Cyberspectrum #23

X-Band Satellites Data-link

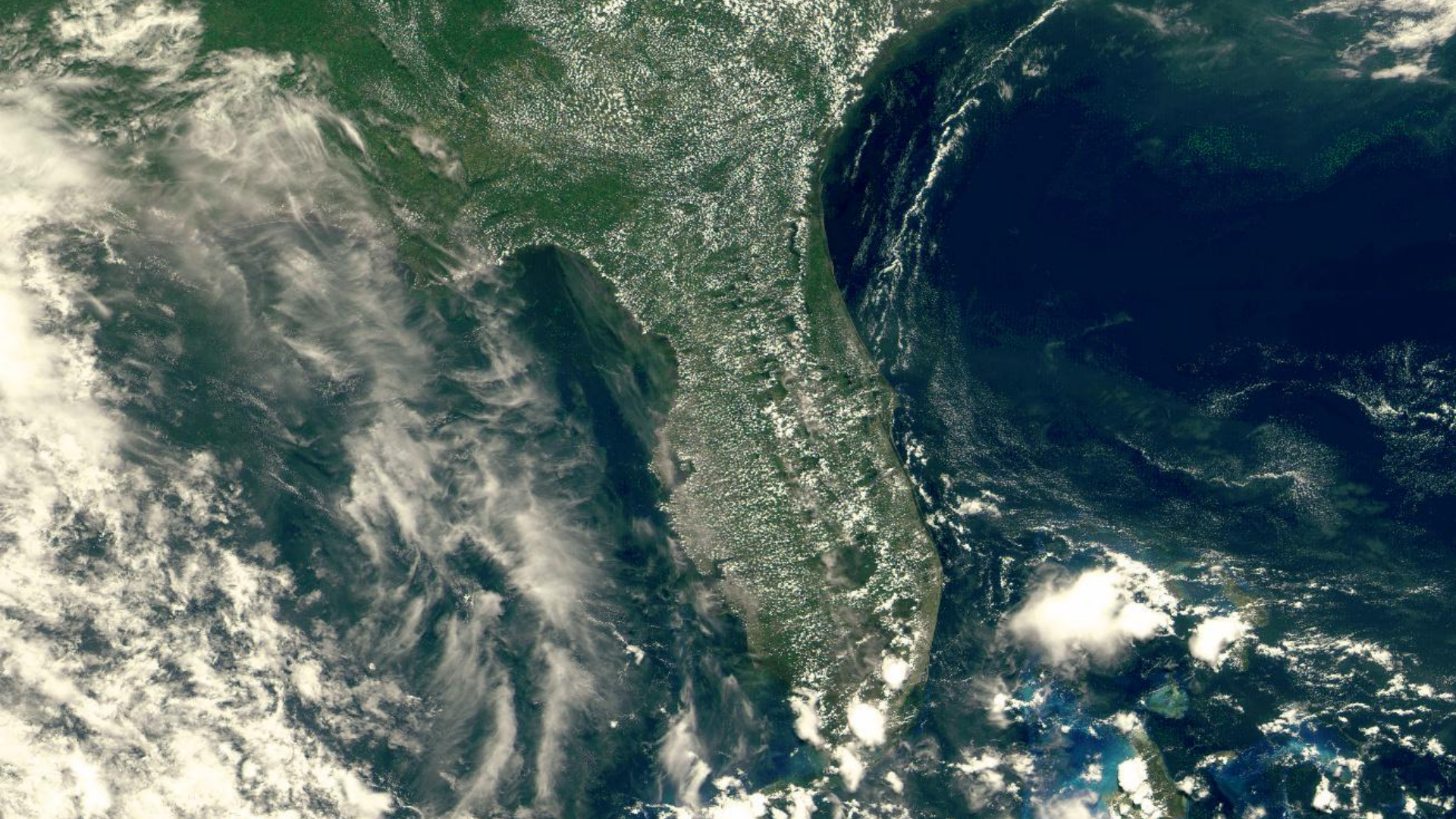
Wireless Village
DEF CON 26

Luigi Freitas Cruz
@luigifcruz

9 August 2018

Open Satellite Project

- Non-profit organization.
- Open-Source Software.
- Focused in Weather Satellites.
- Five Datalinks Currently Supported.
- Mainly Geostationary Spacecraft.
- Awesome Earth Pictures!



GOES-16 - L-Band HRIT

Level: Starter

- L-Band Signal (1.694.100 MHz)
- Low Bandwidth (~1 MHz)
- Fixed Position (Geostationary)
- Standard low overhead encoding

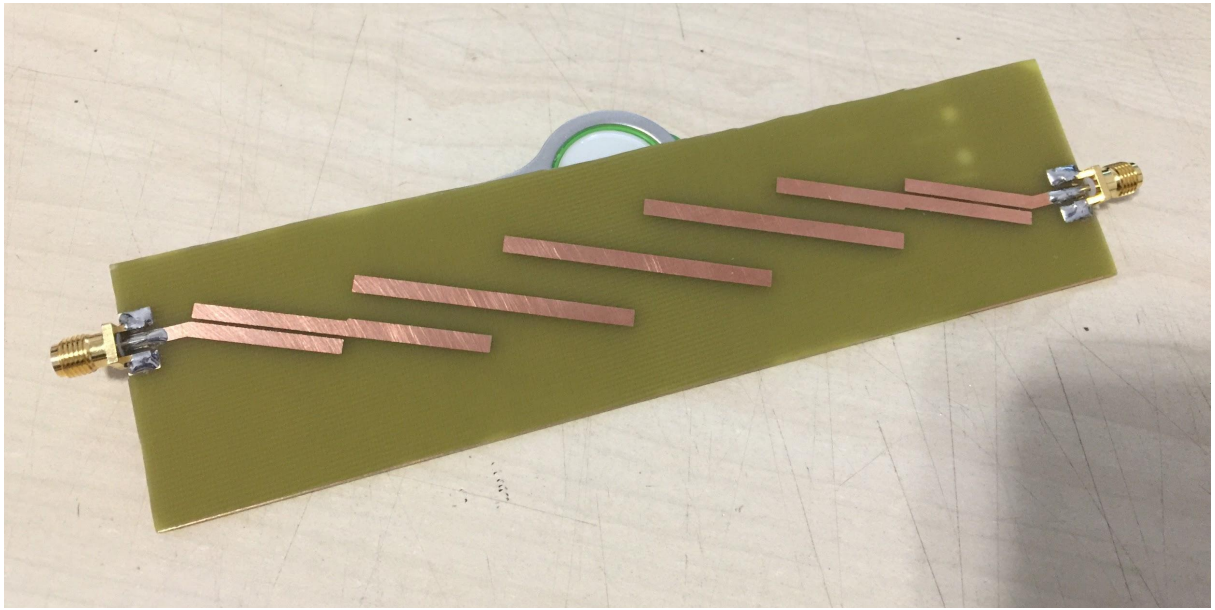
Wi-Fi/GSM Grid Antenna

$21 RTL-SDR V3

Also required:

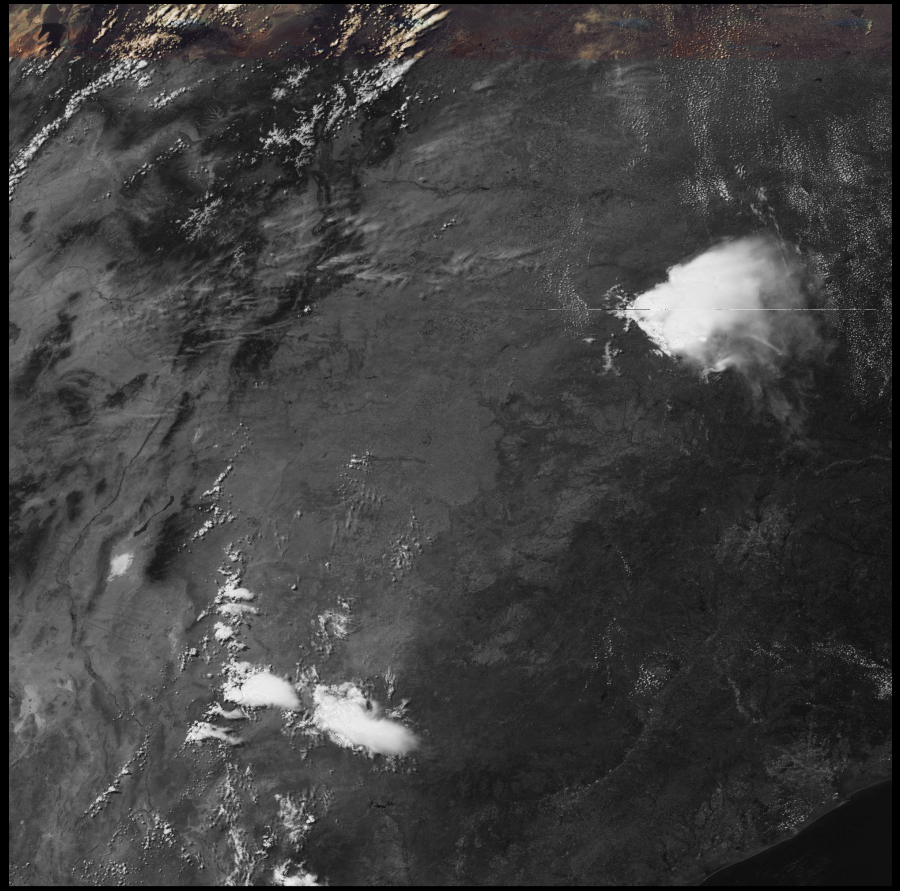
+ L-Band LNA
+ L-Band Bandpass Filter

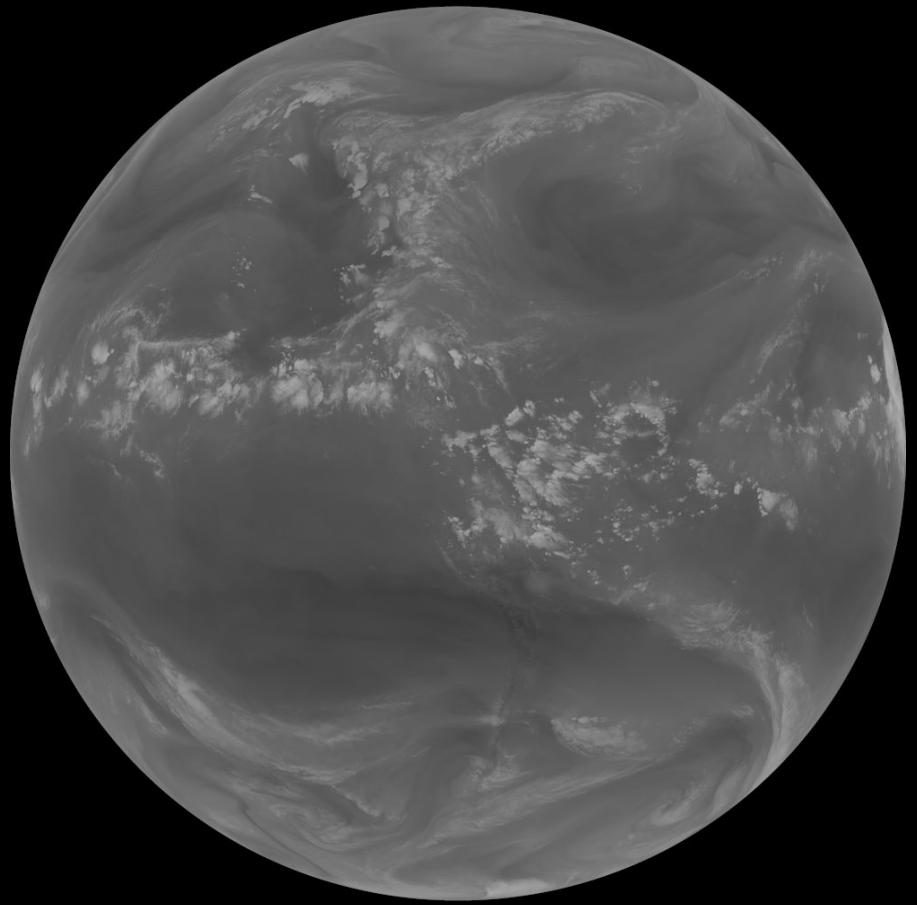
L-Band Bandpass Filter



- 5th Order Butterworth Bandpass Filter
- Coupled Microstrip with 50 Ohms Impedance
- 1.67 GHz to 1.72 GHz

Products from GOES-16 HRIT





Next Step for OSP

Polar Orbiting Satellites

X-Band

- NPP/NPOESS - Suomi & NOAA-20
- MODIS - Terra & Aqua
- FengYun

L-Band

- NOAA-19, 18 & 16
- FengYun

Currently Supported

To be supported...

NPP/NPOESS - Suomi & NOAA-20

New generation polar-orbiting earth science satellites from NASA/NOAA.

Current Satellites

- Suomi NPP
- NOAA-20 NPOESS

Planned Satellites

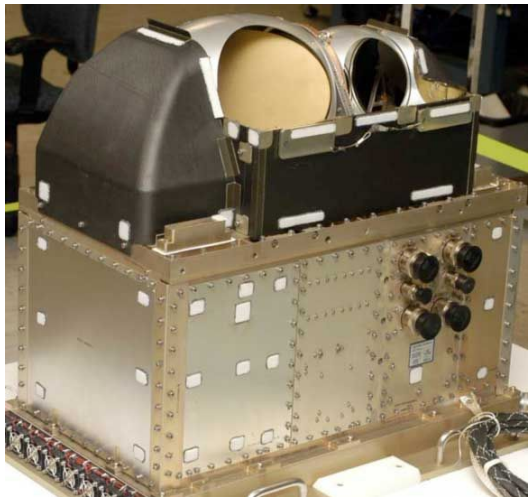
- JPSS-2 ~2021
- JPSS-3 ~2026
- JPSS-4 ~2031

NPP/NPOESS - Instruments

- VIIRS - Visible Infrared Imaging Radiometer Suite
- OMPS - Ozone Mapping and Profiler Suite
- CrIS - Cross-track Infrared Sounder
- ATMS - Advanced Technology Microwave Sounder

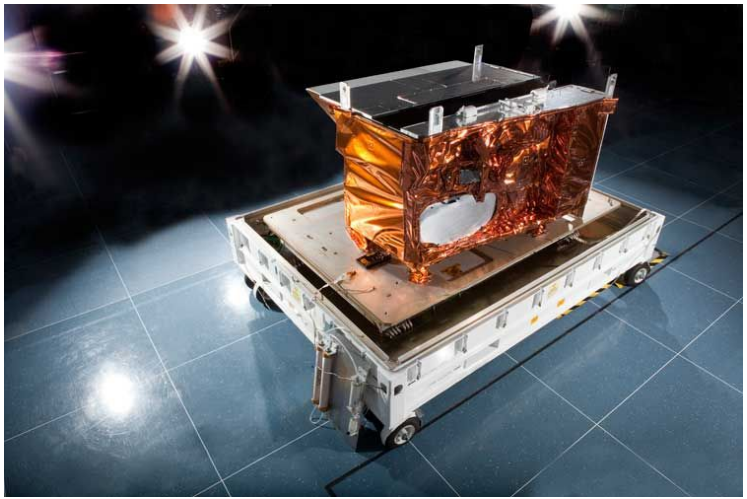
Data from all these instruments are present on the X-Band Datalink.

- Currently Supported by OSP
- To be supported...



ATMS

OMPS

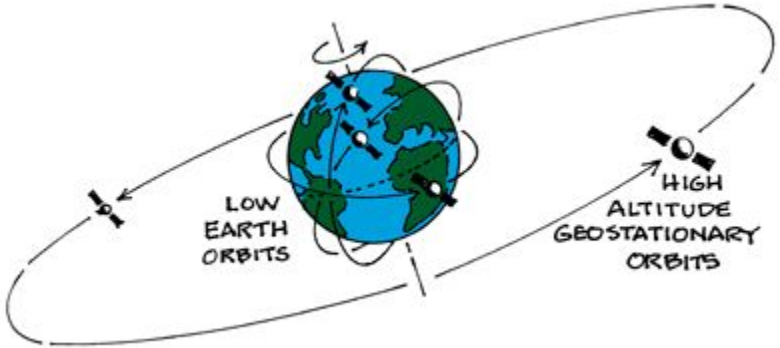


VIIRS

NPP/NPOESS - X-Band High Rate Datalink

Level: Hard

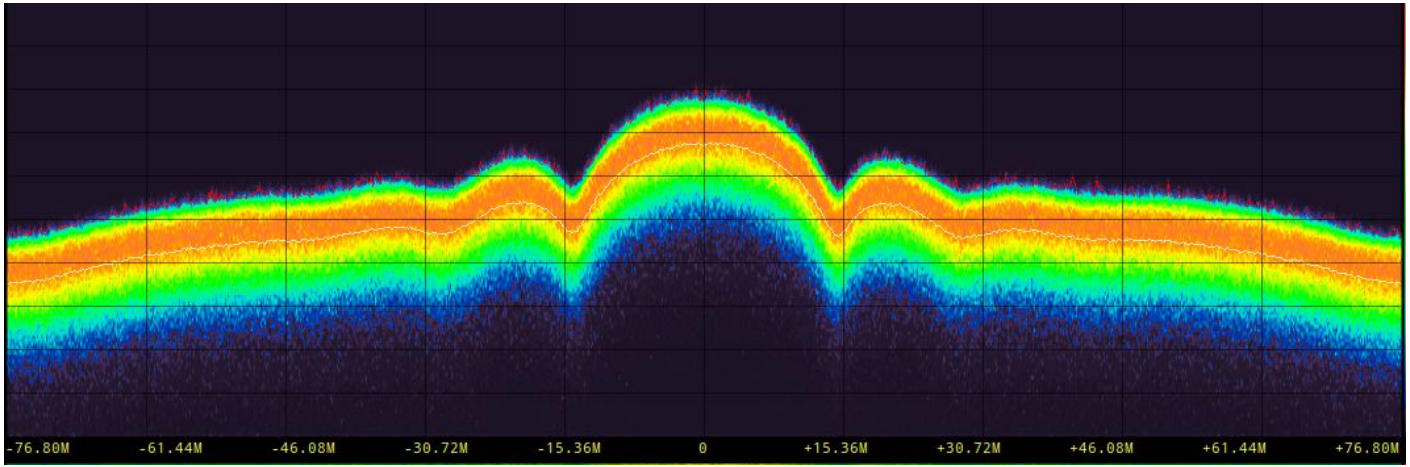
- Moving Fast (Polar Orbit)
- X-Band Signal (>7.8 GHz)
- Huge Bandwidth (30 MHz)



NPP/NPOESS - X-Band High Rate Datalink

Level: Hard

- Moving Fast (Polar Orbit)
- X-Band Signal (>7.8 GHz)
- **Huge Bandwidth (30 MHz)**

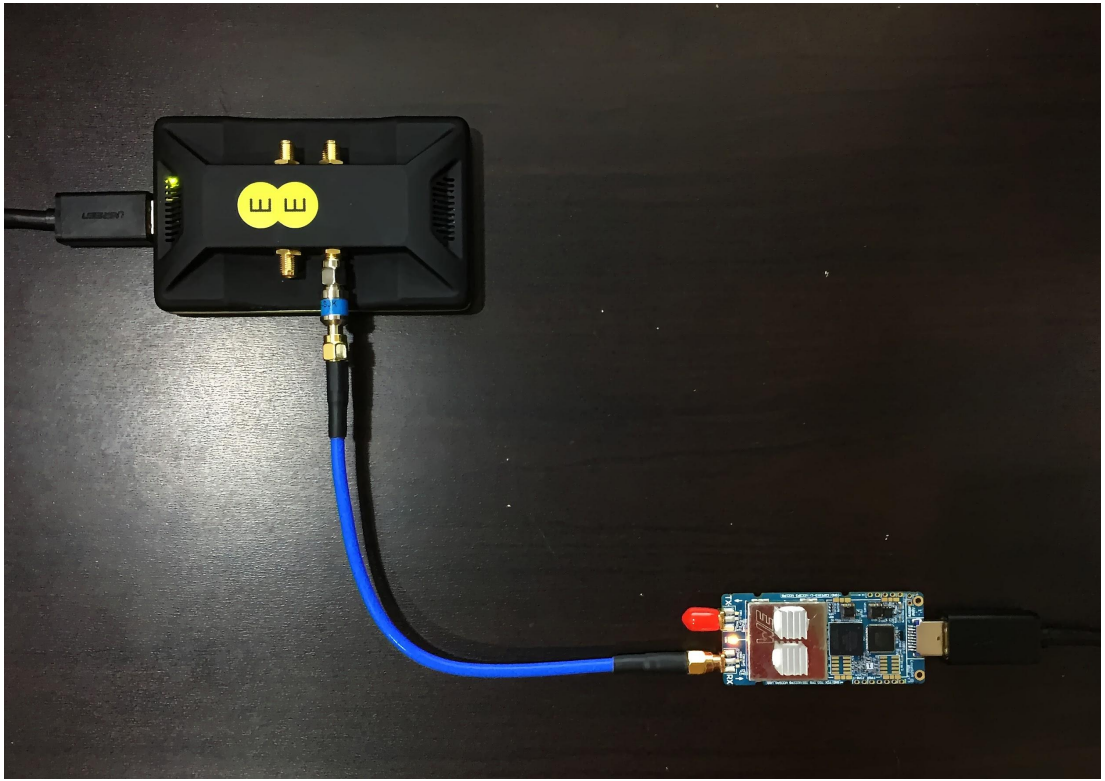


NPP/NPOESS - X-Band High Rate Datalink

Level: Hard

SDRs with Minimum Specs

- LimeSDR USB
- BladeRF
- XTRT
- USRP
- LimeSDR Mini (?)



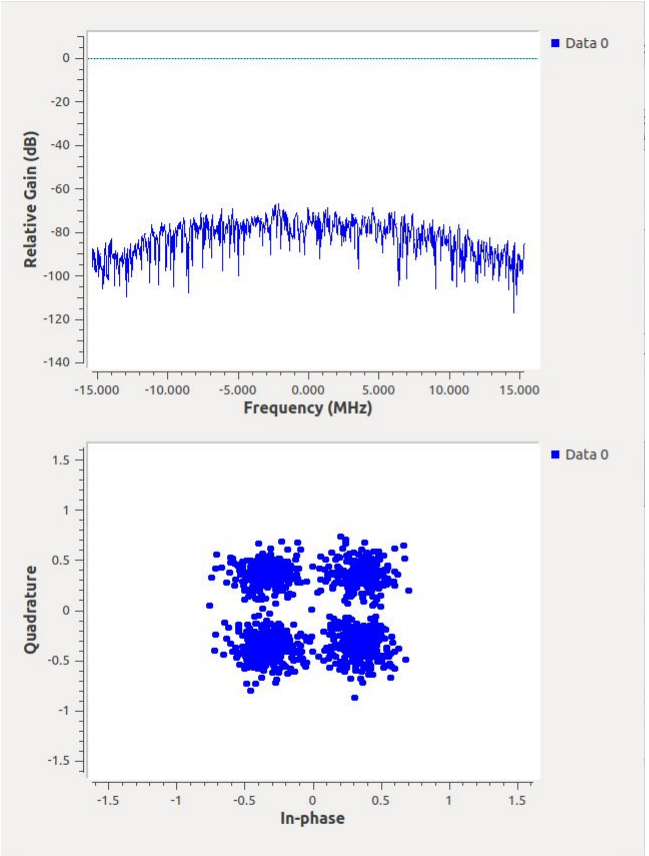
Downconverter still needed.

NPP/NPOESS - X-Band High Rate Datalink

Level: Hard

SDRs with Minimum Specs

- LimeSDR USB
- BladeRF
- XTRT
- USRP
- LimeSDR Mini (It Works!)



Downconverter still needed.

NPP/NPOESS - X-Band High Rate Datalink

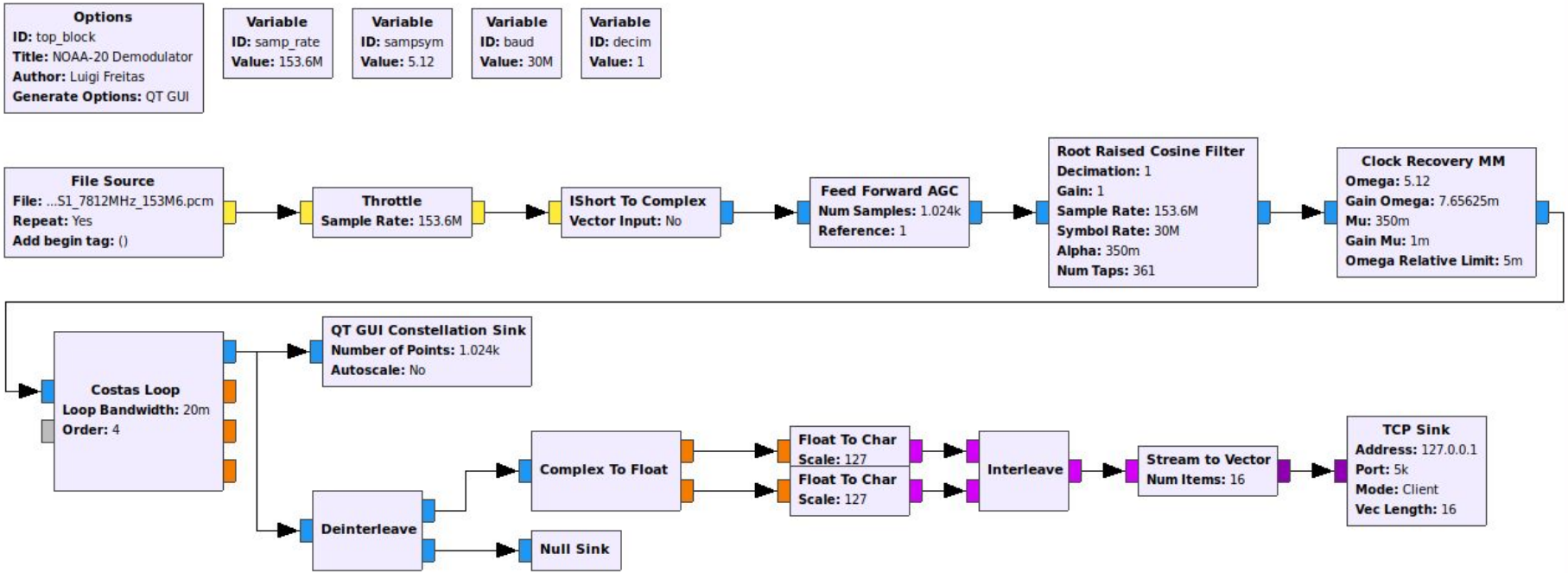
Demodulation

- Made with GNU Radio Companion.
- Just recently became viable.
- Currently impossible to be done in real-time.
- GPU Acceleration can be applied.

Modulation	QPSK
Bandwidth	30 MHz
Frequency	7812 MHz
Polarization	RHCP
I/Q Power Ratio	1:1
TX Power	8 Watts

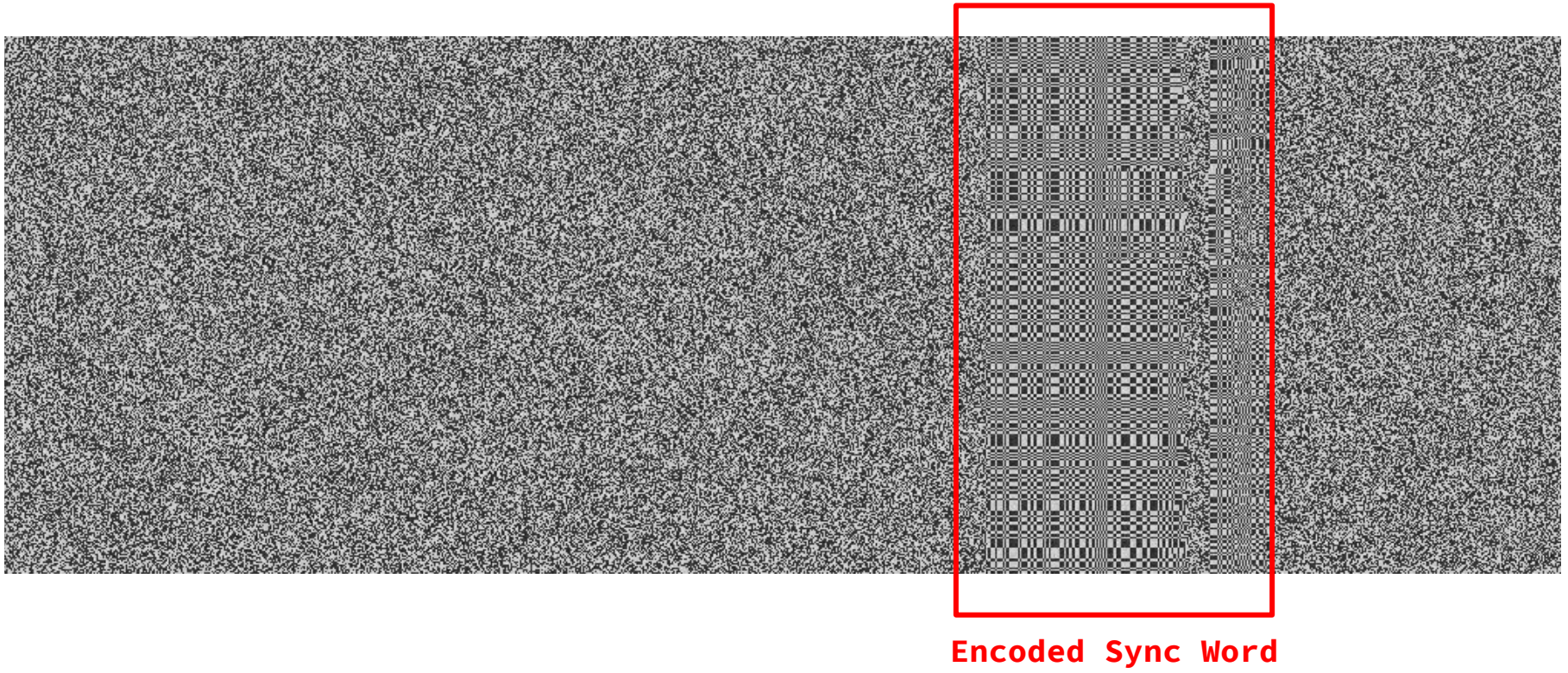
NPP/NPOESS - X-Band High Rate Datalink

Demodulation



NPP/NPOESS - X-Band High Rate Datalink

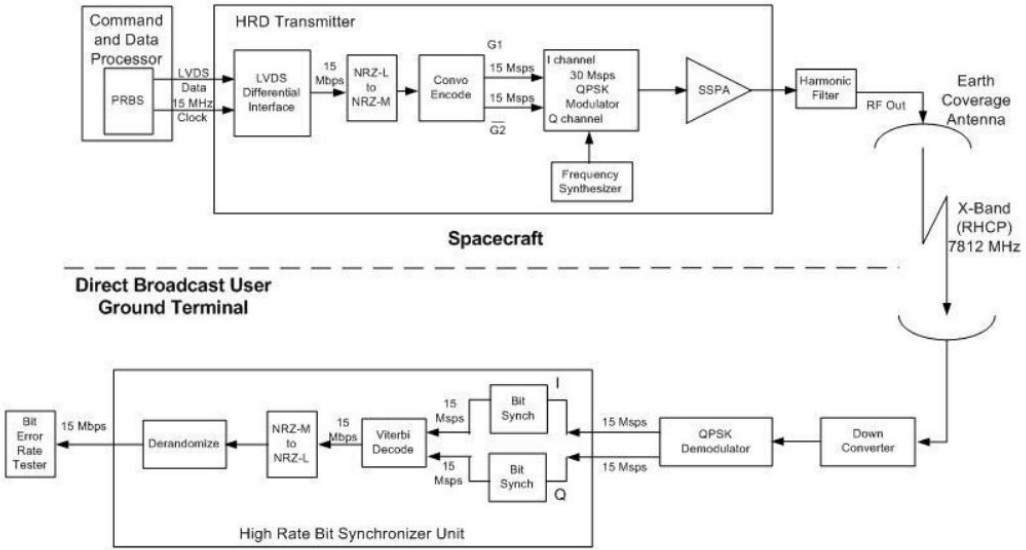
Demodulation



NPP/NPOESS - X-Band High Rate Datalink

Decoding

- Almost identical to the HRIT.
- Differential Encoding Applied.
- No puncturing.



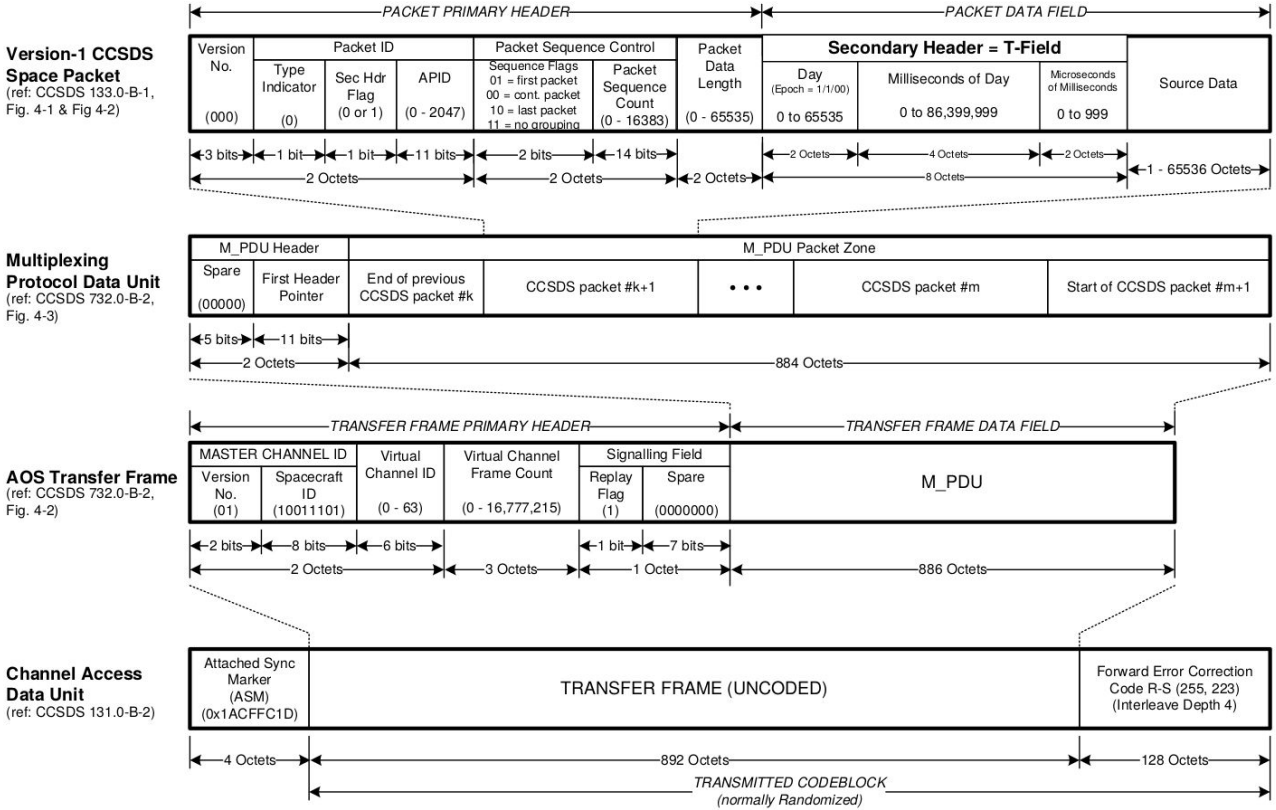
FEC	1/2
Sync Word	0x1ACFFC1D
Input Data Rate	30 Mbps
Output Data Rate	15 Mbps
Differential Encoding	NRZ-M

NPP/NPOESS - X-Band High Rate Datalink

Decoding

NPP/NPOESS - X-Band High Rate Datalink

CCSDS Demuxing



Ready for Instrument Specific Processing

Space Packet

Multiplex Data Unit

Transfer Frame

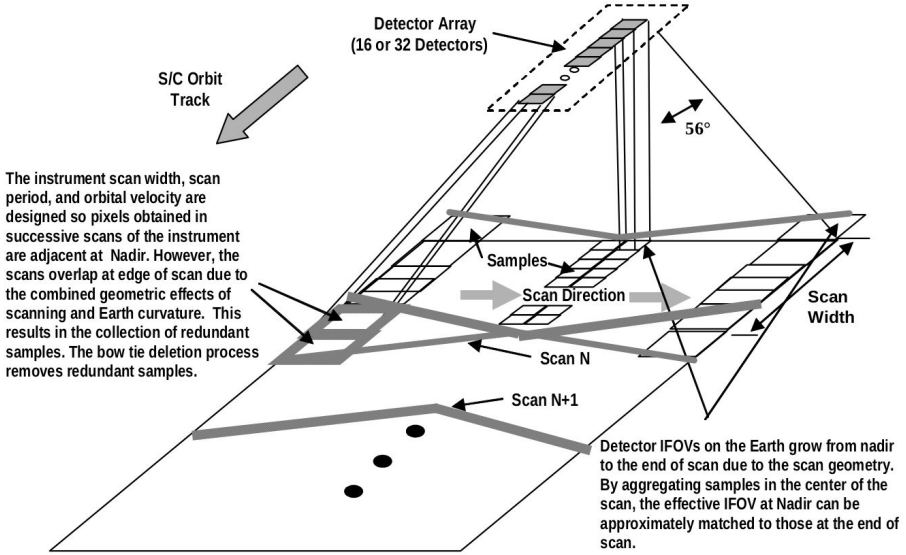
Channel Data Unit

Raw CCSDS Data

NPP/NPOESS - X-Band High Rate Datalink

VIIRS Science Data

- 24 Imager Channels.
- APIDs ranging from 800 to 823.
- 5 High Resolution Channels (375 meters per pixel).
- 17 Moderate Resolution Channels (750 meter per pixel).
- Image Depth: 15-bits Grayscale



NPP/NPOESS - X-Band High Rate Datalink

VIIRS Science Data - Header

	PACKET PRIMARY HEADER							SECONDARY HEADER			USER DATA FIELD						
	Version No.	Packet Identification			Packet Sequence Control (PSC)		Packet Length	Time of Day Start of Data [2]	Number of Packet Segments - 1	Spare	VIIRS Packet ID		HR Format			HR Science Data	
		Type Indicator	Sec Hdr Flag	APID	Sequence Flags	Sequence Count	[1]				VIIRS Sequence Count	Packet Time [2]	Format Version	Instrument Number	Spare	HR Meta Data	Checksum
Bits	3	1	1	11	2	14	16	64	8	8	32	64	8	8	16	1168	16
Octets	2				2		2	8	1	1	4	8	1	1	2	146	2
Value	000	0	1	varies	01	varies	173	varies	varies	zeros	varies	varies	2	2	zeros	varies	varies

0 = Telemetry Packet

1 = Secondary Header Present

Segmented data, First packet. Definition per A.2.2

VIIRS Sequence Count is a running total count of all types of packets sent by VIIRS since power on or 32-bit rollover.

16-bit arithmetic Checksum of HR Meta Data Field. Filled with zeros if not used.

HR Meta Data														
	HAM Side	Scan Synch	Self Test Data Pattern	Reserved	Scan Number	Scan Terminus [2]	Sensor Mode	VIIRS Model	FSW Version	Band Control Word	Partial Start	No. of Samples	Sample Delay	Reserved
Bits	1	1	4	10	32	64	8	8	16	32	16	16	16	944
Octets	2				4	8	1	1	2	4	2	2	2	118
Value	varies	varies	varies	varies	varies	varies	varies	varies	varies	varies	varies	varies	varies	vareis

TOTAL
1168
146

0000 Live Data
0001-1111 Test Data Patterns

Filled with zeros if unused

Filled with zeros if unused

Notes:

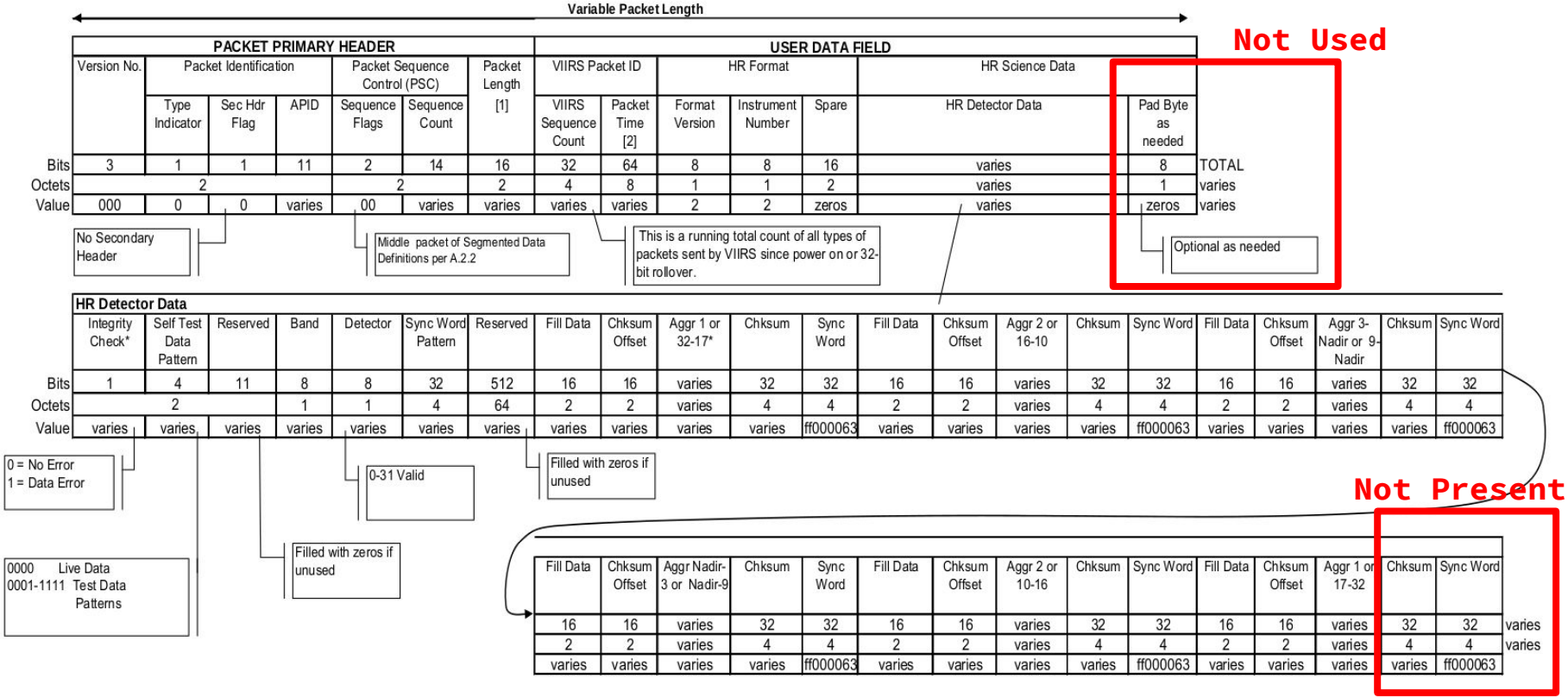
[1] Packet length is the number of bytes after the primary header minus one.

[2] "Time of Day Start of Data", "Packet Time", and "Scan Terminus" fields are 64-bit CCSDS Day Segmented Time Code format as defined in CCSDS 301.0-B-2 (1958 January 1 epoch, 16-bit day, 32-bit msec, 16-bit µsec). "Time of Day Start of Data" field is Start of Scan.

3. All packet fields are big endian.

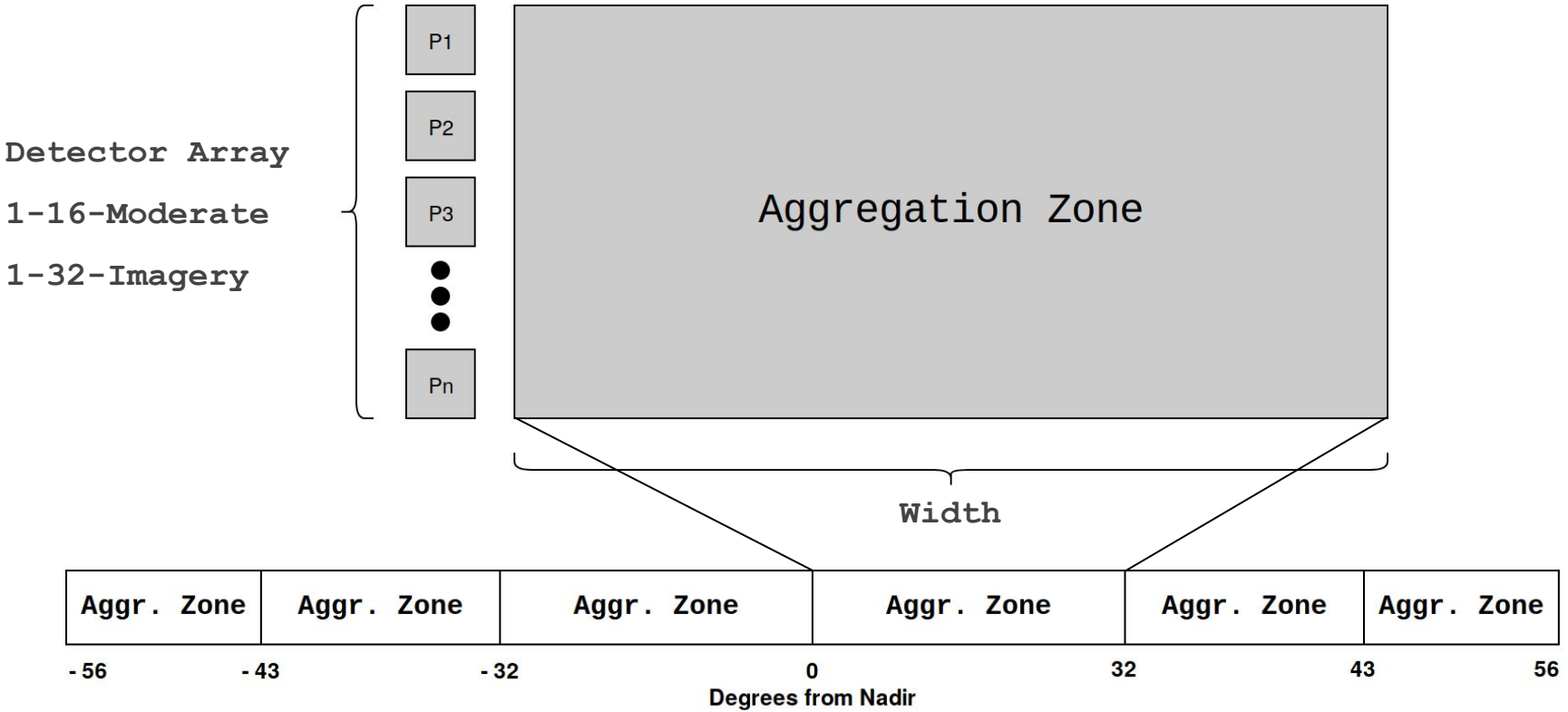
NPP/NPOESS - X-Band High Rate Datalink

VIIRS Science Data - Imager Data Body



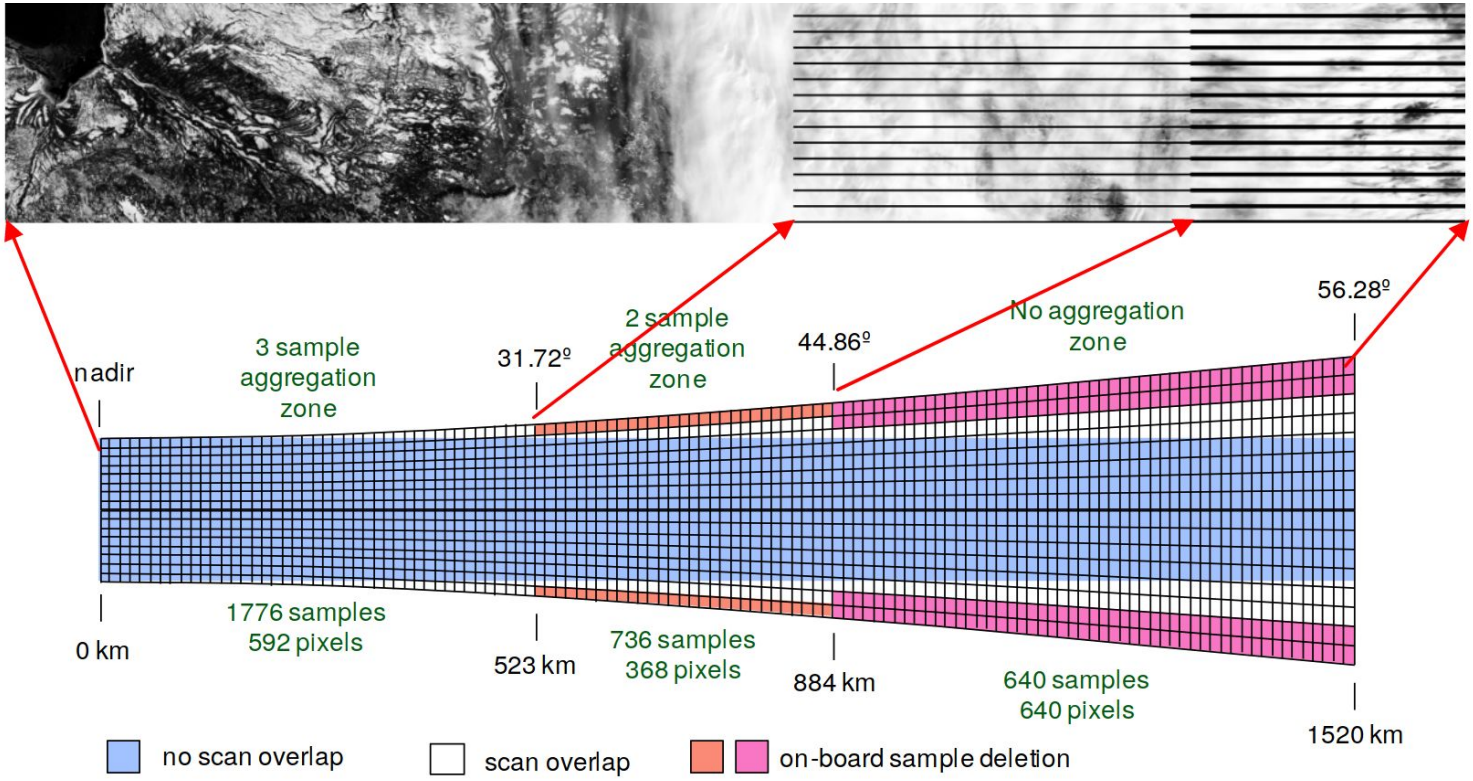
NPP/NPOESS - X-Band High Rate Datalink

VIIRS Science Data



NPP/NPOESS - X-Band High Rate Datalink

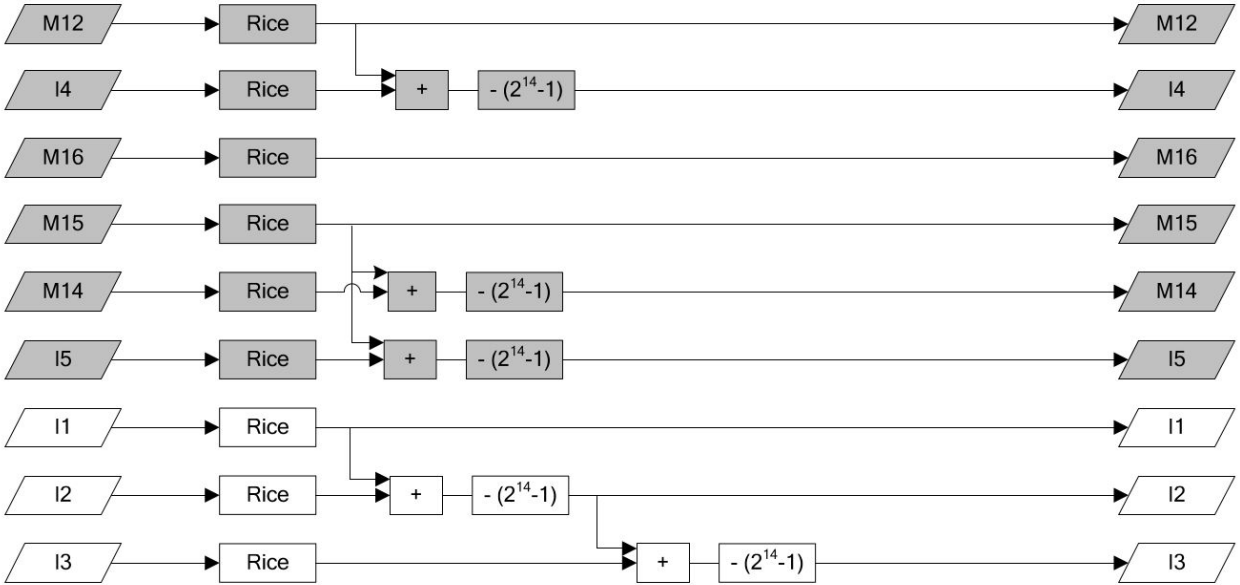
VIIRS Science Data - Bow Tie Deletion

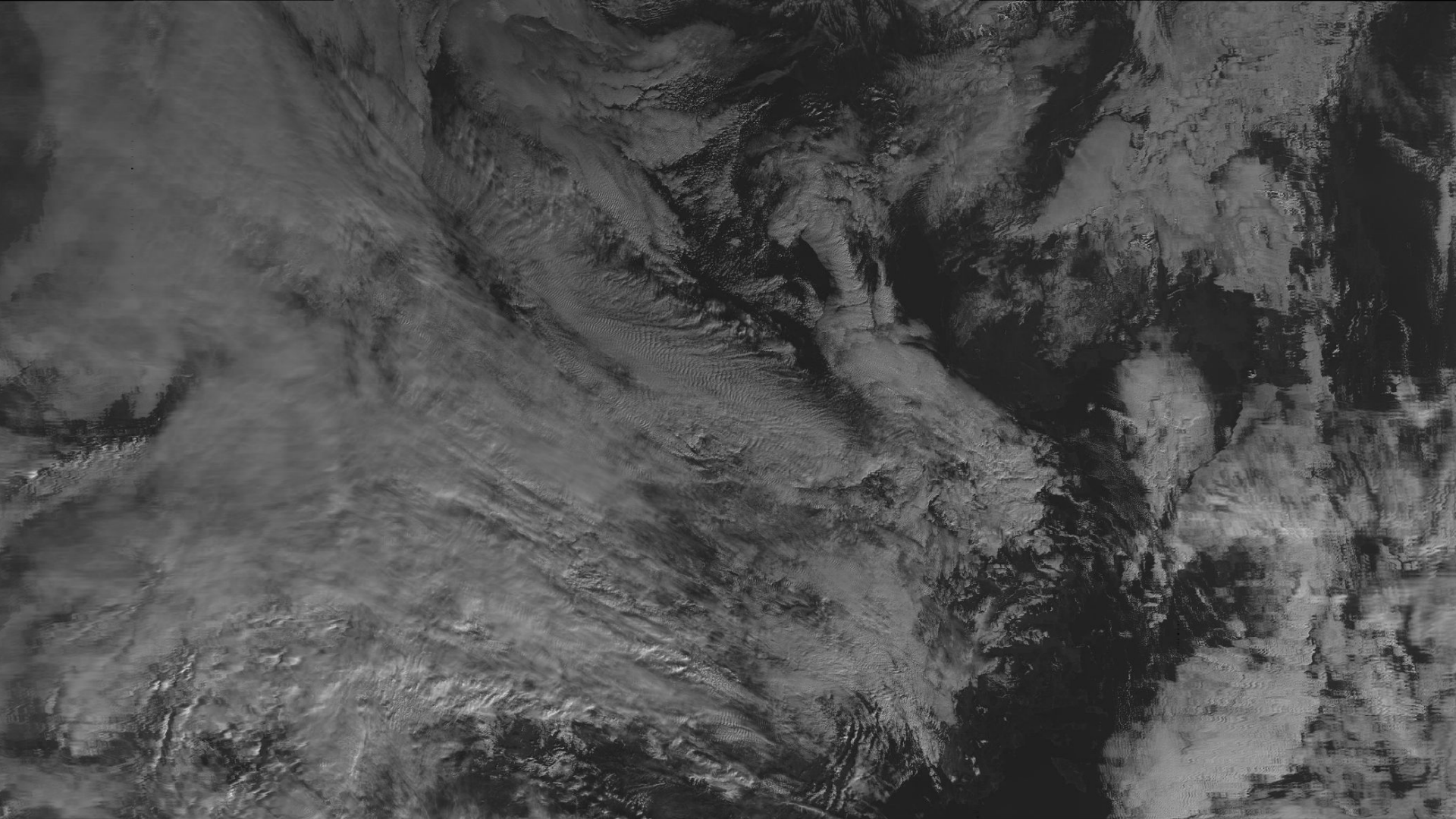


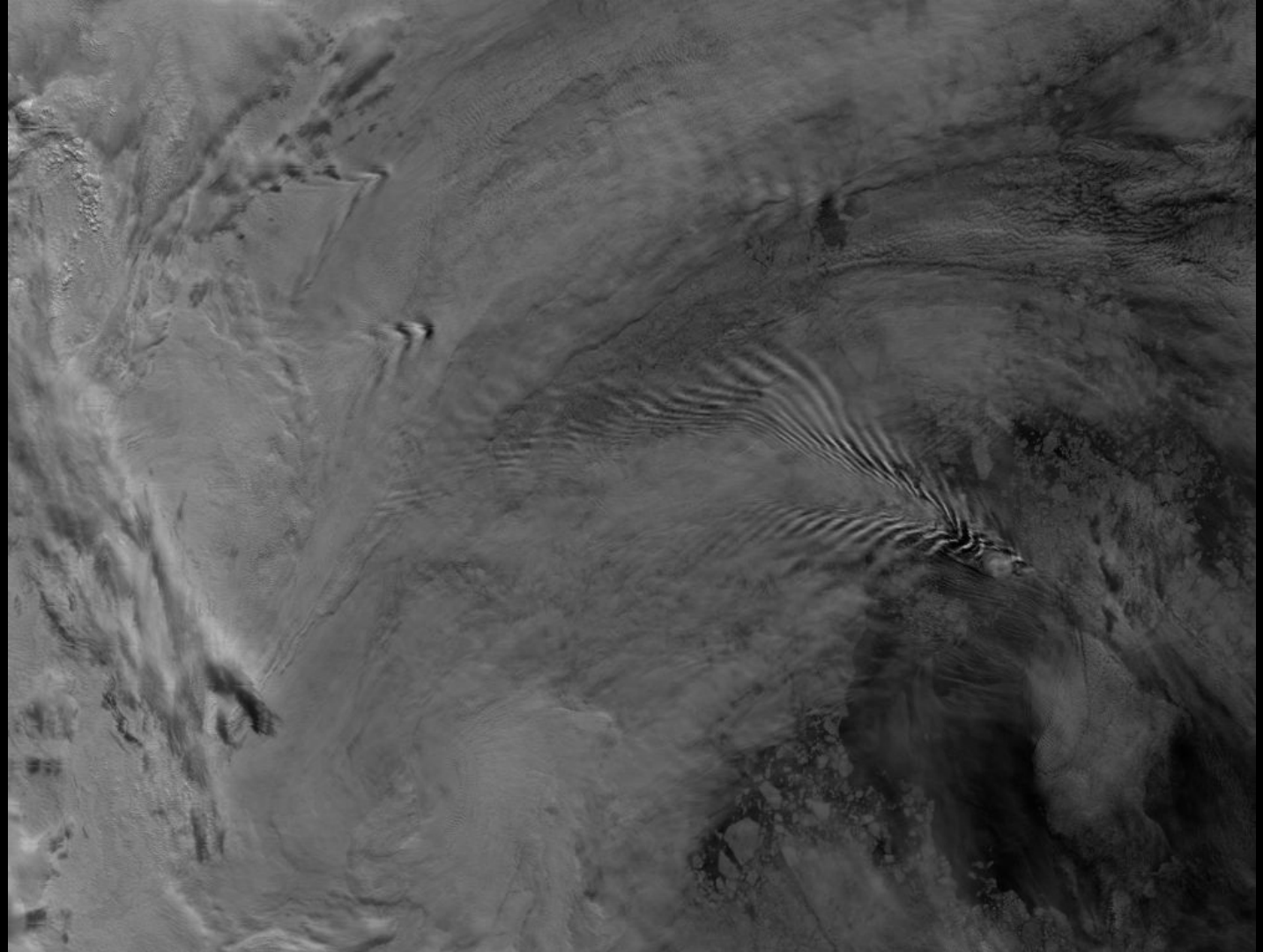
NPP/NPOESS - X-Band High Rate Datalink

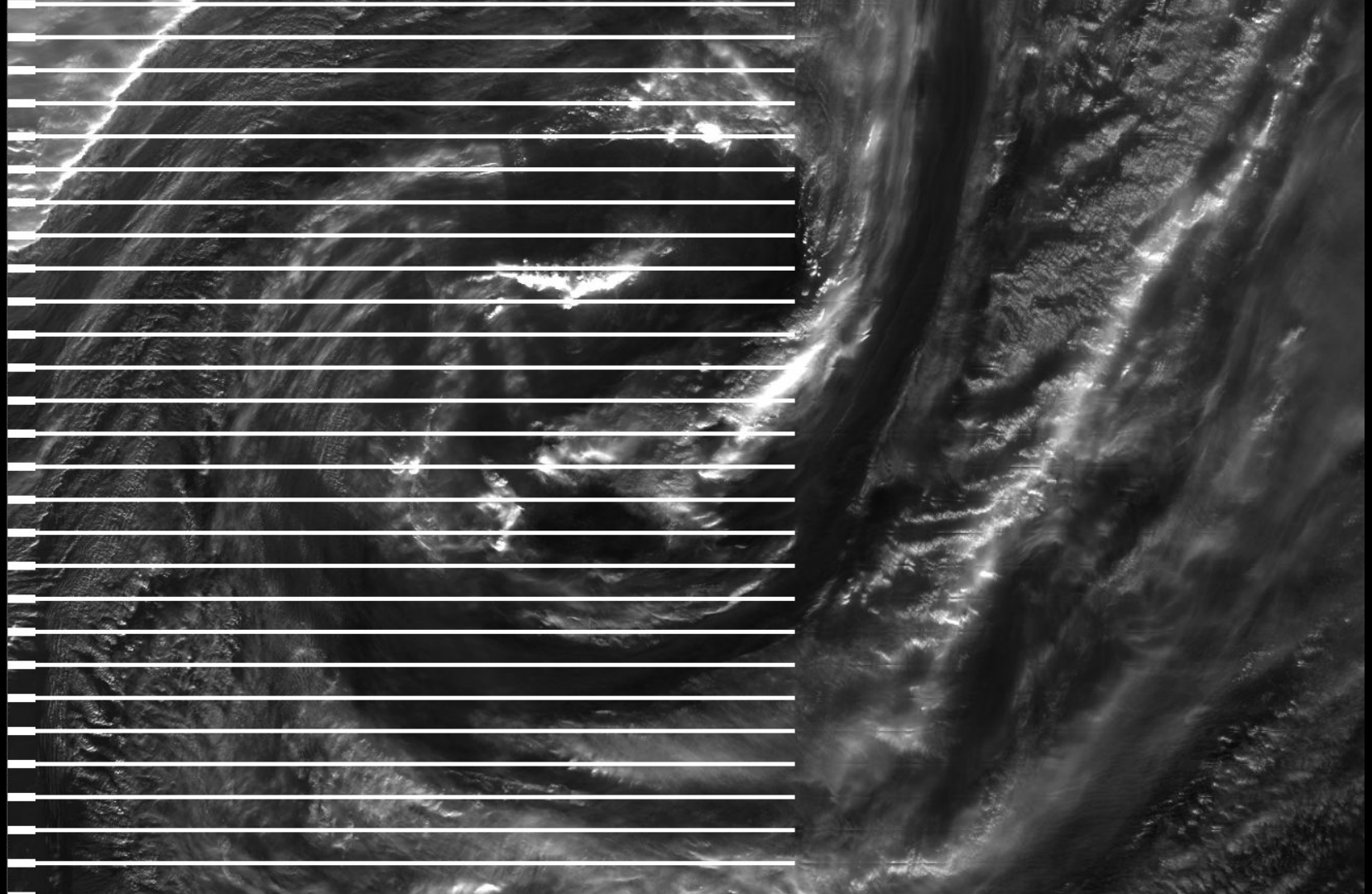
VIIRS Science Data

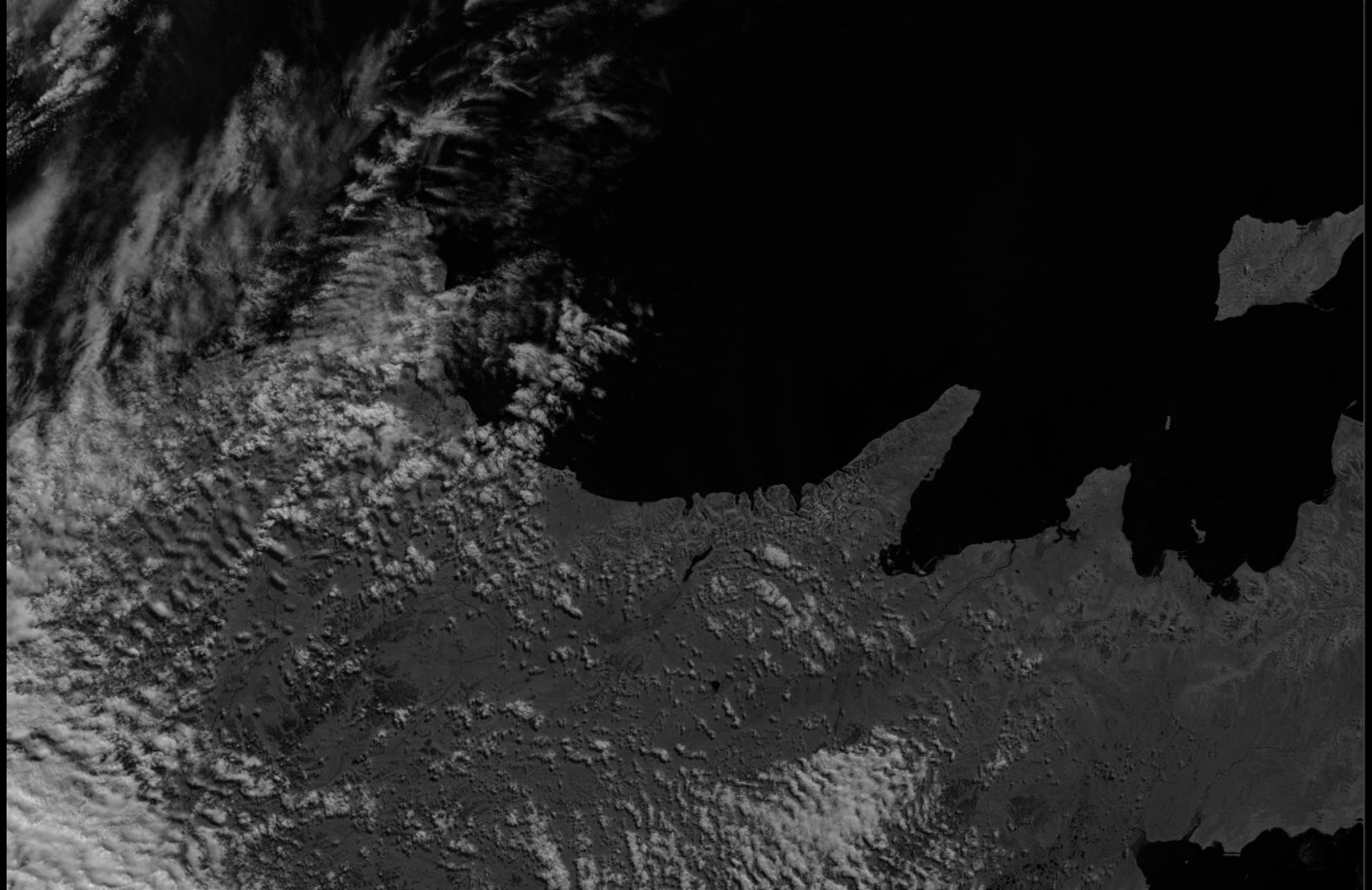
- Every Channel is RICE encoded.
- Additional Differential encoding on some Infrared Channels.

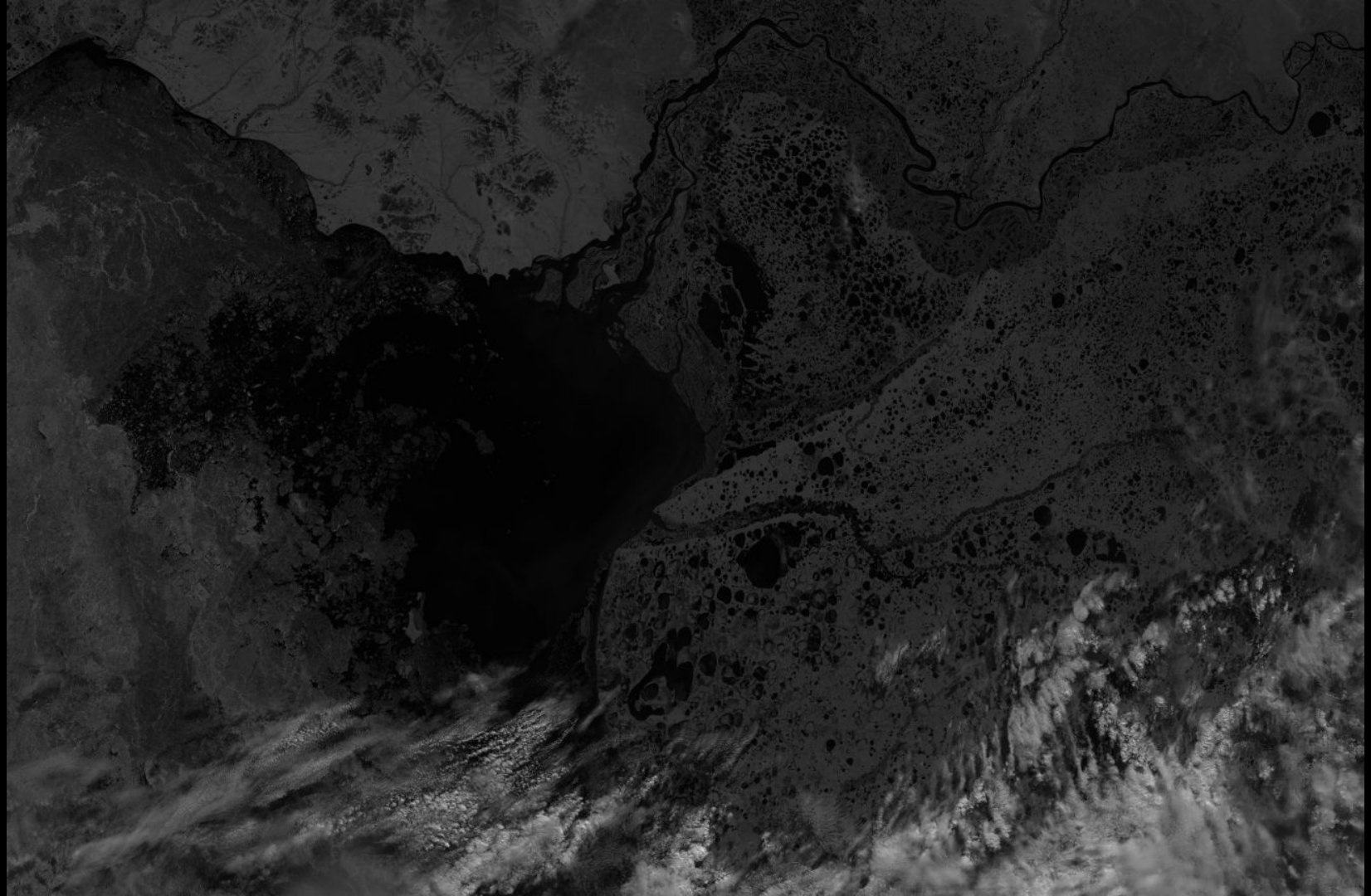












NPP/NPOESS - X-Band High Rate Datalink

Toolset Availability

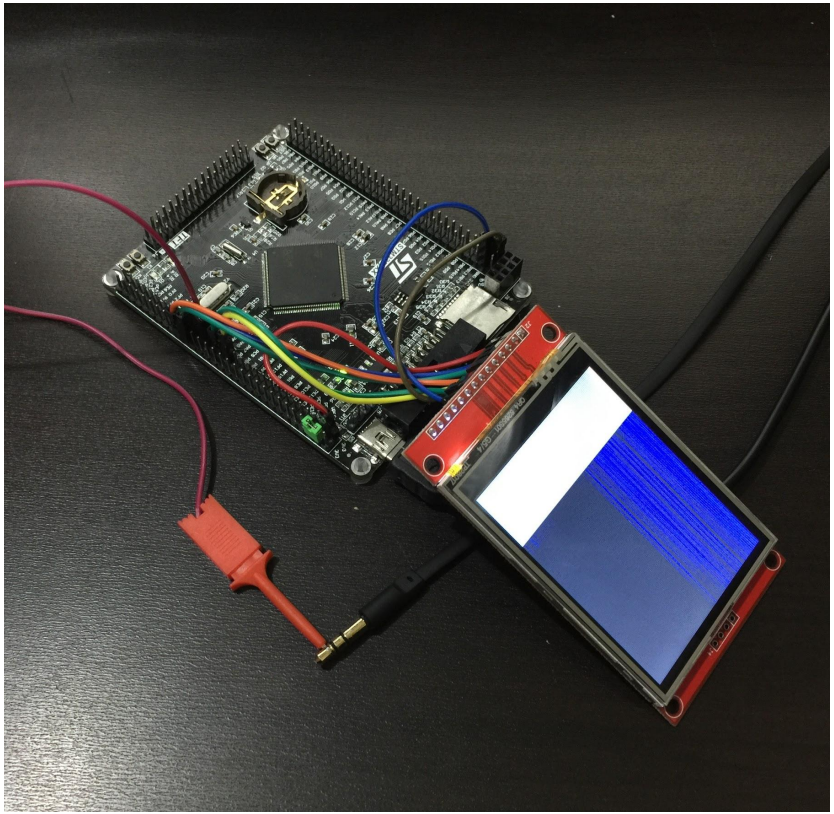
Later this month at
Open Satellite Project GitHub Page.

http://github.com/opensatelliteproject/

Bonus

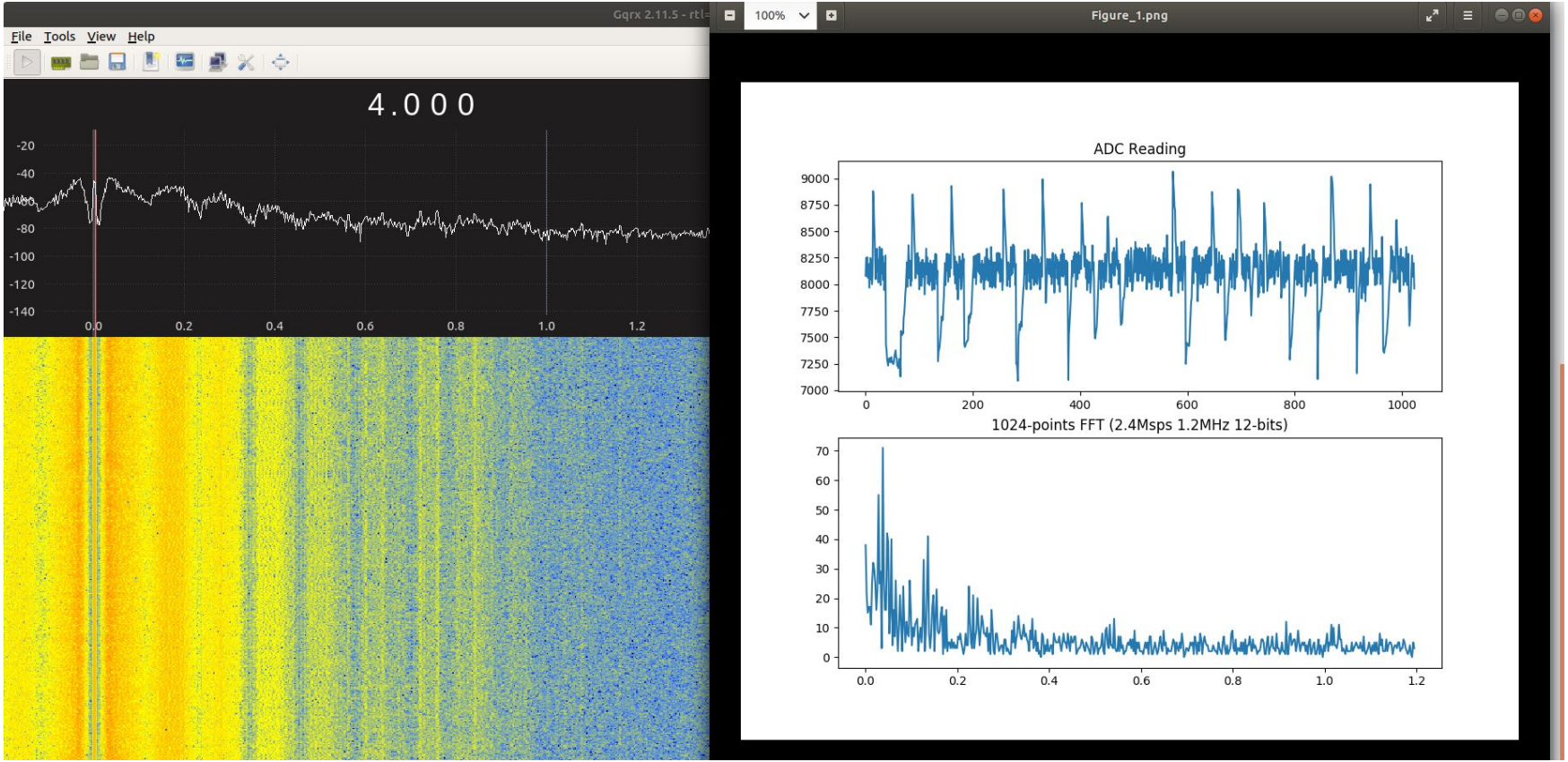
The Worst SDR Ever

- Made with dirty cheap parts from China.
- Based on STM32 Cortex-M3 & Cortex-M4.
- Hardware Float Point Unit.
- Built-in 7.4 Msps ADC with 12-bits resolution.
- Support external SDRAM up to 8 megabits.
- OSS based on the OpenCM3 Library.
- DSP Assembly Cores Provided by ST.
- Will support demodulation core in the future.
- Tuner can be added (R820T2).
- Great to learn how SDRs works.



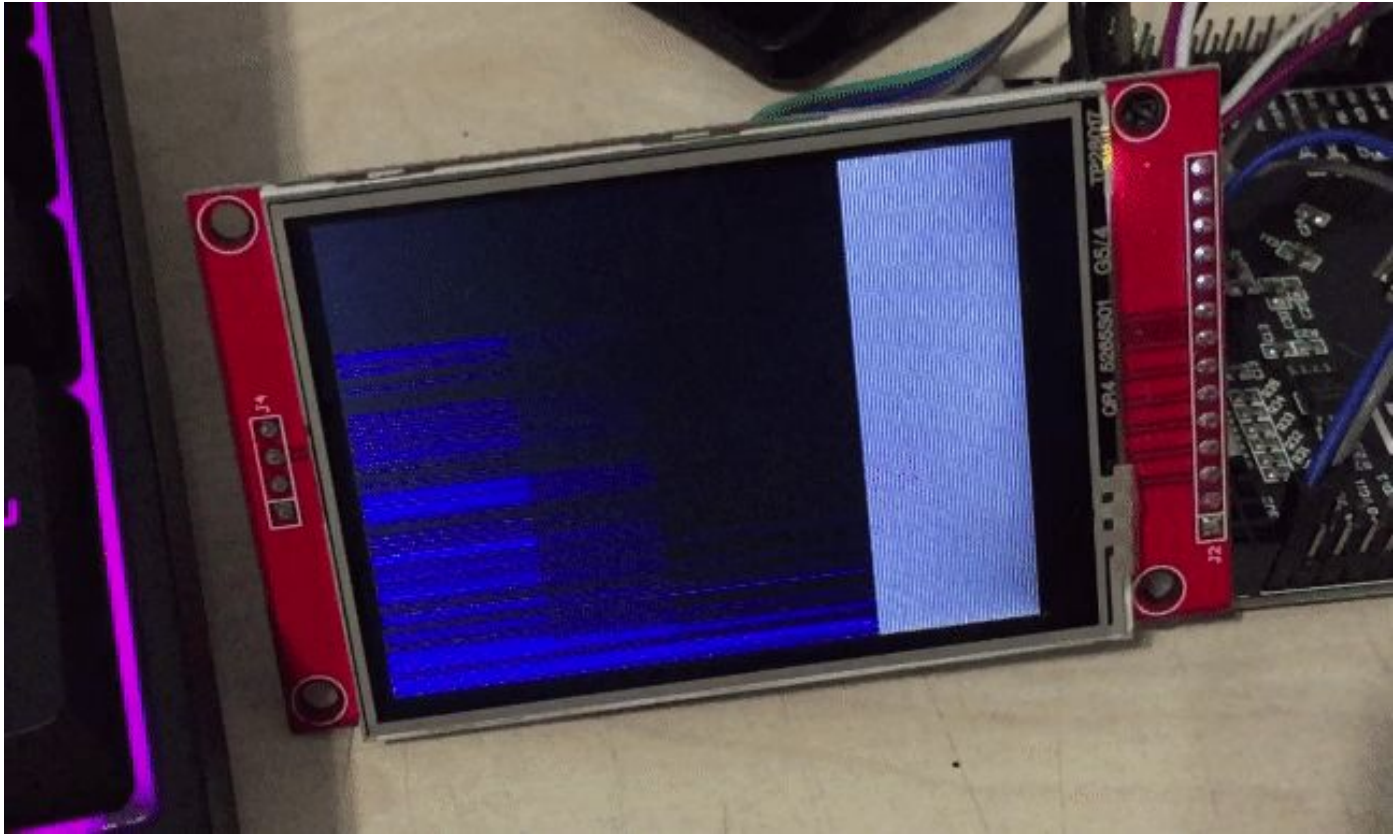
Bonus

The Worst SDR Ever



Bonus

The Worst SDR Ever



Any Questions?

My Contact

Luigi Freitas Cruz
luigifcruz@gmail.com
Twitter, Keybase: @luigifcruz
GitHub: @luigifreitas

Slides will be available at:
https://luigifreitas.me

Special Thanks

Lucas Teske
@lucasteske

Oleg_meteo
www.sat.cc.ua
@MeteoOleg