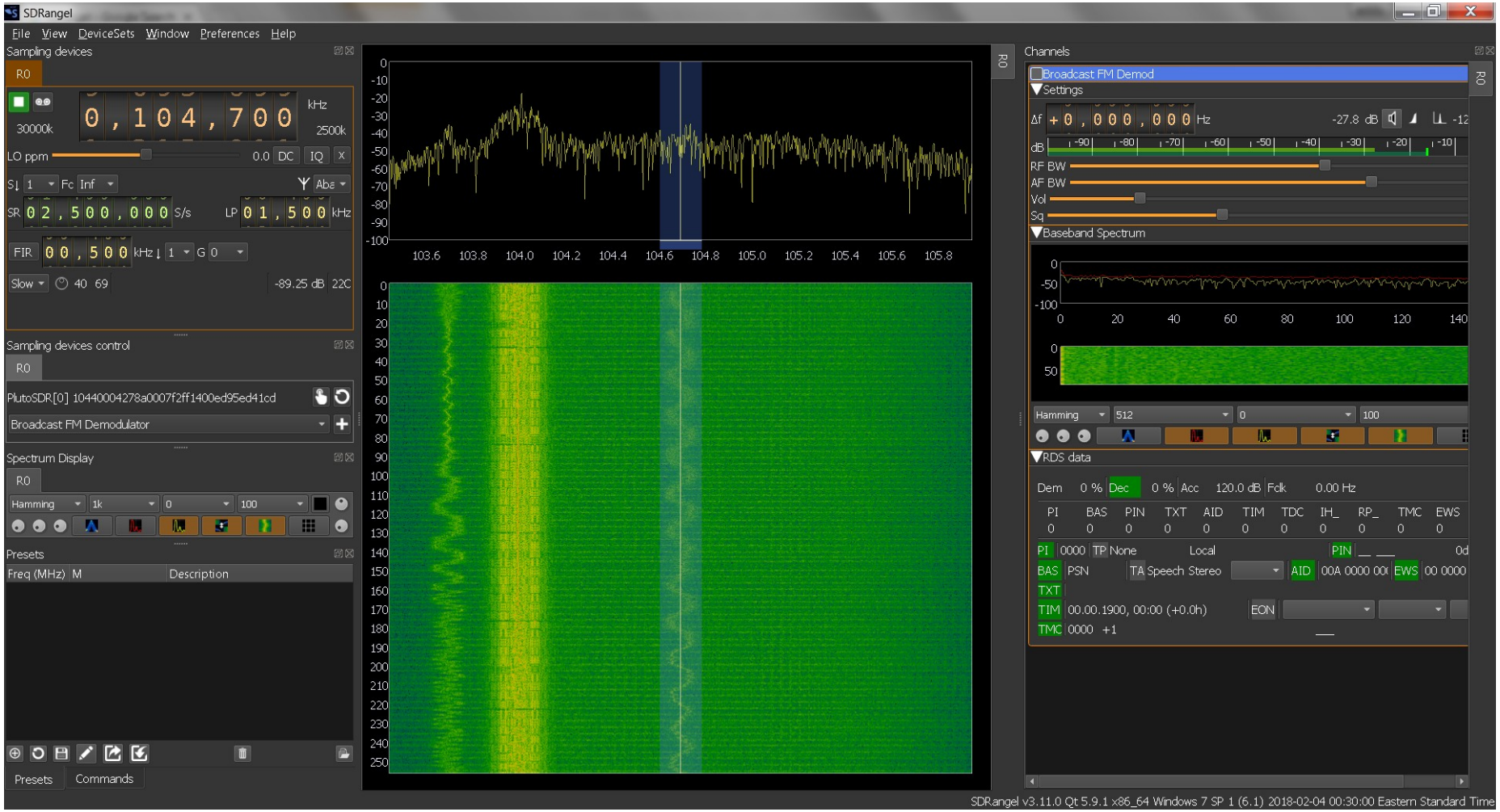


ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

SDRangel

https://github.com/f4exb/sdrangel

- **SDRangel** is an Open Source Qt5 / OpenGL 3.0+ SDR and signal analyzer frontend to various hardware (including Pluto)
- C, C++
- Decoders built in
- Linux, Windows

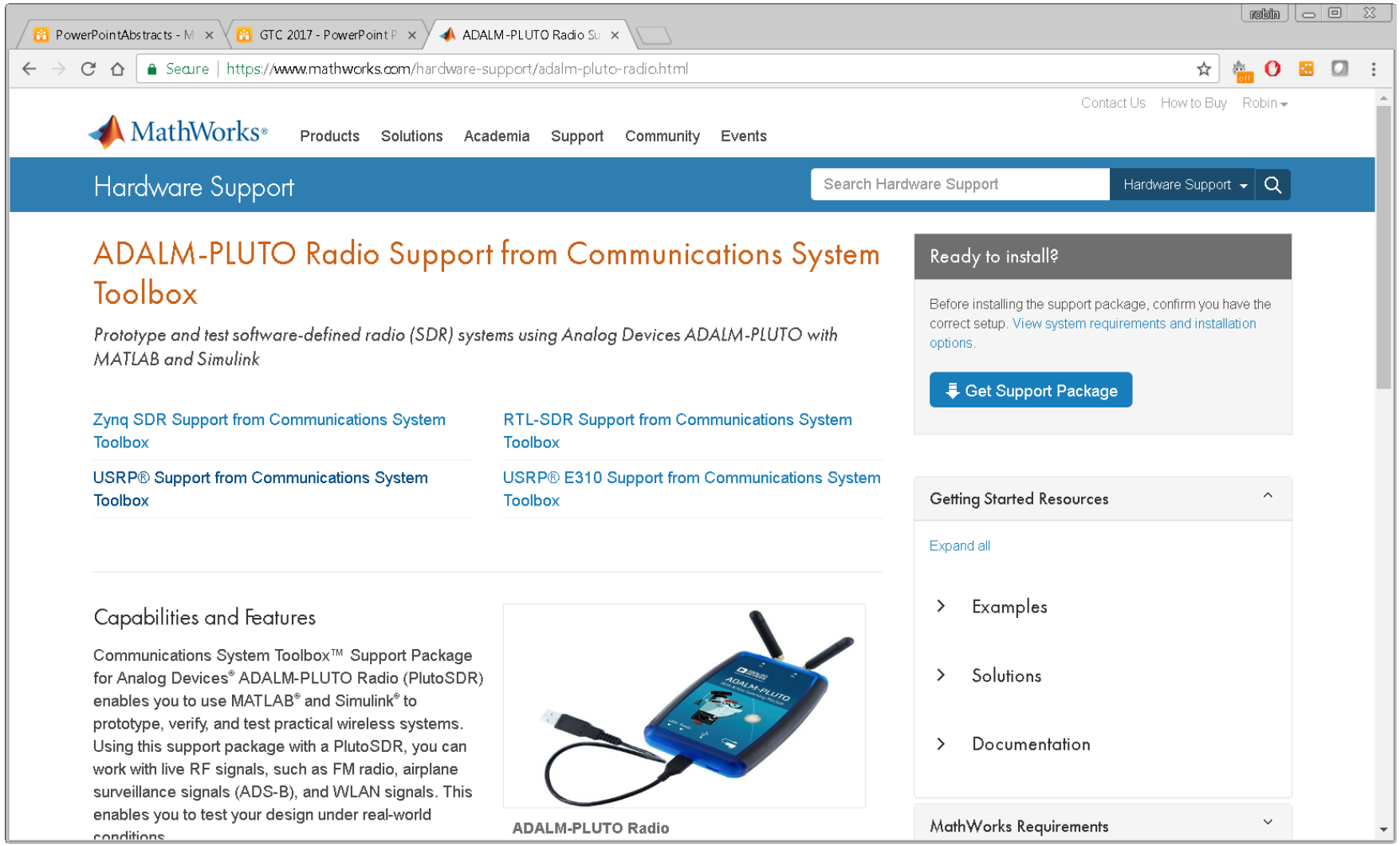


ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

MATLAB

https://www.mathworks.com/adi-pluto

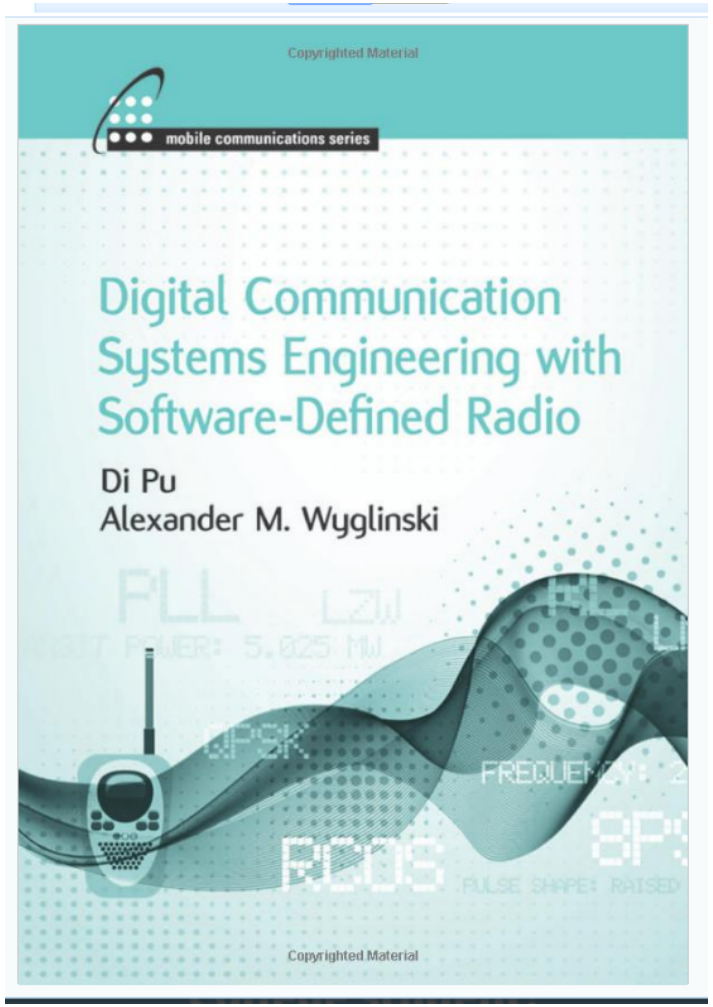
- Native MATLAB and Simulink support
  - Hardware Support Package
- ADI's IIO system object
  - On github



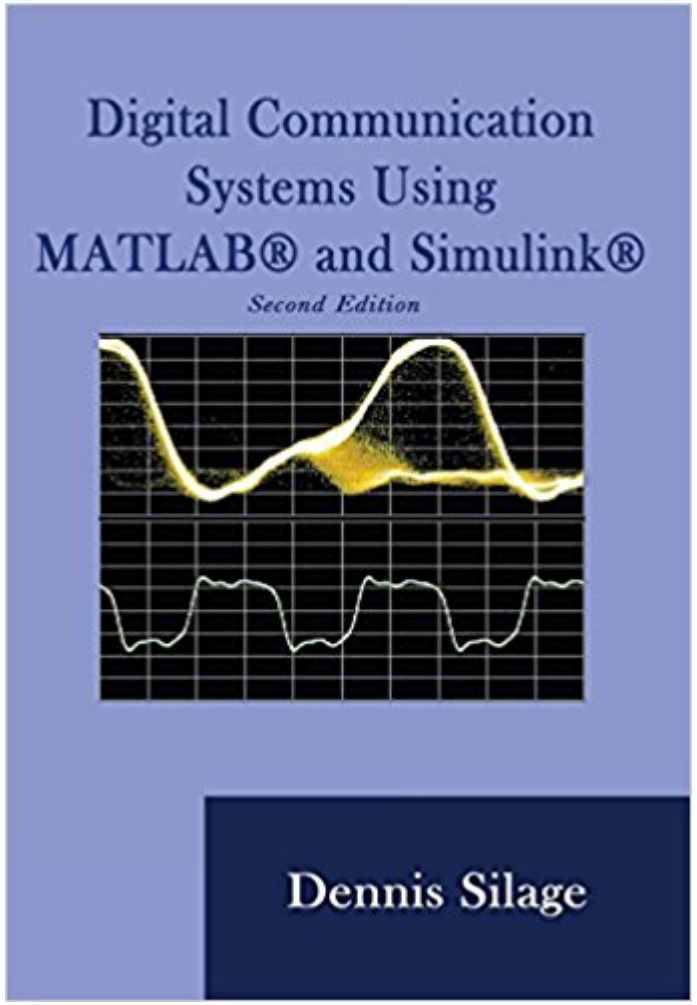
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

The most important thing in education : TextBooks and Labs

- Dr. Alex Wyglinski
  - WPI
- Dr. Di Pu
- Dr. Travis Collins



- Dr. Dennis Silage
  - Temple



ADALM-PLUTO runs embedded Linux!

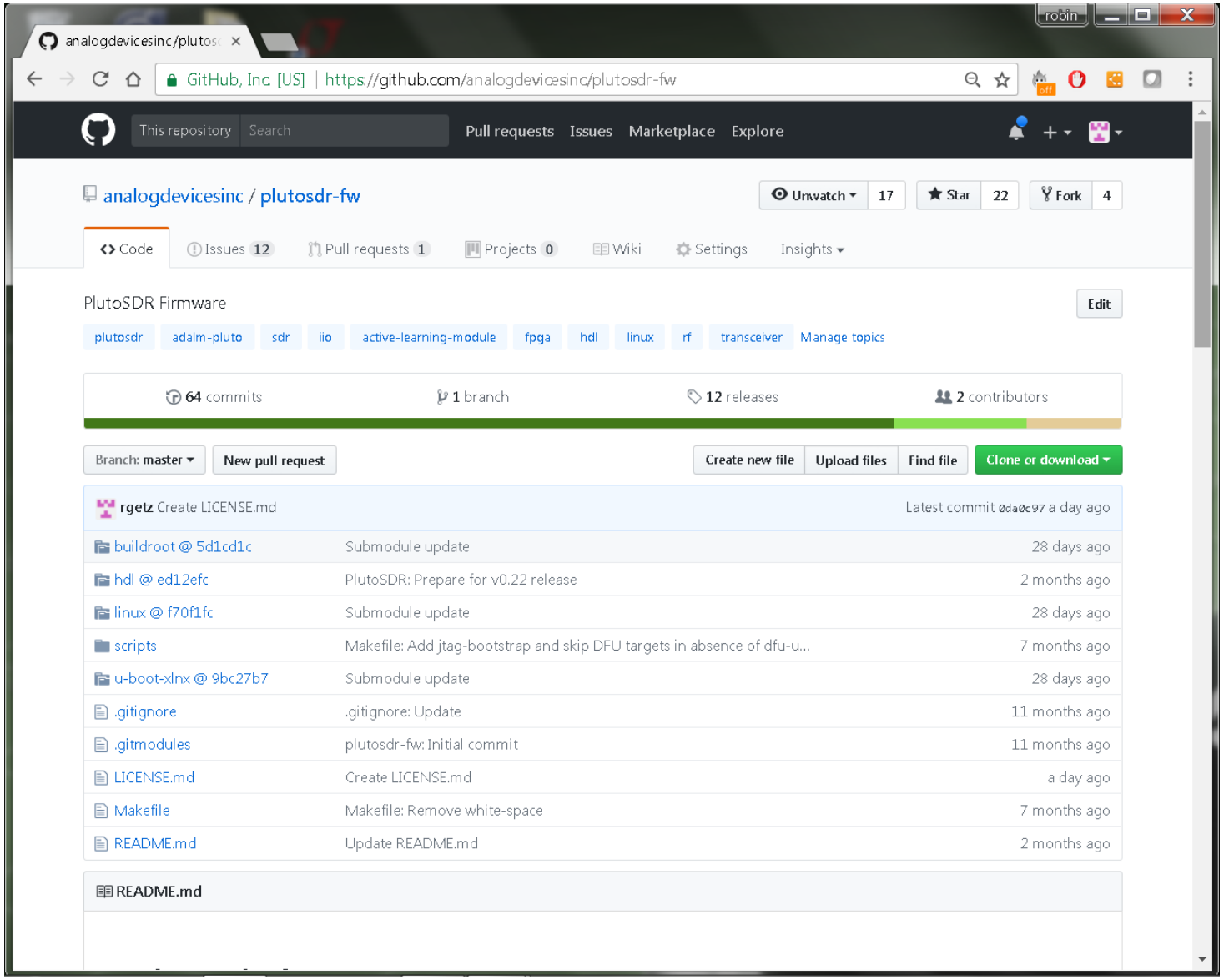
- U-Boot
- Linux 4.6.0 kernel
  - Root password:
  - “analog”
- buildroot
  - Busybox
- ~2 second boot time
- 32Mbytes of Flash
- 512Mbytes of DDR3

- Boot process
  - U-Boot boots from SPI flash
    - Checks button,
      - if pressed DFU flash mode
    - Checks boot mode
      - Previous kernel can tell U-Boot to go into different modes
        - `# device_reboot`
        - `Usage: /usr/sbin/device_reboot {ram|sf|reset|verbose|break}`
        - `  sf     : Reboot and enter Serial Flash DFU mode`
        - `  ram    : Reboot and enter RAM DFU mode`
        - `  reset  : Reboot`
        - `  verbose: Reboot and start serial console Verbose`
        - `  break  : Reboot and HALT in u-boot`
      - DFU ram mode – loads image into RAM and boots it – great for testing
    - Default load U-Boot FIT image, and check CRC, then boot it

Interact with U-Boot via serial console with UART adapter ADALM-JTAGUART

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Open Source Firmware



Build Instructions:

```
git clone --recursive https://github.com/analogdevicesinc/plutosdr-fw.git
cd plutosdr-fw
export CROSS_COMPILE=arm-xilinx-linux-gnueabi-
export PATH=$PATH:/opt/Xilinx/SDK/2016.2/gnu/arm/lin/bin
export VIVADO_SETTINGS=/opt/Xilinx/Vivado/2016.2/settings64.sh
make
```

Results in

File	Comment
pluto.frm	Main PlutoSDR firmware file used with the USB Mass Storage Device
pluto.dfu	Main PlutoSDR firmware file used in DFU mode
boot.frm	First and Second Stage Bootloader (u-boot + fsbl + uEnv) used with the USB Mass Storage Device
boot.dfu	First and Second Stage Bootloader (u-boot + fsbl) used in DFU mode
uboot-env.dfu	u-boot default environment used in DFU mode
plutosdr-fw-vX.XX.zip	ZIP archive containg all of the files above
plutosdr-jtag-bootstrap-vX.XX.zip	ZIP archive containg u-boot and Vivao TCL used for JATG bootstrapping

Building the firmware images

- Download and install Xilinx FPGA Tools
  - Vivado HLx **2016.4: WebPACK** and Editions - Linux Self Extracting Web Installer
  - During installation check under design tools **Software Development Kit (SDK)**
  - Under devices SoC make sure **Zynq-7000** is selected
  - Xilinx gcc tools are distributed as 32-bit binaries you may need to add 32-bit libs

```
michael@HAL9000:~/devel$ dpkg –add-architecture i386
michael@HAL9000:~/devel$ apt-get update
michael@HAL9000:~/devel$ sudo apt-get install libc6:i386 libstdc++6:i386
```

- Install other build dependencies

```
michael@HAL9000:~/devel$ sudo apt-get install git build-essential fakeroot libncurses5-dev libssl-dev ccache
michael@HAL9000:~/devel$ sudo apt-get install dfu-util u-boot-tools device-tree-compiler libssl1.0-dev mtools
```

- Clone and build the Firmware image

```
michael@HAL9000:~/devel$ git clone --recursive https://github.com/analogdevicesinc/plutosdr-fw.git
michael@HAL9000:~/devel$ cd plutosdr-fw
michael@HAL9000:~/devel/plutosdr-fw$ export CROSS_COMPILE=arm-xilinx-linux-gnueabi-
michael@HAL9000:~/devel/plutosdr-fw$ export PATH=$PATH:/opt/Xilinx/SDK/2016.4/gnu/arm/lin/bin
michael@HAL9000:~/devel/plutosdr-fw$ export VIVADO_SETTINGS=/opt/Xilinx/Vivado/2016.4/settings64.sh
michael@HAL9000:~/devel/plutosdr-fw$ make
```

Customizing the PlutoSDR filesystem

- Customize buildroot target packages

```
michael@HAL9000:~/devel/plutosdr-fw$ cd buildroot
michael@HAL9000:~/devel/plutosdr-fw/buildroot$ make menuconfig
michael@HAL9000:~/devel/plutosdr-fw/buildroot$ make savedefconfig
michael@HAL9000:~/devel/plutosdr-fw/buildroot$ cd ..
michael@HAL9000:~/devel/plutosdr-fw$ make
```

- Customize buildroot busybox tools

```
michael@HAL9000:~/devel/plutosdr-fw/buildroot$ make busybox-menuconfig
michael@HAL9000:~/devel/plutosdr-fw/buildroot$ cp output/build/busybox-*/.config board/pluto/busybox-*.config
michael@HAL9000:~/devel/plutosdr-fw$ make
```

Customizing the PlutoSDR filesystem
Adding files

- For temporary modifications
  - Modify the target filesystem directly and then rebuild the image
- For permanent additions
  - **Post-build scripts**
    - Are shell scripts called after Buildroot builds all the selected software, but before the rootfs images are assembled.

```
michael@HAL9000:~/devel/plutosdr-fw$ cp ~/foobar.sh buildroot/output/target/sbin/
michael@HAL9000:~/devel/plutosdr-fw$ make
```

- **Filesystem overlays**
  - A tree of files that is copied directly over the target filesystem after it has been built.

```
michael@HAL9000:~/devel/plutosdr-fw$ cat buildroot/board/pluto/post-build.sh
[ – snip –]
${INSTALL} -D -m 0644 ${BOARD_DIR}/input-event-daemon.conf ${TARGET_DIR}/etc/
[– snip --]
```

Cross-compiling external applications using sysroot

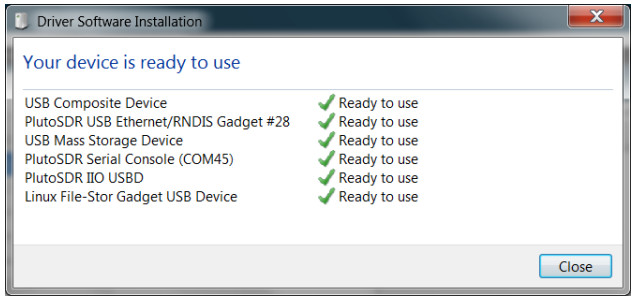
- Along with each PlutoSDR firmware release we also provide the buildroot generated sysroot.

```
michael@HAL9000:~/devel$ wget https://github.com/analogdevicesinc/plutosdr-fw/releases/download/v0.27/sysroot-v0.27.tar.gz
michael@HAL9000:~/devel$ tar xzvf sysroot-v0.27.tar.gz
michael@HAL9000:~/devel$ git clone https://github.com/PlutoSDR/dump1090.git
michael@HAL9000:~/devel$ cd dump1090
michael@HAL9000:~/devel/dump1090$ CC=arm-xilinx-linux-gnueabi-gcc CFLAGS=--sysroot=../staging LDFLAGS=--sysroot=../staging make

arm-xilinx-linux-gnueabi-gcc --sysroot=../staging -c dump1090.c
arm-xilinx-linux-gnueabi-gcc --sysroot=../staging -c anet.c
arm-xilinx-linux-gnueabi-gcc -g -o dump1090 dump1090.o anet.o --sysroot=../staging -liio -lpthread -lm -lad9361

michael@HAL9000:~/devel/dump1090$  scp dump1090 root@192.168.2.1:/sbin/
```

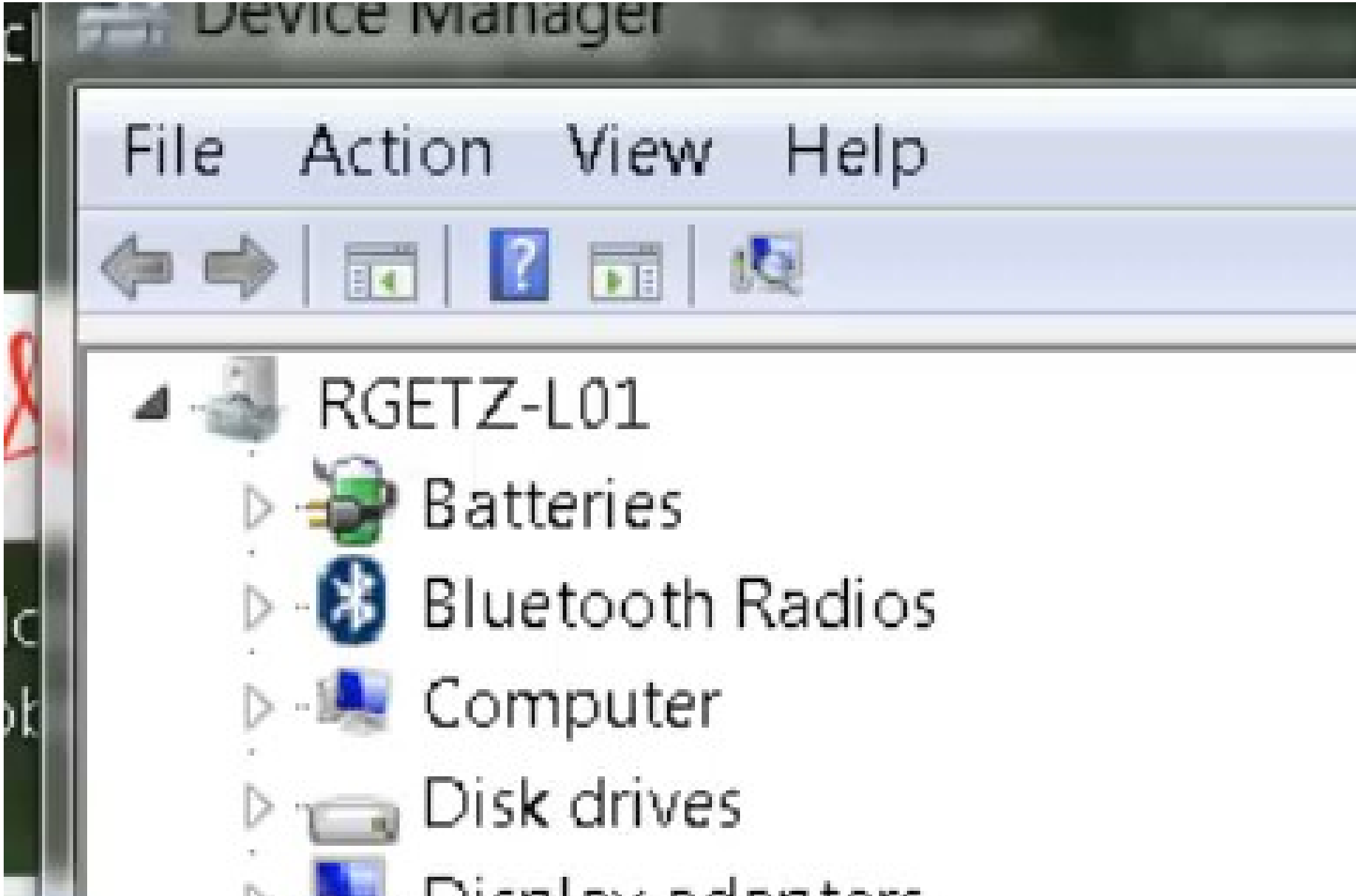
- This allows you to later compile dynamically linked applications that can be executed on the PlutoSDR.

Cross platform

- Runs on Windows



- Linux and OS-X



ADALM-PLUTO Docs – online now!
https://wiki.analog.com/university/tools/pluto

- Docs are on the wiki
- Made public mid Feb
- Needs more
  - if you want to help let us know

ADALM-PLUTO Support Model

- Buy ADALM-PLUTO

→ buy.analog.com
- **digikey.com**
- **mouser.com**
- **arrow.com**

- AD9363 Design Files
- AD9363 Datasheet

→ www.analog.com

- Application and Drivers for Linux and No-OS
  - Linux IIO: Linux Abstraction for Data Converters
- No-OS drivers
- HDL
- U-Boot
- buildroot

→ github.com/analogdevicesinc

- Documentation
- PCB Schematics, Gerbers, BOM

→ wiki.analog.com

- Online support via EngineerZone
  - Virtual Classroom (for ADALM-PLUTO)
  - Wideband RF Transceiver Community
  - FPGA Reference Design Community
  - Linux and Microcontroller Devices Drivers Comm.

→ ez.analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Support

EngineerZone™
ANALOG DEVICES SUPPORT COMMUNITY

- https://ez.analog.com/community/university-program
  - ADALM-PLUTO users
- https://ez.analog.com/community/fpga
  - FPGA Developers
- https://ez.analog.com/community/linux-device-drivers/linux-software-drivers
  - libiio users and developers
  - Driver users and developers

Stupid Tricks

- Run scripts from USB drive (supported in default image)
  - The Pluto will automount any USB mass storage device such as thumb drive or Hard Drives. The automounter will then look for some special file names:
    - `runme[0-9].sh` which it will run as a shell script
    - `runme[0-9]` which it will run as a binary file.

```
#!/bin/sh

# the default directory the script runs in is /dev, so change to the drive
cd /media/sda1/

# create a file
touch foobar

# change the RX_LO to 2.4GHz
iio_attr -a -c  ad9361-phy RX_LO frequency 2400000000

ACTION=remove_all /lib/mdev/automounter.sh
```

Replace the input-event-daemon .conf file

Default file:

```
#
# /etc/input-event-daemon.conf
#

[Global]
listen = /dev/input/event0

[Keys]
BTN_0          = ACTION=remove_all /lib/mdev/automounter.sh
```

Replace it with one from USB drive, which plays back pre-recorded files, record waveforms, or runs custom application, and then restart input-event-daemon

Play a CW at 908,460,000 Hz

```
#!/bin/sh

# the default directory the script runs in is /dev, so change to the drive
cd /media/sda1/

# create a file
touch foobar.txt

echo default-on > /sys/class/leds/led0:green/trigger >> foobar.txt

# Set the LO up
/usr/bin/iio_attr -a -c ad9361-phy TX_LO frequency 908460000 >> foobar.txt

# Set the Sample frequency up, tone will appear at sampling_frequency/32
/usr/bin/iio_attr -a -c -o ad9361-phy voltage0 sampling_frequency 32000000 >> foobar.txt

# Turn the attenuation down
/usr/bin/iio_attr -a -c -o ad9361-phy voltage0 hardwaregain 0 >> foobar.txt

# https://wiki.analog.com/resources/tools-software/linux-drivers/iio-transceiver/ad9361#bist_tone
# Inject 0dBFS tone at Fsample/32 into TX (all channels enabled)
/usr/bin/iio_attr -a -D ad9361-phy bist_tone "1 0 0 0" >> foobar.txt

cd /root

ACTION=remove_all /lib/mdev/automounter.sh
```

Cell phone jammers

Company web site:

This Handheld Selectable 8 band All Cell Phone Signal Jammer & WiFi GPS L1 All in one Jammer High-capacity (USA Version) suit for USA, against 4G LTE networks 3G GSM cellphone signals, and blocking WIFIand GPS L1.And it great use for office, school,home to blocks internet browse,cellphone conversation and GPS signal, one device to coverage all 4G 3G GSM WIFI GPS frequencies,no need any other device to suppress wireless signal in your office,home,school.

FCC web site:

The use of "cell jammers" or similar devices designed to intentionally block, jam, or interfere with authorized radio communications (signal blockers, GPS jammers, or text stoppers, etc.) is a violation of federal law. Also, it is unlawful to advertise, sell, distribute, or otherwise market these devices to consumers in the United States. These devices pose serious risks to critical public safety communications, and can prevent you and others from making 9-1-1 and other emergency calls. Jammers can also interfere with law enforcement communications. Operation of a jammer in the United States may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.

JAMMING CELL PHONES AND GPS EQUIPMENT IS AGAINST THE LAW!

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Record files in the cell phone bands to look for CW

Thanks

- Questions?