# Spectrum Monitoring Network: Trade-Offs, Results, Future Work

Peter Mathys
Department of ECEE
University of Colorado Boulder

# Spectrum Monitoring

Using a single well-equipped truck measuring one location at a time.

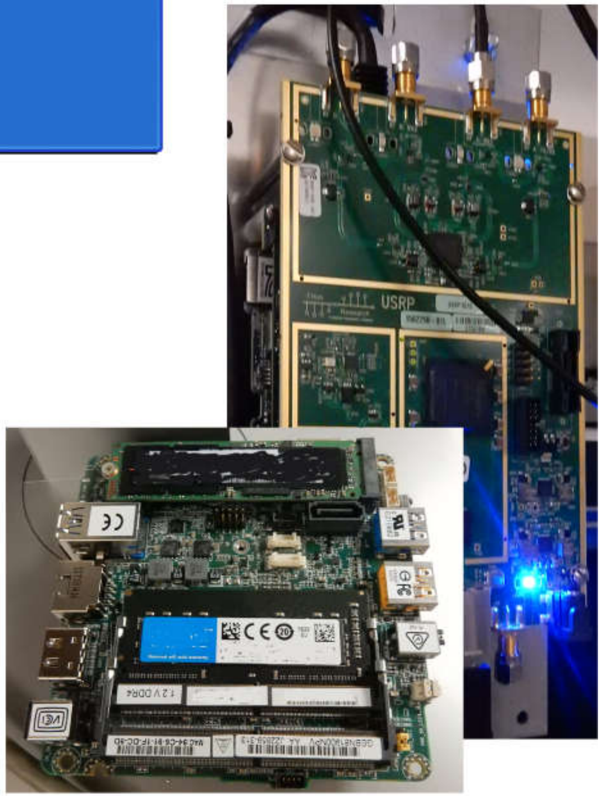

versus


A network of configurable low-cost sensors spread over a wide geographical area.

# What are the Trade-Offs?

Your budget may allow you to buy one of these (Vector Signal Analyzer)

or




20 of these (SDR + single board computer)

# We Need to Look at

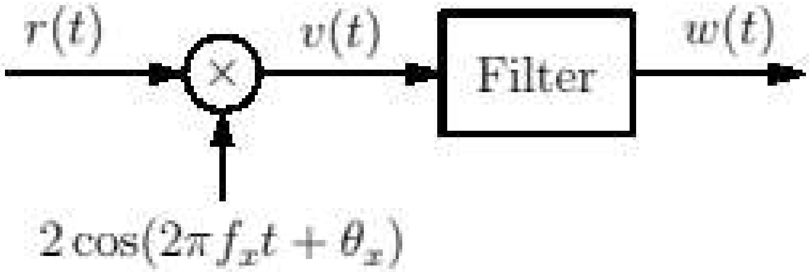
- Radio Receiver Architectures
- Spectrum/Signal Analyzers
- Performance Measurements and Results
- Future Directions
- Measurement Terms/Procedures

# Radio Receiver Architectures

- Frequency Translation
- Superheterodyne Receiver (SHR)
  - Some History
- Direct Conversion Receiver (DCR)
  - Some History
  - Modern Version

# Frequency Translation

- Mixer with Filter for Frequency Translation




- Let $r(t) = s(t)\cos(2\pi f_c t + \theta_c)$
- Then $$v(t) = s(t)[\cos(2\pi(f_x - f_c)t + \theta_x - \theta_c) + \\ + \cos(2\pi(f_x + f_c)t + \theta_x + \theta_c)]$$

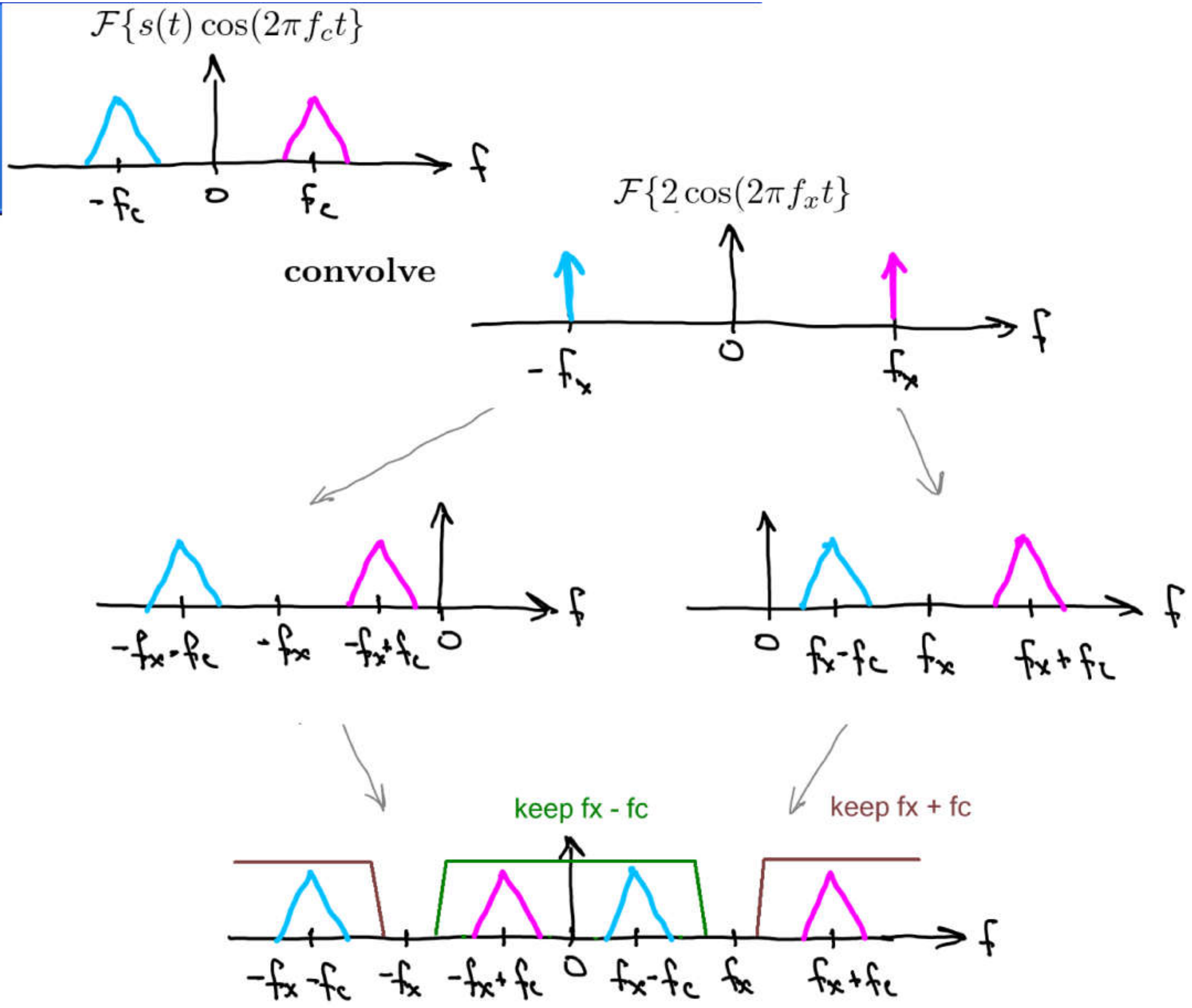
# In Frequency Domain

$$\mathcal{F}\{s(t)\cos(2\pi f_c t\}$$

convolved with

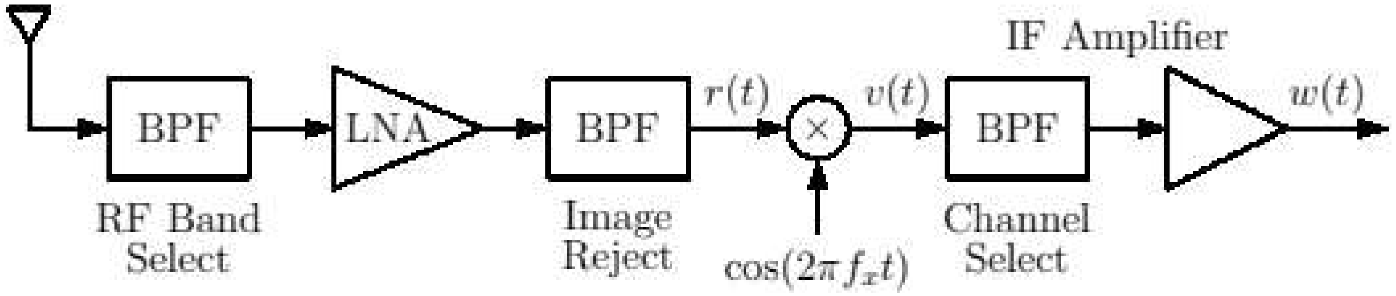
$$\mathcal{F}\{2\cos(2\pi f_x t\}$$

Keep signal at fx – fc
or signal at fx + fc.



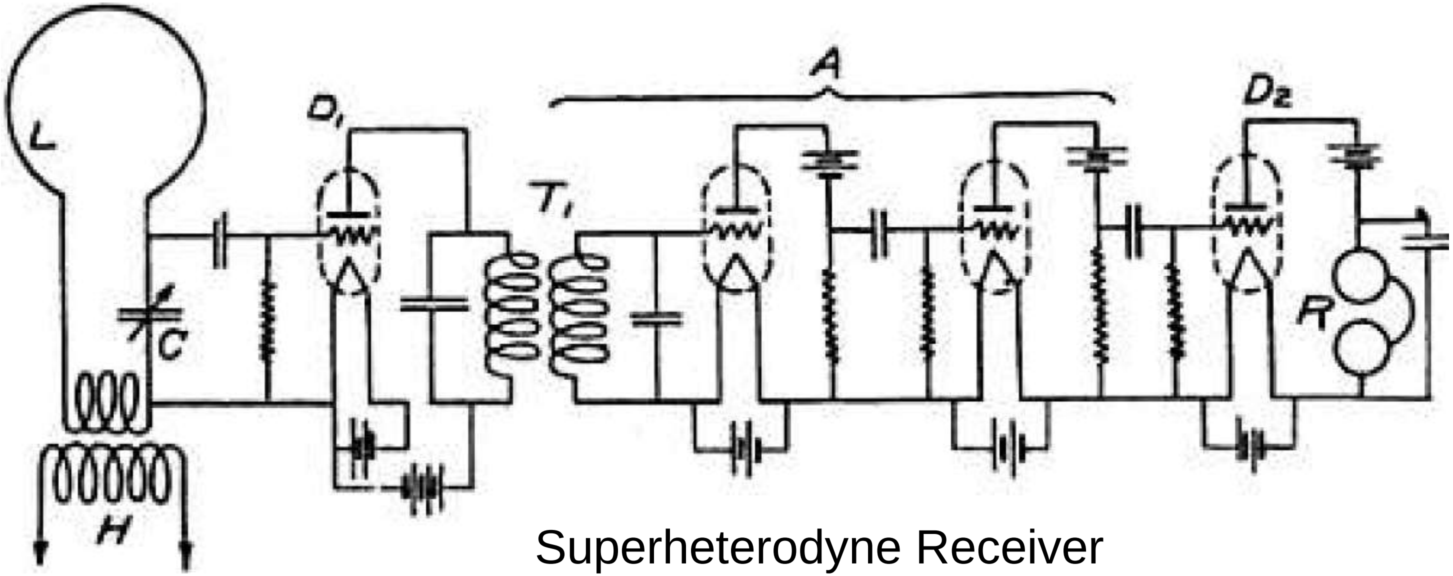
# Superheterodyne Receiver (SHR)

- Block diagram




- Multiplication by cos(2*pi*fx*t) performs frequency translation
- Three bandpass filters (BPF) and two amplifiers needed for single conversion SHR.

# Edwin H. Armstrong (~1920)



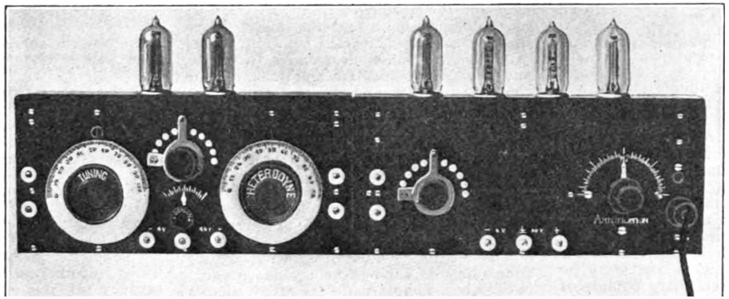


From “A New System of Shortwave Amplification, 1921

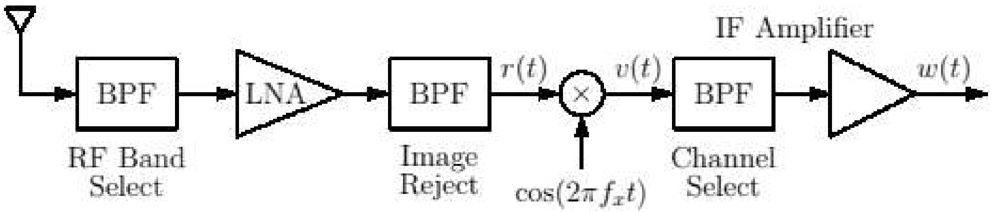
Superheterodyne Receiver

L,C: Tuned receiving circuit

H: Heterodyne oscillator input
D1: Mixer non-linearity
A: IF amplifier
D2: Envelope detector



# Image Frequency of SHR




$$r(t) = \gamma s(t)\cos(2\pi f_c t)$$

$$v(t) = \frac{\gamma}{2} s(t)[\cos(2\pi(f_x - f_c)t) + \cos(2\pi(f_x + f_c)t)]$$

$$w(t) = \rho\, s(t)\cos(2\pi(f_x - f_c)t)$$

$$f_{IF} = |f_x - f_c| \quad \begin{array}{llll} \text{if} & f_x > f_c & \Rightarrow & f_c = f_x - f_{IF} = f_{c1} \\ \text{if} & f_x < f_c & \Rightarrow & f_c = f_x + f_{IF} = f_{c2} \end{array}$$

One of fc1, fc2 is the desired receive frequency, the other is the image frequency.

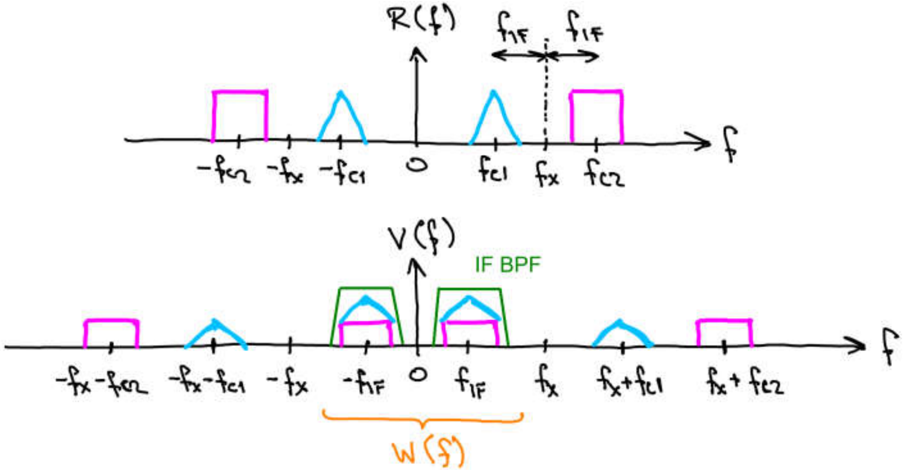


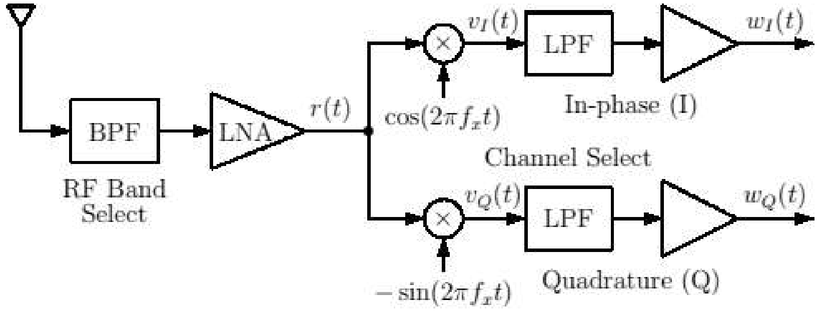

Image reject filter (2’nd BPF) passes signal at desired receive frequency and rejects signal at image frequency.

# Superheterodyne Receiver

- Advantages
  - No local oscillator (LO) leakage
  - RF band select filter suppresses out of band signals before LNA
  - Not affected by second order non-linearities
- Disadvantages
  - Need to reject image frequency
  - Needs three bandpass filters (BPF), some tunable or switchable
  - Difficult to integrate BPFs with high Q on a chip

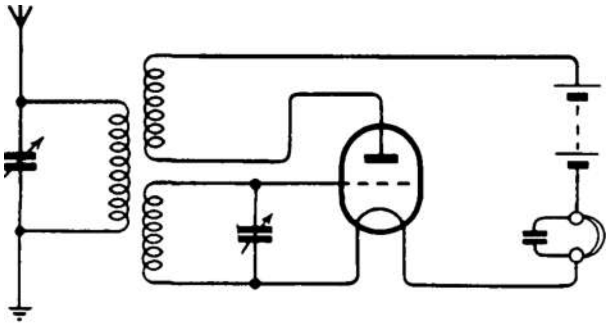
# Direct Conversion Receiver (DCR)

- Also called homodyne or synchrodyne
- Block diagram of modern version

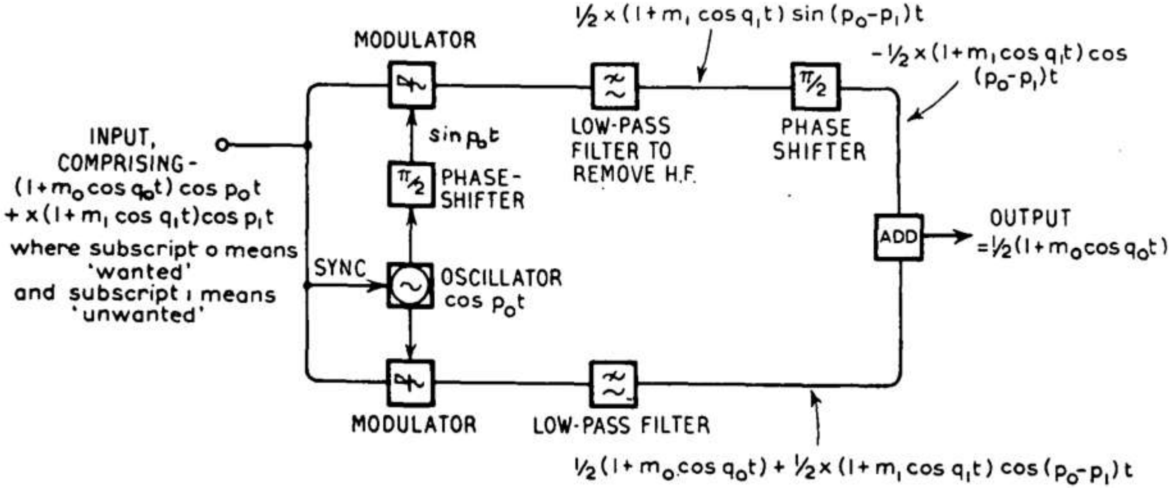



- Mixing directly down to baseband (IF = 0)
- Filtering at baseband using digital signal processing (DSP)
- Minimal signal processing at RF frequencies

# Early Versions of the DCR



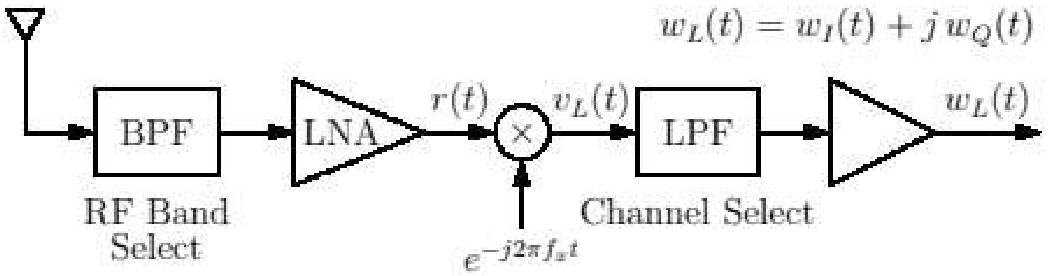
F.M. Colebrook, “Homodyne”, 1924. It is an oscillating detector which amplifies the (weak) received carrier to improve demodulation of AM signals.

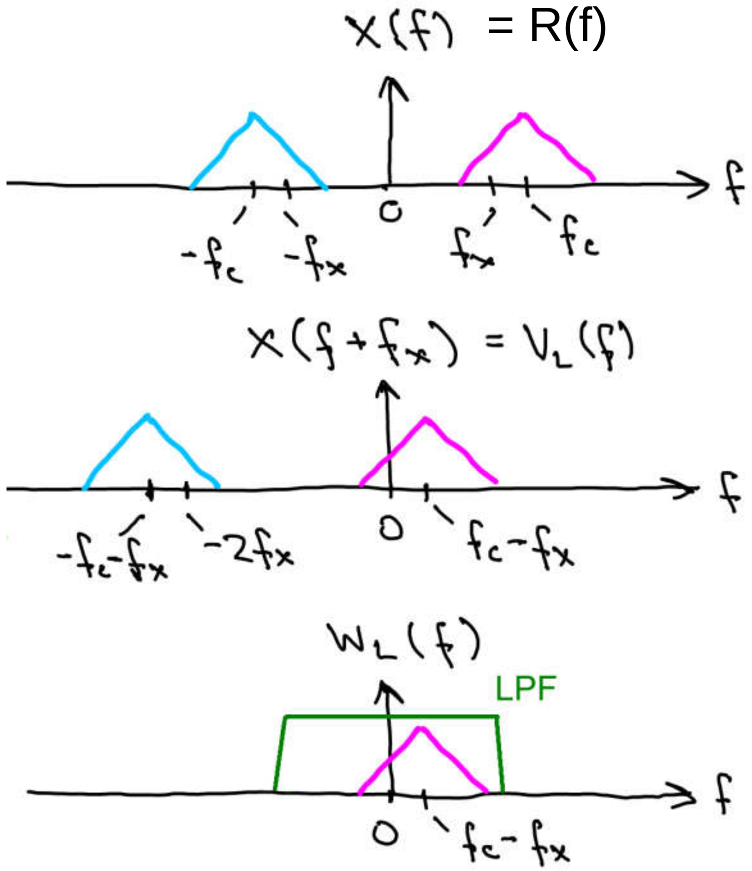



L. Gabrilovitch, 1936 (redrawn by T.G. Tucker). Used to separate AM signals with overlapping sidebands.

The modern form of the DCR with explicit I-Q signal outputs seems to have appeared only in the late 1970’s or early 1980’s.

# Complex-Valued Form of DCR




Multiplication by $e^{-j2\pi f_x t}$ is a frequency shift

$$x(t)\, e^{-j2\pi f_x t} \quad \Leftrightarrow \quad X(f + f_x)$$

# Direct Conversion Receiver

- Advantages
  - No image frequency problem since $f_{IF} = 0$
  - Most filtering done at baseband, can use DSP
  - Only one LO needed => less phase noise
- Disadvantages
  - DC offset and spurs from LO leakage
  - I-Q imbalance leads to crosstalk between I,Q channels
  - Flicker or 1/f noise which increases at low frequencies

# Other Effects for both SHR, DCR

- Amplifiers exhibit non-linearities and mixers are inherently non-linear devices
- Third order intermodulation products (IM3) affect both SHR and DCR, second order products (IM2) affect mostly DCR
- Phase noise of local oscillators affect SHR more than DCR
- Modern implementations use sampling and analog to digital conversion (ADC)
- Dynamic range is directly affected by number of bits of ADC, SQNR for 8 bits: 50 dB, 12 bits: 74 dB, 16 bits: 98 dB

# Intermodulation Distortion (IMD)

Model: $y(t) = k_0 + k_1 x(t) + k_2 x^2(t) + k_3 x^3(t) + \ldots$

Two-Tone Signal: $x(t) = A_1 \cos(2\pi f_1 t) + A_2 \cos(2\pi f_2 t)$

$x^2(t)$ has IM2 term: $A_1 A_2 \cos(2\pi(f_1 - f_2)t)$

$x^3(t)$ has IM3 terms: $\frac{3}{4} A_1^2 A_2 \cos(2\pi(2f_1 - f_2)t)$, $\frac{3}{4} A_1 A_2^2 \cos(2\pi(2f_2 - f_1)t)$

Define: $R_{IM2} = \frac{k_2 A^2}{k_1 A}$, $R_{IM3} = \frac{k_3 A^3/4}{k_1 A}$, for $A = A_1 = A_2$

Second order intercept (SOI or IP2) is $A$ for which $R_{IM2} = 1$

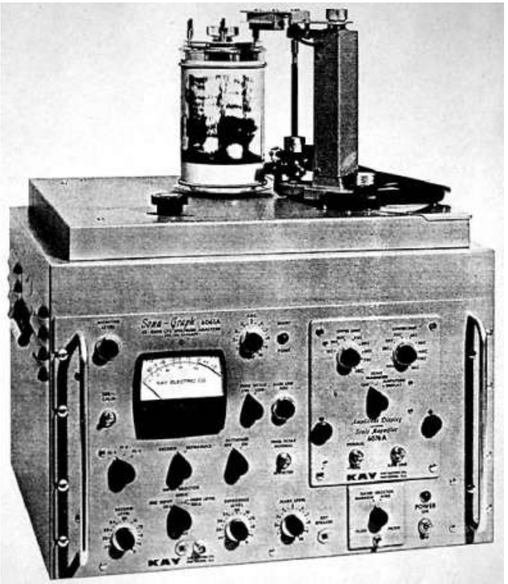
Third order intercept (TOI or IP3) is $A$ for which $R_{IM3} = 1$

Larger values for IP2, IP3 are better

# Spectrum/Signal Analyzers

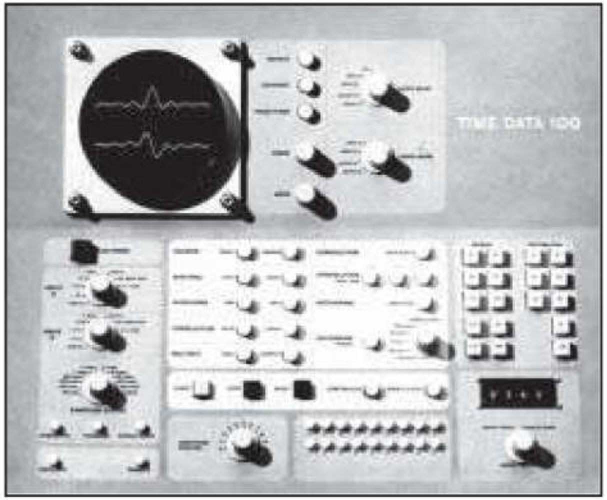
- Laboratory Grade Spectrum Analyzers
  - Some History
- SDRs as Spectrum Analyzers

# Some History



Spectrographs were used during WW2 to analyze “encrypted” voice

The first calibrated spectrum analyzer, 1964, with 2 MHz sweep width



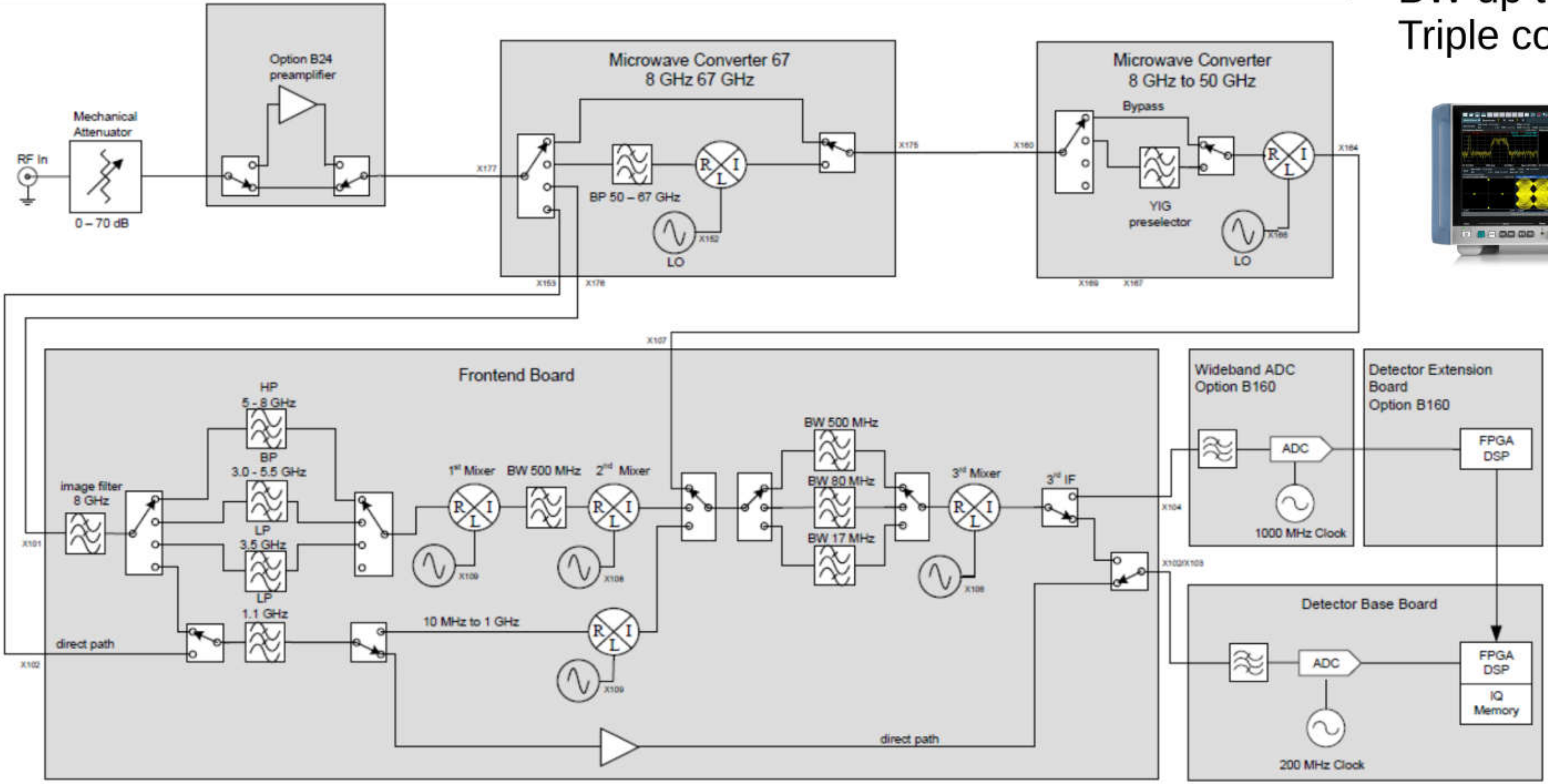
Control panel of first real-time spectrum analyzer using FFT. A 1024-point FFT takes 1 sec

# Spectrum Analyzers

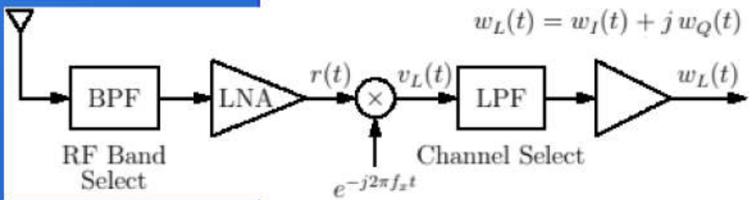
- Spectrum analyzer displays signal power versus frequency
- Two broad analyzer categories
  - Swept-tuned, magnitude only, sequential frequency bands
  - FFT-based, both magnitude and phase, simultaneous bands
- Most spectrum analyzers use SHR front-end
- Vector signal analyzers (VSA) combine superheterodyne technology with high-speed ADCs and digital signal processing to display spectra as well as analyze radar, video and communication signals from I-Q samples

# Block Diagram of High-End Spectrum Analyzer

Price: > 100k
20 Hz – 67 GHz
Up to 18 bit ADC
BW up to 500 MHz
Triple conv. SHR

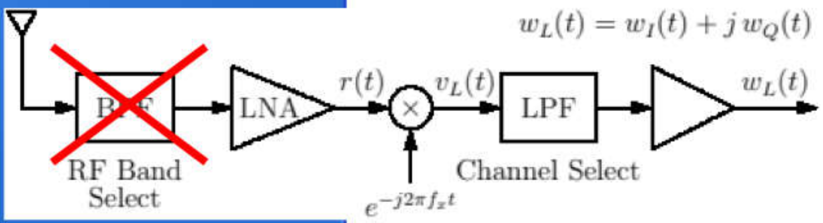


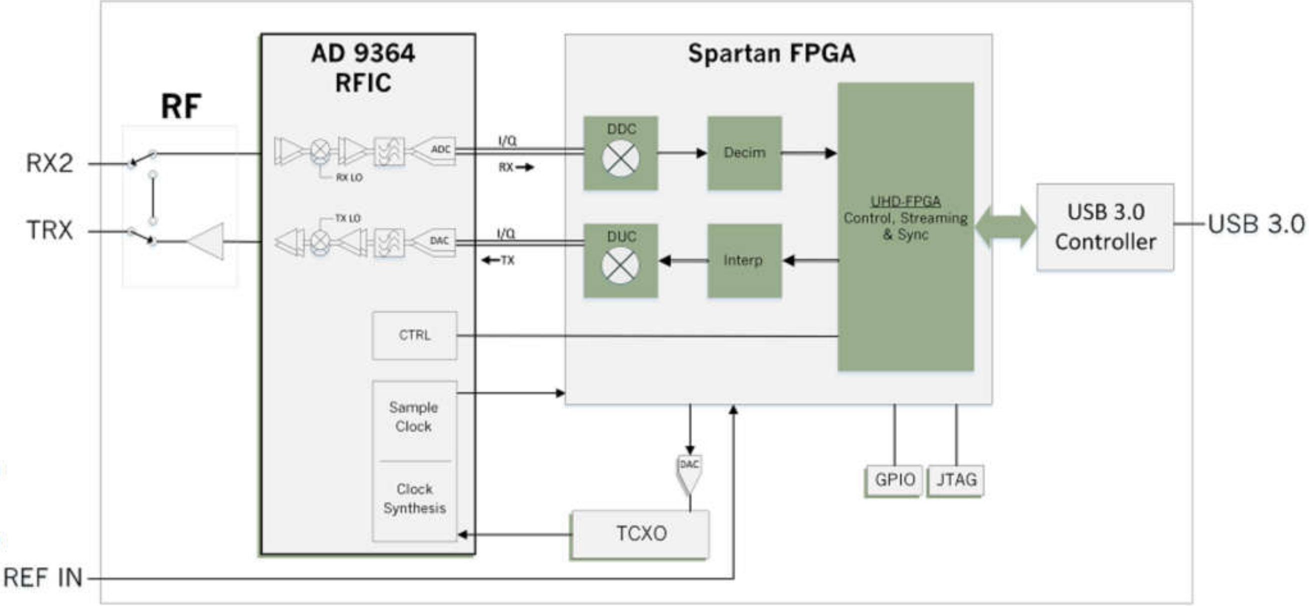

# SDRs as Spectrum Analyzers

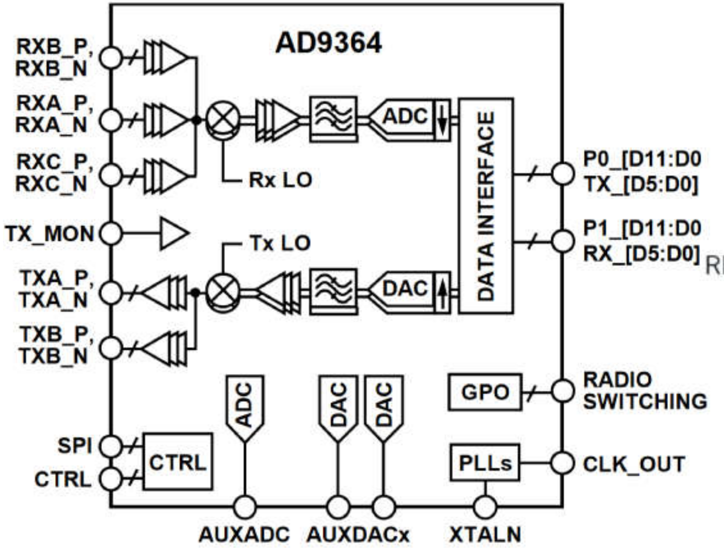



- To reduce cost, SDRs use DCR architecture with minimum of RF filtering
- Implementation as SoC (system on a chip), e.g. AD 9361
- SDRs are calibrated for frequency but not for power
- Higher end SDRs have FPGAs for on-board DSP
- Most signal processing and all display functions take place in external computer, e.g., using GNU Radio
- SDRs can act as VSAs when connected to a computer
- ADC resolution and bandwidth are more limited

# Typical Mid-Grade SDR



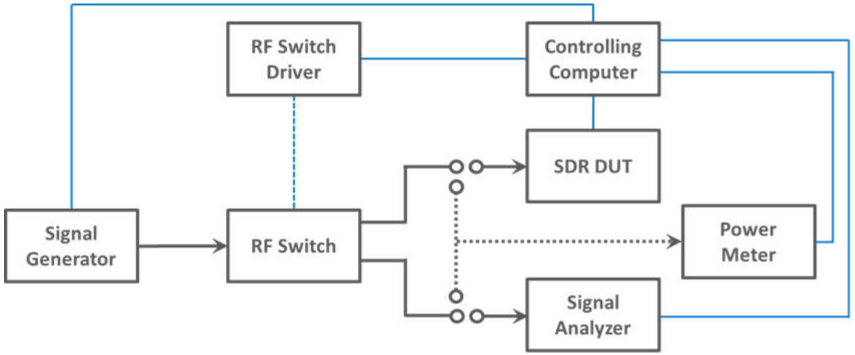



# Performance Measurements and Results

- Measurement Setup and Tools
- Mid-Grade SDR
- Economy-Grade SDR

# Measurement Setup and Tools

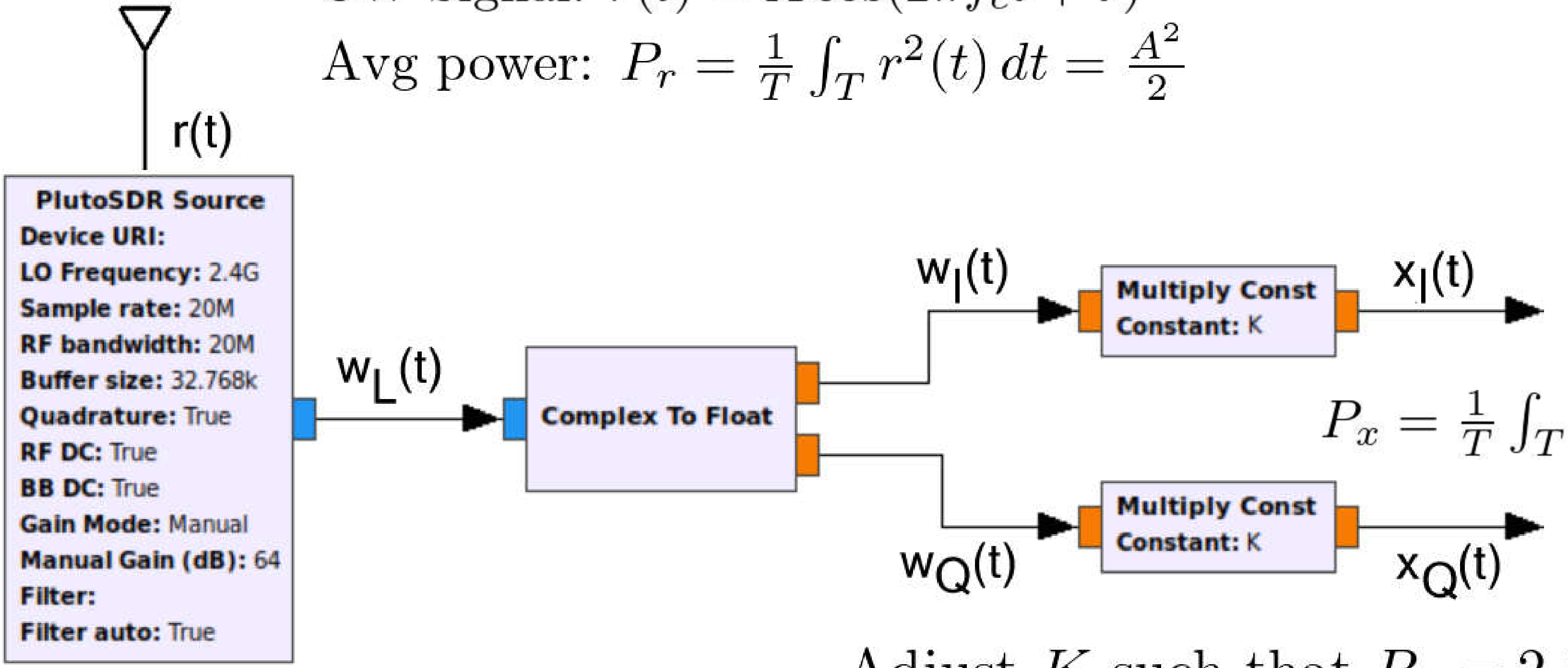
- Gain/power calibration vs freq
- Noise floor, noise figure vs freq
- 1-dB compression point vs freq
- Self-generated spurious response
- Dynamic range vs gain
- IP2 and IP3 vs freq and gain
- Phase noise measurement
- Long-term stability



# Gain Factor Calibration

CW Signal: $r(t) = A\cos(2\pi f_c t + \theta)$

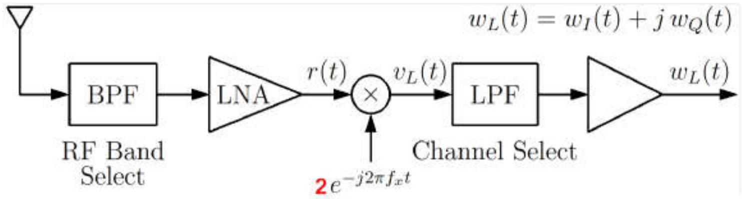
Avg power: $P_r = \frac{1}{T}\int_T r^2(t)\,dt = \frac{A^2}{2}$




$$P_x = \frac{1}{T}\int_T [x_I^2(t) + x_Q^2(t)]\,dt$$

Adjust $K$ such that $P_x = 2\,P_r$

# Gain Factor




There is no single "right" definition. DCR is voltage amplifier but input is real-valued and output is complex-valued. Here we make complex baseband power equal to **two** times input RF power.

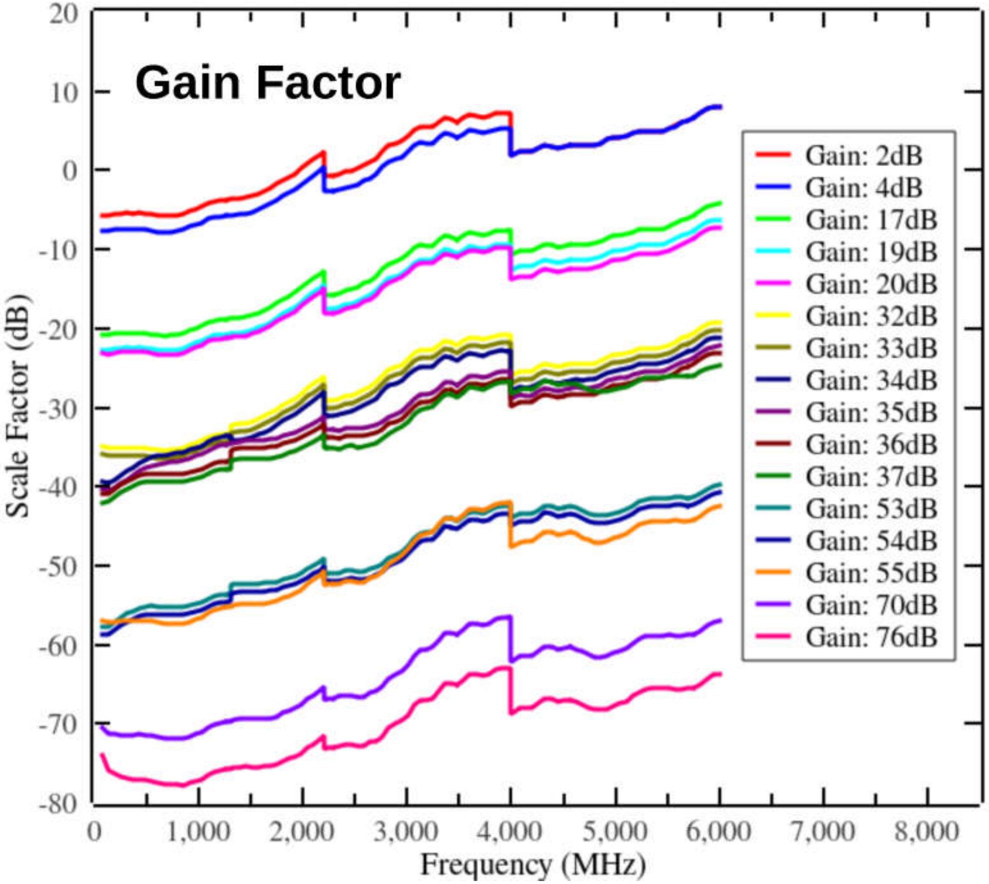
$$r(t) = A\cos(2\pi f_c t + \theta) \qquad \text{CW signal}$$
$$= \mathrm{Re}\{A e^{j2\pi f_c t} e^{j\theta}\}$$
$$= \frac{A}{2}\left[e^{j2\pi f_c t} e^{j\theta} + e^{-j2\pi f_c t} e^{-j\theta}\right]$$

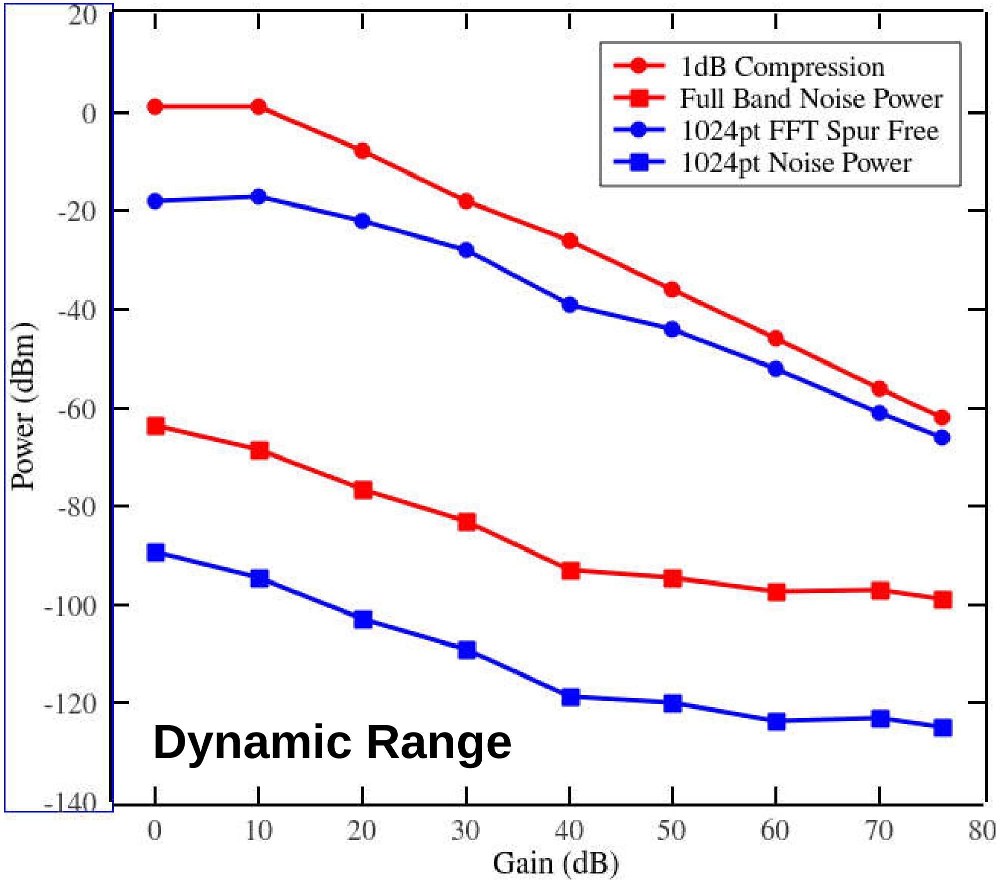
$$v_L(t) = r(t)\, e^{-j2\pi f_x t}$$
$$= \frac{A}{2}\Big[\underbrace{e^{j2\pi(f_c - f_x)t} e^{j\theta}}_{\text{passed by LPF}} + e^{-j2\pi(f_c+f_x)t} e^{-j\theta}\Big]$$

$$2\, w_L(t) = A e^{j2\pi(f_c - f_x)t} e^{j\theta}$$
$$= \underbrace{A\cos(2\pi(f_c - f_x)t + \theta)}_{= w_I(t)} + j\underbrace{A\sin(2\pi(f_c - f_x)t + \theta)}_{= w_Q(t)}$$

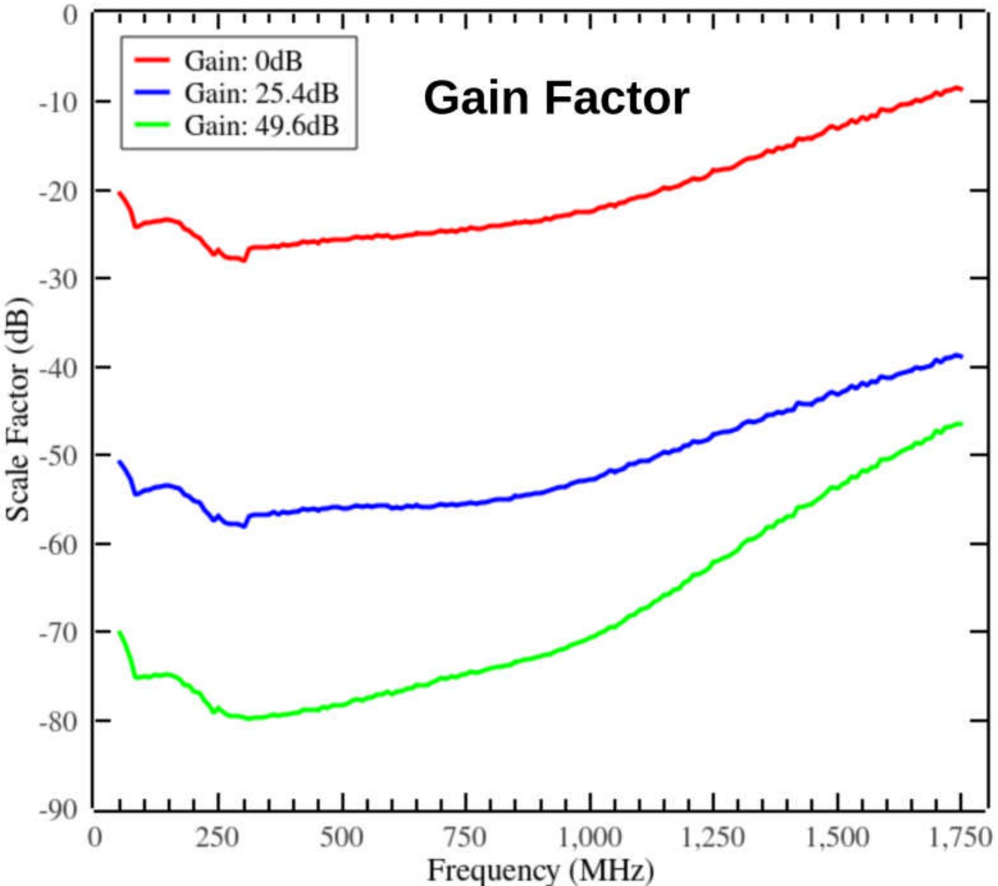
$$P_r = \frac{1}{T}\int_T r^2(t)\,dt = \frac{A^2}{2} \qquad \text{average power}$$
$$P_{w_L} = \frac{1}{T}\int_T |w_L(t)|^2\,dt = \frac{A^2}{2} + \frac{A^2}{2} = A^2 = 2P_r$$

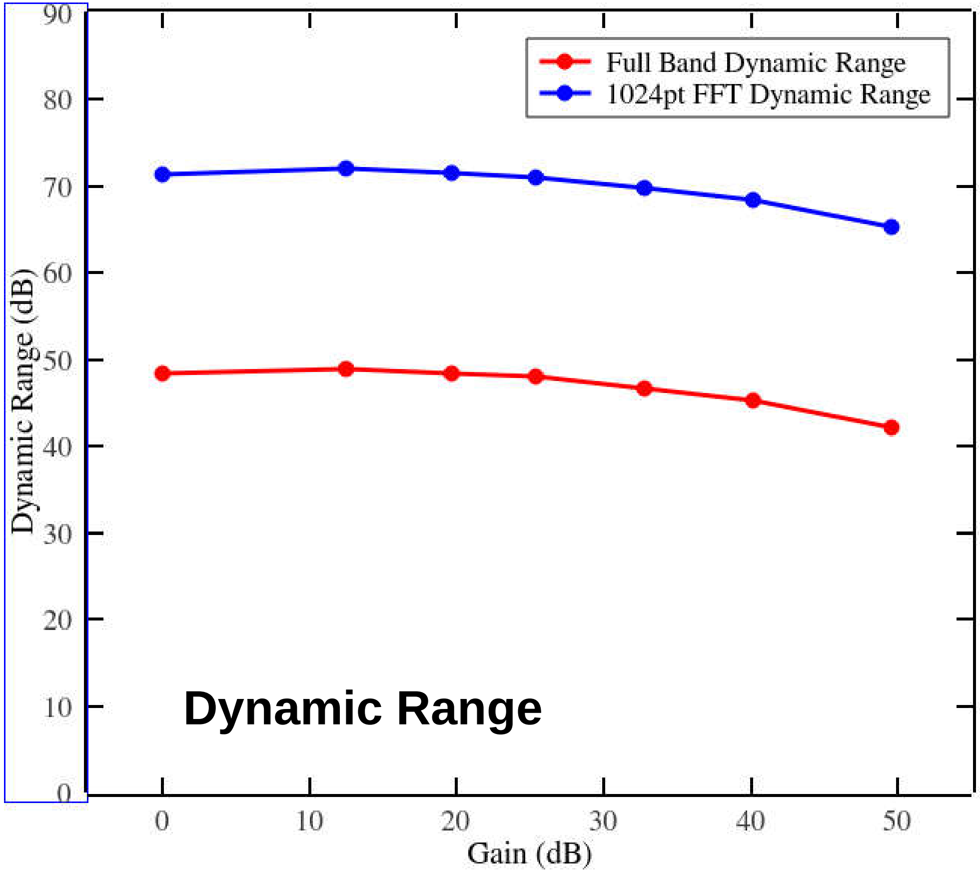
# Mid-Grade SDR



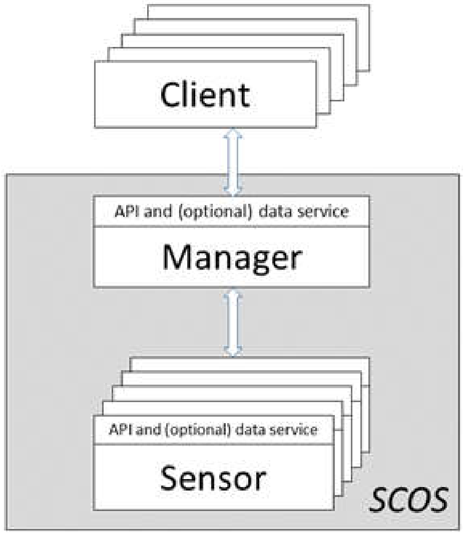
# Economy-Grade SDR



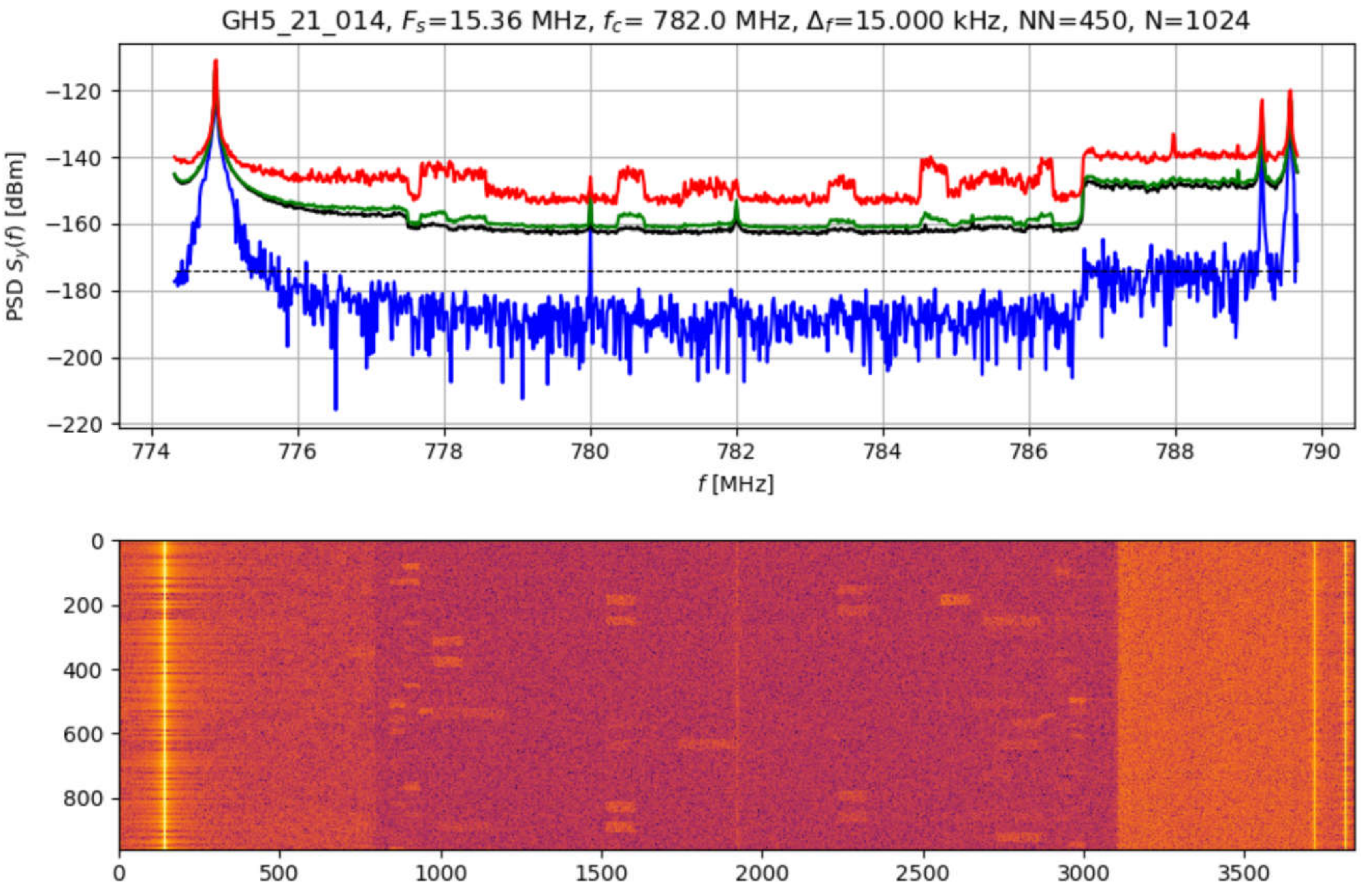
# SCOS

- SCOS: Spectrum Characterization and Occupancy, IEEE 802.22.3
- NTIA/ITS made first reference implementation (BWTB: Boulder Wireless Test Bed)
- SCOS is hardware agnostic
- Web-based interface for sensor tasking
- Data collected using SigMF metadata format
- Several sensors in Boulder and on CU campus active

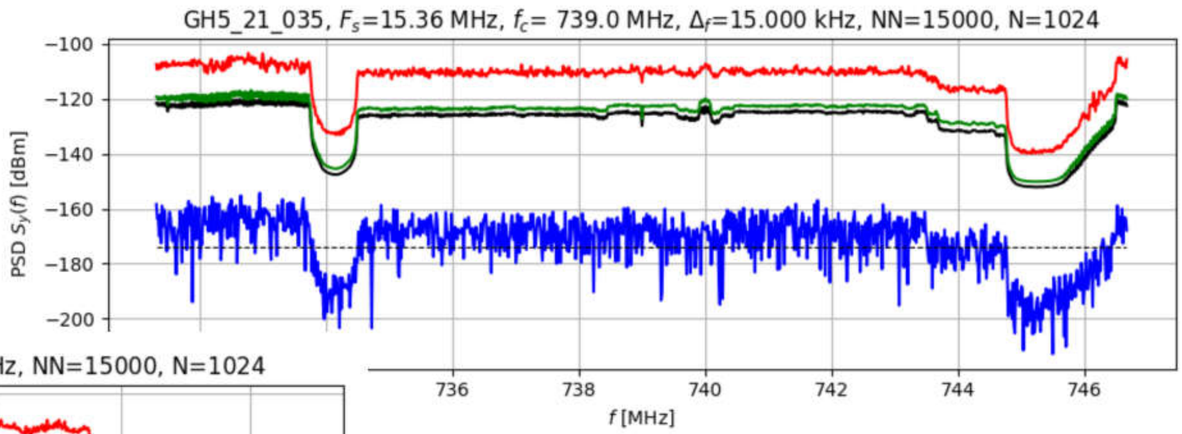


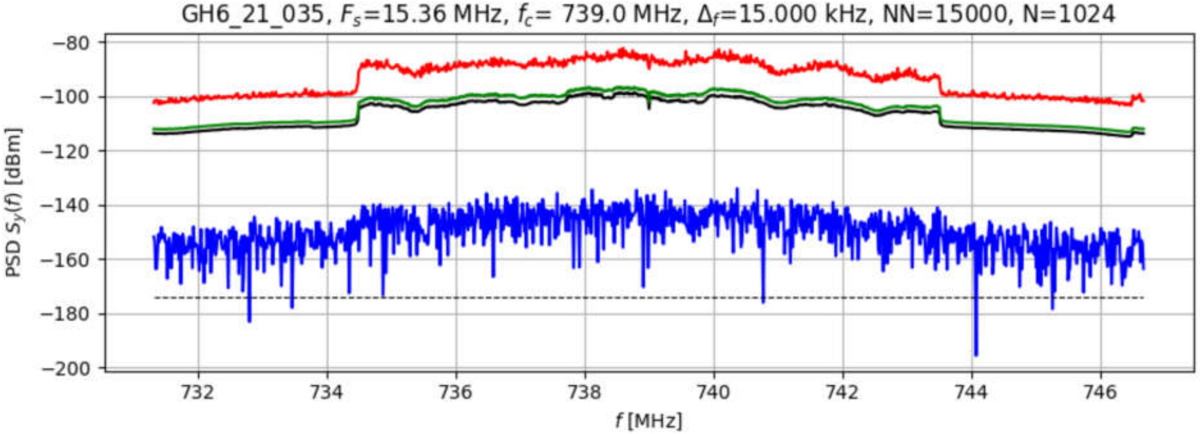
# LTE

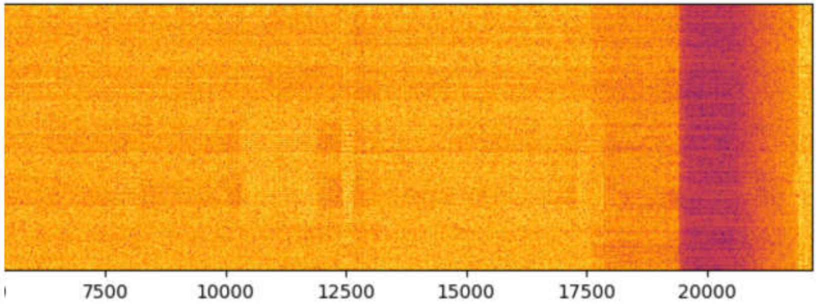
Spectrum of LTE uplink signal at 782 MHz. Noise figure ~14 dB.

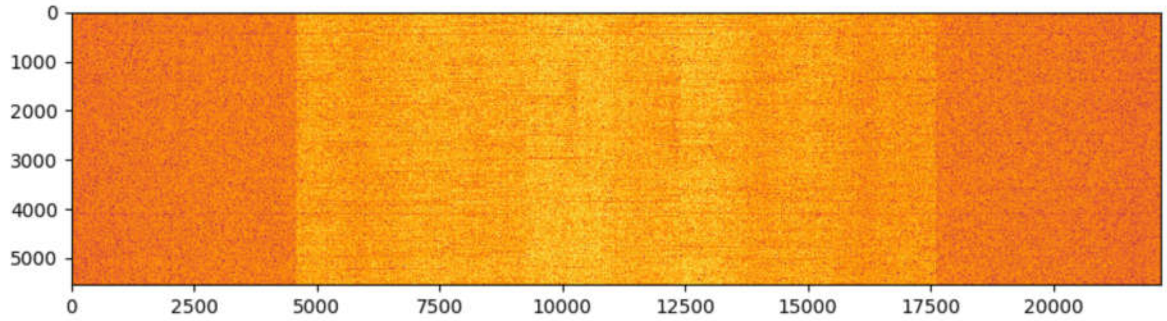


# DL, 739 MHz

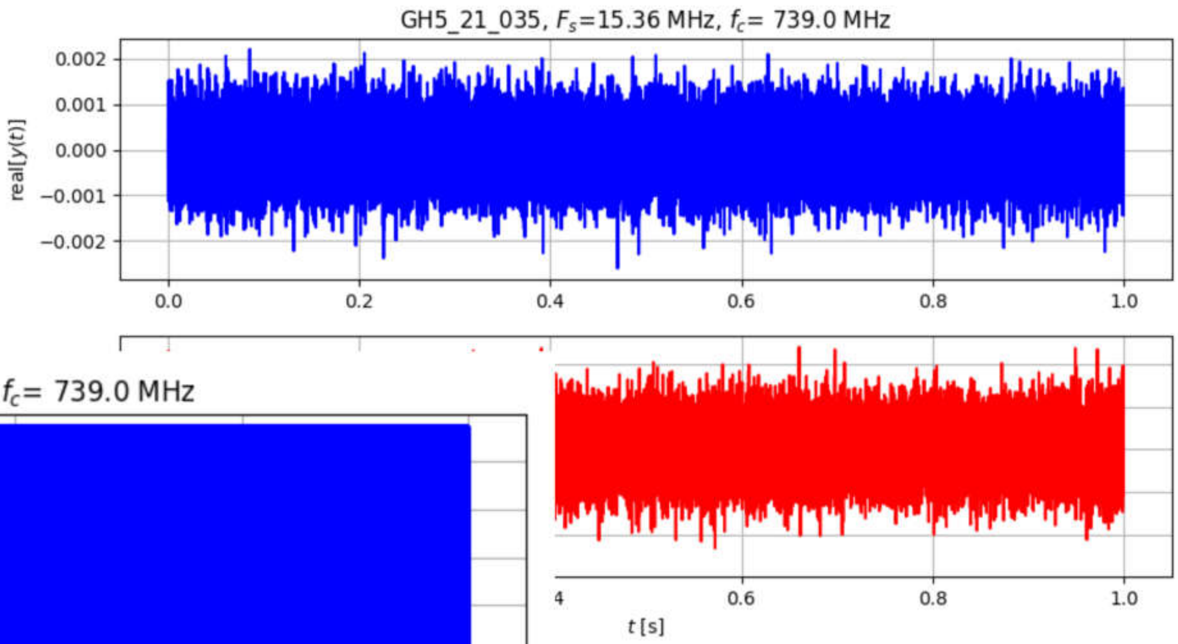

GH5_21_035, $F_s$=15.36 MHz, $f_c$= 739.0 MHz, $\Delta_f$=15.000 kHz, NN=15000, N=1024
PSD $S_y(f)$ [dBm]
−100
−120
−140
−160
−180
−200
736
738
740
742
744
746
$f$ [MHz]

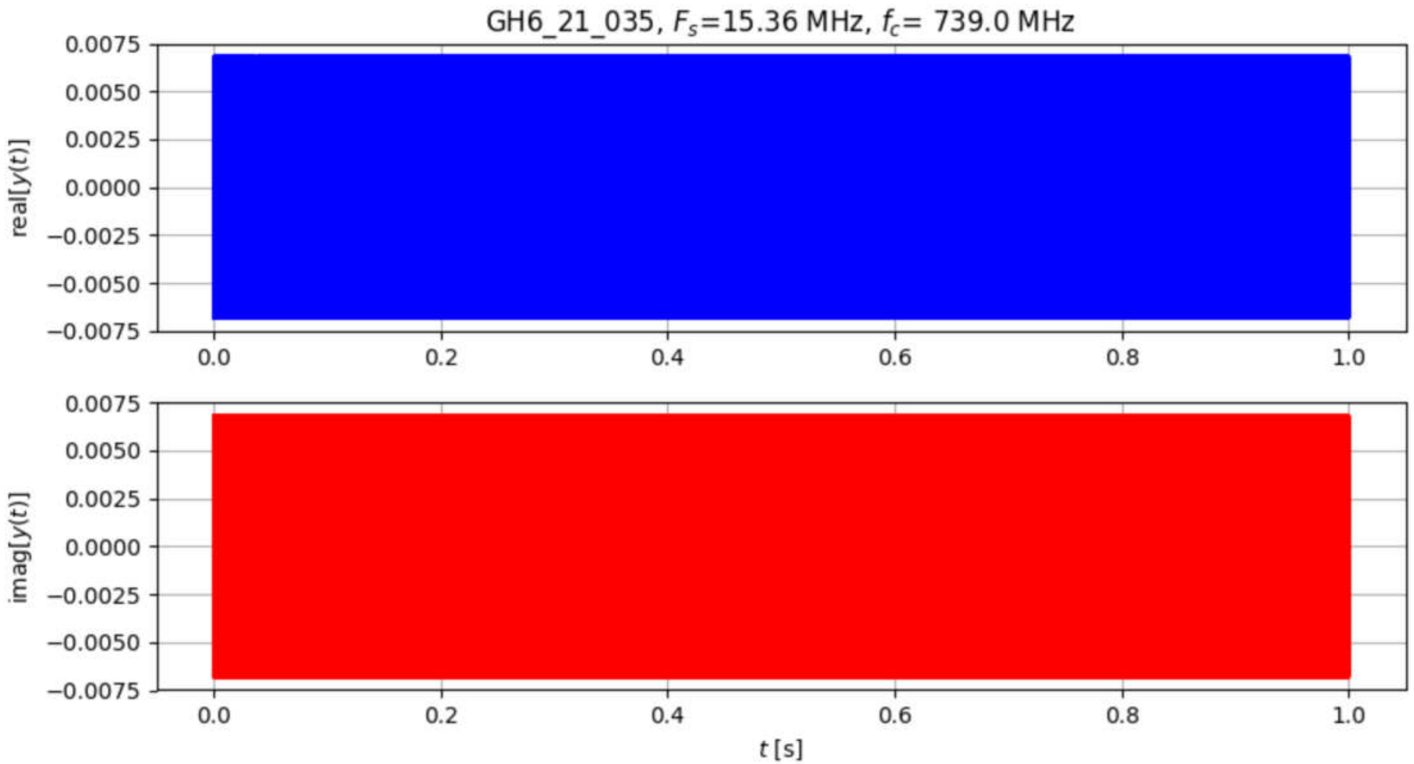

GH6_21_035, $F_s$=15.36 MHz, $f_c$= 739.0 MHz, $\Delta_f$=15.000 kHz, NN=15000, N=1024
PSD $S_y(f)$ [dBm]
−80
−100
−120
−140
−160
−180
−200
732
734
736
738
740
742
744
746
$f$ [MHz]


7500
10000
12500
15000
17500
20000


0
1000
2000
3000
4000
5000
0
2500
5000
7500
10000
12500
15000
17500
20000

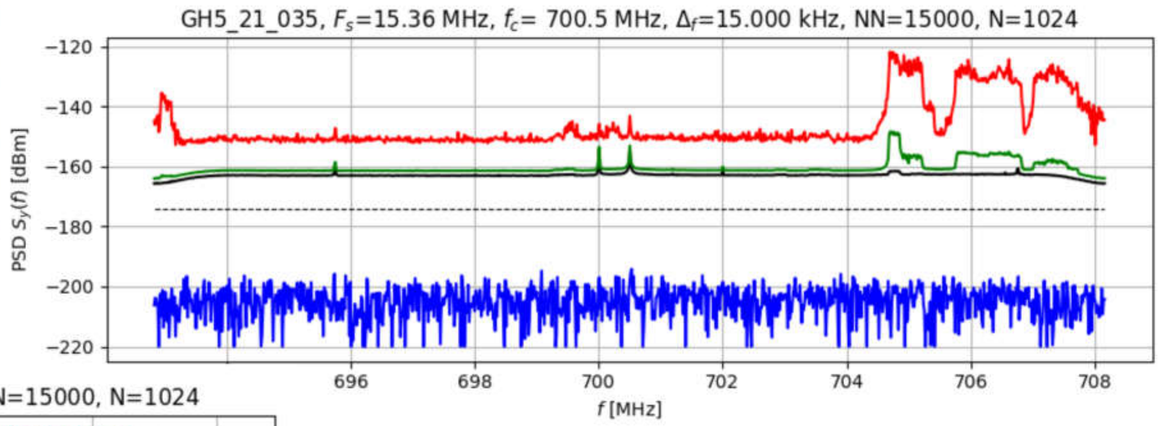
# DL, 739 MHz



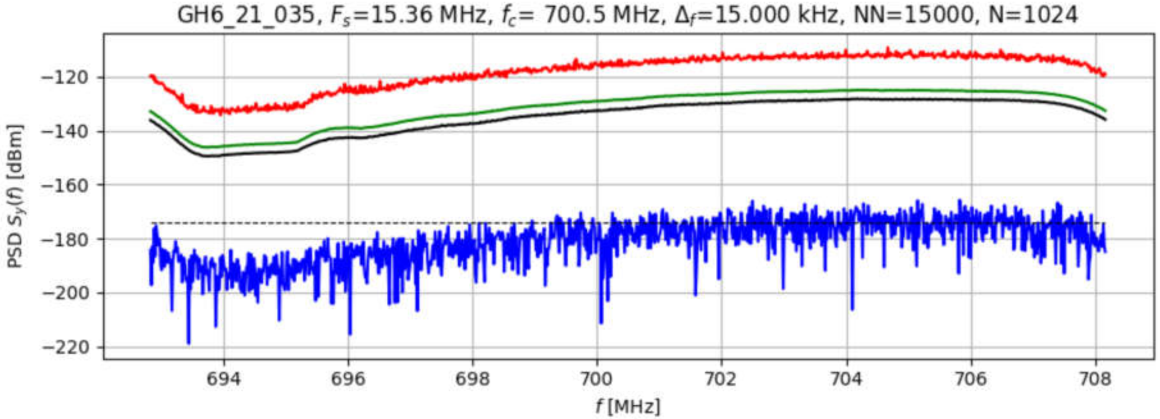




Time domain,
I-Q samples

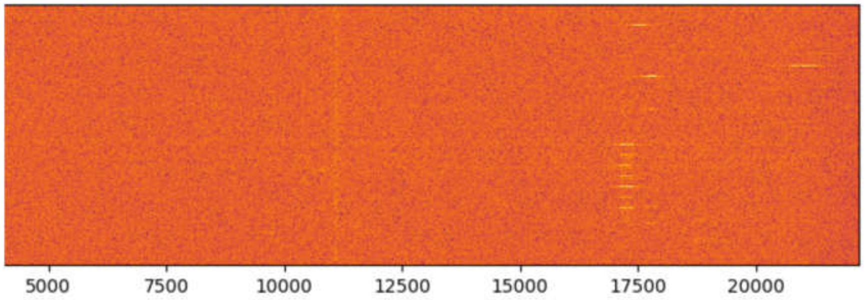
# UL, 700.5 MHz



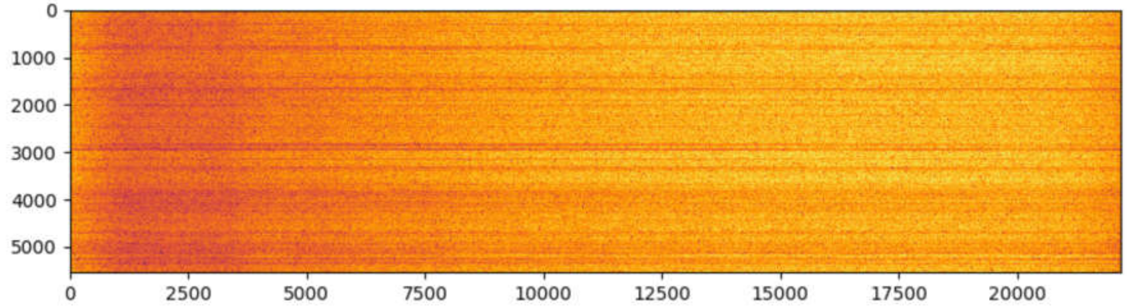
GH5_21_035, $F_s$=15.36 MHz, $f_c$= 700.5 MHz, $\Delta_f$=15.000 kHz, NN=15000, N=1024
PSD $S_y(f)$ [dBm]
−120
−140
−160
−180
−200
−220
696
698
700
702
704
706
708
$f$ [MHz]

GH6_21_035, $F_s$=15.36 MHz, $f_c$= 700.5 MHz, $\Delta_f$=15.000 kHz, NN=15000, N=1024
PSD $S_y(f)$ [dBm]
−120
−140
−160
−180
−200
−220
694
696
698
700
702
704
706
708
$f$ [MHz]

5000
7500
10000
12500
15000
17500
20000

0
1000
2000
3000
4000
5000
0
2500
5000
7500
10000
12500
15000
17500
20000

# Lessons to be Learned

- When calibrated, the selected mid-grade SDR performs very well.
- Gain, noise figure, and 1-dB compression point calibration versus frequency is necessary for each unit, but can be automated.
- The major problem is over-driving the RF front-end by strong out of band signals.
- This can be corrected using an RF band select filter (increases price and decreases versatility).

# Future Directions

- Increase number of sensors, decrease cost and size.
- Use sensor network for real-time RF propagation measurements exploiting existing transmitters.
- Create mobile network, e.g., using public transportation vehicles.
- Use machine learning (ML) to deal with sensor imperfections.
- Use ML to identify network anomalies and locate intentional and unintentional RF intruders.

# Acknowledgement

- I would like to thank my colleagues at ITS, in particular Todd Schumann for making all the sensor measurements and Jeff Wepman, Adam Hicks, Linh Vu, Heather Ottke, and Mike Cotton as discussion partners.