

Blind Signal Analysis

Balint Seeber, Applications Engineer



balint@ettus.com

[@spenchdotnet](https://www.spenchdotnet)

Notes and links in PDF comments on each slide

Recap

- Lots of different types of satellites
- Variables:
 - Purpose: comms, weather, MIL, amateur
 - Payload: transponders, cameras/sensors
 - Orbit: **L**ow **E**arth **O**rbital, geostationary (geosync)
 - Frequencies: uplink, downlink, beacon, command
- Two categories:
 - **Intelligent**: communication with on-board systems
 - **Dumb**: relay information with linear transponders

Wide-area re-broadcast

- RF megaphone (e.g. satellite TV)
- Single dish sends beam on uplink to satellite
- Linear transponder shifts raw RF to downlink frequency, re-transmitted via spot beams
- Cover any entire country

- Linear transponders are **dumb**: re-broadcast anything onto coverage area



TT&C and UPC

- **T**elemetry, **T**racking and **C**ommand
- Need to be able to send commands to satellite
 - Change payload configuration
 - Multiplexing
 - Switch between redundant systems
 - Orbit
- Check on health of satellite/payload
 - Beacon + telemetry
- Measure affect of weather (combat rain fade)
 - **U**plink **P**ower **C**ontrol
 - Turn up transmitter power (keep at min. = save \$\$\$)

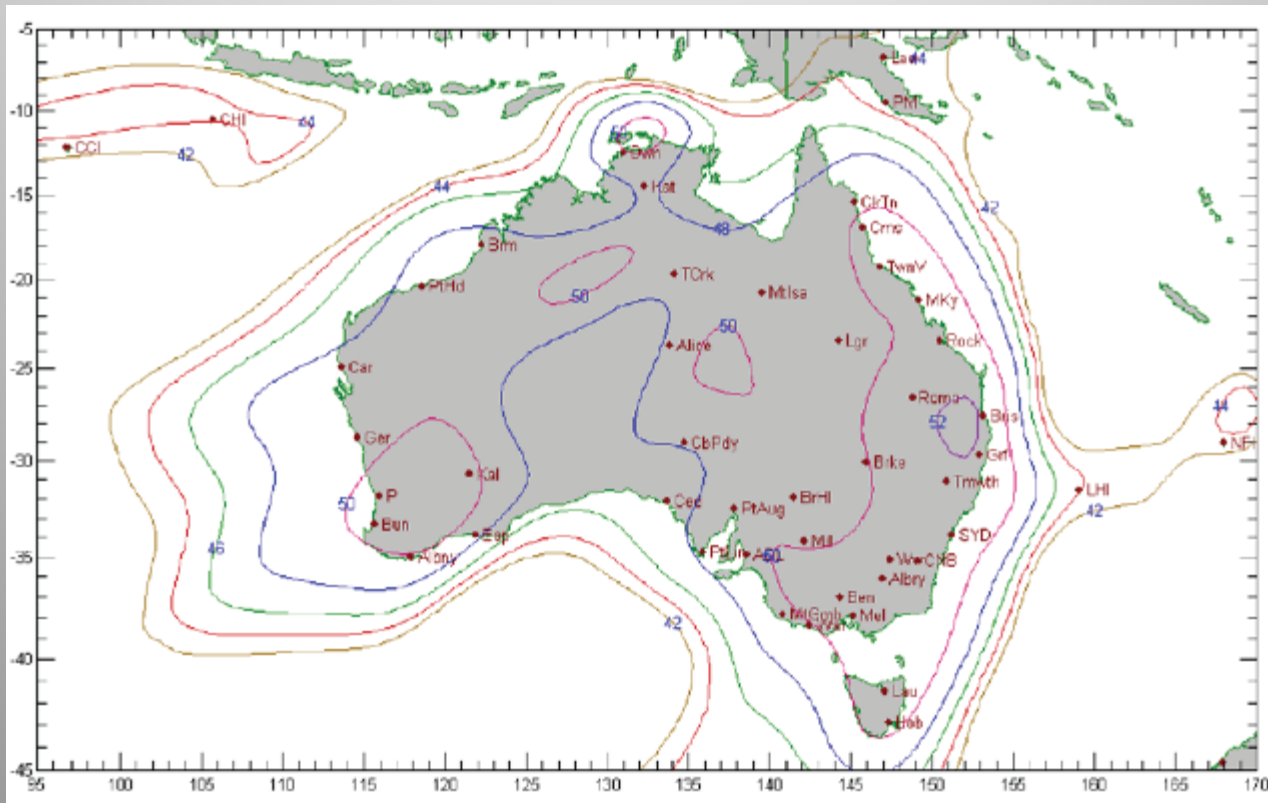


Optus D1



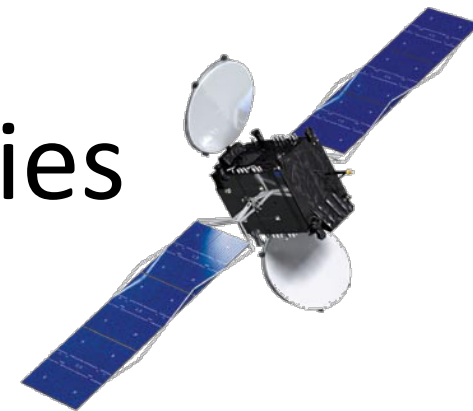
- 24 Ku band transponders
 - Multiplexed spot beams service Aus and NZ
 - Uplink: 14.0 - 14.5 GHz
 - Downlink: 12.25 - 12.75 GHz
 - Bandwidth: 54 MHz
- Mainly TV (wideband DVB-S)
 - ABC, SBS, Se7en, Nin9, SkyNZ
- Some other (narrowband) things...

FNA Beam Coverage

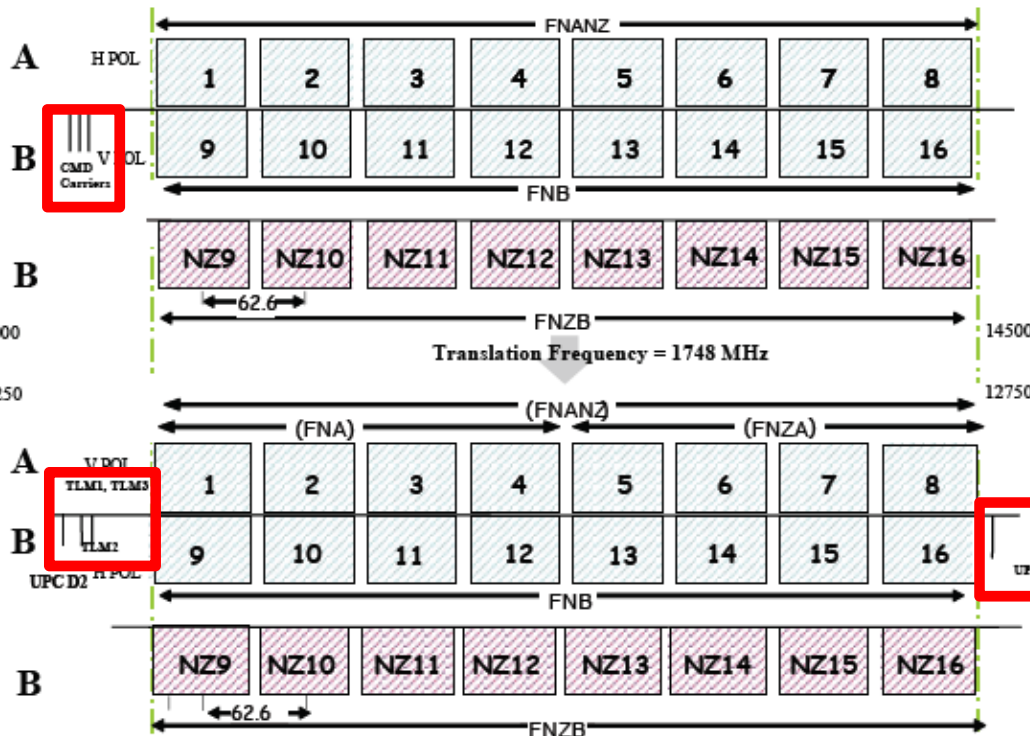


Effective Isotropic Radiated Power (EIRP)

D1 Channel Frequencies



Uplink



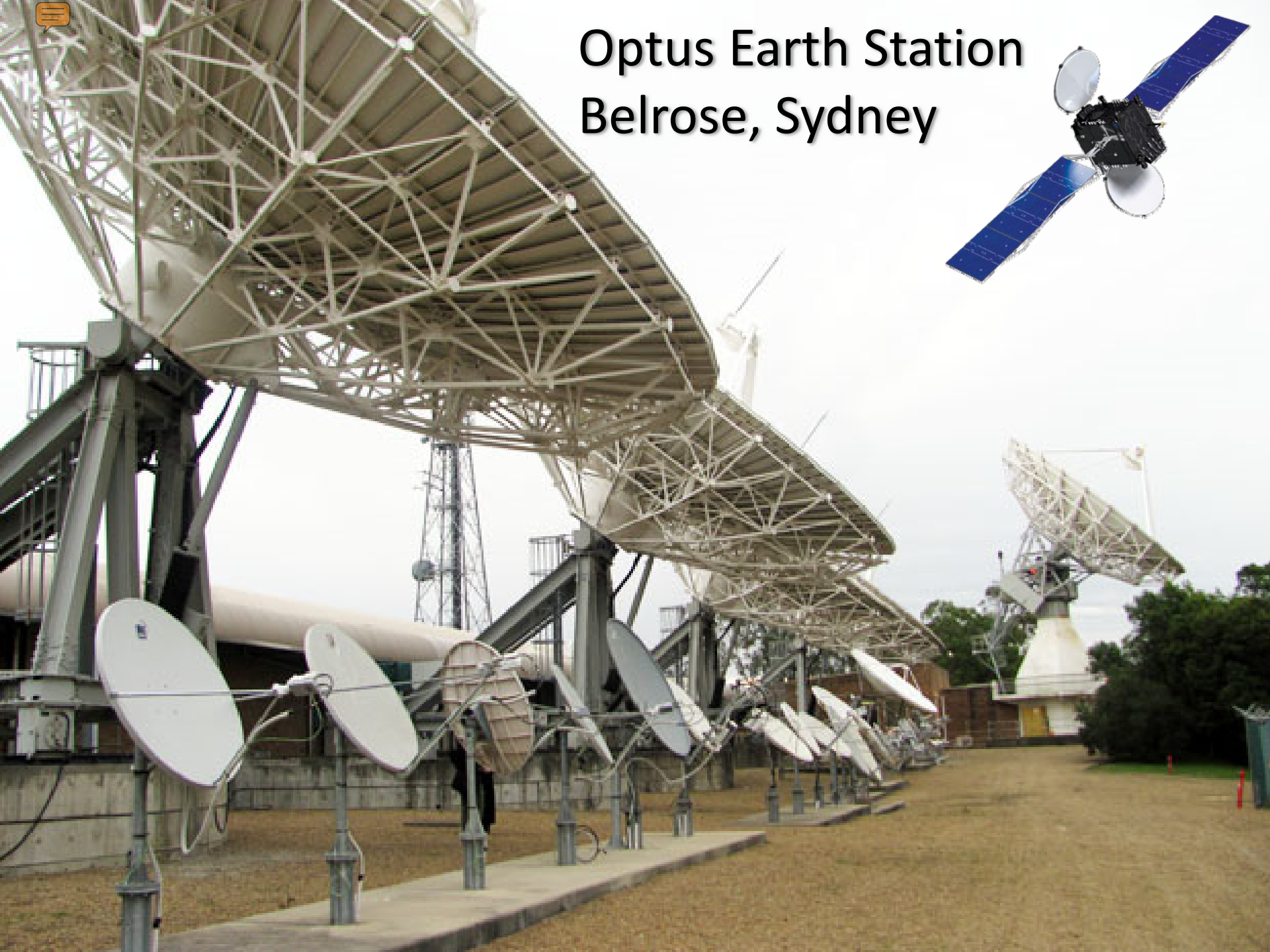
FSS Australia Centre Frequencies (MHz)		
Channel	Uplink	Downlink
1	14029.90	12281.90
2	14092.50	12344.50
3	14155.10	12407.10
4	14217.70	12469.70
5	14280.30	12532.30
6	14342.90	12594.90
7	14405.50	12657.50
8	14468.10	12720.10
9	14029.90	12281.90
10	14092.50	12344.50
11	14155.10	12407.10
12	14217.70	12469.70
13	14280.30	12532.30
14	14342.90	12594.90
15	14405.50	12657.50
16	14468.10	12720.10
TLM1		12243.25
TLM2		12245.25
TLM3		12243.25
UPC		12749.50

FSS NZ Centre Frequencies (MHz)		
Channel	Uplink	Downlink
NZ9	14029.90	12281.90
NZ10	14092.50	12344.50
NZ11	14155.10	12407.10
NZ12	14217.70	12469.70
NZ13	14280.30	12532.30
NZ14	14342.90	12594.90
NZ15	14405.50	12657.50
NZ16	14468.10	12720.10

Downlink

D1

Optus Earth Station Belrose, Sydney





Challenger Drive

Description Optus Earth Station, Challenger Drive, BELROSE

Address Belrose NSW 2085

Position -33.7173419166118, 151.211467206693

<< first < prev 1 2 3 4 5 6 7 8 next > last >>

Icon	Freq	Em Des	Client	Links	Menu
	12.765 GHz	28M0G7W	3GIS Pty Limited	1	▶
	13.031 GHz	28M0G7W	3GIS Pty Limited	1	▶
	13.087 GHz	28M0G7W	DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED	1	▶
	12.821 GHz	28M0G7W	DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED	1	▶
	13.031 GHz	28M0F7W	DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED	1	▶
	12.765 GHz	28M0F7W	DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED	1	▶
	10.735 GHz	40M0D7W	Foxtel Management Pty Limited	1	▶
	11.225 GHz	40M0D7W	Foxtel Management Pty Limited	1	▶
	10.815 GHz	40M0D7W	Foxtel Management Pty Limited	1	▶
	11.305 GHz	40M0D7W	Foxtel Management Pty Limited	1	▶

< first < prev 1 2 3 4 5 6 7 8 next > last >>

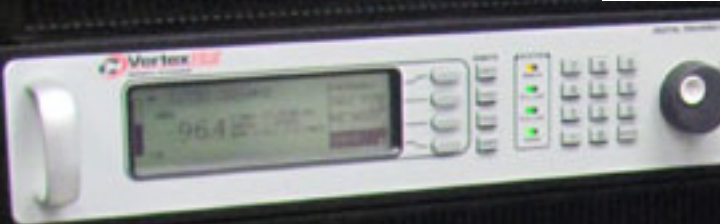
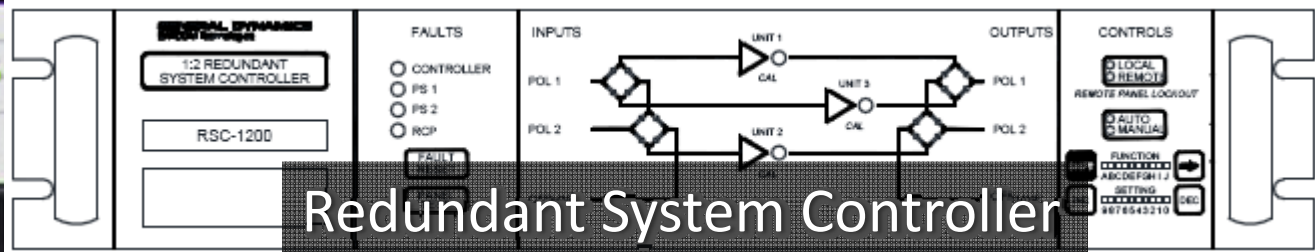
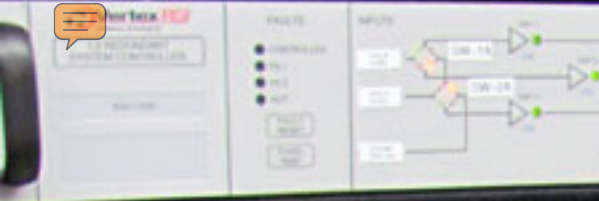


Spot the
satellite
modem



Radyne Comstream
Satellite Modem
DMD-15

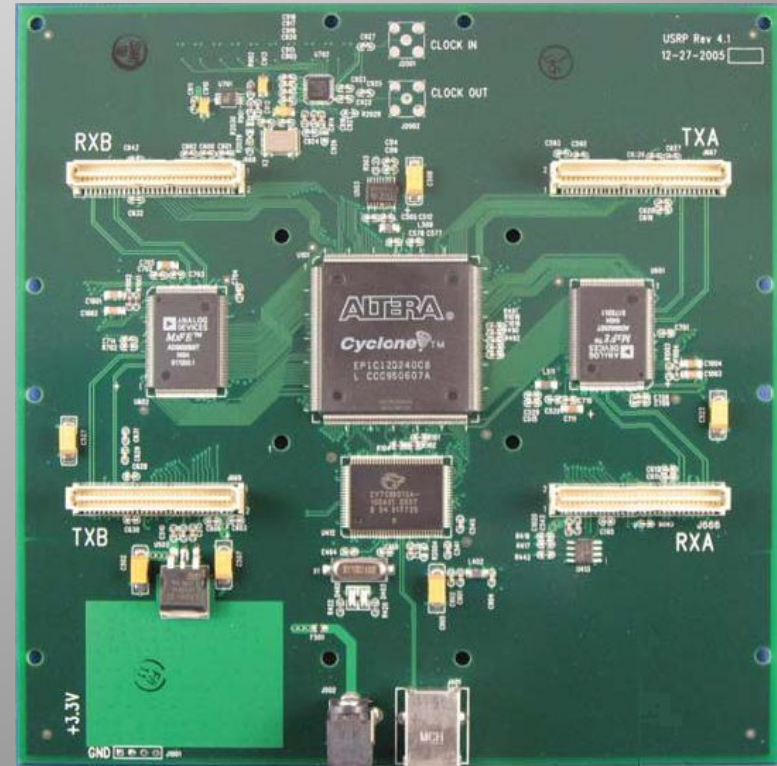
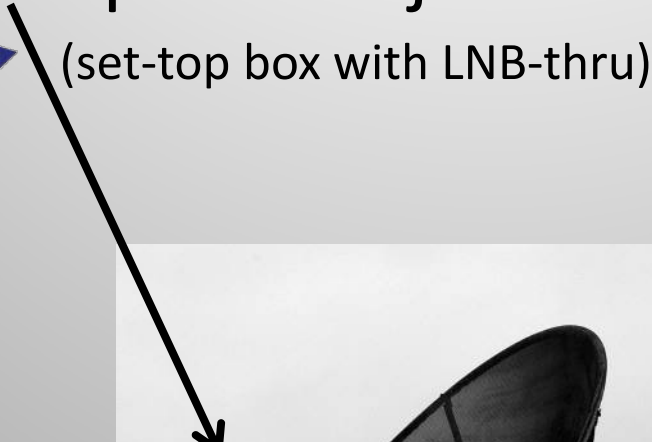
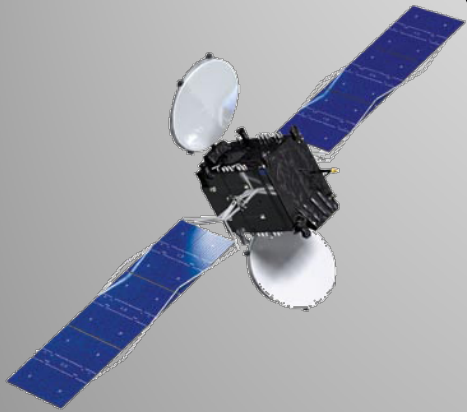






What you need

Dish + LNB + power injector + USRP + GNU Radio
(set-top box with LNB-thru)





Low Noise Block down-converter



Subtract 11.3 GHz from downlink frequency: 950 - 1450 MHz

Ku Band High Power TM Transmitters



Applications

- Satellite TC&R subsystems
- Telemetry and ranging transmission and modulation

Main features

- Ku Band
- Compatible with most of bus interfaces (command & telemetry formats)
- Power supplies 22 to 100V
- High power output, 8W EOL, 10W BOL (through SSPA)
- Flight Proven design
- Modulation Index selection
 - By Command
 - Automatic according to modulating tones number

Technologies

- Microwave Integrated Circuit
- Surface Mount Printed Circuit Board
- Thick Film Hybrid

Background

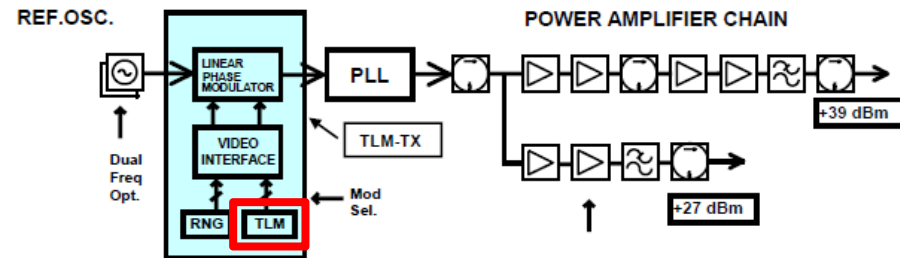
- AMC 14 - AMC 15 - AMC 16
- BSAT 2 A - BSAT 2 B
- BSAT 2 C
- BSAT3A
- ECHOSTAR 10
- ECHOSTAR 7
- GE 2A (NIMIQ2)
- HORIZON 2
- JCSAT 10
- JCSAT 11
- JCSAT 9
- NEWSKIES 6
- NEWSKIES 7
- OPTUS D1
- OPTUS D2
- Panamsat 11
- RAINBOW
- Thor2

Technical Description

- The unit consists of two modules:
 - MPLL module
 - Baseplate module

- The baseplate module houses the DC/DC converter board, which supplies the power voltages to the RF section, and the telemetry interface board, and the Solid State Power Amplifier (SSPA).
- The MPLL module includes all the microwave and RF circuitry to generate and modulate the Ku-band carrier. The modulation inputs interface is implemented on the Telemetry Interface board that is usually tailored on customer's requirements
- The reference crystal oscillator generates a frequency at about 100 MHz, depending on the exact transmitter frequency. The design is based upon a grounded-base configuration with an AT-cut quartz crystal resonator, oscillating in overtone mode. An analog thermal compensation network is implemented.
- Modulation indices may be selected by commands or, as option, automatic selection may be implemented. In this case a specific circuit keeps constant the total power of the modulation signal in presence of one, two or three input signals, in whatever combination
- The signal level emerging from the loop is about +10dBm. The following medium power Ku-band amplifier chain provides +27 dBm power level; it is composed by three single ended stages using GaAs FET devices. The following SSPA, delivering 8W E.O.L. power level, is a single ended design, based on two power GaAs FET devices
- As an option, the unit can be equipped with an extra, independent amplifier chain, having an output power up to 0.5 W E.O.L. In this case the transmitter unit can operate in two functional modes: low power mode (0.5W), with high power output isolated (<-30dBm) and high power mode (8W), with low power output isolated (-15dBm)

Ku Band High Power Telemetry Transmitter Block Diagram



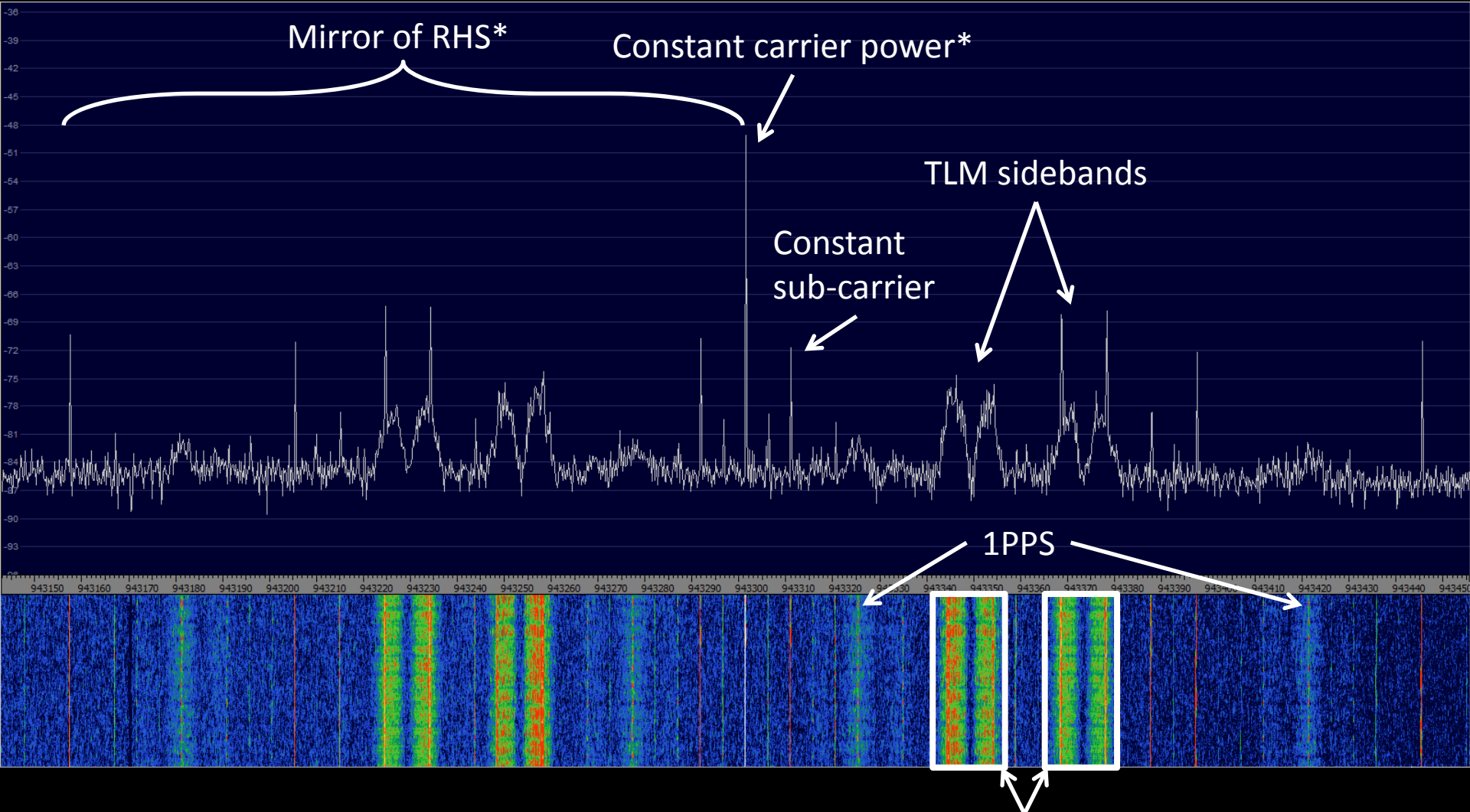
Main Performances

Output Frequency	10.7 – 12.7 GHz
Frequency Stability	± 10 ppm Std Stability Opt ± 5 ppm High Stability Opt
Output Power Level	≥ 38.5 dBm (7W) EOL, up to 40dBm (10W) BOL (25C)
Extra Output	≥ 27 dBm EOL Dual Power Opt
Output Phase Noise	< 4 deg _{rms} @ 10 Hz to 1 MHz
PM modulation index	Up to 2.4 radpk
Mod.Index Selection	By command Automatic according to mod.tones number
Modulation Linearity	± 3%
Modulation Op.Mode	TM1, TM2, RNG1, RNG2, RNGS + TMs
DC/DC converter	55/71V – 22/43V (16Vpp max in the range for best efficiency)
Command Interface	HLC
Qualification Temp. Range	-25 / +65 °C

Mass, Dimensions and Consumption

DC Power Consumption	High power mode <55W Low power mode <18W (Dual Power Opt)
Mass Properties	< 2 kg
Outline Dimensions	250 x 130 x 80 mm

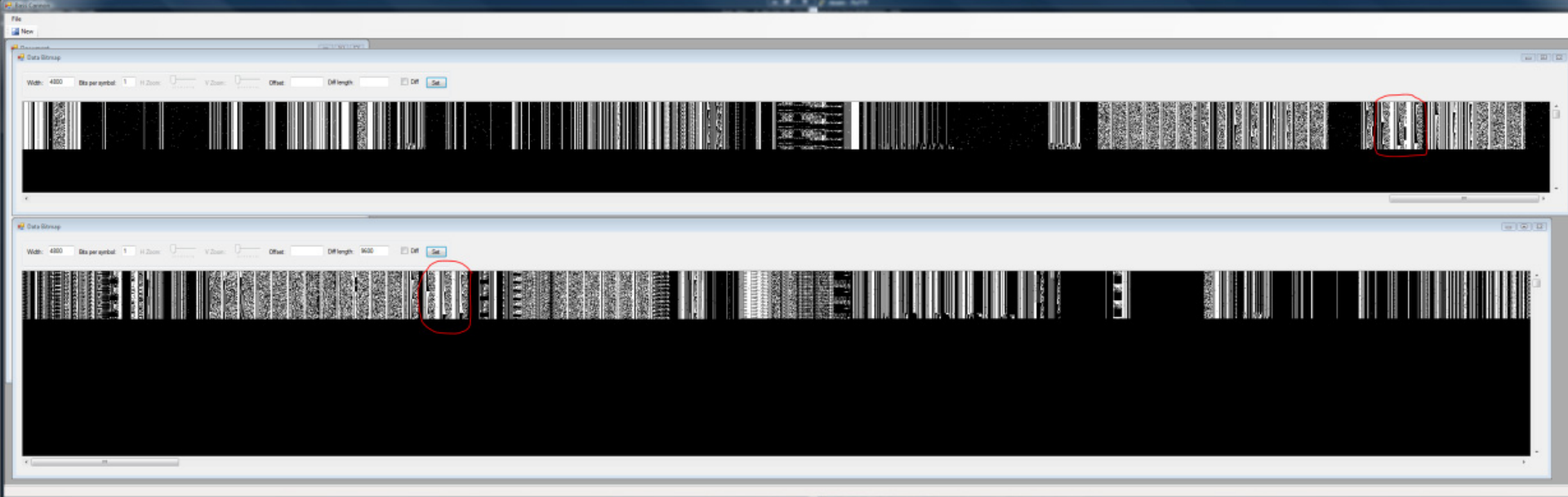
D1 TLM1: 12243.25 MHz

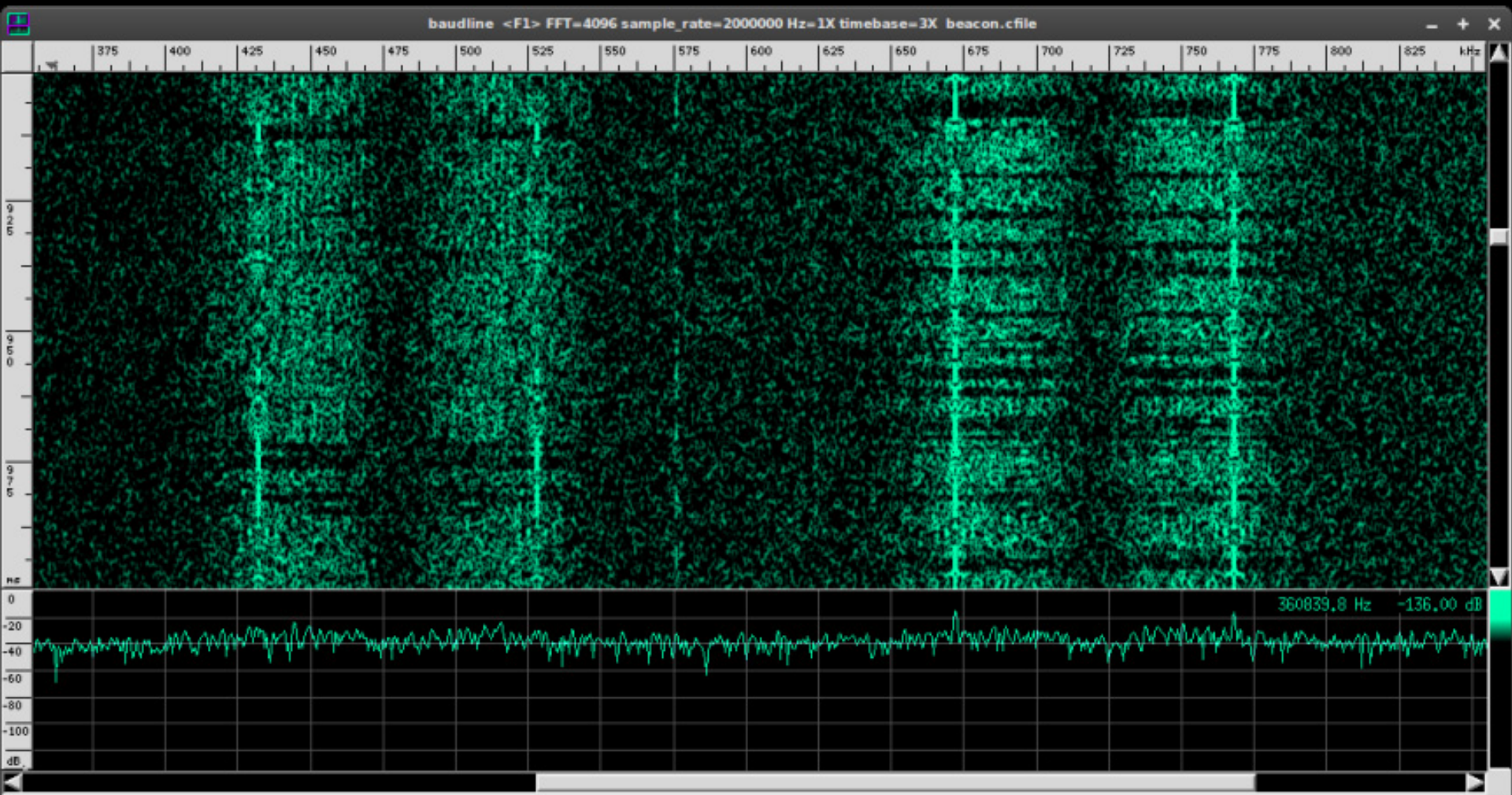


Beacon with **Phase Modulation*** (PM): 1PPS and two telemetry streams (sidebands)



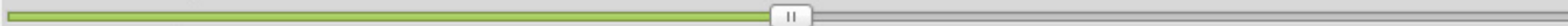
Visualisation





BB Scope Demod Pow Cyclo FAC # Quad Mag Test

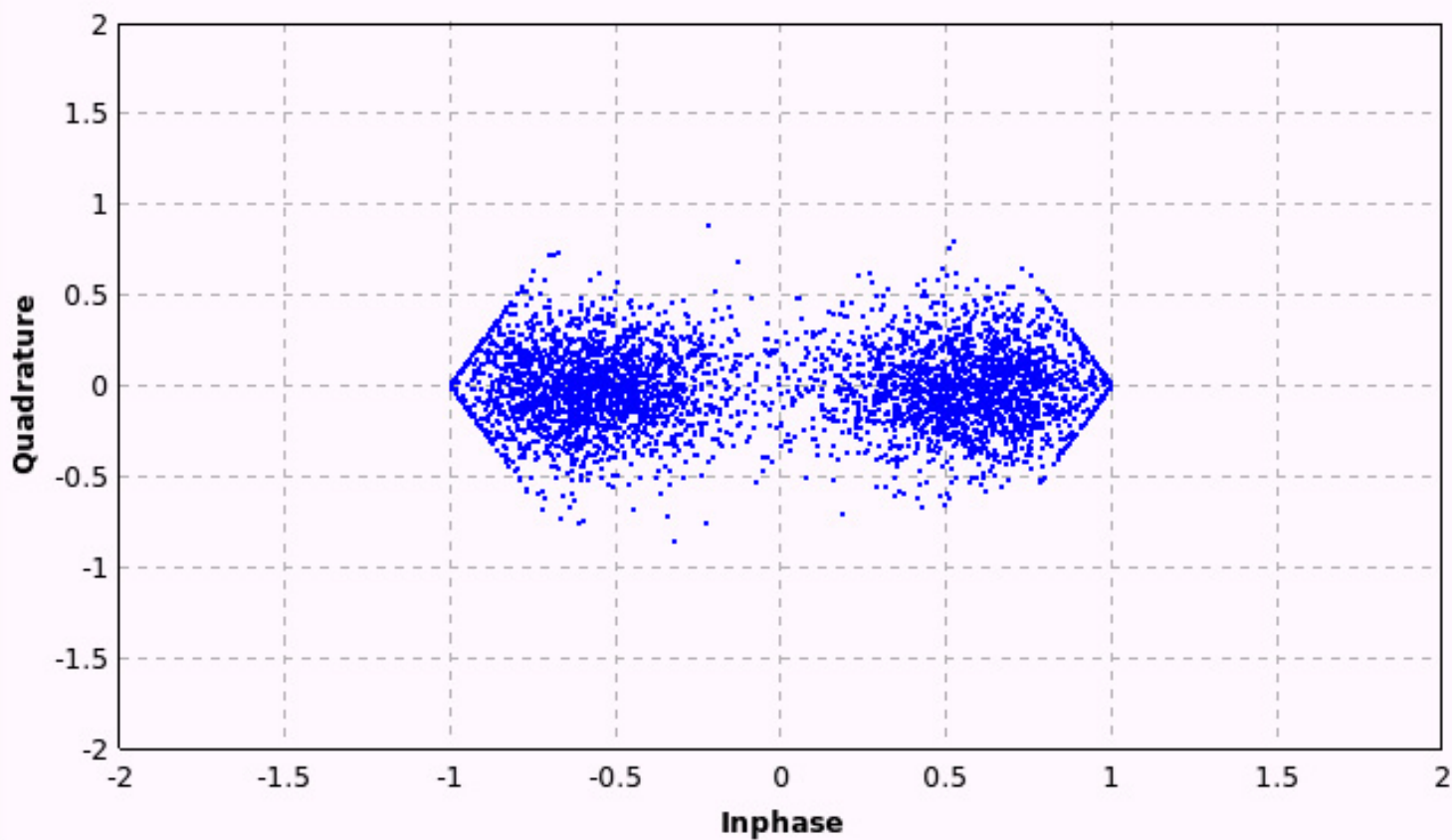
Symbol rate (fine): 0



sym_rate_coarse: 0

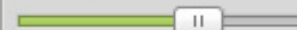


Symbol rate: 9600



Options

Alpha: 5m



Gain Mu: 5m

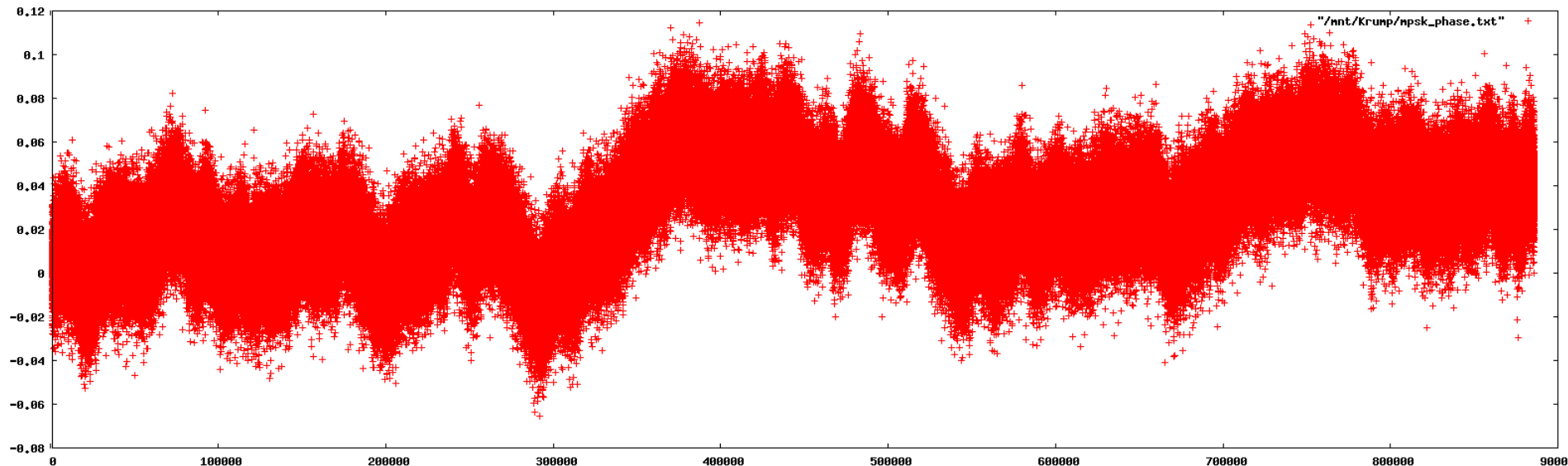
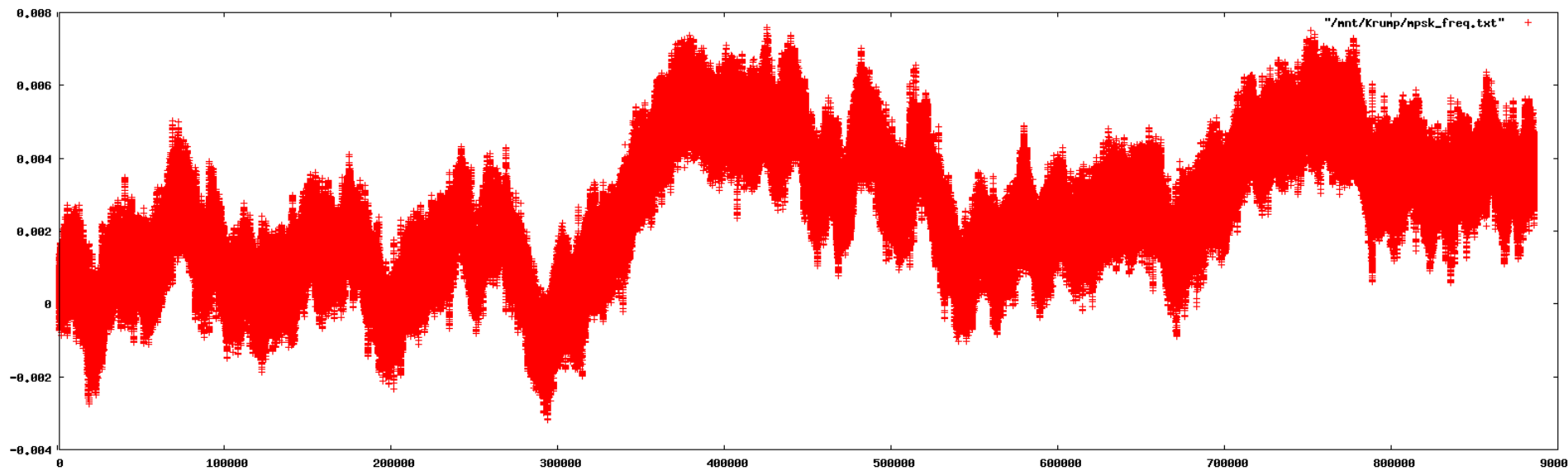


Marker: Dot Medium



Run

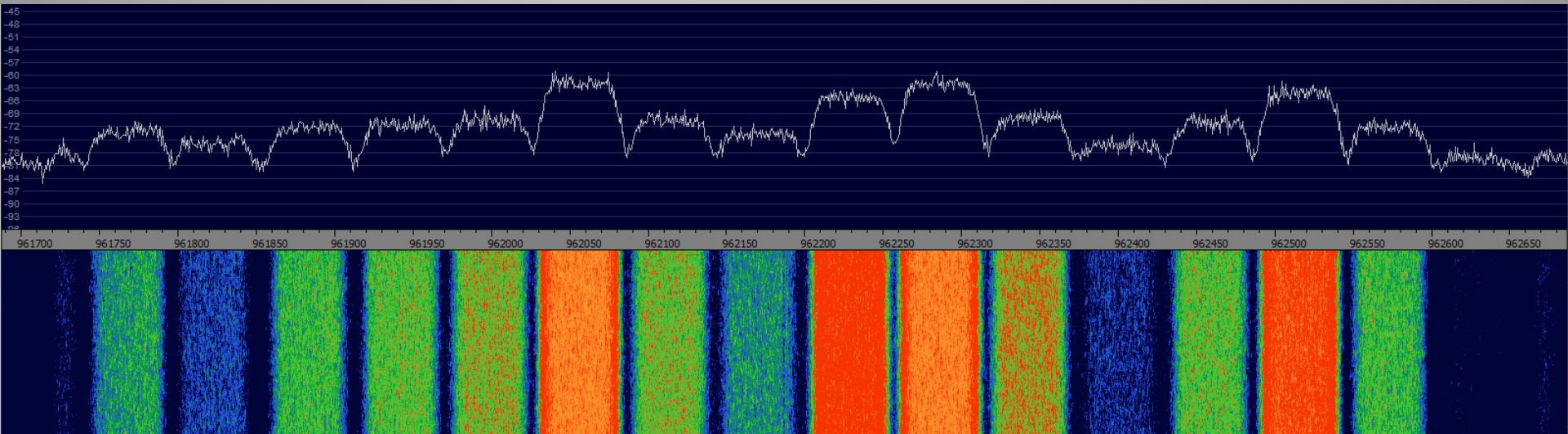
PSK Debug Output





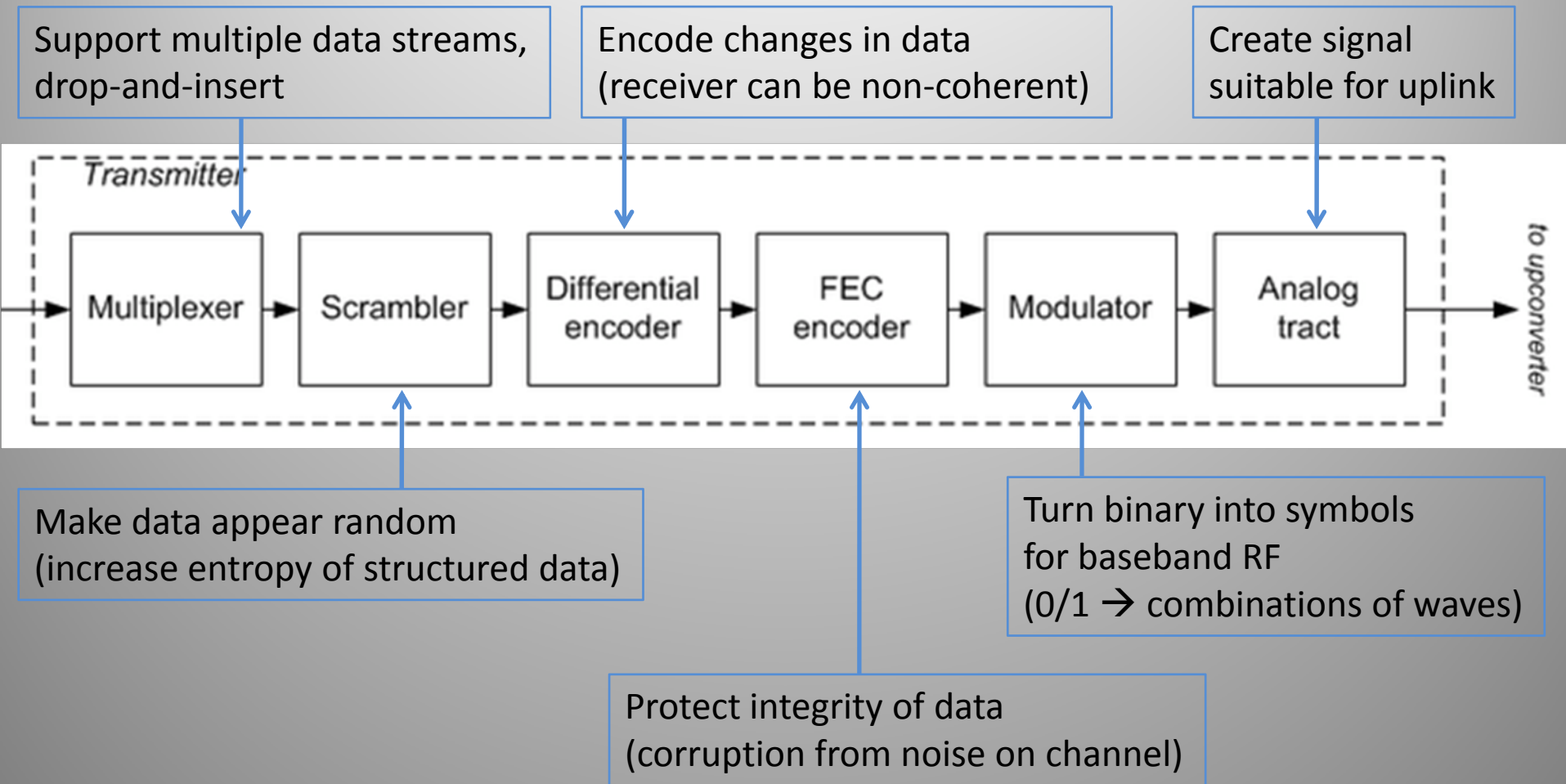
Data Streams

- All sorts of continuous streams of varying bandwidth
- Streams created by manipulating raw data to optimise for transmission over long distance
- Receiver must be able to lock on and decode





Modulation: pick your parameters



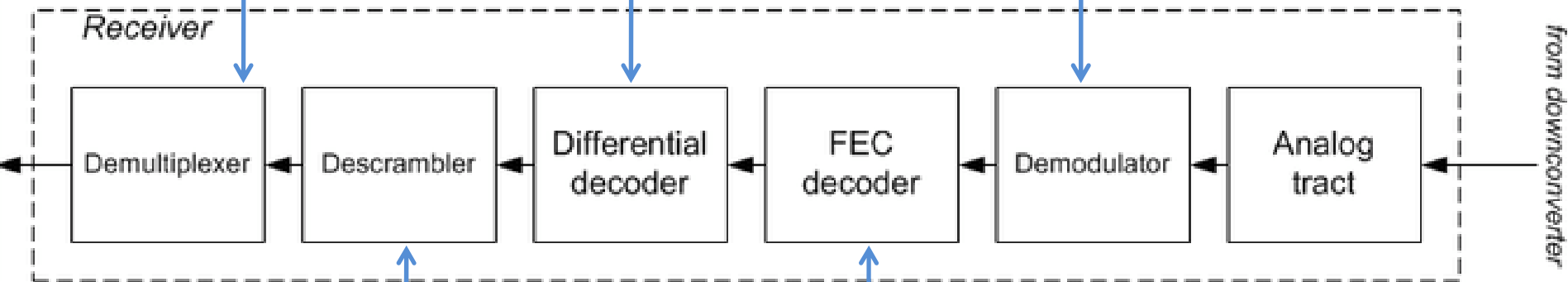


Demodulation: easy when you know

Are there multiple streams?
How are they multiplexed?

Is it differential, or
what defines a 0/1?


What is the modulation?
Symbol rate? Require coherence?
What is the phase difference?
Need to conjugate complex plane?



Possible to determine if it is scrambled
(calculate stats), but what is the scrambler?
Is it additive or multiplicative?
How is it synchronised?

Which FEC(s) is used?
Is it a concatenated code?
What is the code rate?
What is the block size?
How is it synchronised?





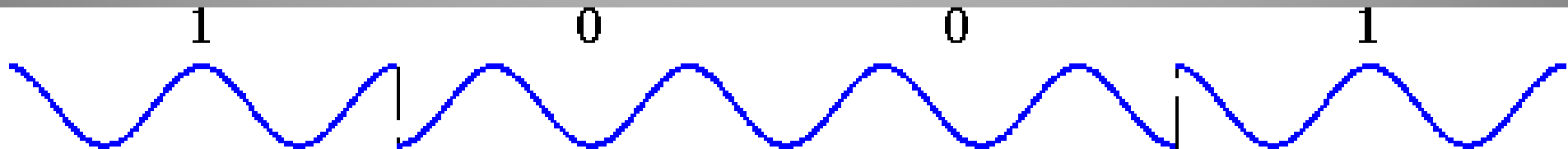
If you don't know...

- Try the most common/default options (RTFMM):
 - Modulation: **Phase Shift Keying** (BPSK, QPSK)
 - Convolutional code: NASA, K=7 (Voyager Probe)
 - Scrambler: IESS-803 (**Intelsat Business Service**)
- Still need to try each combination of:
 - Differential decoding, synchronisation offset, symbol mapping
- Best option is to try every permutation automatically
- Assuming decent SNR, low **Bit Error Rate** is an indicator you're heading the right way!



Aside: PSK, Symbols & Bits

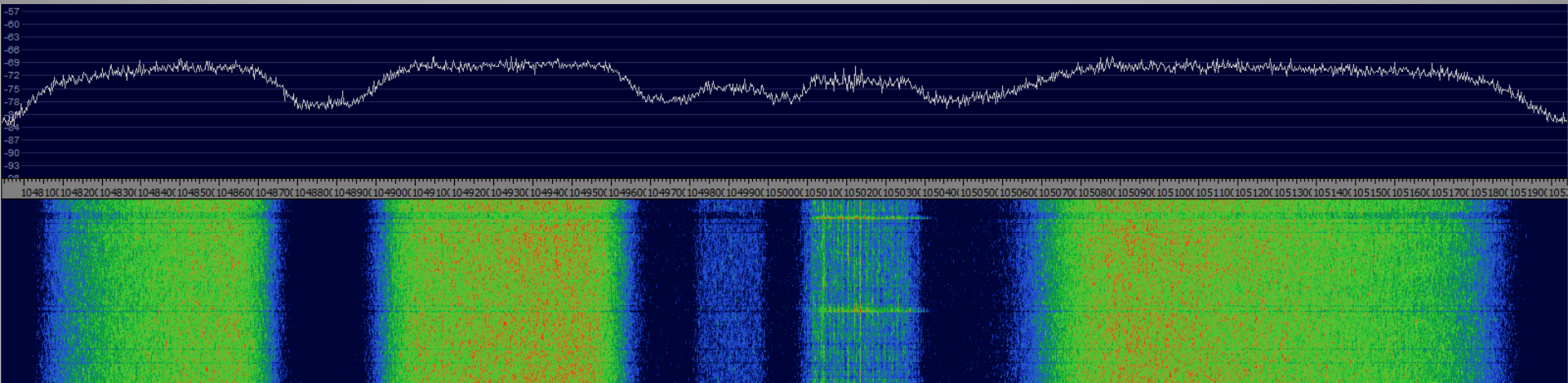
- PSK uses changes in phase of a signal (carrier) to convey data
- Demodulator detects phase changes and outputs symbols
- Order of PSK determines # bits in 1 symbol
 - Many bits/symbol thanks to imaginary numbers (I/Q)
- Raw bit rate = symbol rate x (# bits/symbol)
 - Binary PSK (BPSK): 1 bit/symbol
 - Quaternary PSK (QPSK): 2 bits/symbol
 - 8PSK: 3 bits/symbol, etc...



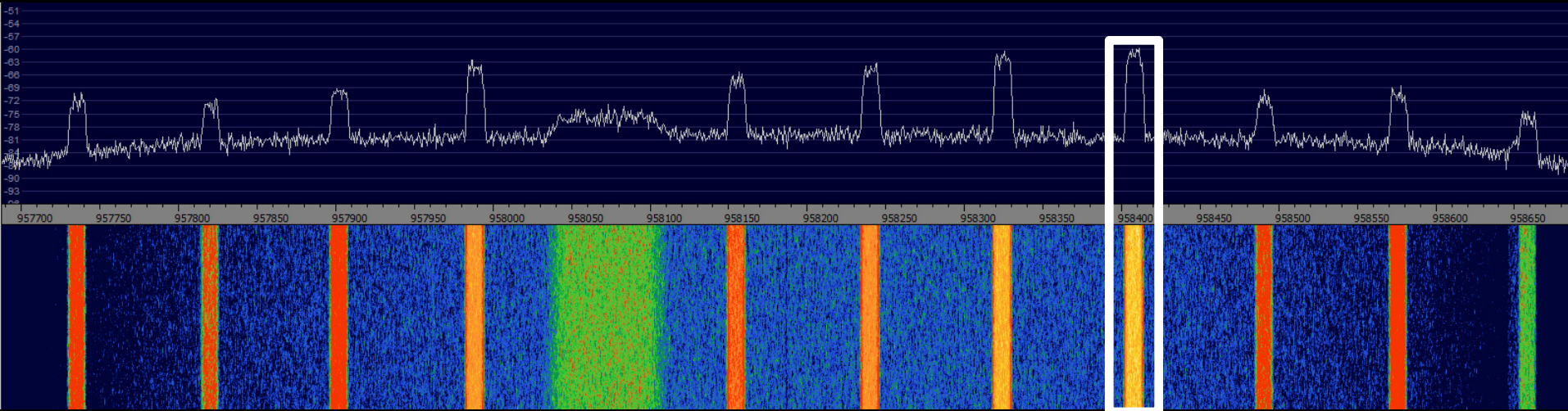


Determining modulation & rate

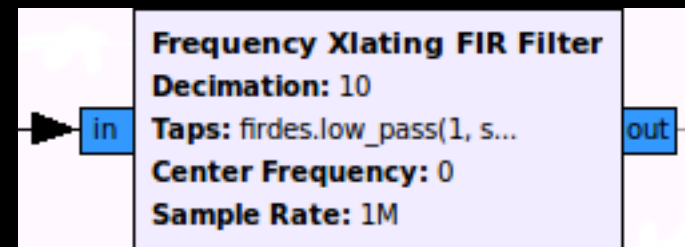
- Assuming PSK, easy to determine:
 - Modulation order: multiply the signal by itself
 - Symbol rate: multiply the signal by a lagged version of itself (cyclostationary analysis)
- Only a few GR blocks required do this



Let's try one...

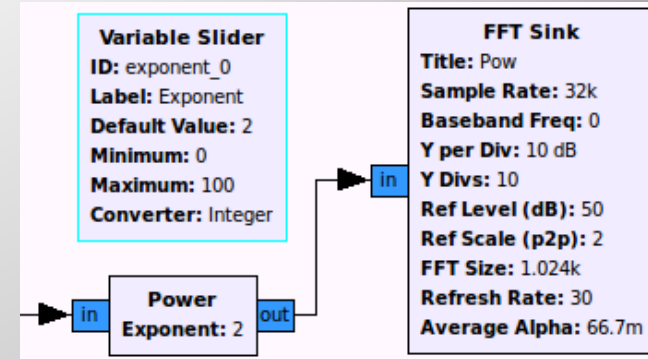


- Feed entire baseband spectrum into GR
- Perform 'channel selection' to isolate stream of interest (create new baseband centred on stream)



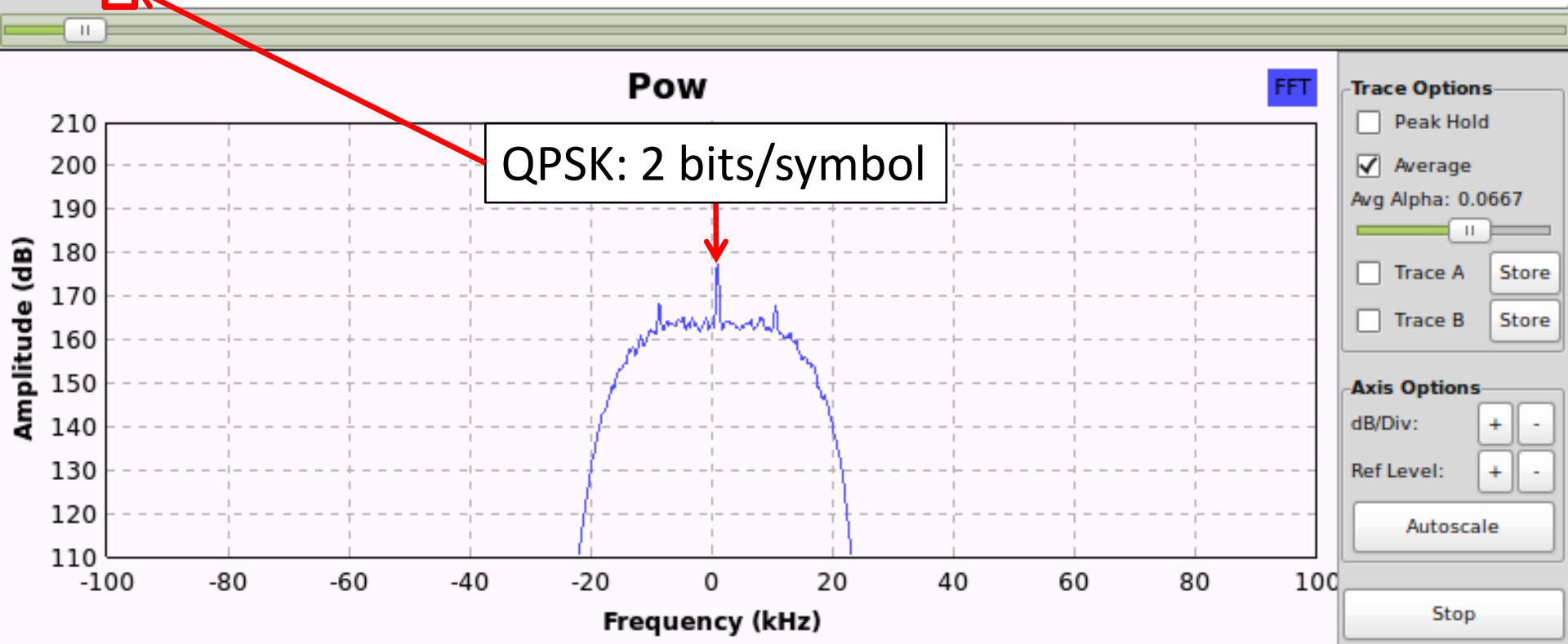
Determine PSK order

- Start at 2 and go up
- Stop when spike appears



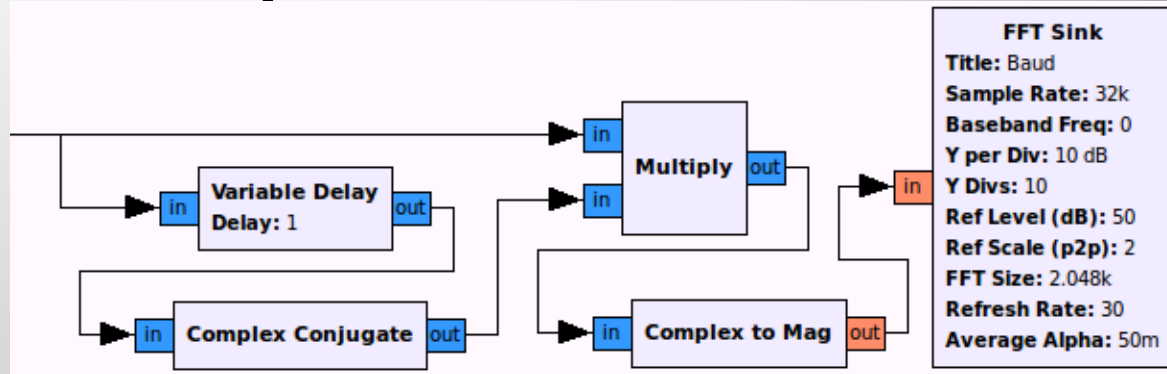
Exponent:

4

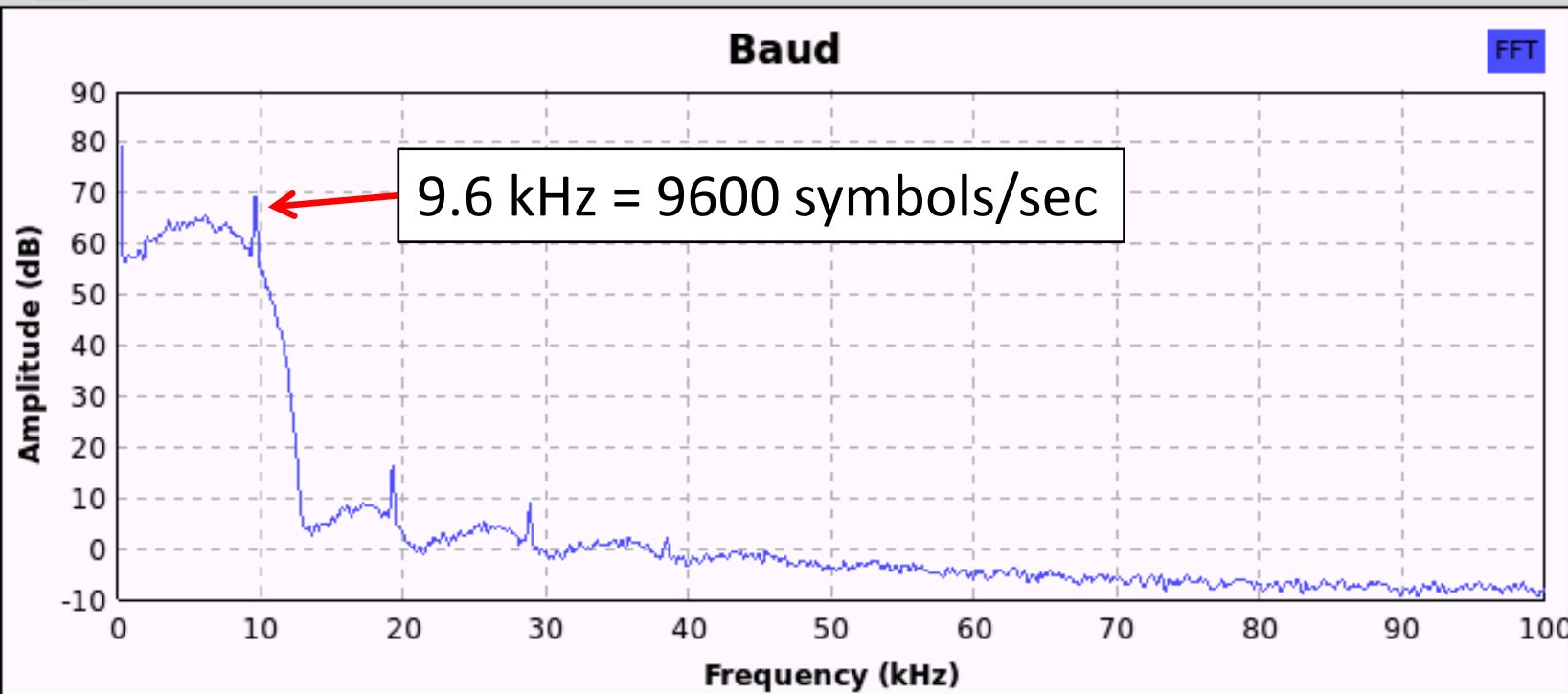


Determine Symbol Rate

- Find first peak



Nominal samples per symbol: 2



Trace Options

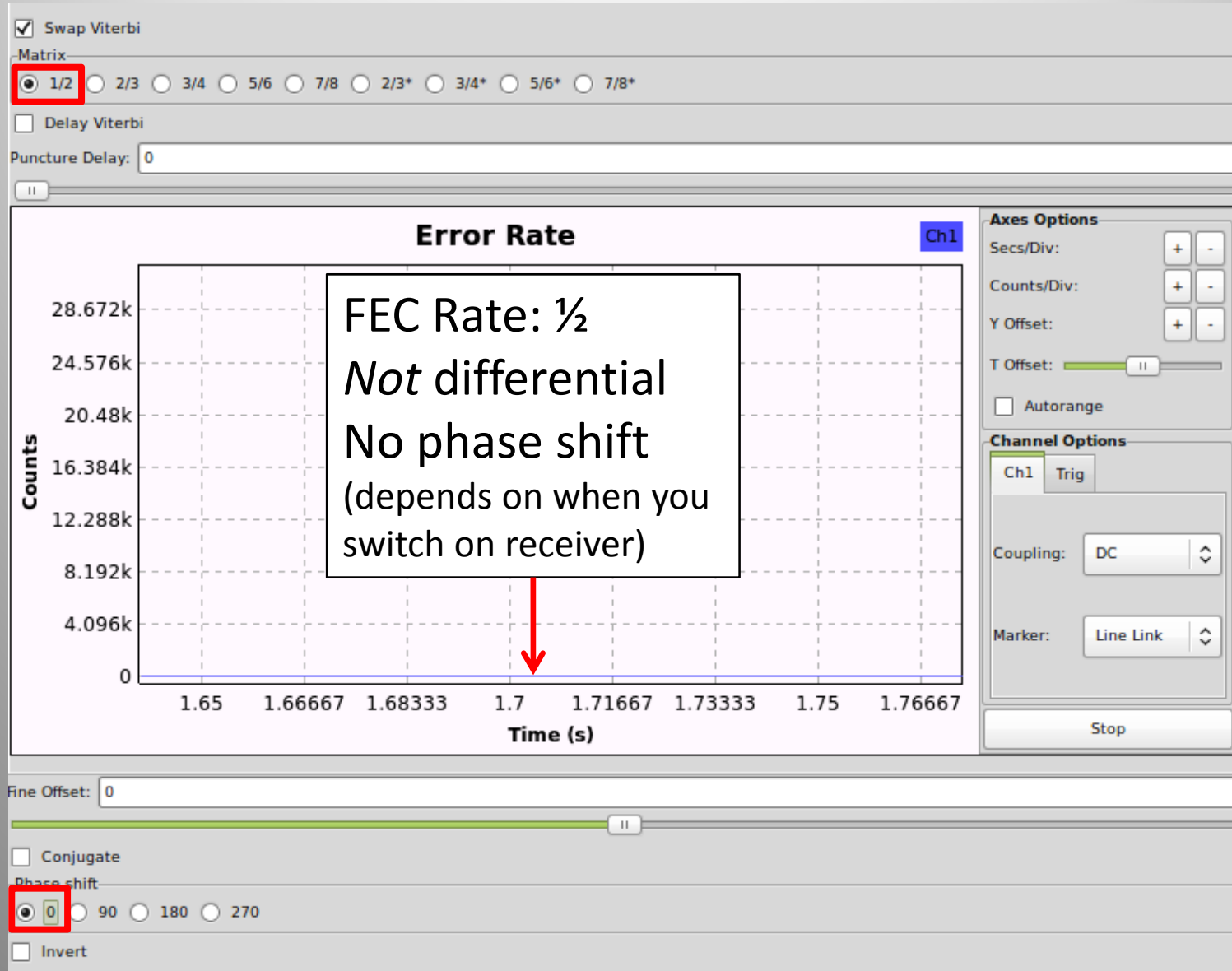
- Peak Hold
- Average
- Avg Alpha: 0.0500
- Trace A
- Trace B

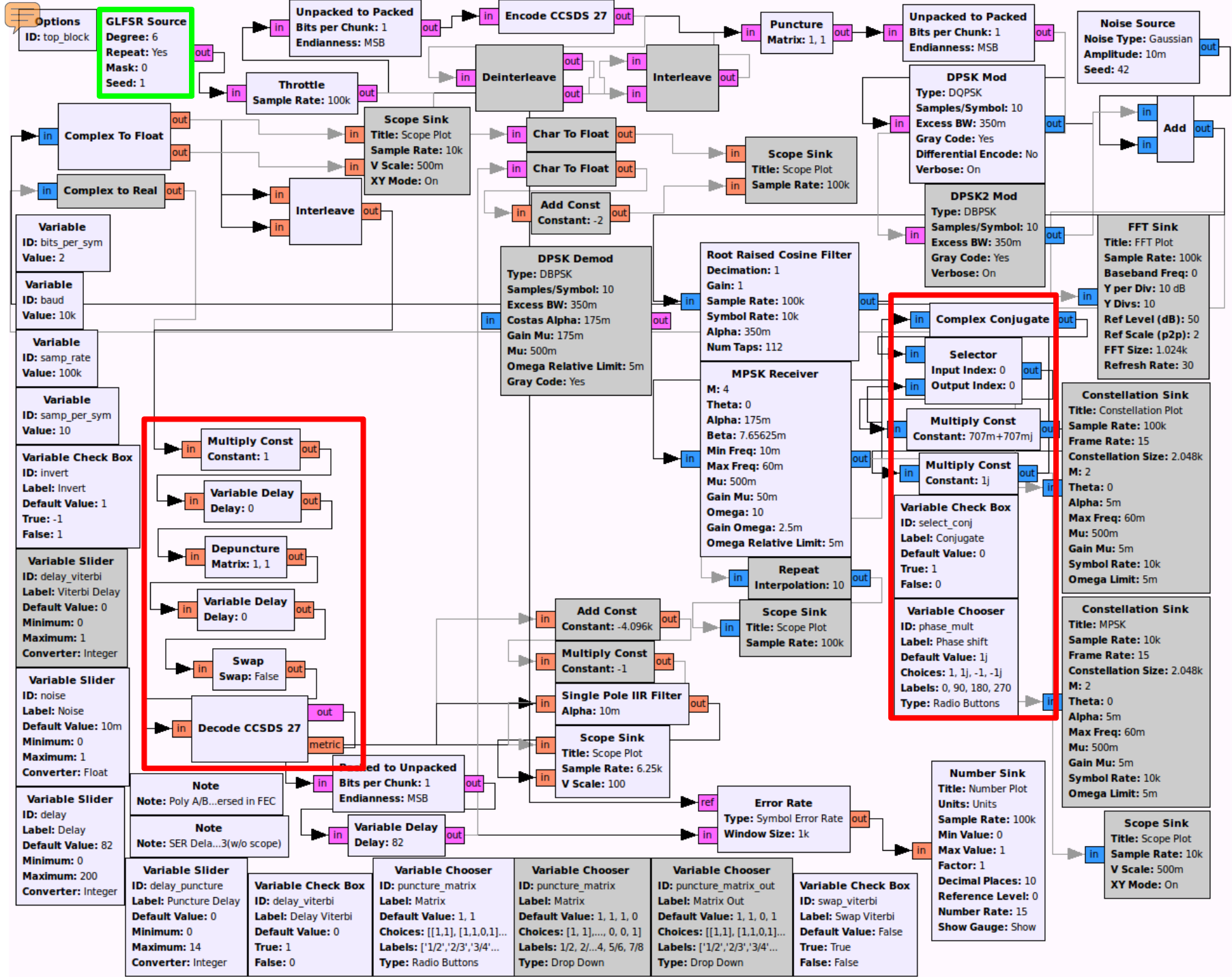
Axis Options

dB/Div:

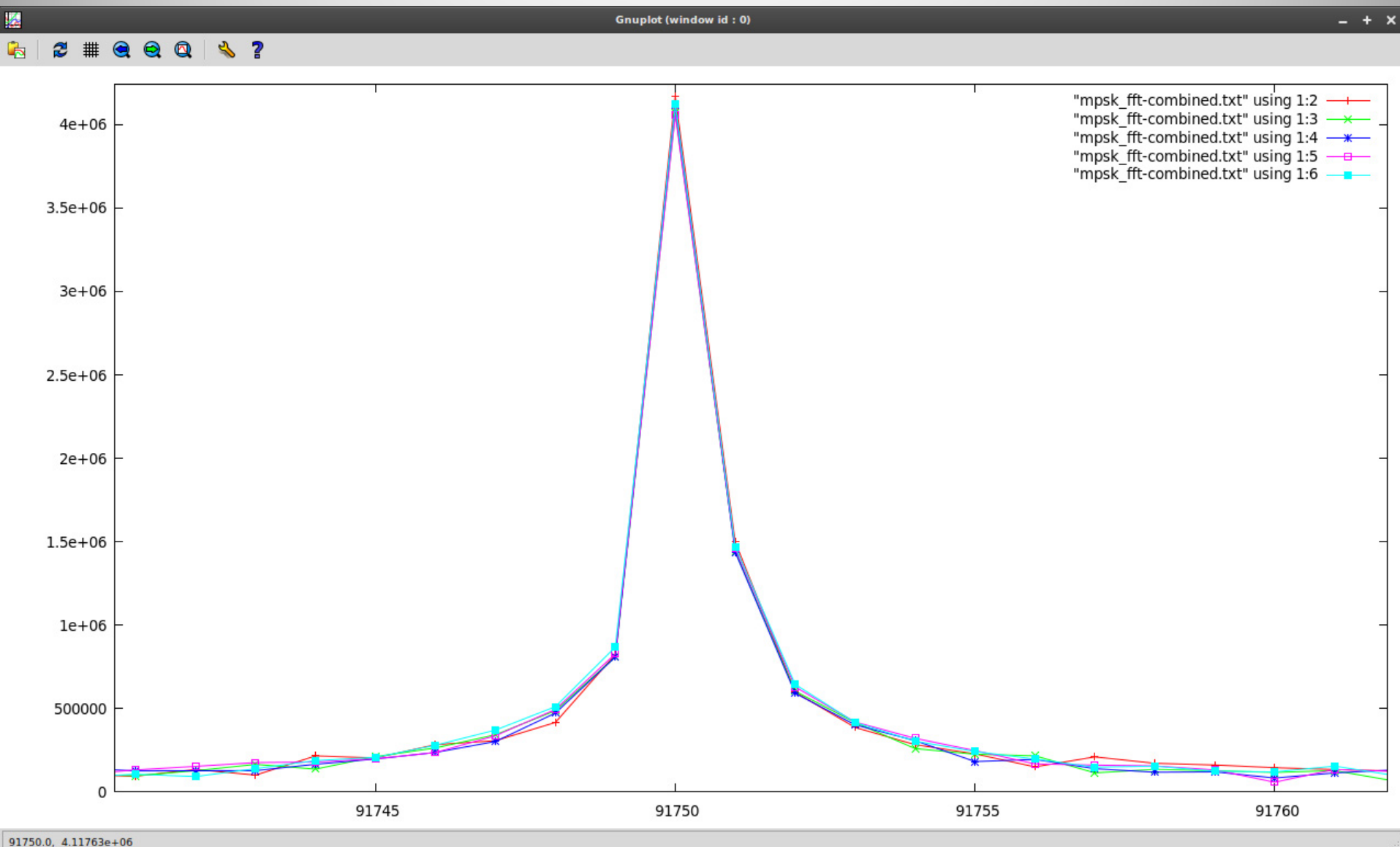
Ref Level:

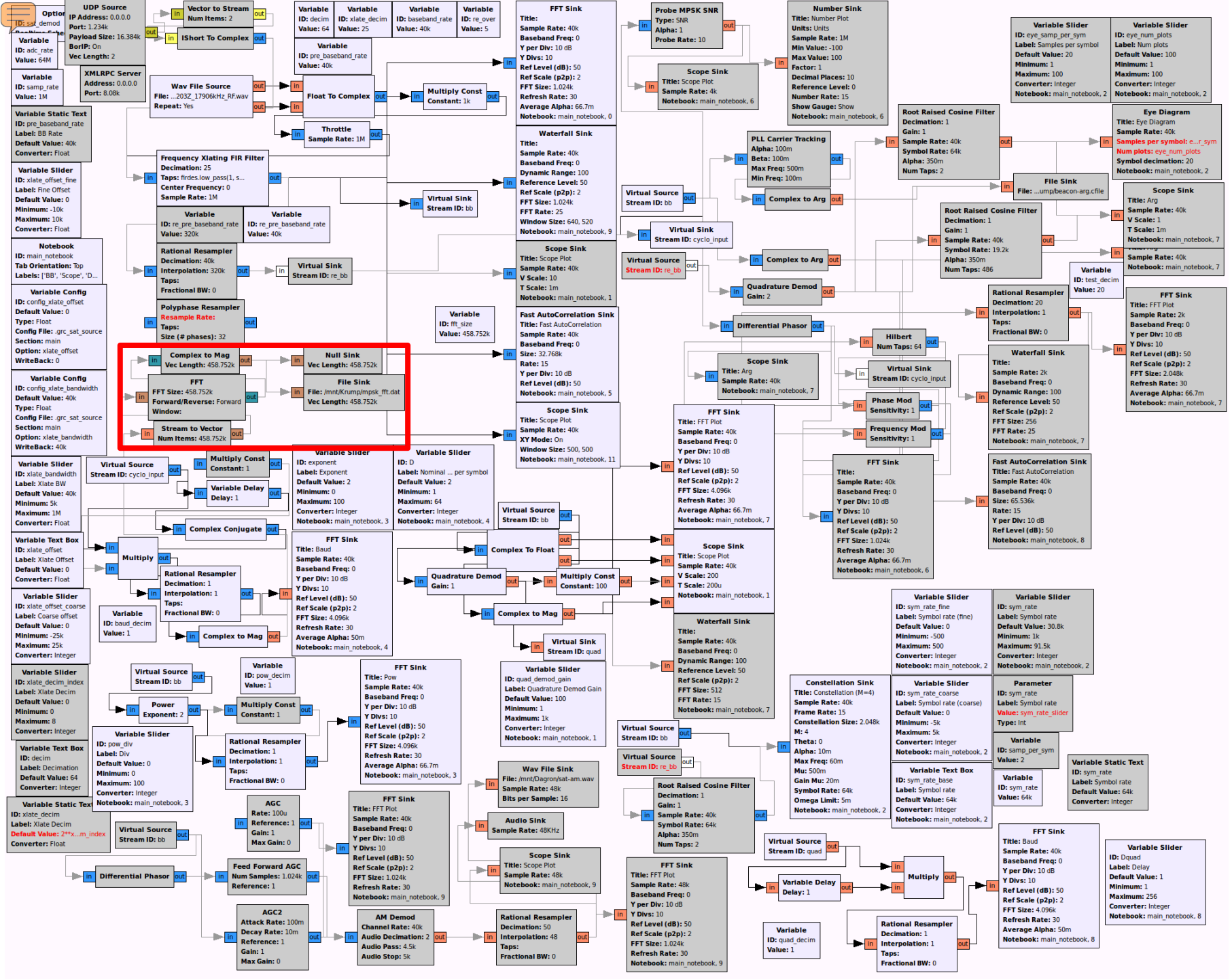
Try synchronisation & FEC

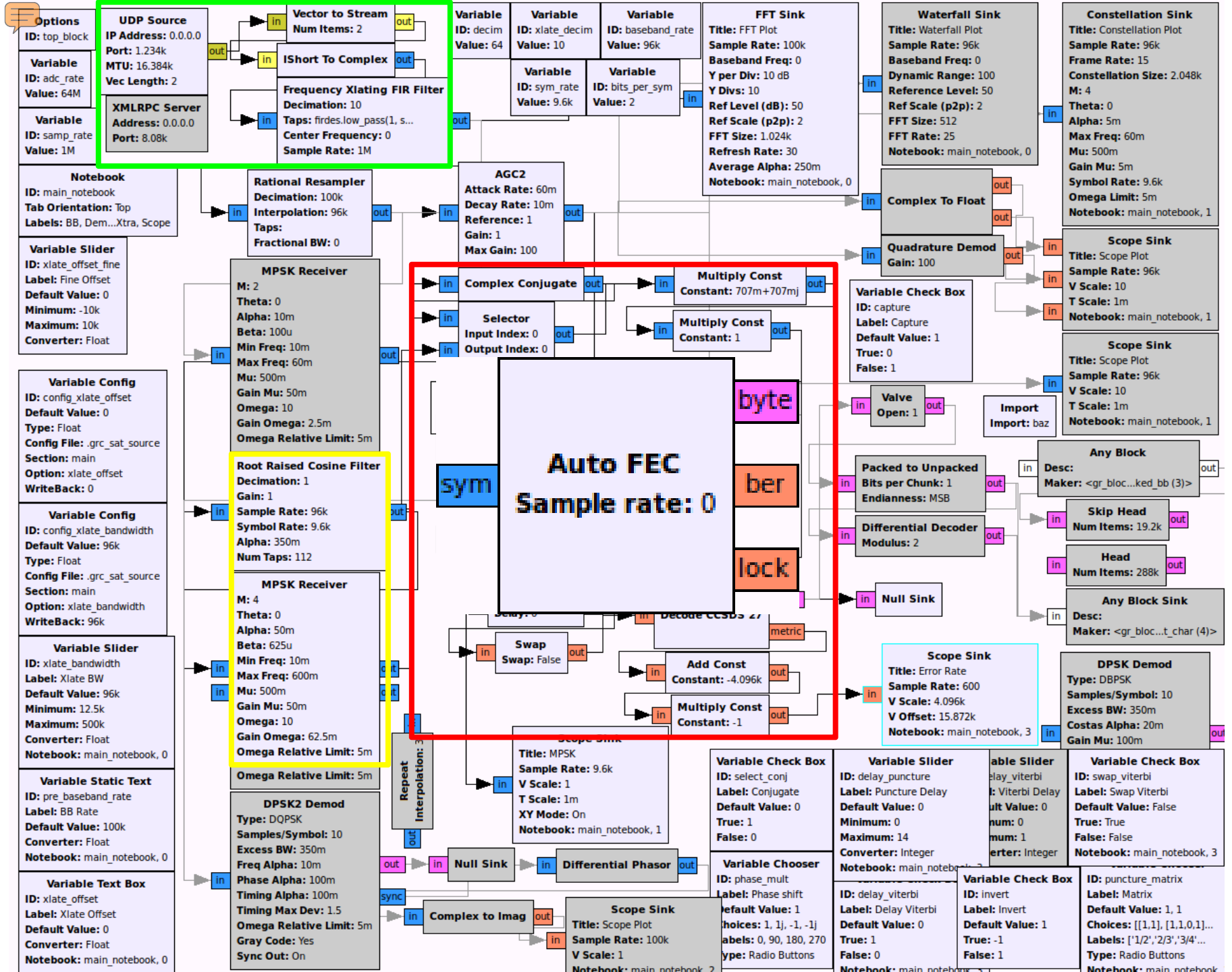




Find Precise Symbol Rate







Options

ID: top_block

Variable ID: adc_rate Value: 64M

Variable ID: samp_rate Value: 1M

UDP Source IP Address: 0.0.0.0 Port: 1.234k MTU: 16.384k Vec Length: 2

XMLRPC Server Address: 0.0.0.0 Port: 8.08k

Vector to Stream Num Items: 2

IShort To Complex

Frequency Xlating FIR Filter Decimation: 10 Taps: firdec.low_pass(1, 5, ... Center Frequency: 0 Sample Rate: 1M

Variable ID: decim Value: 64

Variable ID: xlate_decim Value: 10

Variable ID: baseband_rate Value: 96k

Variable ID: sym_rate Value: 9.6k

Variable ID: bits_per_sym Value: 2

FFT Sink Title: FFT Plot Sample Rate: 100k Baseband Freq: 0 Y per Div: 10 dB Y Divs: 10 Ref Level (dB): 50 Ref Scale (p2p): 2 FFT Size: 1.024k Refresh Rate: 30 Average Alpha: 250m Notebook: main_notebook, 0

Waterfall Sink Title: Waterfall Plot Sample Rate: 96k Baseband Freq: 0 Dynamic Range: 100 Reference Level: 50 Ref Scale (p2p): 2 FFT Size: 512 FFT Rate: 25 Notebook: main_notebook, 0

Constellation Sink Title: Constellation Plot Sample Rate: 96k Frame Rate: 15 Constellation Size: 2.048k M: 4 Theta: 0 Alpha: 5m Max Freq: 60m Mu: 500m Gain Mu: 5m Symbol Rate: 9.6k Omega Limit: 5m Notebook: main_notebook, 1

Notebook ID: main_notebook Tab Orientation: Top Labels: BB, Dem...Xtra, Scope

Variable Slider ID: xlate_offset_fine Label: Fine Offset Default Value: 0 Minimum: -10k Maximum: 10k Converter: Float

Rational Resampler Decimation: 100k Interpolation: 96k Taps: Fractional BW: 0

AGC2 Attack Rate: 60m Decay Rate: 10m Reference: 1 Gain: 1 Max Gain: 100

Multiply Const Constant: 707m+707mj

Multiply Const Constant: 1

Complex To Float

Quadrature Demod Gain: 100

Scope Sink Title: Scope Plot Sample Rate: 96k V Scale: 10 T Scale: 1m Notebook: main_notebook, 1

Scope Sink Title: Scope Plot Sample Rate: 96k V Scale: 10 T Scale: 1m Notebook: main_notebook, 1

Variable Config ID: config_xlate_offset Default Value: 0 Type: Float Config File: .grc_sat_source Section: main Option: xlate_offset WriteBack: 0

MPSK Receiver M: 2 Theta: 0 Alpha: 10m Beta: 100u Min Freq: 10m Max Freq: 60m Mu: 500m Gain Mu: 50m Omega: 10 Omega Relative Limit: 5m

Complex Conjugate

Selector Input Index: 0 Output Index: 0

Multiply Const Constant: 1

byte

ber

lock

Auto FEC Sample rate: 0

Variable Check Box ID: capture Label: Capture Default Value: 1 True: 0 False: 1

Valve Open: 1

Any Block Desc: <gr_bloc...ked_bb (3)>

Variable Config ID: config_xlate_bandwidth Default Value: 96k Type: Float Config File: .grc_sat_source Section: main Option: xlate_bandwidth WriteBack: 96k

Root Raised Cosine Filter Decimation: 1 Gain: 1 Sample Rate: 96k Symbol Rate: 9.6k Alpha: 350m Num Taps: 112

sym

Decode CSBS

Swap Swap: False

Add Const Constant: -4.096k

Multiply Const Constant: -1

Packed to Unpacked Bits per Chunk: 1 Endianness: MSB

Differential Decoder Modulus: 2

Import Import: baz

Skip Head Num Items: 19.2k

Head Num Items: 288k

Any Block Sink Desc: <gr_bloc...t_char (4)>

Variable Slider ID: xlate_bandwidth Label: Xlate BW Default Value: 96k Minimum: 12.5k Maximum: 500k Converter: Float Notebook: main_notebook, 0

MPSK Receiver M: 4 Theta: 0 Alpha: 50m Beta: 625u Min Freq: 10m Max Freq: 600m Mu: 500m Gain Mu: 50m Omega: 10 Omega Relative Limit: 5m

Scope Sink Title: MPSK Sample Rate: 9.6k V Scale: 1 T Scale: 1m XY Mode: On Notebook: main_notebook, 1

Null Sink

Differential Phasor

Scope Sink Title: Error Rate Sample Rate: 600 V Scale: 4.096k V Offset: 15.872k Notebook: main_notebook, 3

DPSK Demod Type: DBPSK Samples/Symbol: 10 Excess BW: 350m Costas Alpha: 20m Gain Mu: 100m

Variable Static Text ID: pre_baseband_rate Label: BB Rate Default Value: 100k Converter: Float Notebook: main_notebook, 0

DPSK2 Demod Type: DQPSK Samples/Symbol: 10 Excess BW: 350m Freq Alpha: 10m Phase Alpha: 100m Timing Alpha: 100m Timing Max Dev: 1.5 Omega Relative Limit: 5m Gray Code: Yes Sync Out: On

Scope Sink Title: Scope Plot Sample Rate: 100k V Scale: 1 Notebook: main_notebook, 2

Complex to Imag

Scope Sink Title: Scope Plot Sample Rate: 100k V Scale: 1 Notebook: main_notebook, 2

Variable Check Box ID: select_conj Label: Conjugate Default Value: 0 True: 1 False: 0

Variable Slider ID: delay_puncture Label: Puncture Delay Default Value: 0 Minimum: 0 Maximum: 14 Converter: Integer Notebook: main_notebook, 3

Variable Slider ID: viterbi_delay Label: Viterbi Delay Default Value: 0 Minimum: 0 Maximum: 1 Converter: Integer

Variable Check Box ID: swap_viterbi Label: Swap Viterbi Default Value: False True: True False: False Notebook: main_notebook, 3

Variable Text Box ID: xlate_offset Label: Xlate Offset Default Value: 0 Converter: Float Notebook: main_notebook, 0

Variable Slider ID: delay_viterbi Label: Delay Viterbi Default Value: 0 True: 1 False: 0 Notebook: main_notebook, 3

Variable Check Box ID: invert Label: Invert Default Value: 1 True: -1 False: 1

Variable Slider ID: puncture_matrix Label: Matrix Default Value: 1, 1 Choices: [[1,1], [1,1,0,1]...] Labels: ['1/2', '2/3', '3/4'...] Type: Radio Buttons Notebook: main_notebook, 3

Auto FEC

Creating Auto-FEC:

```
sample_rate:          800000
ber_threshold:        2048
ber_smoothing:        0.01
ber_duration:         8192
ber_sample_decimation: 1
settling_period:     4096
pre_lock_duration:    8192
```

De-puncturer relative rate: 1.000000

==> Using throttle at sample rate: 800000

==> Using lock throttle rate: 50000

Auto-FEC thread started: Thread-1

Skipping initial samples while MPSK receiver locks: 4096

Reached excess BER limit: 11437.1352901 , locked: False , current puncture matrix: 0 , total samples received: 12289

Applying lock value: 0

Beginning search...

Applying rotation: 1j

Reached excess BER limit: 11870.4144919 , locked: False , current puncture matrix: 0 , total samples received: 24586

Applying rotation: 1

Applying conjugation: 0

Locking current XForm

=====

FEC locked: 1/2

=====

Applying lock value: 1

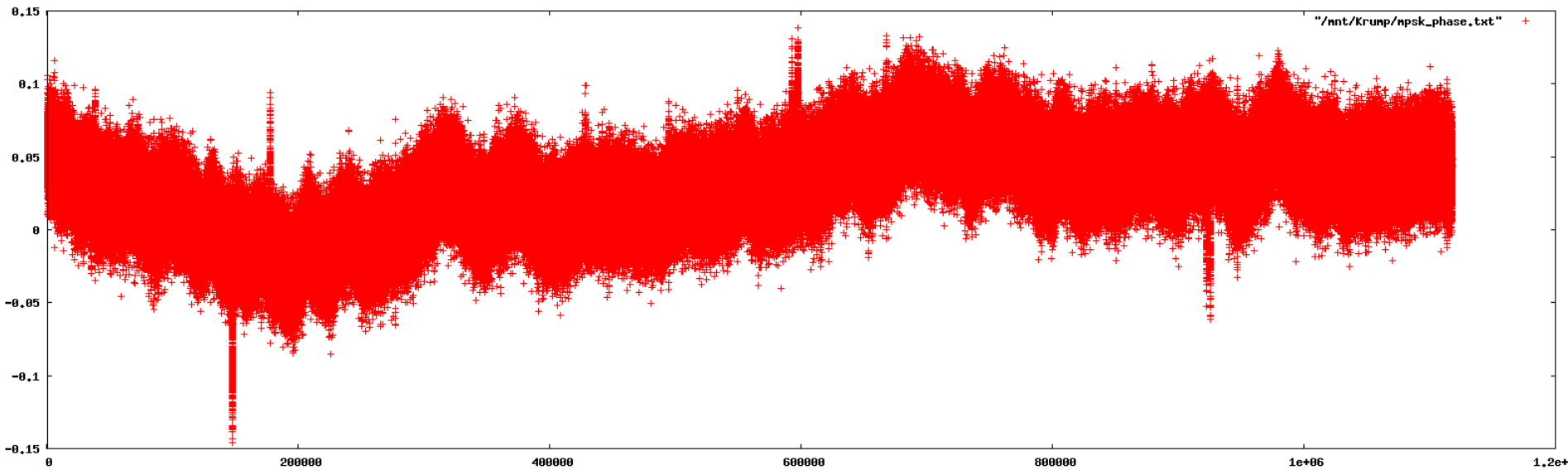


Demodulated & error-corrected

- Symbol rate = 9600 symbols/sec
- Pre-FEC raw bit rate = 19200 bits/sec
- Post-FEC raw bit rate = 9600 bits/sec ($\frac{1}{2}$ rate)

- Visualise data: look for additional clues
 - Differential encoding
 - Scrambling
 - Structure

QPSK Phase Debug



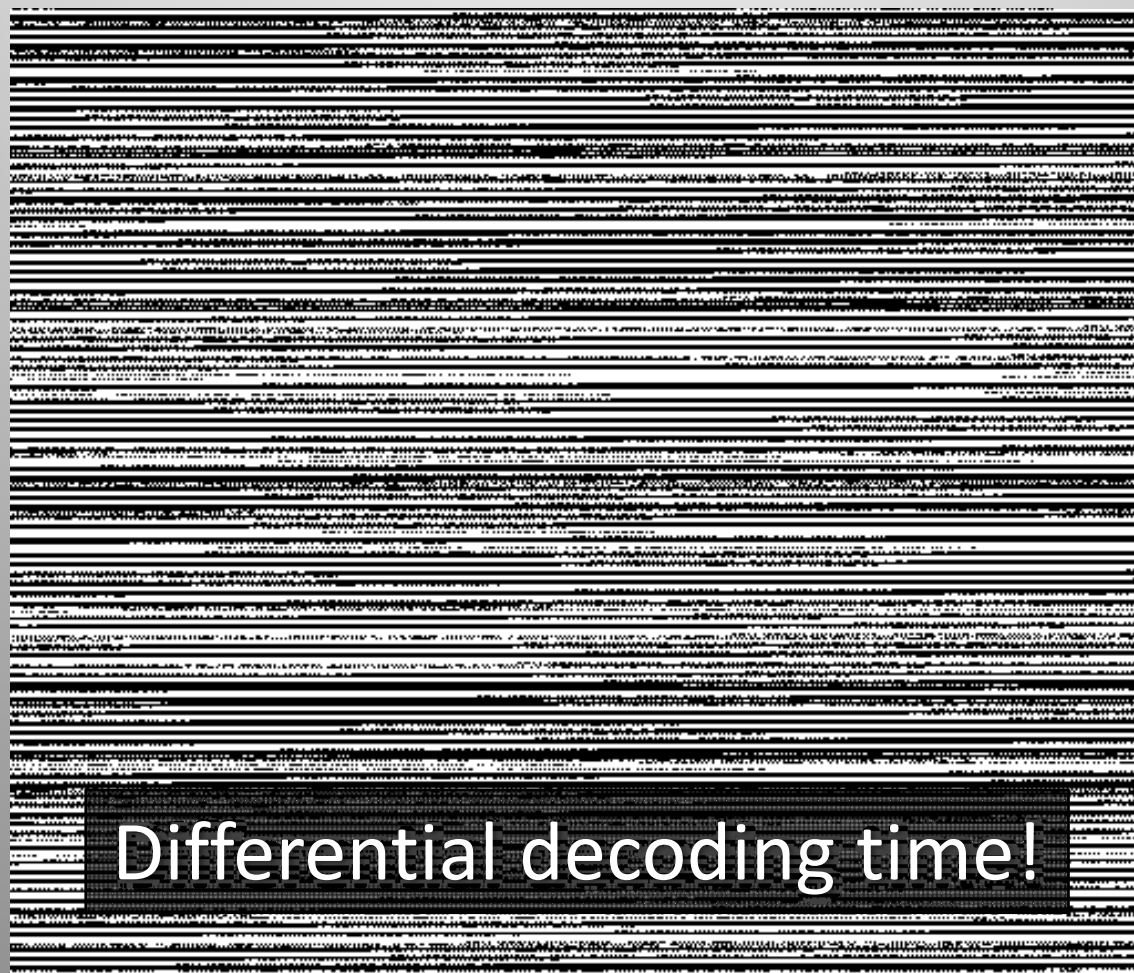
Visualisation

- Raw data (0: black, 1: white)



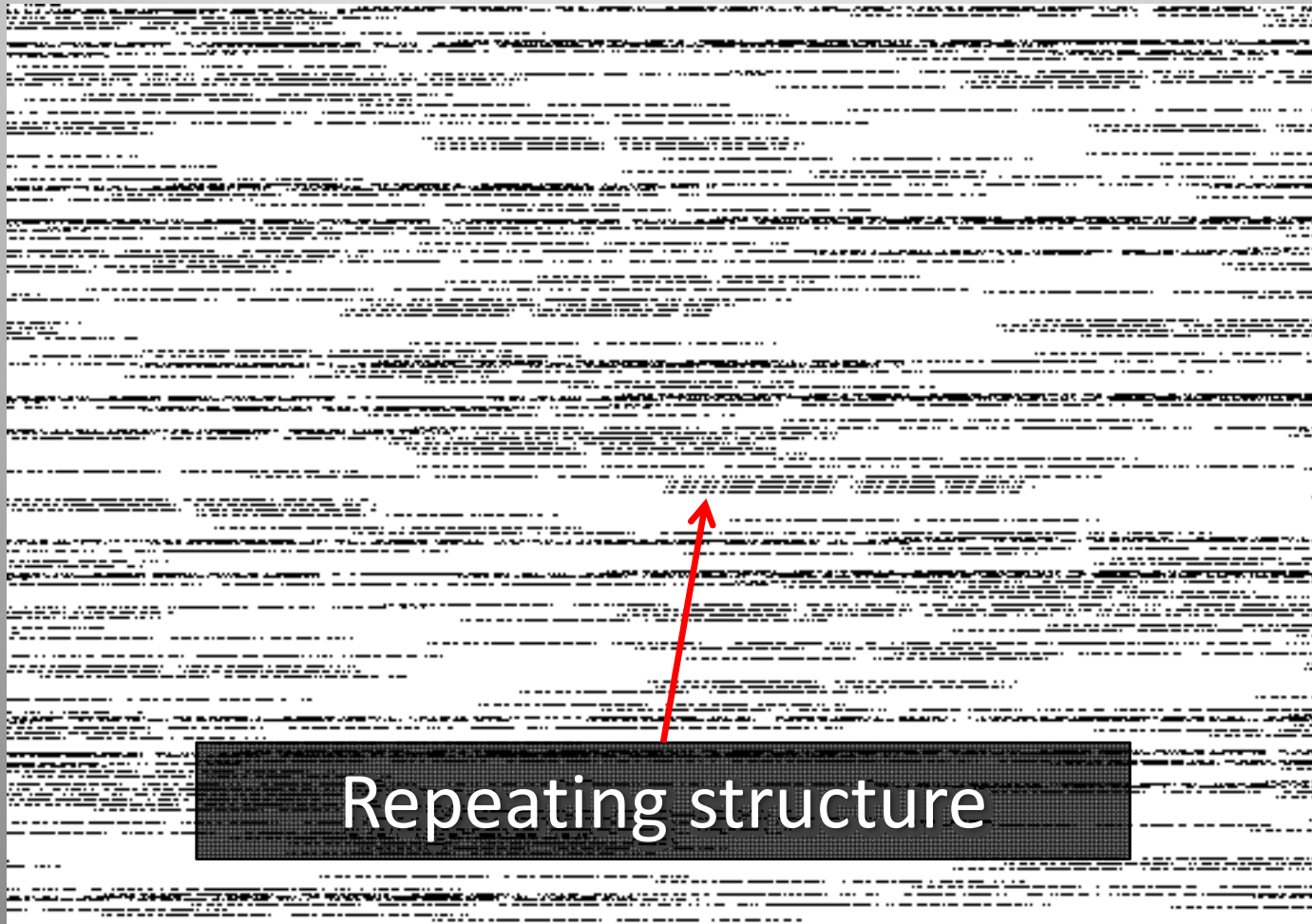
De-scrambled

- Better, but long runs of 0s and 1s (not ideal)



Diff. decoded & de-scrambled

- Structured, asynchronous packets of data!



Repeating structure

Pattern Search

- Search for repeating strings of bits
- Try to find frame header
- Clue: sudden increase in # of occurrences

```
44 bits #0002-0002[+0000, /0000]: 00000001000011101000000010001011101111111011 (dFdd1017080)
44 bits #0002-0002[+0000, /0000]: 000000011000000011111000010111101010101111111 (feabd0f8180)
44 bits #0002-0002[+0000, /0000]: 00000001100001011110000101111010101011111111 (feabd0fa180)
44 bits #0004-0004[+0000, /0000]: 0000000110000011000010001011110101010111111111 (feabd10c180)
```

```
43 bits #0000-0005[+0001, /0000]: 0110111100110000001001100110001000011000000 (1846640cf6)
```

```
42 bits #0002-0002[+0000, /0000]: 000000011001000111010011000011000010000000 (430cb8980)
42 bits #0002-0002[+0000, /0000]: 000000010000010000100000011001101100000010 (10366042080)
42 bits #0002-0002[+0000, /0000]: 000000011001000100011011000000111110000000 (7c0d88980)
42 bits #0001-0003[+0000, /0000]: 000000010000111010000000100010111011111110 (1fd1017080)
42 bits #0003-0003[+0000, /0000]: 000000011000100111010011000011000010000000 (430cb9180)
42 bits #0000-0004[+0002, /0000]: 000000110000011000010001011110101010111111 (3f55e8860c0)
```

```
41 bits #0002-0002[+0000, /0000]: 00000001000011001001110000100111110000000 (3e4393080)
41 bits #0003-0003[+0000, /0000]: 00000001000101001001110000001111110000000 (3f0328280)
41 bits #0001-0003[+0000, /0000]: 00000001000011101000000011110110110000001 (1036f017080)
41 bits #0000-0003[+0001, /0000]: 000000010000111010000000100010111011111110 (fee880b840)
41 bits #0000-0004[+0002, /0000]: 000000010000111010000000101000001010111110 (1f505017080)
41 bits #0006-0006[+0000, /0000]: 0000000100000100001000001011111110000000 (3fa042080)
```

```
40 bits #0002-0002[+0000, /0000]: 11000010001011111100101000001000110000000 (18829f443)
40 bits #0002-0002[+0000, /0000]: 0110000101111111010100001000110000000111 (e0310afe86)
40 bits #0002-0002[+0000, /0000]: 0000000100001110100000001000101100111111 (fcd1017080)
40 bits #0002-0002[+0000, /0000]: 0001110100101110011010000001000110000001 (81881674b8)
40 bits #0000-0003[+0001, /0000]: 00000001000011101000000011110110110000001 (81b780b840)
40 bits #0000-0003[+0001, /0000]: 00000001000100111010011000011000010000000 (21866c8c0)
40 bits #0001-0004[+0000, /0000]: 0000000100001110100000001000101110111111 (fd1017080)
40 bits #0001-0004[+0000, /0000]: 0000000100001110100000001111011011000000 (36f017080)
40 bits #0001-0005[+0000, /0000]: 0000000100001110100000001010000010101111 (f505017080)
40 bits #0006-0006[+0000, /0000]: 0000000100000100001000000101111110000000 (1fa042080)
```

```
39 bits #0002-0002[+0000, /0000]: 1111101001011110011110100001000110000000 (c42f3a5f)
39 bits #0002-0002[+0000, /0000]: 001000000011111110100101110000101111111 (7f43a5fc04)
39 bits #0002-0002[+0000, /0000]: 000000010101010100100011010001111000001 (41e2c4aa80)
39 bits #0002-0002[+0000, /0000]: 011101001011100110100000010001100000010 (2062059d2e)
39 bits #0002-0002[+0000, /0000]: 0111110100101110011110100001000110000000 (1885e74be)
39 bits #0002-0002[+0000, /0000]: 010110100101110001100000001000110000000 (c4063a5a)
39 bits #0000-0003[+0001, /0000]: 000000100010100100111000000111111000000 (1f81c9440)
39 bits #0000-0004[+0001, /0000]: 000000100001110100000001000101110111111 (7ee880b)
39 bits #0000-0004[+0001, /0000]: 000000100001110100000001111011011000000 (1b780b8)
39 bits #0000-0005[+0002, /0000]: 0000001000011101000000010100000010101111 (7a8280b)
39 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (1fd0210)
39 bits #0166-0172[+0000, /0000]: 111111010011000100110001001100100010000000 (9919197)
```

```
38 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (fd021040)
```

```
38 bits #0000-0172[+0166, /0000]: 11111101001100010011000100110010000000 (4c8c8cbf)
```

```
37 bits #0002-0002[+0000, /0000]: 11101100000000111010110110000001000000 (40dae037)
```

```
37 bits #0002-0002[+0000, /0000]: 101010010111101101101000000100011000000 (6205bd2d)
```

```
38 bits #0002-0002[+0000, /0000]: 00011000010111001011010000100011000000 (c42d3a18)
38 bits #0002-0002[+0000, /0000]: 00110000101111100110100001000110000000 (6216740c)
38 bits #0001-0003[+0000, /0000]: 00000001010101010010001101000111100000 (1e2c4aa80)
38 bits #0000-0003[+0001, /0000]: 11111010010111001111010000100011000000 (c42f3a5f)
38 bits #0000-0003[+0001, /0000]: 01110100101110011010000001000110000001 (2062059d2e)
38 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (fd021040)
38 bits #0000-0172[+0166, /0000]: 11111101001100010011000100110010001000000 (4c8c8cbf)
```

```
37 bits #0002-0002[+0000, /0000]: 11101100000000111010110110000001000000 (40dae037)
37 bits #0002-0002[+0000, /0000]: 10110100101111101101101000000100011000000 (6205bd2d)
37 bits #0002-0002[+0000, /0000]: 000000011110110000101110011010101111111 (1fd6743780)
37 bits #0000-0003[+0001, /0000]: 0000001010101010010001101000111000000 (f1625540)
37 bits #0000-0010[+0008, /0000]: 0000000100000100001000000101111111010 (bfa042080)
37 bits #0000-0010[+0008, /0000]: 0000000100000100001000000101111110110 (dfa042080)
37 bits #0000-0010[+0008, /0000]: 0000000100000100001000000101111110001 (11fa042080)
```

Preceding 1s are just part of 'idle' stream when no data is being sent

Frame analysis

- Header
 - SYN SYN SYN (EBCDIC)
- Character-oriented encoding:
 - SOH
 - STX
 - ETX
 - CRC (CCITT-16)
- Numbers of fixed-length messages
 - Each contains an ID

The hex dump shows a sequence of bytes with corresponding ASCII characters. Annotations include: a green box around the first three '32' bytes (EBCDIC SYN); a blue box around the first four bytes of the first message ('32 32 32 01'); a red box around the first four bytes of the second message ('0c 40 10 02'); a yellow box around the first four bytes of the third message ('fd 09 32 32'); a green box around the '09' byte; a purple box around the last four bytes of the frame ('15 58 .X'); and a red box around the last four bytes of the second message ('88 53 10 03'). Arrows point from the list items to these specific bytes.

32	32	32	01	222.
0c	40	10	02	.@..
fd	09	32	32	..22
00	c3	ff	18
80	70	00	09	.p..
20	4c	0c	f9	L..
00	00	1f	d7
00	00	00	00
00	01	0c	86
e8	55	ff	18	.U..
80	70	00	50	.p.P
1f	2c	0e	74	.,.t
00	00	1f	cf
00	00	00	00
00	01	0c	7c	...
e8	55	ff	18	.U..
80	70	01	aa	.p..
12	8a	07	ce
00	00	1f	ef
00	00	00	00
00	01	0d	73	...s
e8	58	ff	18	.X..
80	40	04	4c	.@.L
03	8b	01	c8
07	02	30	02	..0.
19	8c	00	00
00	76	00	88	.v..
88	53	10	03	.S..
15	58	.	X	

Un-pack & find patterns

Diagram illustrating the un-packing and finding of patterns in a data stream. The data is organized into rows, each representing a message header and its corresponding data. The data is annotated with various patterns and bit-level information.

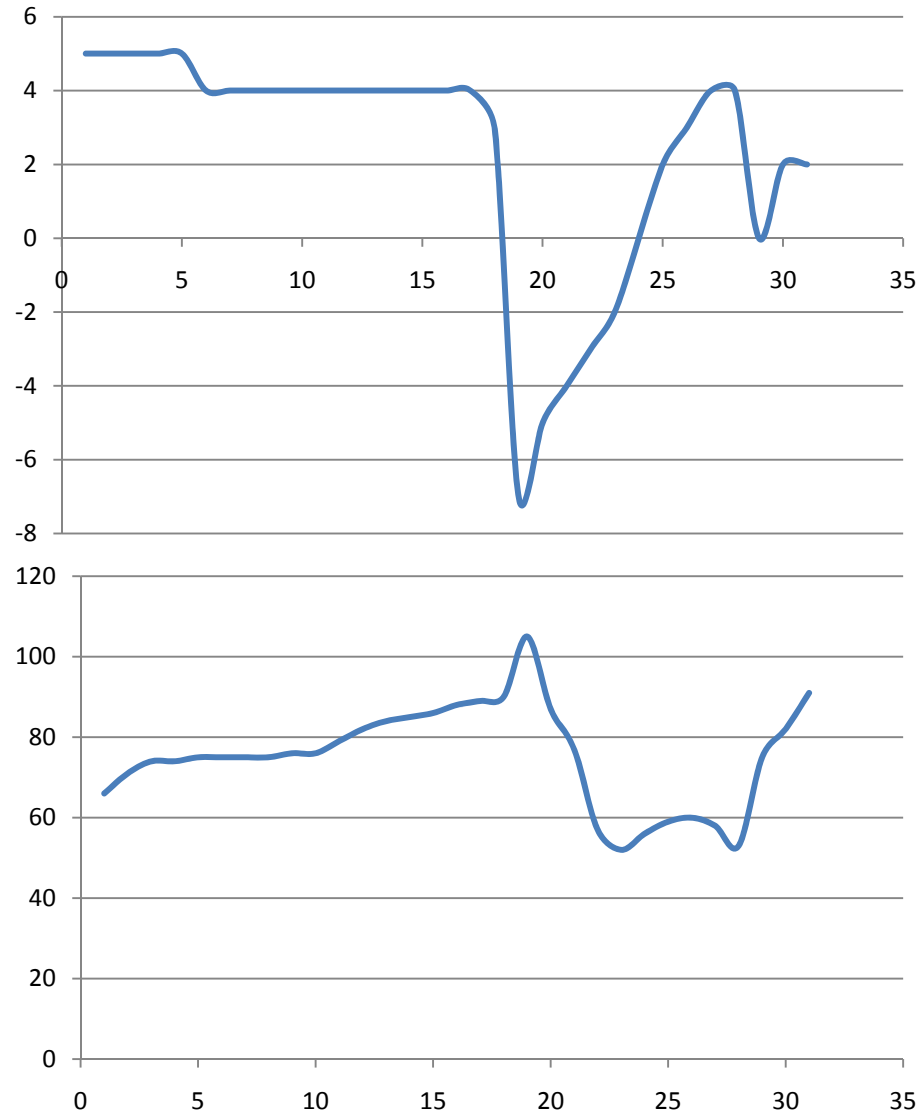
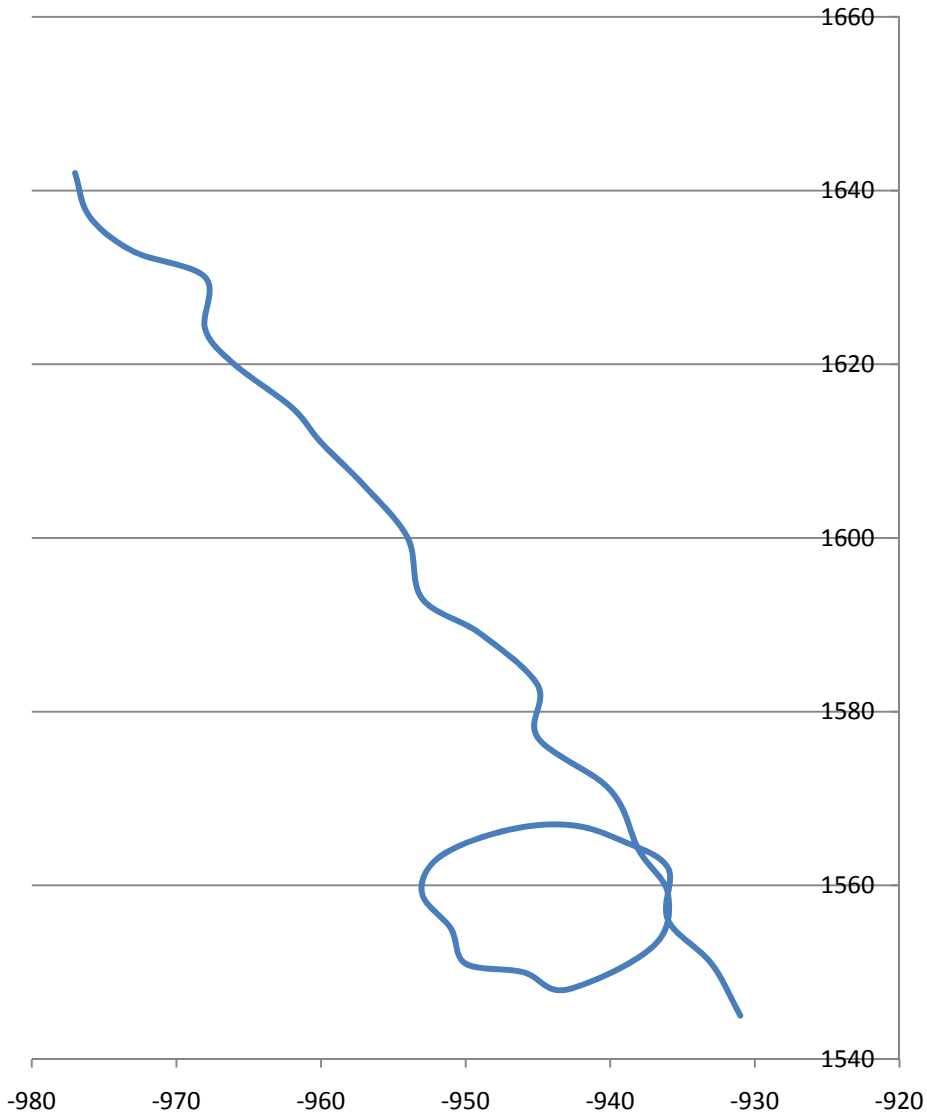
Annotations:

- Message header**: Indicated by a bracket above the first few columns of each row.
- 16-bit signed**: Indicated by a yellow arrow pointing to the 16-bit data field.
- 8-bit signed**: Indicated by a green arrow pointing to the 8-bit data field.
- BCD**: Indicated by a cyan arrow pointing to the BCD data field.

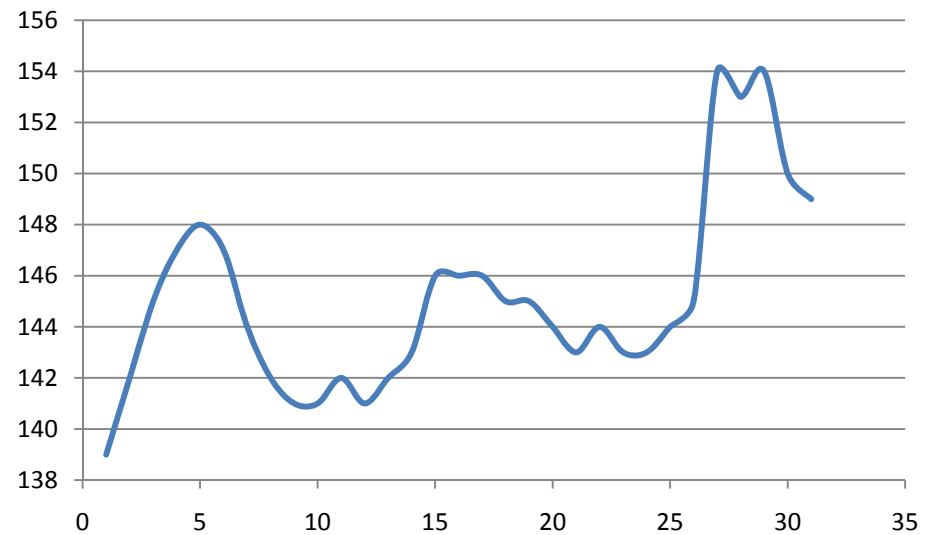
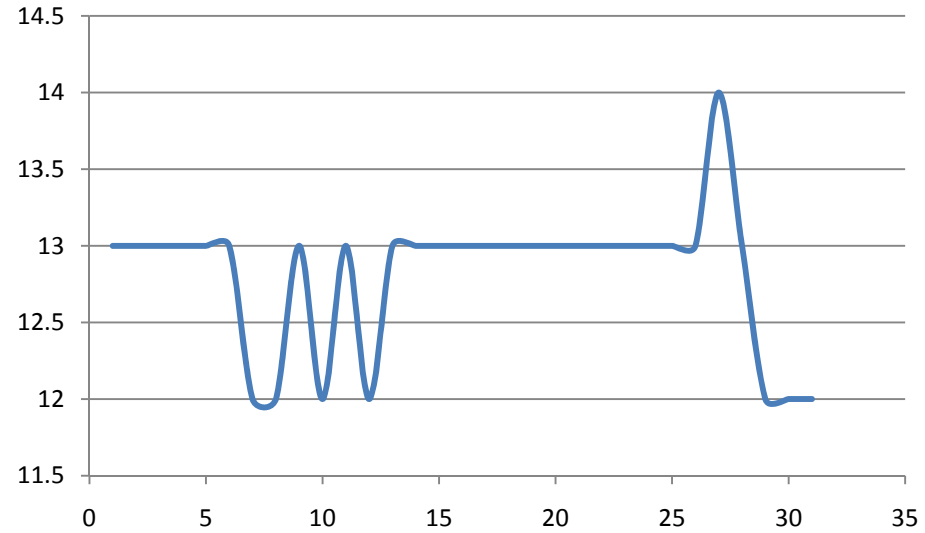
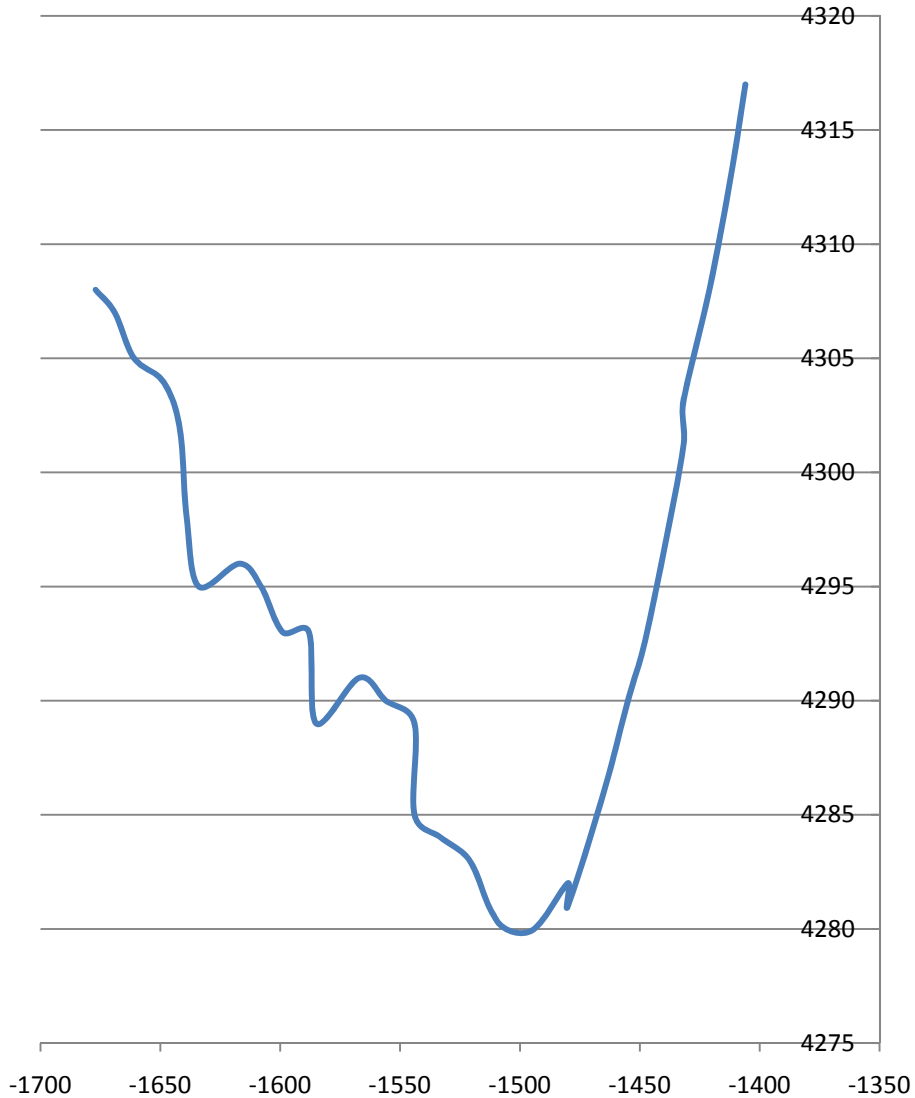
The data is presented in a table format, with columns representing different fields and their values. A large white question mark is overlaid on the data, indicating a search for patterns.

#	Header	16-bit signed	8-bit signed	BCD	Other
0001	[20 049 200]	(1/1) ff 18 80 70 01 24 e9 ae ed 26 1a 07 31 90 19 fa 00 00	03 02 00	72 e9 2e	
0034	[20 051 161]	(1/1) ff 18 80 70 01 24 e9 c7 ed 24 1a 07 31 90 19 fa 00 00	03 02 00	72 e9 2d	
0067	[20 053 121]	(1/1) ff 18 80 70 01 24 e9 d9 ed 2c 1a 07 31 90 19 fa 00 00	03 02 00	71 e9 2d	
0101	[20 055 082]	(1/1) ff 18 80 70 01 24 e9 ee ed 2f 1a 07 31 90 19 fa 00 00	03 02 00	71 e9 2d	
0134	[20 057 043]	(1/1) ff 18 80 70 01 24 e9 ff ed 30 1a 07 31 90 19 fa 00 00	03 03 00	72 e9 2e	
0167	[20 059 004]	(1/1) ff 18 80 70 01 24 e9 00 ed 20 1a 07 31 90 19 fa 00 00	03 02 00	72 e9 2d	
0200	[20 060 221]	(1/1) ff 18 80 70 01 24 e9 01 ed 21 1a 07 31 90 19 fa 00 00	03 02 00	73 e9 2d	
0233	[20 062 182]	(1/1) ff 18 80 70 01 24 e9 02 ed 22 1a 07 31 90 19 fa 00 00	03 02 00	72 e9 2d	
0266	[20 064 142]	(1/1) ff 18 80 70 01 24 ea 4d ed 4c 1a 07 31 90 19 fa 00 00	03 03 00	74 e9 2c	
0299	[20 066 103]	(1/1) ff 18 80 70 01 24 ea 62 ed 4f 1a 07 31 90 19 fa 00 00	03 03 00	71 e9 2c	
0332	[20 068 064]	(1/1) ff 18 80 70 01 24 ea 75 ed 54 1a 07 31 90 19 fa 00 00	03 04 00	70 e9 2c	
0365	[20 070 025]	(1/1) ff 18 80 70 01 24 ea 80 ed 62 1a 07 31 90 19 fa 00 00	03 03 00	6d e9 2d	
0398	[20 071 242]	(1/1) ff 18 80 70 01 24 ea 98 ed 64 1a 07 31 90 19 fa 00 00	03 02 00	6b e9 2d	
0431	[20 073 203]	(1/1) ff 18 80 70 01 24 ea a7 ed 6e 1a 07 31 90 19 fa 00 00	03 00 00	6c e9 2d	
0464	[20 075 164]	(1/1) ff 18 80 70 01 24 ea bc ed 70 1a 07 31 90 19 fa 00 00	03 00 00	6c e9 2d	
0497	[20 077 125]	(1/1) ff 18 80 70 01 24 ea c3 ed 73 1a 07 31 90 19 fa 00 00	02 99 00	6d e9 2d	
0530	[20 079 086]	(1/1) ff 18 80 70 01 24 ea d8 ed 76 1a 08 31 90 19 fa 00 00	03 00 00	6b e9 2b	
0563	[20 081 047]	(1/1) ff 18 80 70 01 24 ea e3 ed 79 1a 08 31 90 19 fa 00 00	03 01 00	69 e9 2b	
0596	[20 083 008]	(1/1) ff 18 80 70 01 24 ea f0 ed 7c 1a 08 31 90 19 fa 00 00	03 01 00	66 e9 2b	
0630	[20 084 225]	(1/1) ff 18 80 70 01 24 ea fd ed 7f 1a 08 31 90 19 fa 00 00	03 01 00	67 e9 2b	
0663	[20 086 187]	(1/1) ff 18 80 70 01 24 eb 02 ed 82 1a 08 31 90 19 fa 00 00	03 01 00	6a e9 2c	
0696	[20 088 148]	(1/1) ff 18 80 70 01 24 eb 19 ed 85 1a 08 31 90 19 fa 00 00	03 01 00	70 e9 2c	
0729	[20 090 109]	(1/1) ff 18 80 70 01 24 eb 36 ed 88 1a 08 31 90 19 fa 00 00	03 03 00	73 e9 2c	
0762	[20 092 069]	(1/1) ff 18 80 70 01 24 eb 53 ed 8b 1a 08 31 90 19 fa 00 00	03 03 00	75 e9 2b	
0795	[20 094 030]	(1/1) ff 18 80 70 01 24 eb 70 ed 8e 1a 08 31 90 19 fa 00 00	03 03 00	76 e9 2b	
0828	[20 095 247]	(1/1) ff 18 80 70 01 24 eb 8d ed 91 1a 08 31 90 19 fa 00 00	03 03 00	75 e9 2b	
0861	[20 097 208]	(1/1) ff 18 80 70 01 24 eb a2 ed 94 1a 08 31 90 19 fa 00 00	03 02 00	74 e9 2b	
0894	[20 099 169]	(1/1) ff 18 80 70 01 24 eb b9 ed 97 1a 08 31 90 19 fa 00 00	03 03 00	72 e9 2b	
0927	[20 101 130]	(1/1) ff 18 80 70 01 24 eb c6 ed 9a 1a 08 31 90 19 fa 00 00	03 03 00	71 e9 2b	
0960	[20 103 091]	(1/1) ff 18 80 70 01 24 eb dd ed 9d 1a 08 31 90 19 fa 00 00	03 03 00	70 e9 2b	
0993	[20 105 052]	(1/1) ff 18 80 70 01 24 eb ef ed c9 1a 08 31 90 19 fa 00 00	03 03 00	70 e9 2b	
1026	[20 107 013]	(1/1) ff 18 80 70 01 24 ec 03 ed cd 1a 08 31 90 19 fa 00 00	03 03 00	71 e9 2b	

Graphing the Data



Graphing the Data





ShowOptions

Select Sound Card

Select Sample Rate

Minimize

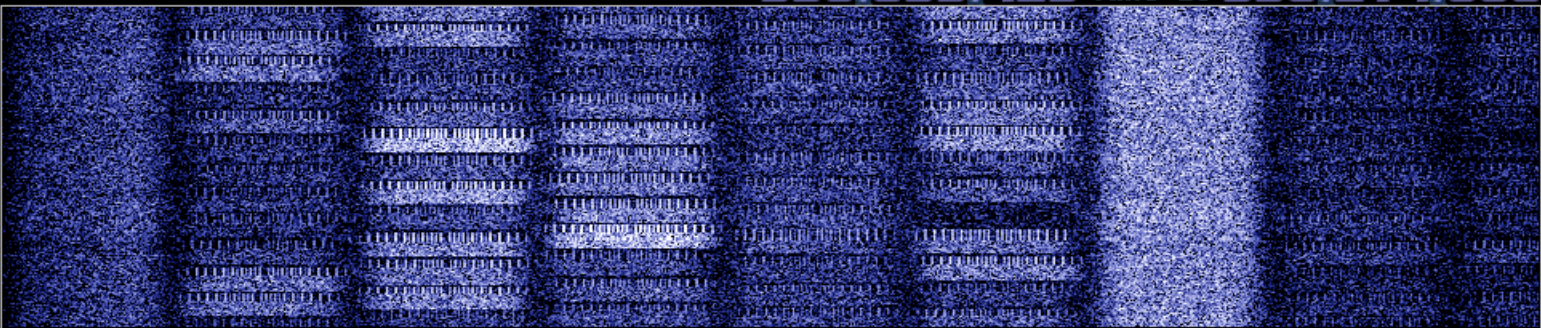
About

Exit

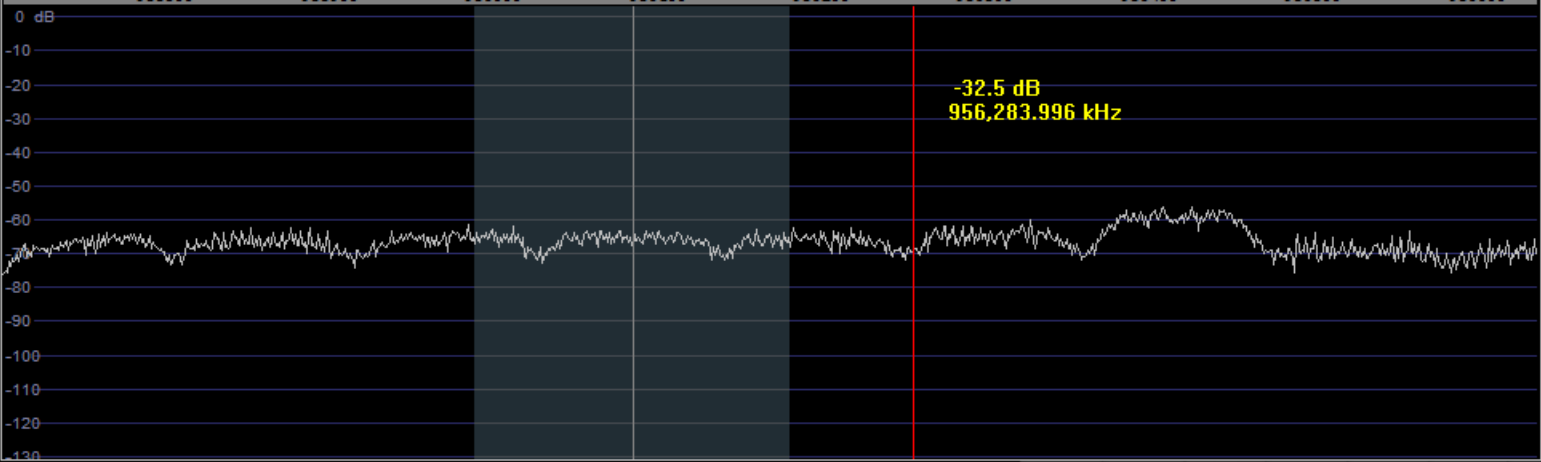
Gain

Contrast

956.099.425 Tune LO 956.214.660



955800 955900 956000 956100 956200 956300 956400 956500 956600



-32.5 dB
956,283.996 kHz

Speed

/10

F

Rev

WF Avg

RBW 976.6 Hz

AM

ECSS

FM

LSB

USB

CW

DRM

Gain

Contrast



Wide BW FM
Post D. BP Filter
Deemph. 50uS
Hc 3000 Hz
Lc 250 Hz

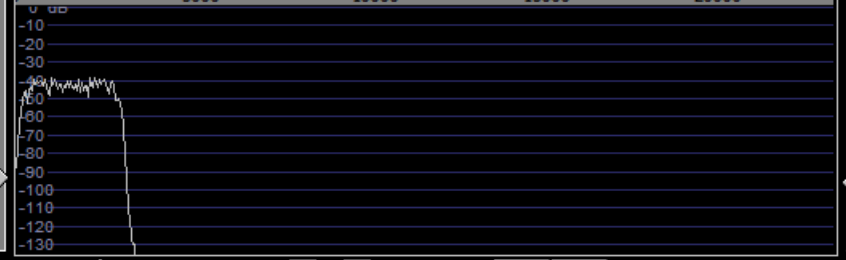
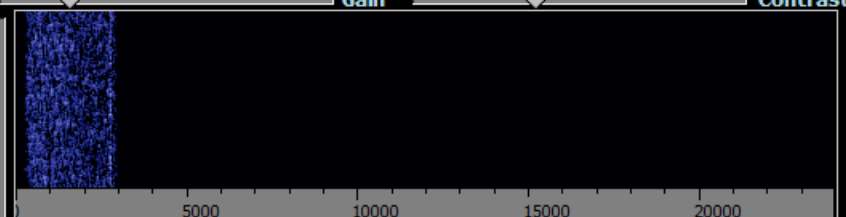
Vol

Mute
avg
bs
sql

Squelch

Avg SP1 Avg SP2

6 2



Speed

F

N

WF Avg

RBW 46.9 Hz

HSDR 20110725 070652Z 956215kHz RF.wav
Jul 25, 2011 - 07:07:46Z



Privilege

Time Mix Freq.

ZAP AFC Nlock
N. Red. CW Peak
NB Notch1
Disp Notch2

Notch
F1 1000.0 Hz
BW1 200 Hz
F2 1500.0 Hz
BW2 200 Hz

24/10/2011 11:40:36 PM

CPU Load

WRplus (8%)
Total (10%)



ShowOptions

Select Sound Card

Select Sample Rate

Minimize

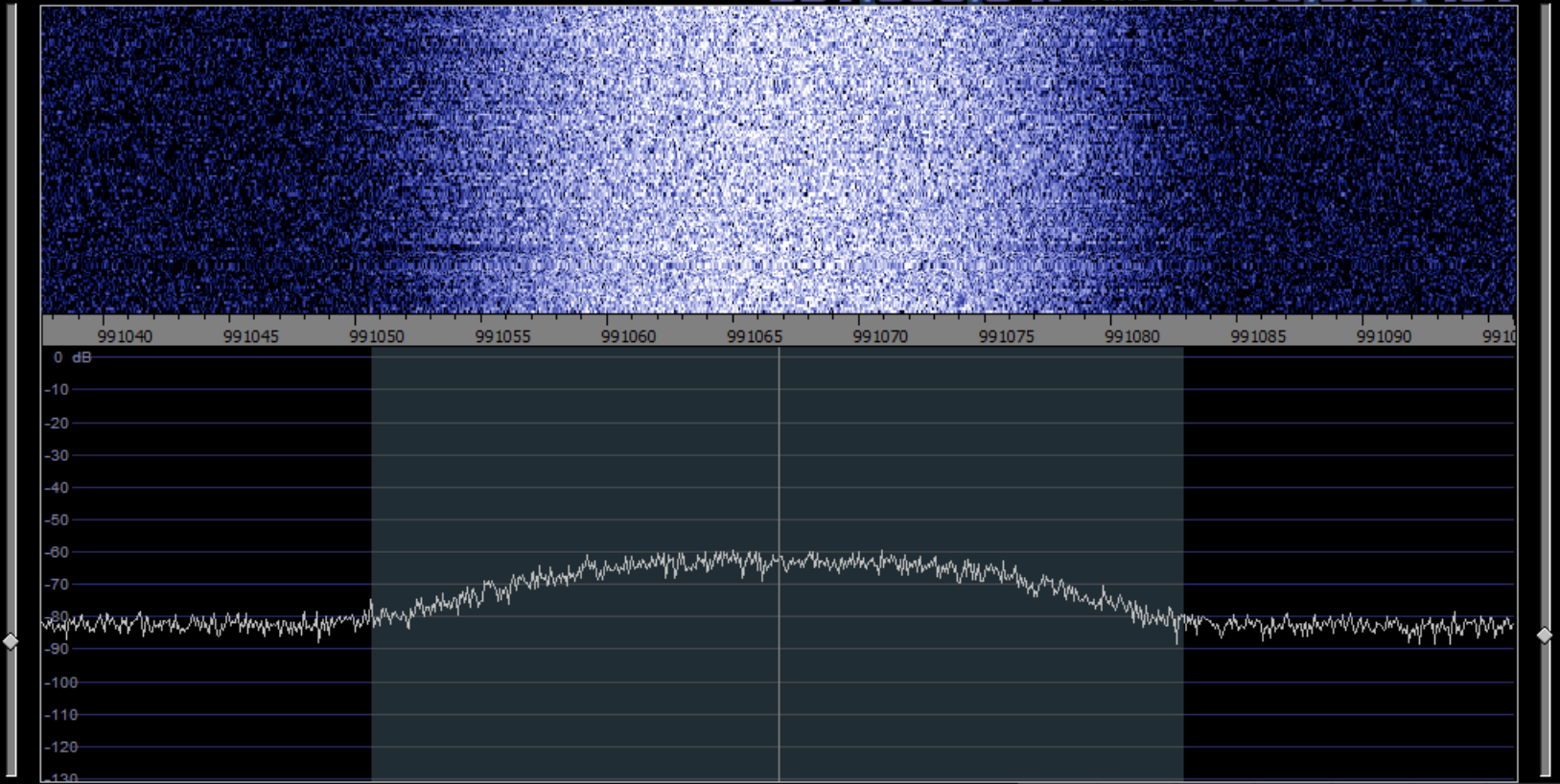
About

Exit

Gain

Contrast

991.066.847 Tune LO 990.995.401



Speed

/10

F

Rev

WF Avg

<

>

RBW 61.0 Hz

AM

ECSS

FM

LSB

USB

CW

DRM

Gain

Contrast



Mid BW FM

Hc 3000 Hz
Lc 250 Hz

Vol

Mute

avg

bs

sql

-102

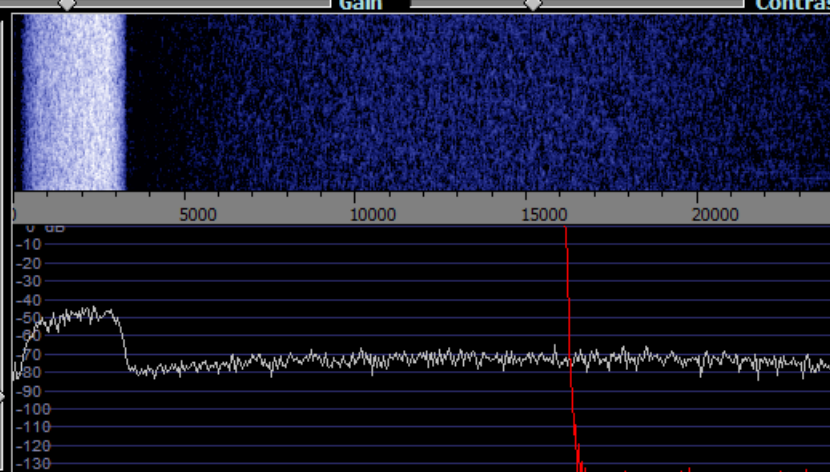
Squelch

Avg SP1

Avg SP2

6

2



Speed

F

N

WF Avg

<

>

RBW 46.9 Hz

HSDR 20110725 065558Z 990995kHz RF.wav
Jul 25, 2011 - 06:56:43Z



Privilege

Time Mix Freq.

ZAP

AFC

Mlock

N. Red.

CW Peak

NB

Notch1

Desp

Notch2

Notch

F1 1000.0 Hz

BW1 200 Hz

F2 1500.0 Hz

BW2 200 Hz

25/10/2011 12:40:25 PM

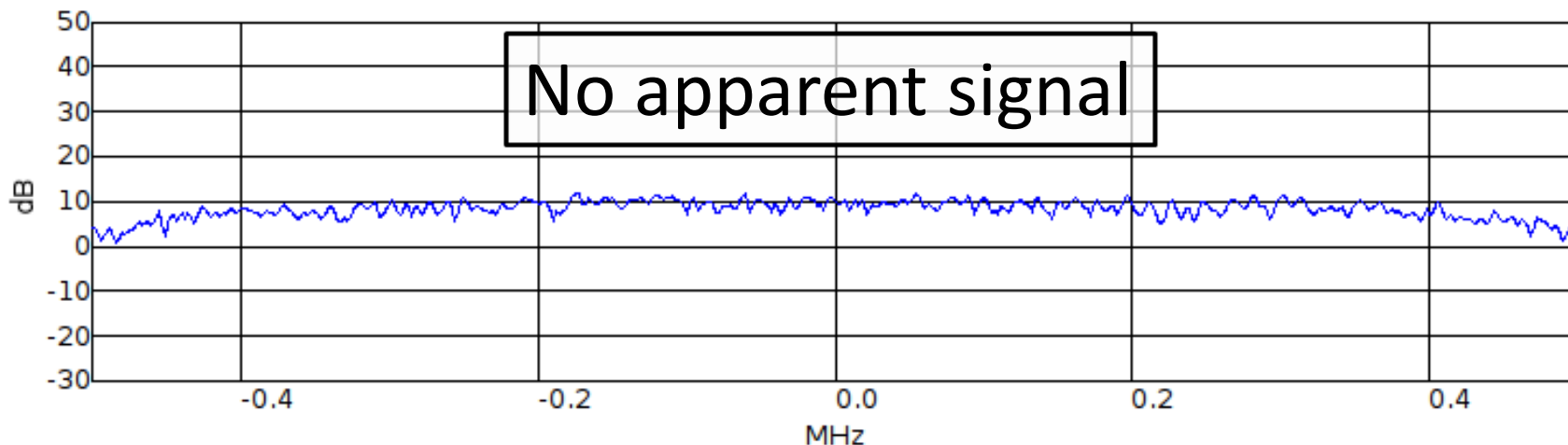
CPU Load



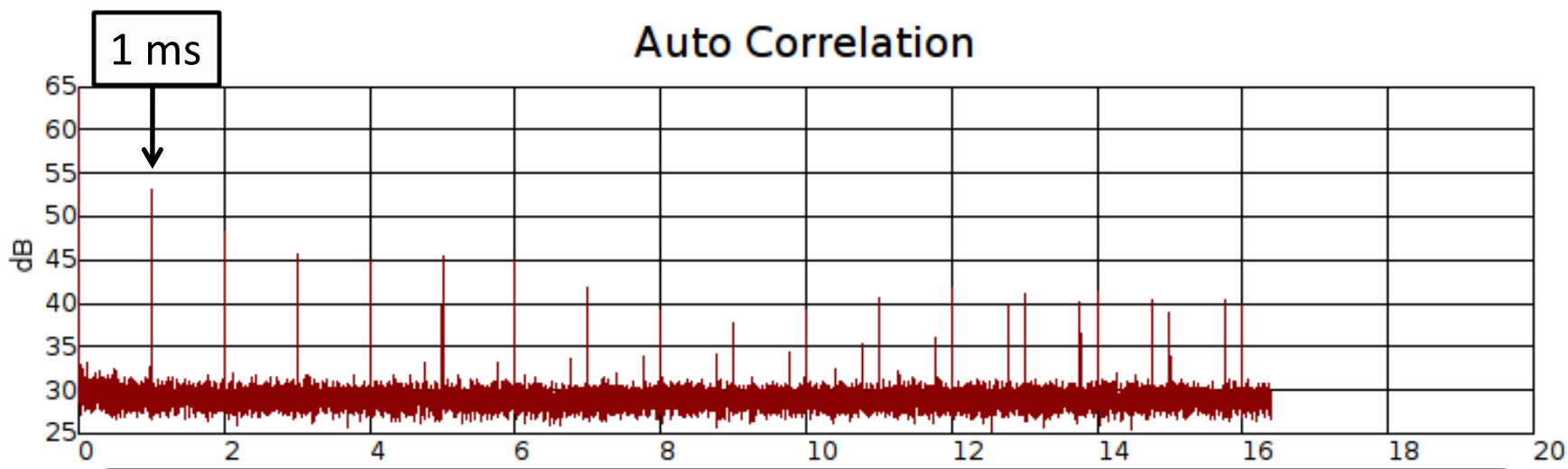
WRplus (14%)
Total (25%)

File

FFT



Auto Correlation



Cyclic 1023 bit code @ 1.023 MHz chip rate

Center freq: 1.57542G

Decim:

Fs@USB: 1M

DBS Rx

Analog BB: 1.5755G

DDC: 80

OK

CDMA Detection with GRC

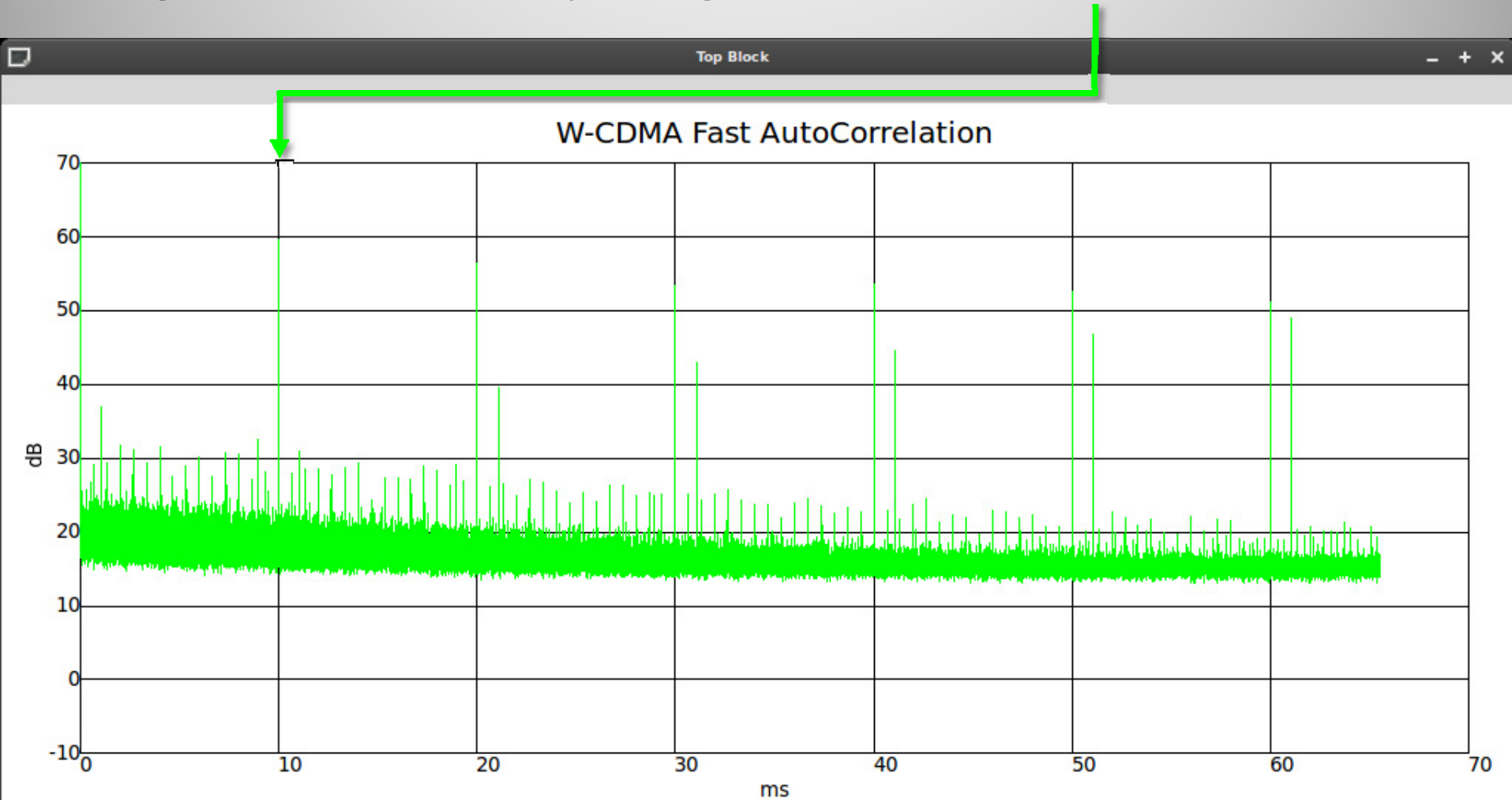
The screenshot displays the GNU Radio Companion (GRC) interface for a W-CDMA detection project. The main workspace contains three parallel signal paths, each starting with a USRP Source block and ending with a specific analysis sink. The paths are annotated with text boxes:

- 2.1 GHz 3G:** The top path uses a USRP Source (Unit 0, Decimation 20, Frequency 2.1125G, Gain 10 dB, Side A, RX Antenna RX2) connected to a Waterfall Sink (Title: Waterfall Plot, Sample Rate 3.2M, Baseband Freq 0, Dynamic Range 100, Reference Level 50, Ref Scale (p2p) 2, FFT Size 512, FFT Rate 15). An annotation box states: "Visualise intensity of frequency components over time".
- 850 MHz NextG:** The middle path uses a USRP Source (Unit 0, Decimation 20, Frequency 842.5M, Gain 25 dB, Side A, RX Antenna RX2) connected to an FFT Sink (Title: FFT Plot, Sample Rate 3.2M, Baseband Freq 0, Y per Div 10 dB, Y Divs 10, Ref Level (dB) 50, Ref Scale (p2p) 2, FFT Size 1.024k, Refresh Rate 30). An annotation box states: "Visualise instantaneous frequency spectrum".
- L1 GPS:** The bottom path uses a USRP Source (Unit 0, Decimation 20, Frequency 1.57542G, Gain 15 dB, Side A, RX Antenna RX2) connected to a Fast AutoCorrelation Sink (Title: W-CDMA F...Correlation, Sample Rate 3.2M, Baseband Freq 0, Size 131.072k, Rate 5, Y per Div 10 dB, Ref Level (dB) 50, Average Alpha 300m, Window Size 1.024k, 240). An annotation box states: "Find repeating patterns buried within a signal".

On the left side, there are control panels for "Options" (ID: top_block), "Variable" (ID: decim, Value: 20), "Variable" (ID: samp_rate, Value: 3.2M), and "Variable Slider" (ID: gain, Label: Gain, Default Value: 20, Minimum: 0, Maximum: 50, Converter: Float). The top menu bar includes File, Edit, View, Build, and Help. The toolbar contains various icons for file operations and execution. The top status bar shows the project name "W-CDMA.grc" and the current directory "/home/mint/Documents - GNU Radio Companion". The right sidebar shows a "Blocks" list with categories like Sources, Sinks, Graphical Sinks, Operators, Type Conversions, Stream Conversions, Misc Conversions, Synchronizers, Level Controls, and Filters. The bottom status bar shows the loading and showing status of the project files.

3G W-CDMA

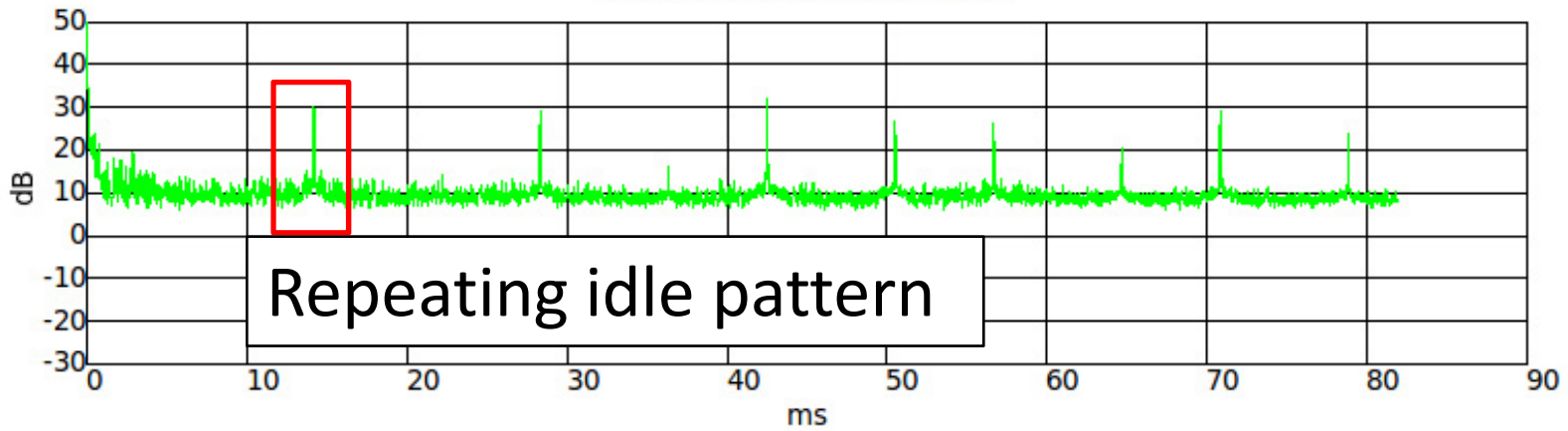
Signature of UMTS: repeating data in CPICH at 10 ms intervals



TETRA

BB Demod Xtra

Fast AutoCorrelation



Scope Plot



Axes Options

Secs/Div: + -

Counts/Div: + -

Y Offset: + -

T Offset: ||

Autorange

Channel Options

Ch1 Ch2 Trig XY

Coupling: DC

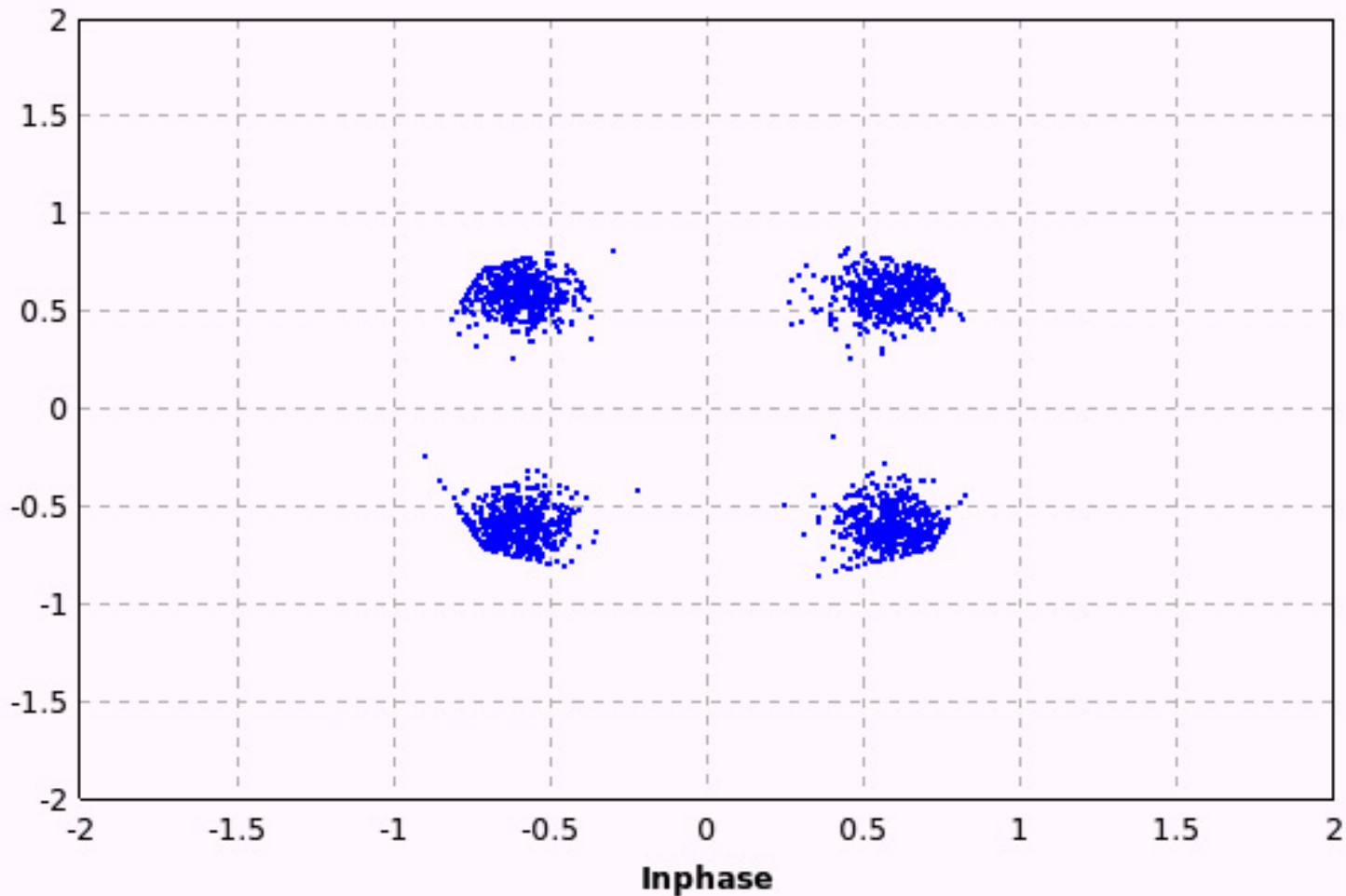
Marker: Line Link

BB

Demod

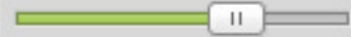
Xtra

TETRAz

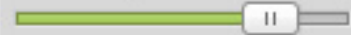


Options

Alpha: 10m



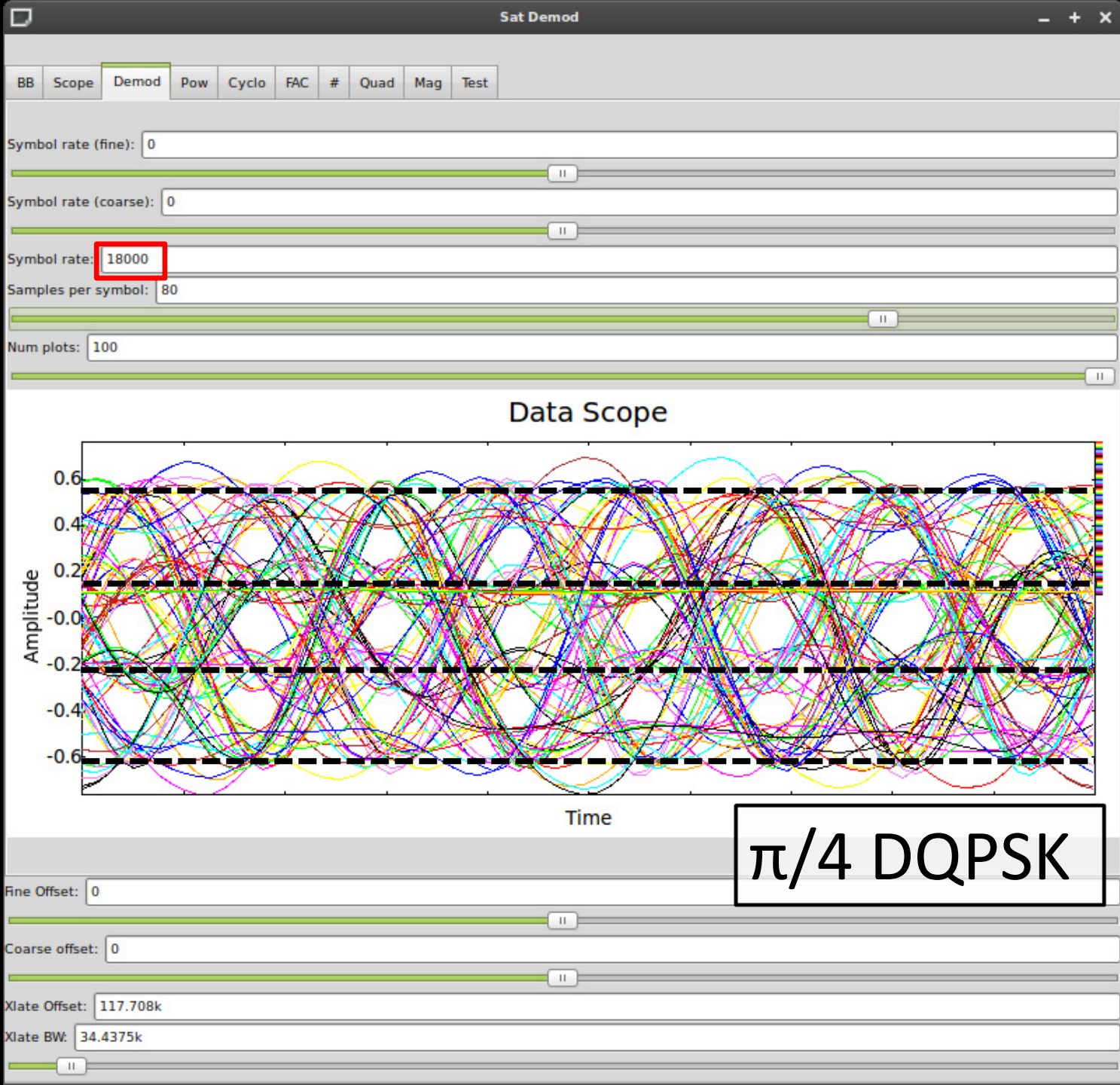
Gain Mu: 50m



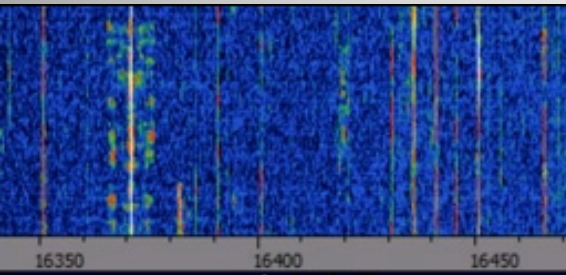
Marker: Dot Medium



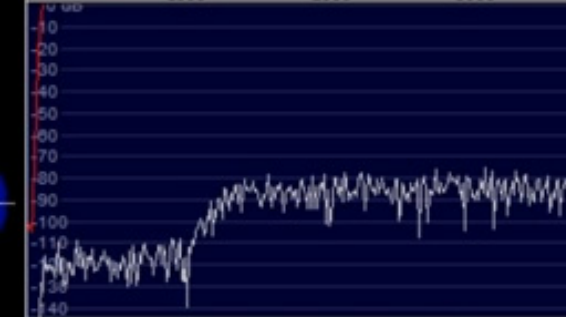
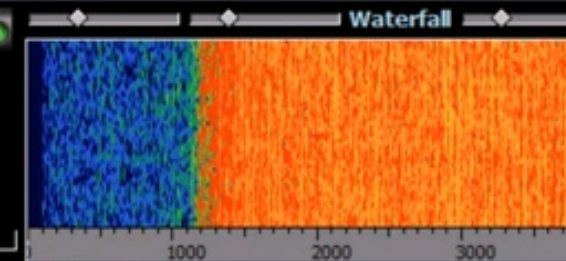
Stop



STANAG 4285



-34.3 dB
16,401.322 kHz



STANAG-4285

STANAG-4285 is specified by the NATO (North Atlantic Treaty Organization) Military Agency for Standardization in "Characteristics of 1200 / 2400 / 3600 Bits per Second Single Tone Modulators / Demodulators for HF Radio Links" (16. February 1989).

Parameter	Value
Frequency range	HF
Operation modes	Broadcast/Simplex FEC
Modulation	8-PSK
Center frequency	1800 Hz
Symbol rate	2400 Bd
Receiver settings	DATA, CW, LSB or USB
Input format(s)	AF, IF

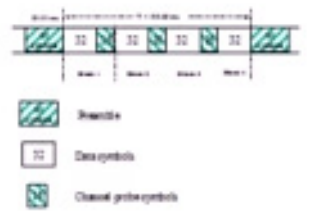
The modulation technique used in this mode consists of **phase shift keying** (8-PSK) of a single tone sub-carrier of 1800 Hz. The modulation speed (symbol rate) is always 2400 Bd.

Using different M-PSK modulations and FEC (Forward Error Correction) coding rates, serial binary user information (raw data) accepted at the line side input can be transmitted at different user data rates.

STANAG 4285 single tone waveform has the following characteristics which may be selected from **Options [Frame Format...]**:

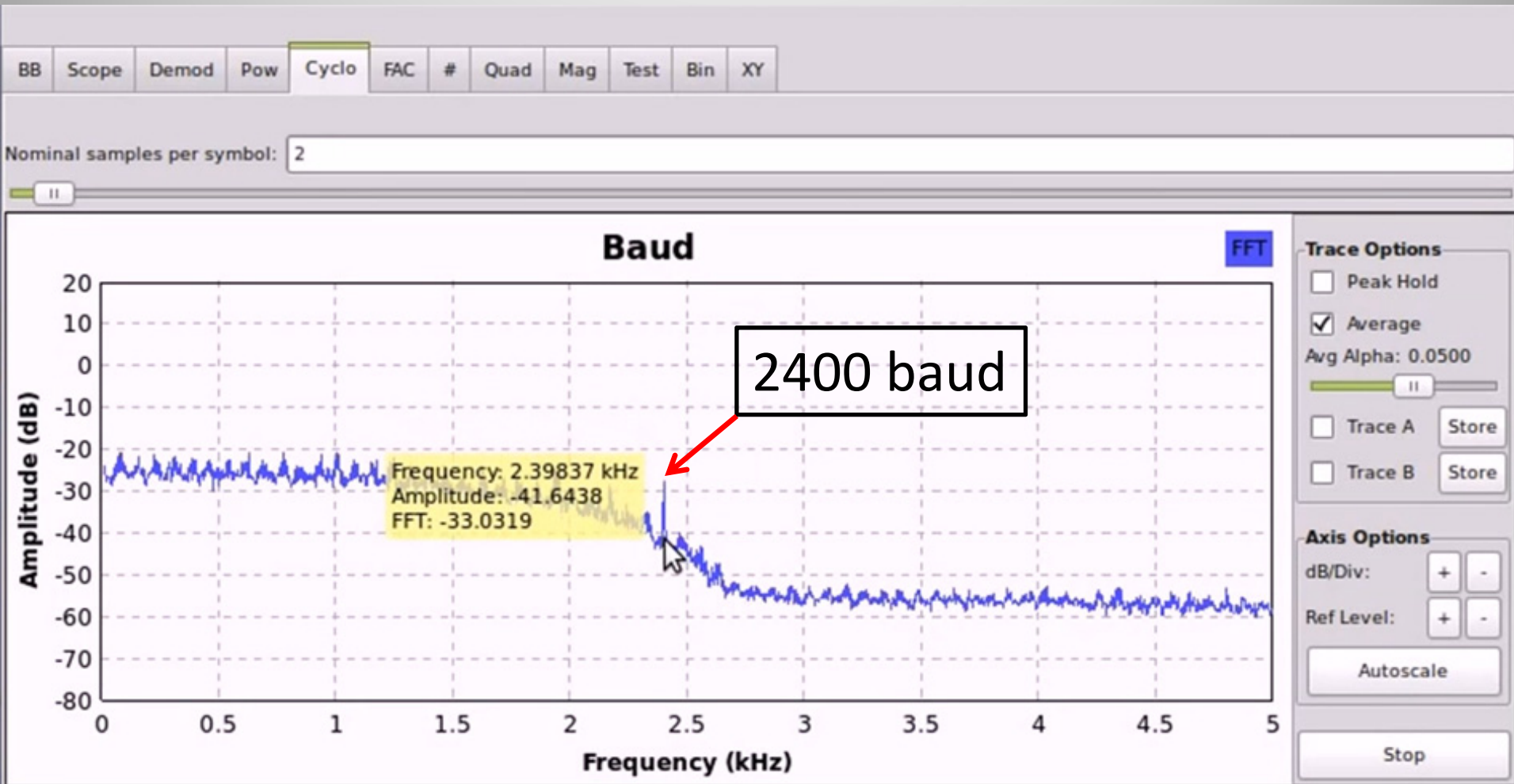
Baud Rate	User data rate (bps)	User data rate (bps)	FEC coding rate	Interleaver	No. of unknown 8-phase symbols (User Data)	No. of known 8-phase symbols (Channel Probe)
2400	2400	3 (8-PSK)	2 / 3	SHORT or LONG	32	16
2400	1200	2 (QPSK)	1 / 2	SHORT or LONG	32	16
2400	600	1 (BPSK)	1 / 2	SHORT or LONG	32	16
2400	300	1 (BPSK)	1 / 4	SHORT or LONG	32	16
2400	150	1 (BPSK)	1 / 8	SHORT or LONG	32	16
2400	75	1 (BPSK)	1 / 16	SHORT or LONG	32	16
2400	3600	3 (8-PSK)	No coding	ZERO	32	16
2400	2400	2 (QPSK)	No coding	ZERO	32	16
2400	1200	1 (BPSK)	No coding	ZERO	32	16

The user data is transmitted using a continuous frame structure. Each frame begins with a 33.33 ms preamble containing 80 symbols, the next 176 symbols are divided into four 32-symbol data segments and three 16-symbol channel probe segments.

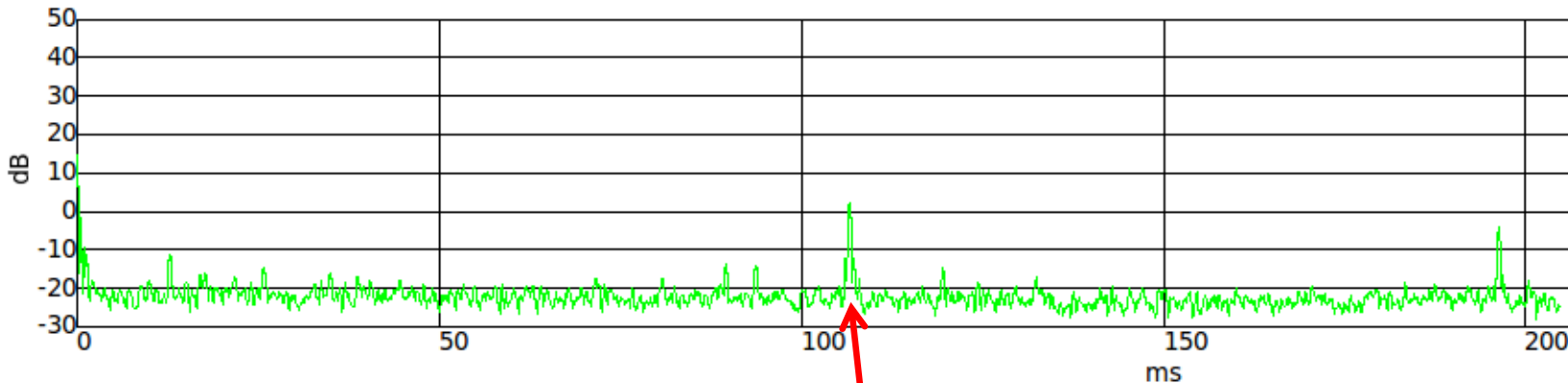


At the end of transmission, a certain bit-pattern (in hexadecimal notation, 4B65A5B2, MSB first) is sent to **mark** the end of message (EOM). The

STANAG 4285



Fast AutoCorrelation



80 (preamble) +
4 x 32 (data) +
3 x 16 (channel probe)
@ 2400 bps
= **106.66 ms**

Fine Offset: 0

Coarse offset: 0

Xlate Offset: -306.325k

Xlate BW: 5k

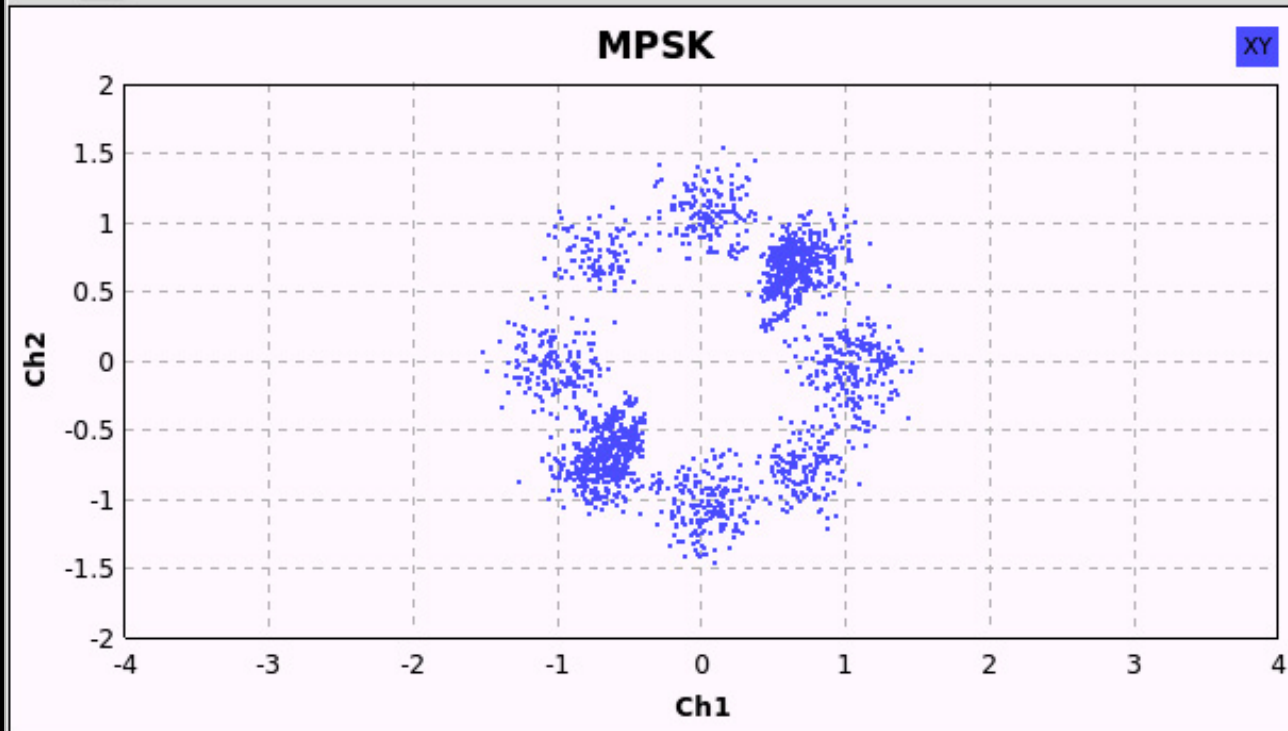


BB Demod Xtra Eye Histo FEC PSK FAC

Gain Mu: 10.481m



Alpha: 20.96m



Axes Options

X/Div: + -

Y/Div: + -

X Off: + -

Y Off: + -

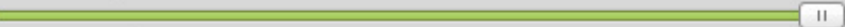
Autorange

Channel Options

Ch1	Ch2	Trig	XY
Channel X: Ch 1 ⌵			
Channel Y: Ch 2 ⌵			
Marker: Dot Med ⌵			

Stop

Fine Offset: 0

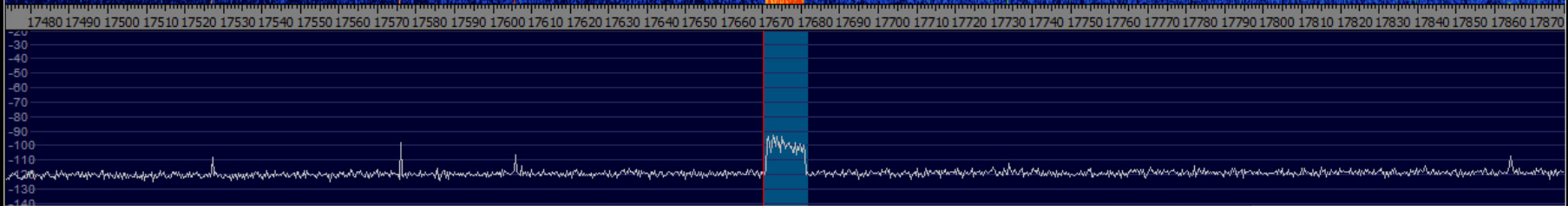


Xlate Offset: -306.325k

Xlate BW: 5k



Digital Radio Mondiale



AM ECSS FM LSB USB CW **DRM**

Locked
LO(B) **0017,905,579** FreqMgr
Tune **0017,670,027** ExtIO
Volume#
Level

5-units Squelch +20 +40

Soundcard [F5] HSDR_20111228_222203Z_17906kHz_RF.wav
Samplerate [F6] Dec 28, 2011 - 22:23:09Z
Options [F7]

Info / Update [F9]
Full Screen [F11]

Minimize [F3]
Exit [F4]

NR NB Notch
Mute AGC Off Despread
CW ZAP CW AFC CW Peak CW FullBw

27/02/2012 6:13:03 PM
CPU:HSDR (21%)
CPU:Total (34%)

Phase

Waterfall Spectrum RBW 30.5 Hz 2 Avg Speed
Zoom

1000 2000 3000 4000 5000 6000 7000 8000 9000 10000 11000

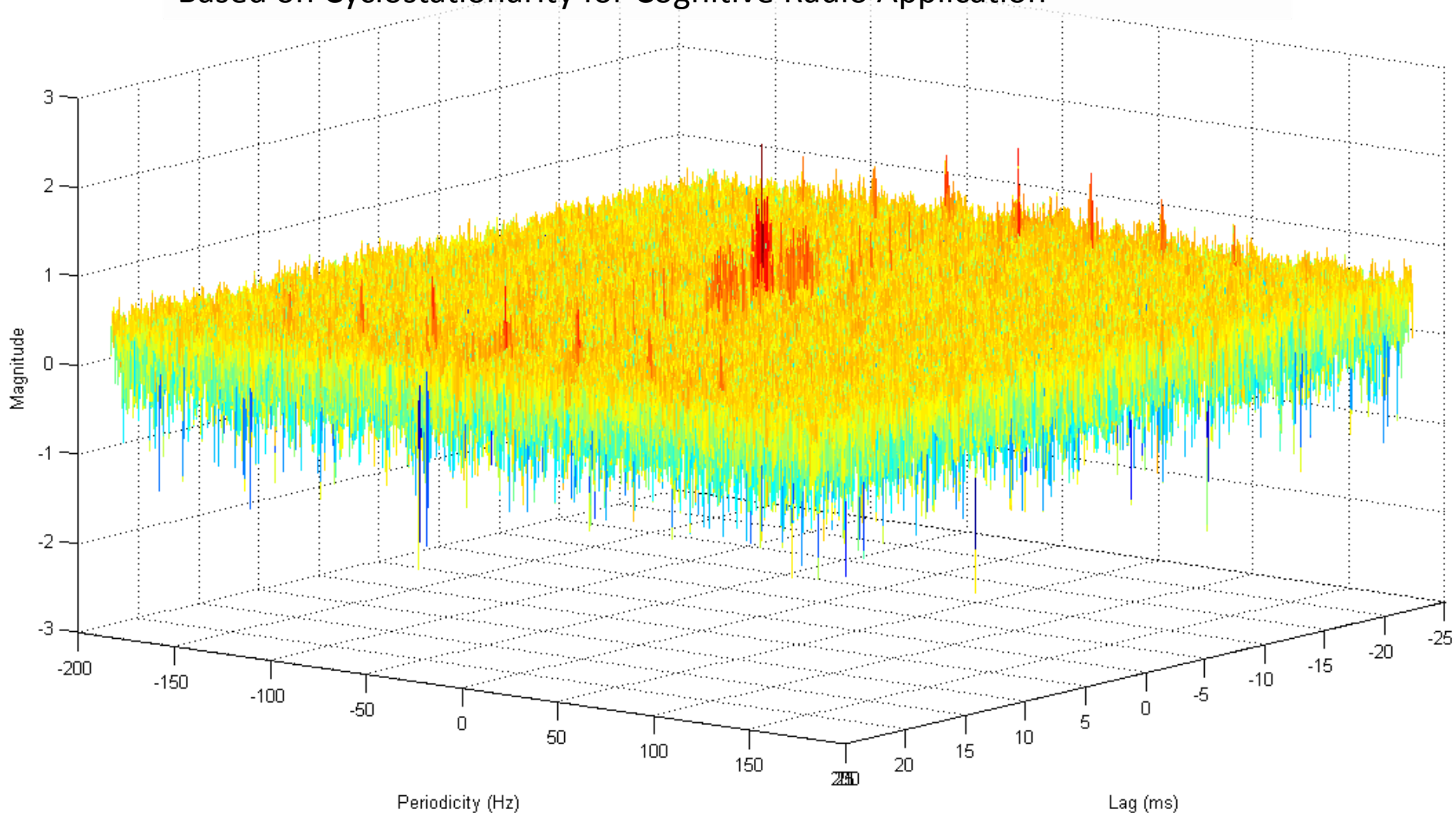
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-140

Waterfall Spectrum RBW 23.4 Hz 1 Avg Speed



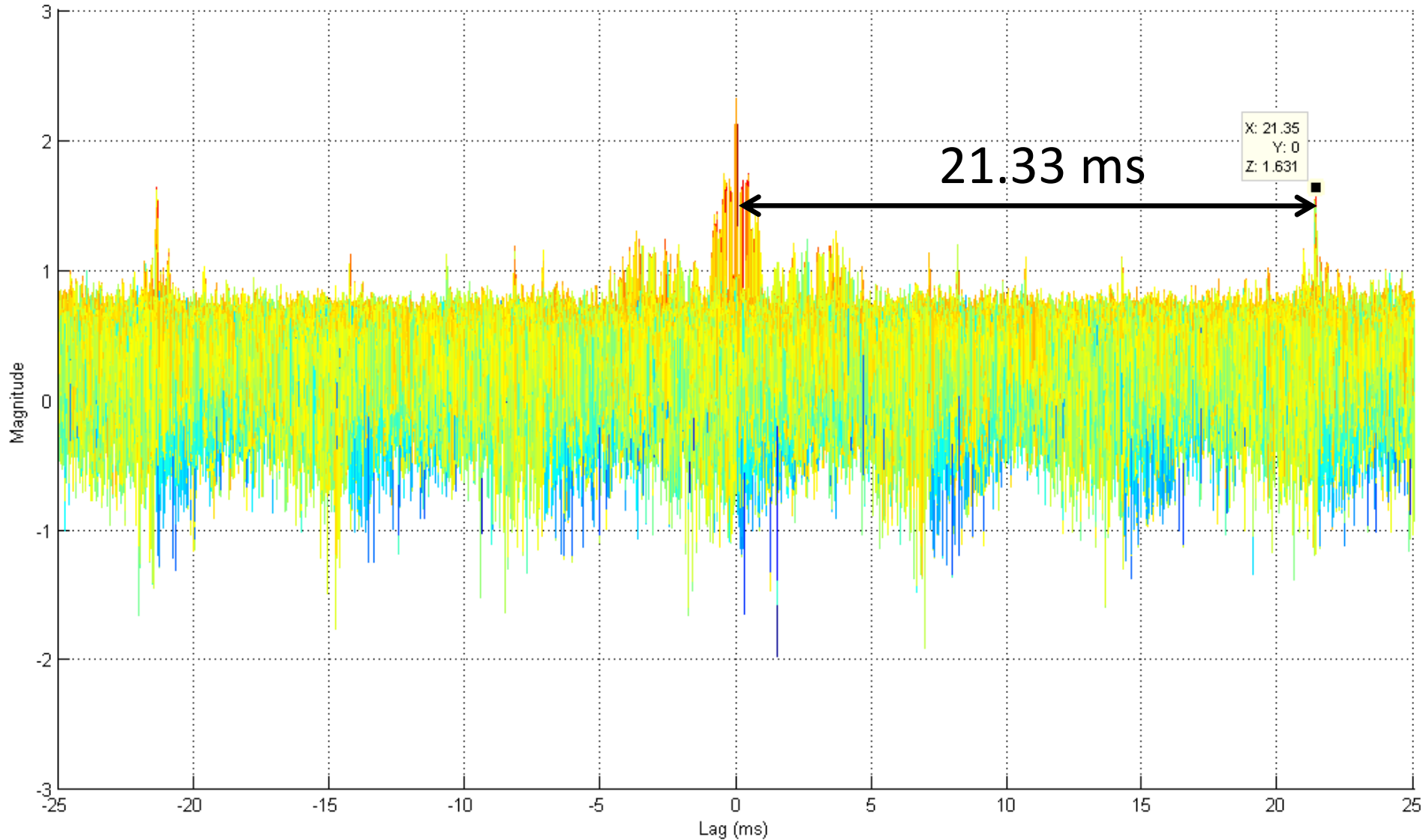
Cyclic Autocorrelation Function

Han, Sohn & Mounq, "A Blind OFDM Detection and Identification Method Based on Cyclostationarity for Cognitive Radio Application"

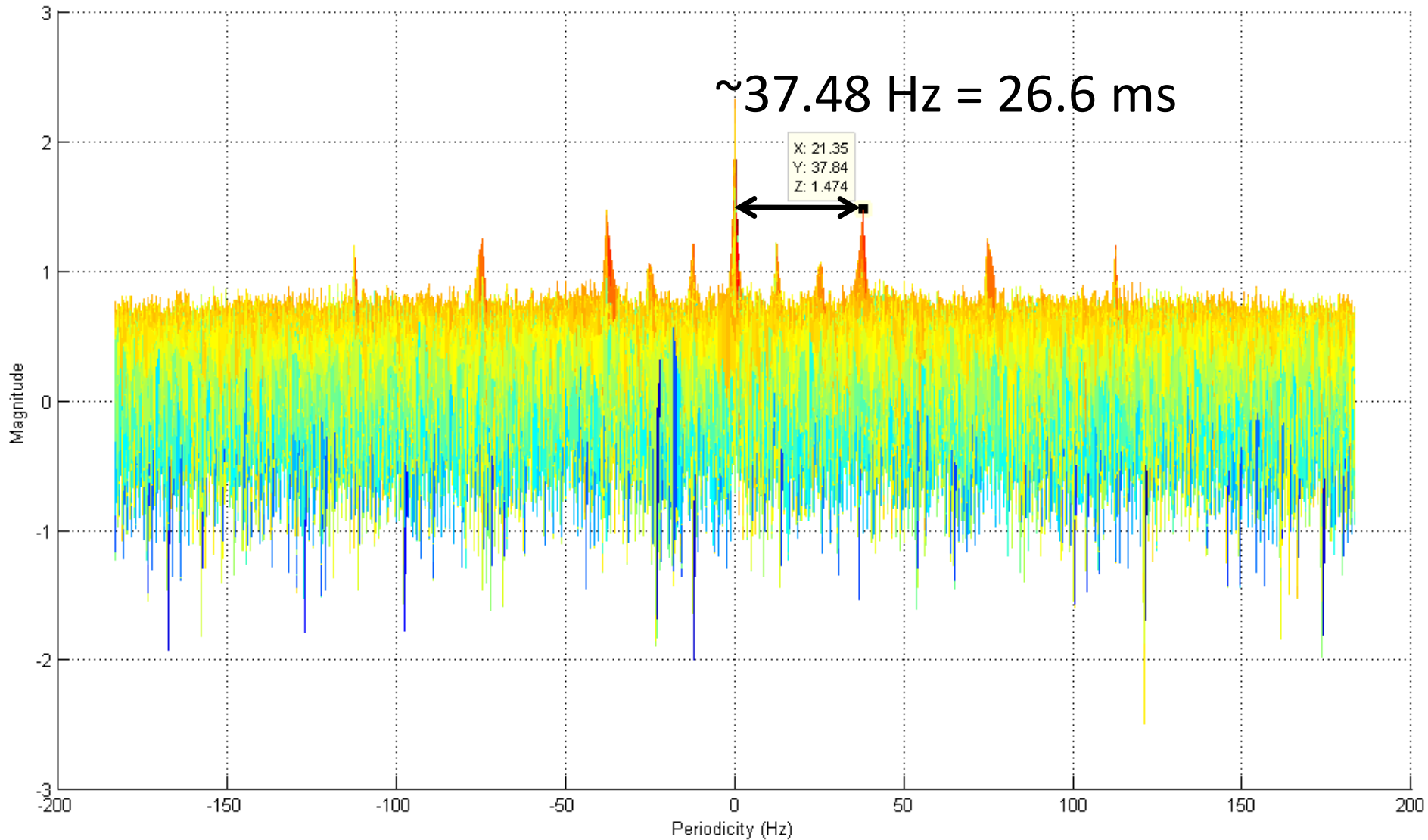




Un-guarded Symbol Time

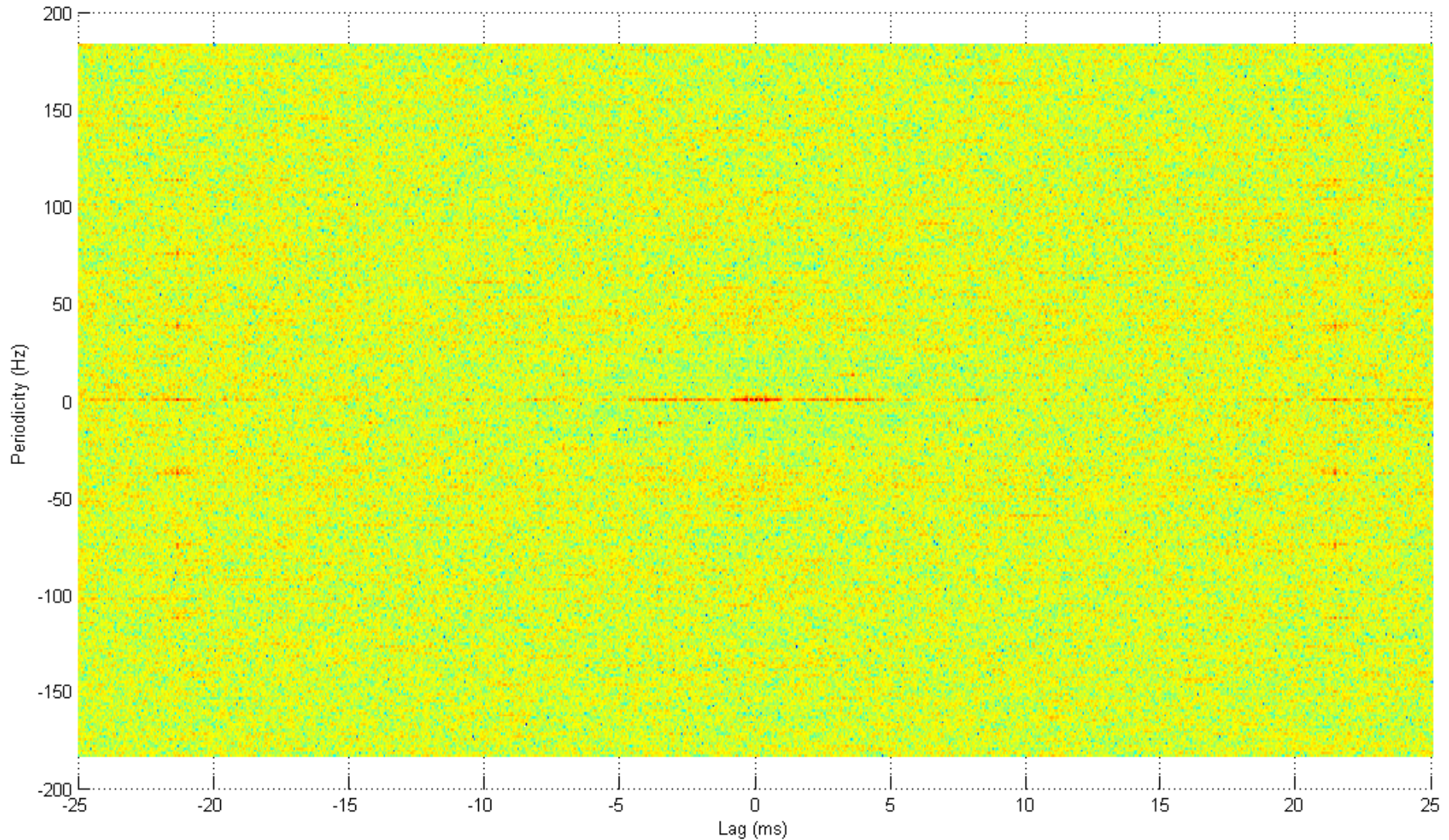


Total Symbol Duration





Top-down DRM Symmetry



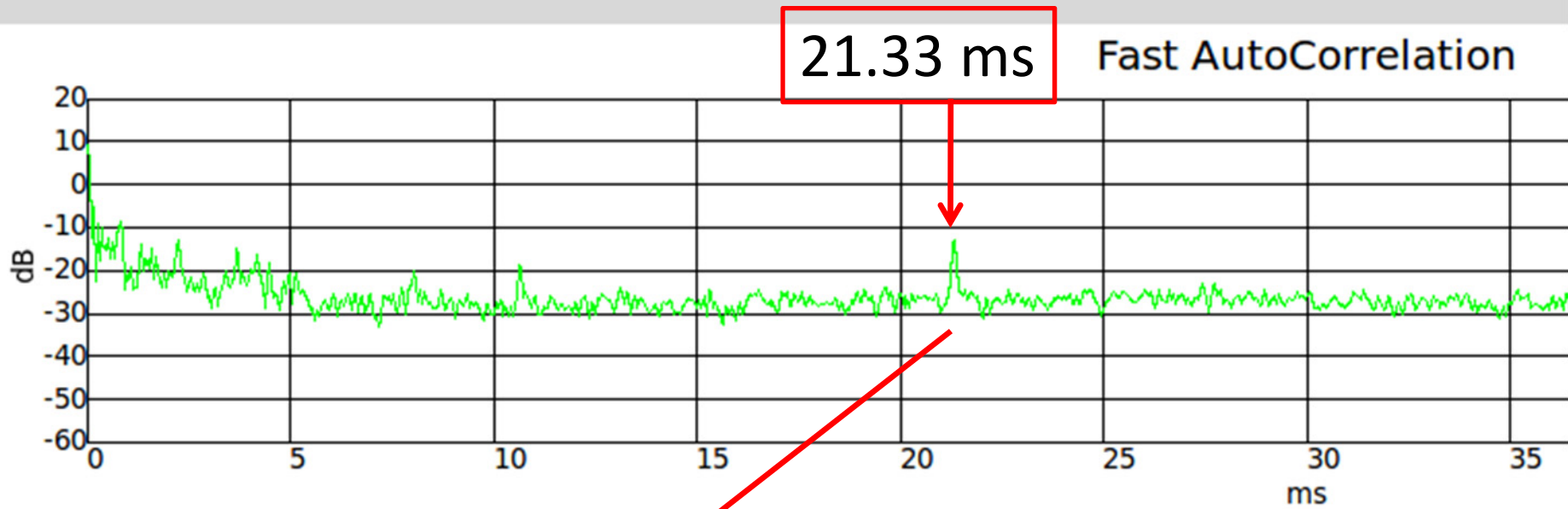


DRM Class B

<u>Modulation property</u>	<u>Value</u>
Un-guarded symbol time	21.33 ms
Sub-carrier spacing	46 7/8 Hz
Guard interval	5.33 ms
Total symbol duration	26.66 ms
Guard interval ratio	1/4
Symbols per frame	15

← 1 / (21.33 ms)

BB FAC Cyc CAF Test



$$(1 \text{ Msps} / 50) \times 21.33 \text{ ms} = 426.6$$

Fine Offset: 0

Coarse offset: 0

Xlate Offset: 229.8k

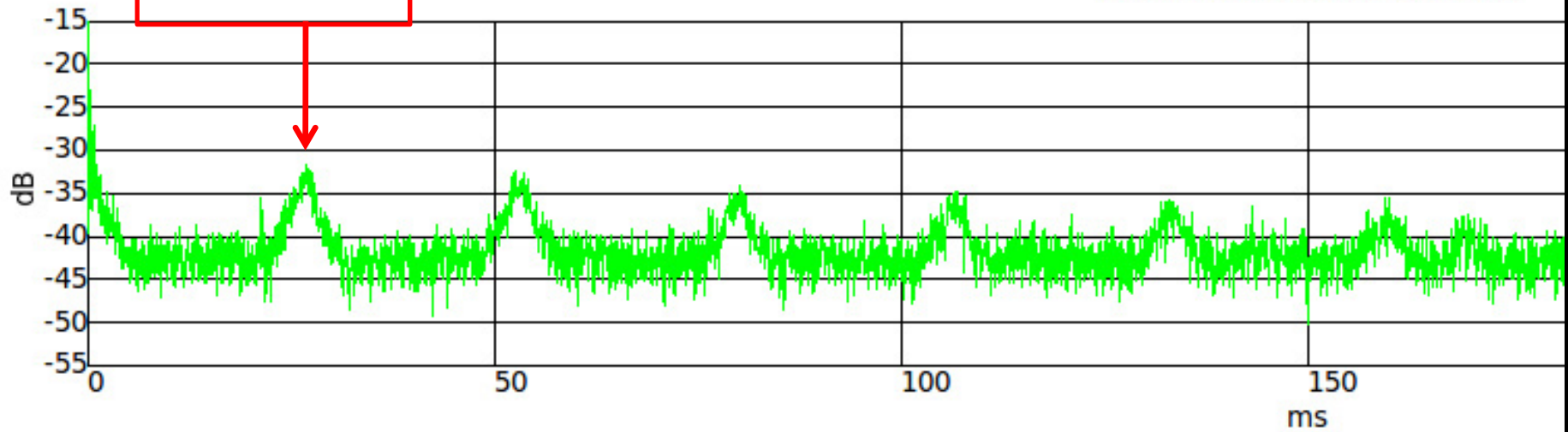
Xlate BW: 10.97k

Cyclo Lag: 427

BB FAC Cyc CAF Test Channels

26.66 ms

Fast AutoCorrelation



Fine Offset: 0

Coarse offset: 0

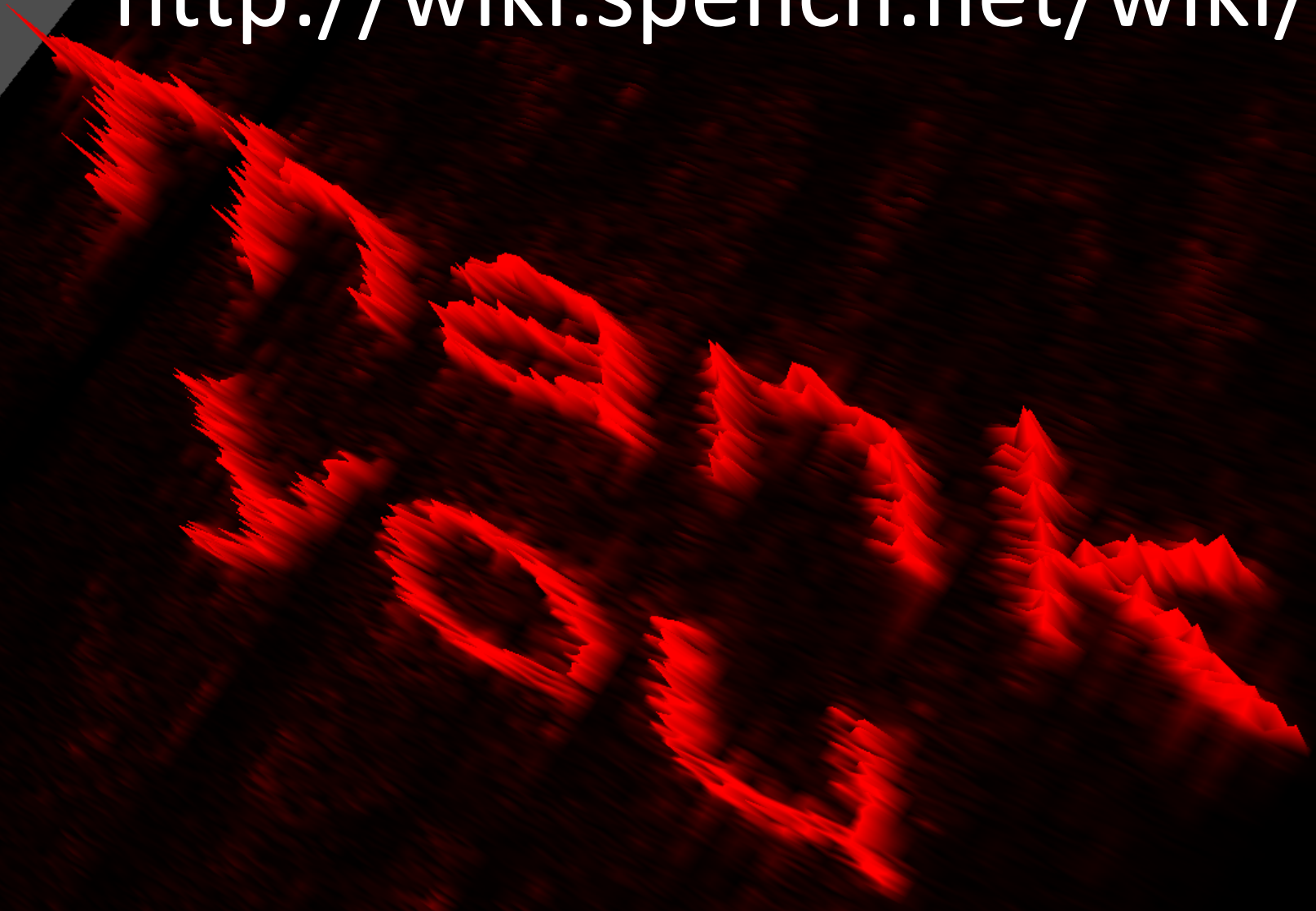
Xlate Offset: 229.8k

Xlate BW: 10.97k

Cyclo Lag: 427



<http://wiki.spench.net/wiki/RF>



balint@ettus.com

@spenchnet