What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

A radio in which some or all of the physical layer functions are software-defined.
What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

A radio in which some or all of the physical layer functions are software-defined.

Processing is defined by programmed algorithms, not HW.
What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

*A radio in which some or all of the physical layer functions are software-defined.*

Processing is defined by programmed algorithms, not HW.

(‘Software-Defined Radio’ [SDR] is the same thing)
Processing Blocks

- From the, “Okay, that’s useful,” to the “Whoa. that’s awesome.”
Unified Workflow from Design → Deployment

- Simulate
- Hardware-in-the-Loop Prototyping
- Deploy
Out of Tree Modules

The Comprehensive GNU Radio Archive Network (CGRAN) is a free open source repository for 3rd party GNU Radio applications a.k.a Out Of Tree Modules that are not officially supported by the GNU Radio project.

Browse~Checkout~Hack

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Description</th>
<th>Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>gr-eventsstream</td>
<td>scheduler, streaming, bandy</td>
<td>The event stream scheduler</td>
<td>GitHub</td>
</tr>
<tr>
<td>Receiver for Valsa Weather Sonde</td>
<td></td>
<td>Receiver for Valsa Weather Sonde</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-pyst</td>
<td>gui plotting, pust, pust</td>
<td>Python-QT Plotters and Message Tools Repo</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-pcap</td>
<td>pcap, packet</td>
<td>PCAP recording and playback</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-coralccm</td>
<td>hardware, sources</td>
<td>MicrowavePeraeus SDR source module</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-tta</td>
<td>LTE, synchrononization, estimation, PBCCH</td>
<td>LTE downstream receiver blocks</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-nrwa</td>
<td>xtd, gps, nrwa</td>
<td>Interface to NMEA and GPSD sources</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-eea802-11</td>
<td>IEEE 802.11, WIFI, OFDMA</td>
<td>IEEE 802.11 a/g/n Transcripter</td>
<td>GitHub</td>
</tr>
<tr>
<td>An IEEE 802.15.4 (Zigbee) Transceiver</td>
<td>xtd, IEEE 802.15.4, Zigbee</td>
<td>gr-eea802-15-4</td>
<td>GitHub</td>
</tr>
<tr>
<td>gr-uhd-gps</td>
<td>uhdl, gps</td>
<td>GPS blocks to assist in GPS Data logging with UHD and uGPSD0</td>
<td>GitHub</td>
</tr>
</tbody>
</table>
GSoC & SOCIS 2017

- Don’t have to be an RF / DSP / Wireless expert to participate!
- Organized by GNU Radio Community Manager: Martin Braun
- History:
- Ideas for 2017:
  - General: C++ Flowgraph Generation from GRC, Android, Qt Graphics
  - DSP: RADAR, DAB, Filter Design Tools
  - Security: Fuzzing, View-Only, Auditing
- Ideas List must be finalized next week!
GNU Radio Conference

● GRCon17 will be our 7th year
  ○ Finalizing San Diego!
  ○ Mid-September
● GRCon16:
  ○ Hosted in Boulder, Colorado
  ○ 304 Attendees, 20 Sponsors
  ○ 51+ Tech Talks
  ○ 4 Days of Talks
  ○ 1 Day of Hackfest
  ○ Hacking Challenge
GNU Radio Foundation (, Inc.)

- Incorporated last year!
- Current responsibilities:
  - Raising money to support the project
  - Managing finances
  - Holding & managing all IP not owned by the FSF
  - Paying for & maintaining our (significant) AWS infrastructure
  - Putting on GRCon
- Future responsibilities:
  - Funding project development
Virginia Tech Ground Station & Sounding Rocket

- GNU Radio in the rocket, GNU Radio on the ground!
Reverse Engineering Outernet

Blog Post Walkthrough: http://gnuradio.org/blog/reverse-engineering-outernet/
Reverse Engineering Outernet

Blog Post Walkthrough: http://gnuradio.org/blog/reverse-engineering-outernet/
Sniffing VGA Signals

First presented at GRCon14: [Presentation Slides](#)
DEF CON 22 - Michael Ossmann - The NSA Playset: RF Retroreflectors
Resurrecting AMPS

- Schmoocon 2017: Dig Out Your Brick Phone! Bringing AMPS Back with GNU Radio
- gr-amps OOT: https://github.com/unsynchronized/gr-amps
Android!

- Original work all done by Tom Rondeau
Drone Hijacking

STEALING A DRONE WITH SOFTWARE DEFINED RADIO

PHDays (Positive Hack Days) is a yearly forum with a focus on ethical hacking and security. During this year’s forum which took place in June, the organizers set up a competition where the goal was to “steal” or take control of a Syma X8C quadcopter drone. The drone runs on the nRF24L01 module, which from previous posts we have seen can easily be sniffed and decoded with an RTL-SDR or other SDR.

To reverse engineer the drone’s wireless communications system the teams used software defined radios like the HackRF and BladeRF, and also an alternative method involving just using an Arduino and nRF24L01+ receiver chip. Once the signal was received, they used GNU Radio to decode the signal into packets of data. After analyzing the data they found that the data bytes were easily reverse engineered and then were able to transmit their own data packets to control the drone. The post goes into further detail on the specifics of the reverse engineering.

GRCon16 - Drone Hijacking and Other IoT Hacking, Alexander Chemeris
Radio Astronomy

Images from Juha Vierinen’s presentation:
Geophysical Remote Sensing with GNU Radio
Radio Astronomy

- Juha Vierinen’s work at Haystack Observatory
  - Presented at GRCon13: slides, video

- National Radio Astronomy Observatory
  - Presented at Cyberspectrum 10: Using GNU Radio for Astronomy Research, Public Outreach

- Open Source Radio Telescope Project (OSRT)
  - Building a community for open source radio telescopes

- Canadian Centre for Experimental Radio Astronomy (CCERA)
  - Goal: Make something like this accessible to everyone
Signal Metadata Format (SigMF)

- Format for describing recordings of digital samples.
- Open Standard
- Why is this useful?
  - Don’t need hardware
  - Signals you don’t have access to
  - Reproducibility (for science!)
  - Collaborative processing
  - Basically “code comments” for signal data
  - Create feature / characteristic annotations
  - Moving data between tools/workflows and retaining meta-information
- Under active development: [https://github.com/gnuradio/SigMF](https://github.com/gnuradio/SigMF)
Major Development Directions

- Heterogeneous Processing
Major Technical Development Directions

- Heterogeneous Processing
- Development Environment
  - Client / Server Architecture
  - Debugging Utilities
  - Qt5 Graphical Tools
- Improvements to GNU Radio ‘core’
  - Memory Management (e.g., more Zero Copy, better NUMA)
  - Parallel Processing
  - Dynamic Flowgraph Reconfiguration
- Performance Optimization
Come Get Involved!

- Huge variety of fields and skill levels.
- Students, Hobbyists, Professionals
- Very welcoming of new developers.

- Conferences, Hackfests, Meetups
- Mailing List, IRC, Dev Calls
gnuradio.org