Project “ADS-B Receiver and Decoder”

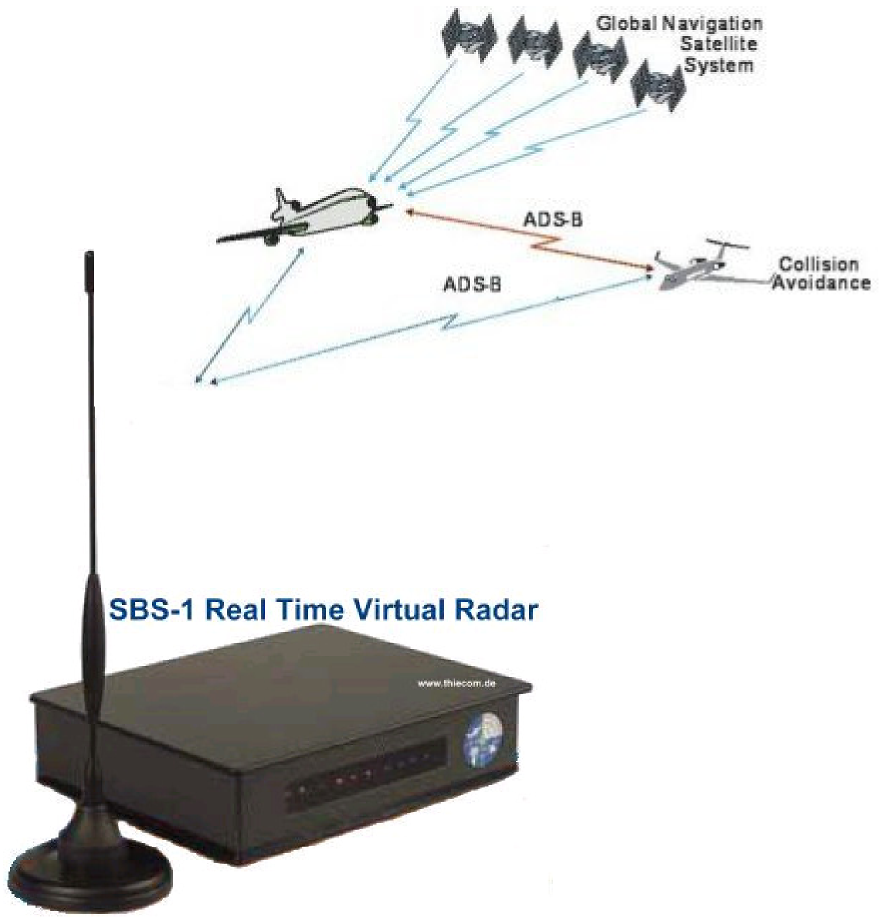
About 50% of all commercial aircraft are transmitting their navigation information (position, speed, heading and more) on 1090MHz.

The protocol and format is not encrypted and can be received by everyone.

Commercial equipment is available, but very expensive.

Some new and cheaper equipment is far away

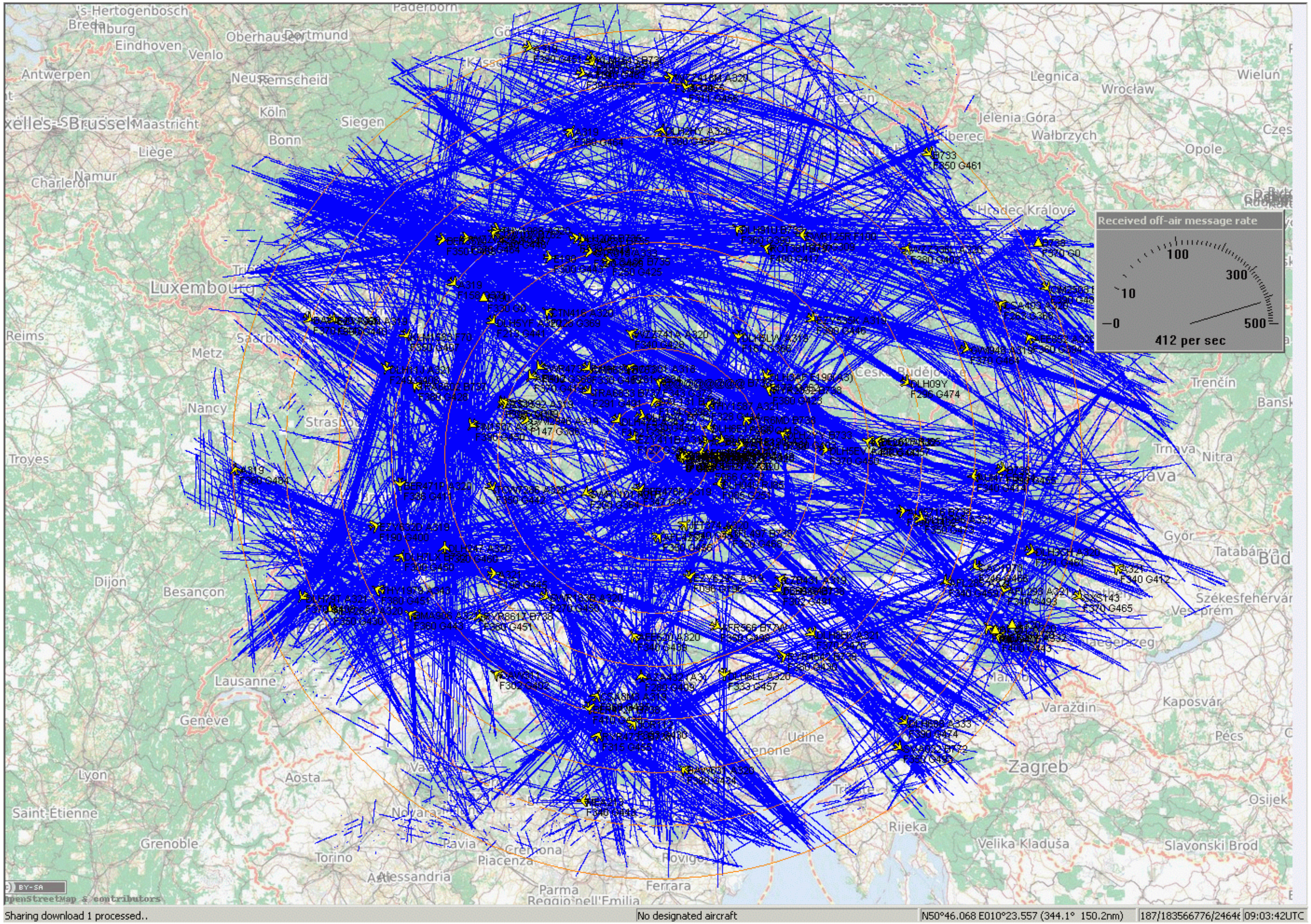
from the performance of the SBS-1



Manufacturer: Kinetic Avionics
Price around EUR 600,-

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

What can we see? ➔ Air traffic up to 275nm distance



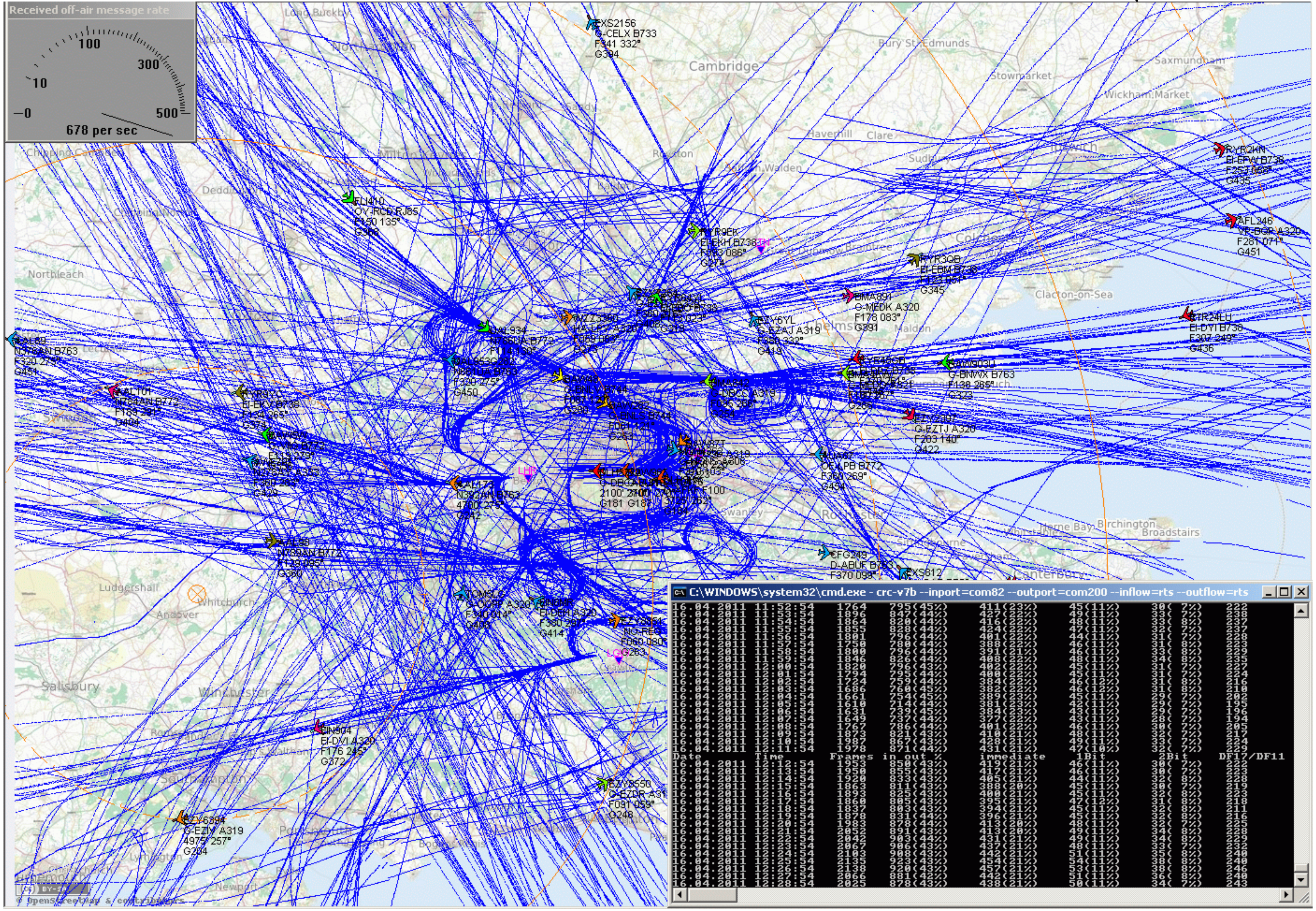
Sharing download 1 processed..

No designated aircraft

N50°46.068 E010°23.557 (344.1° 150.2nm)

187/183566776/2464ϵ 09:03:42UTC

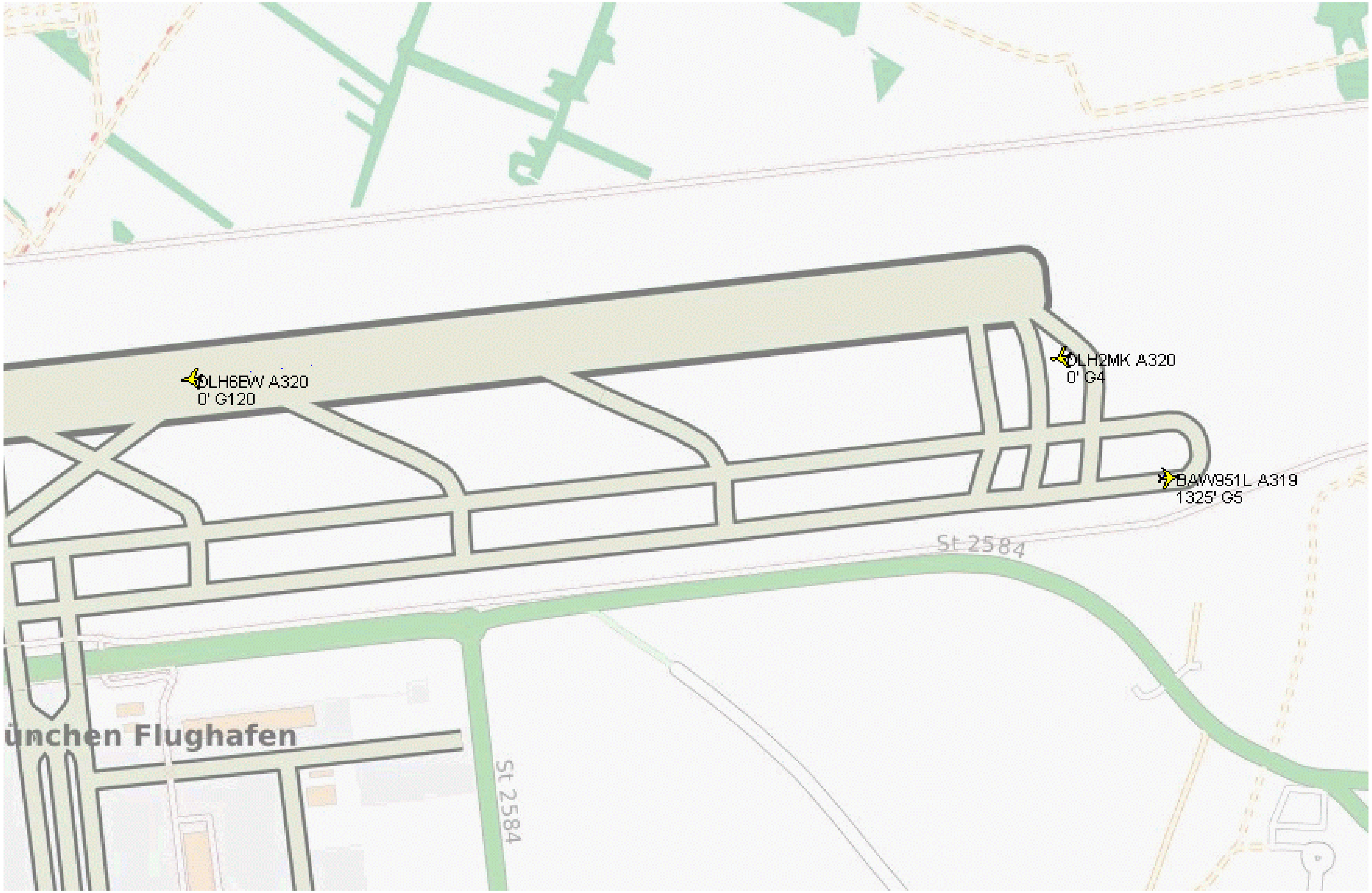
What can we see? ➔ London Traffic (from Andover)



```
C:\WINDOWS\system32\cmd.exe - crc-v7b --inport=com82 --outport=com200 --inflow=rts --outflow=rts
16.04.2011 11:52:54    1764    795(45%)     411(23%)     45(11%)     30( 7%)    222
16.04.2011 11:53:54    1896    847(44%)     427(22%)     49(11%)     33( 7%)    238
16.04.2011 11:54:54    1864    820(44%)     416(22%)     48(11%)     33( 8%)    237
16.04.2011 11:55:54    1855    828(44%)     424(22%)     47(11%)     32( 7%)    237
16.04.2011 11:56:54    1801    796(44%)     401(22%)     44(11%)     31( 7%)    228
16.04.2011 11:57:54    1750    780(44%)     388(22%)     46(11%)     31( 8%)    223
16.04.2011 11:58:54    1800    796(44%)     391(21%)     46(11%)     33( 8%)    229
16.04.2011 11:59:54    1846    826(44%)     408(22%)     48(11%)     34( 8%)    235
16.04.2011 12:00:54    1820    796(43%)     402(22%)     45(11%)     31( 7%)    227
16.04.2011 12:01:54    1794    795(44%)     400(22%)     45(11%)     31( 7%)    224
16.04.2011 12:02:54    1724    759(44%)     384(22%)     46(12%)     31( 8%)    216
16.04.2011 12:03:54    1686    760(45%)     382(22%)     46(12%)     31( 8%)    210
16.04.2011 12:04:54    1661    754(45%)     389(23%)     45(11%)     29( 7%)    202
16.04.2011 12:05:54    1610    714(44%)     381(23%)     42(11%)     29( 7%)    195
16.04.2011 12:06:54    1631    739(45%)     384(23%)     43(11%)     29( 7%)    196
16.04.2011 12:07:54    1649    737(44%)     377(22%)     43(11%)     28( 7%)    194
16.04.2011 12:08:54    1767    786(44%)     401(22%)     46(11%)     30( 7%)    205
16.04.2011 12:09:54    1873    821(43%)     410(21%)     48(11%)     32( 7%)    217
16.04.2011 12:10:54    1987    867(43%)     428(21%)     49(11%)     33( 7%)    224
16.04.2011 12:11:54    1978    871(44%)     431(21%)     47(10%)     32( 7%)    229
Date       Time       Frames in out %      immediate    1Bit        2Bit    DF17/DF11
16.04.2011 12:12:54    1953    850(43%)     419(21%)     46(11%)     30( 7%)    222
16.04.2011 12:13:54    1950    855(43%)     417(21%)     46(11%)     30( 7%)    223
16.04.2011 12:14:54    1920    833(43%)     405(21%)     44(11%)     32( 8%)    228
16.04.2011 12:15:54    1863    811(43%)     388(20%)     45(11%)     30( 7%)    219
16.04.2011 12:16:54    1893    825(43%)     400(21%)     45(11%)     32( 8%)    223
16.04.2011 12:17:54    1860    805(43%)     395(21%)     47(12%)     31( 8%)    218
16.04.2011 12:18:54    1837    803(43%)     394(21%)     45(11%)     32( 8%)    211
16.04.2011 12:19:54    1878    831(44%)     396(21%)     45(11%)     32( 8%)    216
16.04.2011 12:20:54    1983    878(44%)     413(20%)     48(11%)     32( 7%)    225
16.04.2011 12:21:54    2052    891(43%)     413(20%)     49(11%)     34( 8%)    228
16.04.2011 12:22:54    2042    903(44%)     431(21%)     49(11%)     34( 8%)    229
16.04.2011 12:23:54    2067    906(43%)     437(21%)     48(11%)     33( 7%)    232
16.04.2011 12:24:54    2103    908(43%)     442(21%)     51(11%)     35( 8%)    240
16.04.2011 12:25:54    2135    923(43%)     454(21%)     54(11%)     38( 8%)    240
16.04.2011 12:26:54    2138    920(43%)     457(21%)     53(11%)     38( 8%)    246
16.04.2011 12:27:54    2066    881(42%)     442(21%)     51(11%)     36( 8%)    240
16.04.2011 12:28:54    2025    878(43%)     438(21%)     50(11%)     34( 7%)    243
```

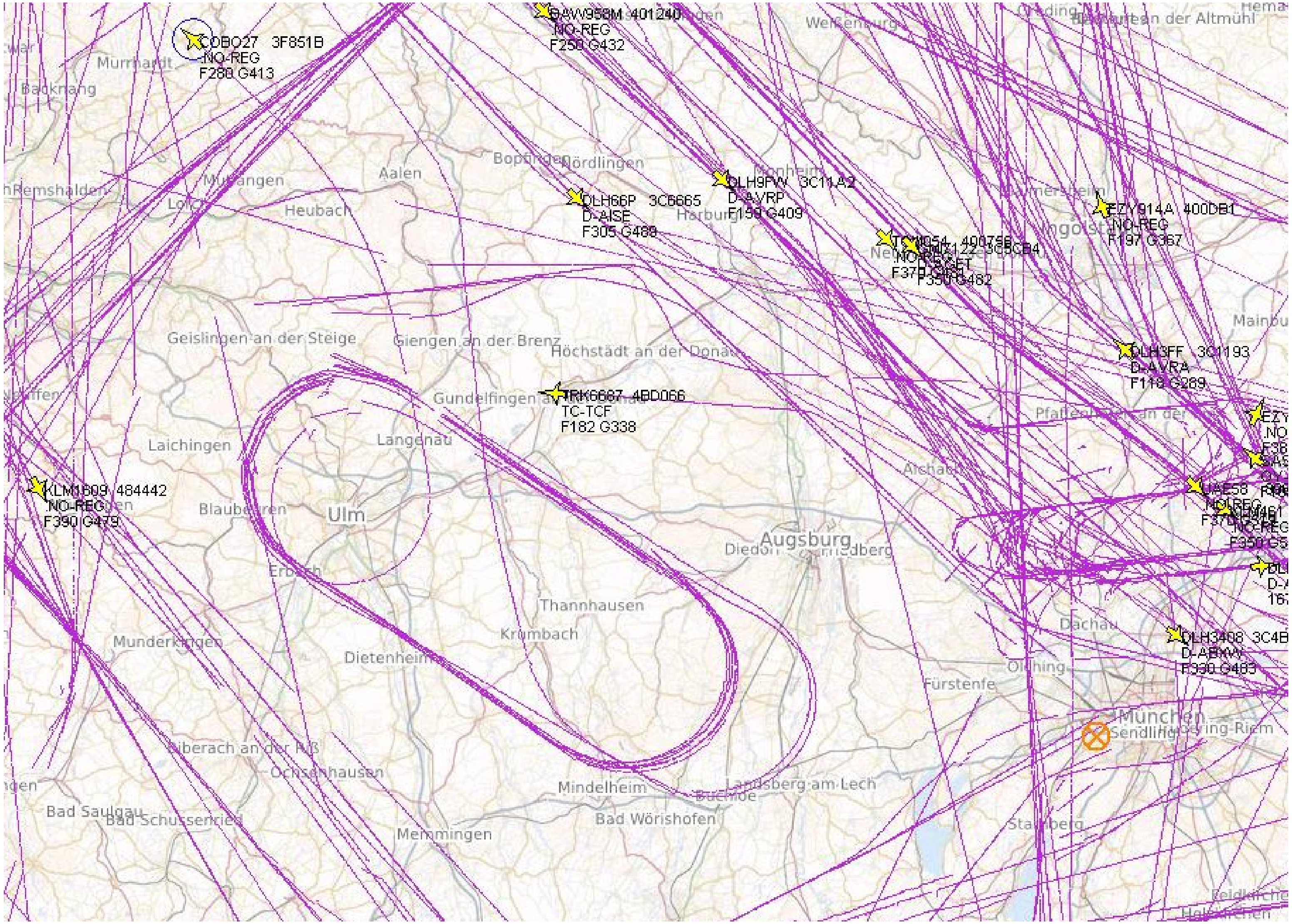
Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

What can we see? ➔ Ground Traffic



Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

What can we see? ➔ Rare situations



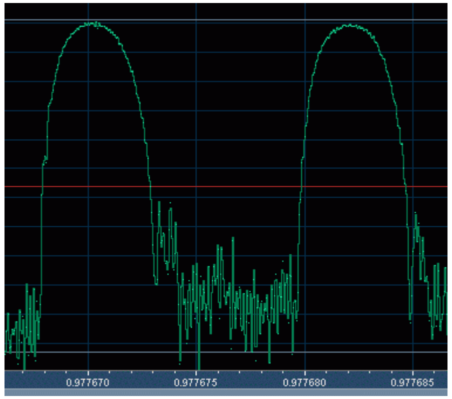
A german air force A310 MRTT tanker practicing refuelling at 20000ft

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

1090MHz Radio Channel Users

1. Distance Measuring Equipment (DME)

   used by planes to determine distance to DME relaying stations

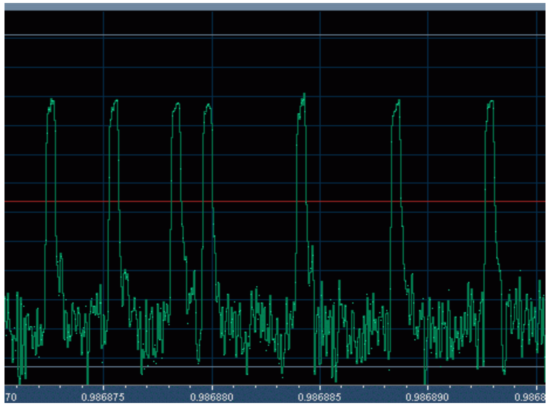


2. Traditional Radar

   (Mark-X, Mode-3/Mode-A, Mode-C)

   frame just contains altitude

   the other just squawk identification



All diagrams shown are just amplitude of transmission, there is no secondary modulation like FM or PSK based
(Uplink is PSK)

1090MHz Radio Channel Users

3. Mode-S
   a. Interrogated by ground station
      1. DF0 (56 Bit)
         - ACAS (general)
         - TCAS (as one sort of ACAS)
      2. DF4 (56 Bit) rollcall reply: altitude (100ft resolution)
      3. DF5 (56 Bit) rollcall reply: squawk
      4. DF11 (56 Bit) transponder capabilities
      5. DF16 (112 Bit) never observed
      6. DF20 (112 Bit) rollcall reply: altitude (25ft resolution)
         + BDS registers (Mode-S enhanced surveillance EHS)
      7. DF21 (112 Bit) rollcall reply: identity
         + BDS registers (Mode-S enhanced surveillance EHS)

1090MHz Radio Channel Users

3. Mode-S (continued)

b. Squitter mode frames (independently transmitted)

1. DF11 (56 Bit) with InterrogatorID set to zero
   Used to get transponder capabilities without Allcall and Rollcall

2. DF17 (112 Bit) 1090 Extended Squitter
   ➔ **contains ADS-B data** (position, heading e.g.)

3. DF18 (112 Bit): same as DF17 but from ground traffic

Mode-S enhanced surveillance

- Uplink Formats UF-4 and UF-4 as rollcall

- Downlink report in DF-20/DF-21 (BDS registers)

  0x40: selected vertical intention

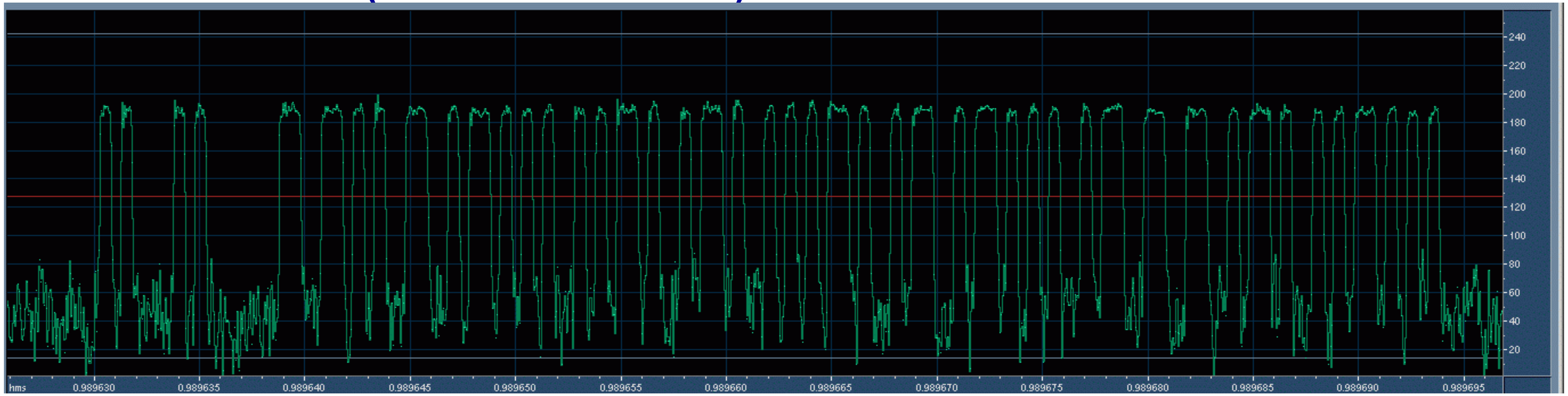
  0x50: track and turn report

  0x51: position report coarse
  (might be used for position reporting, complicated data format)

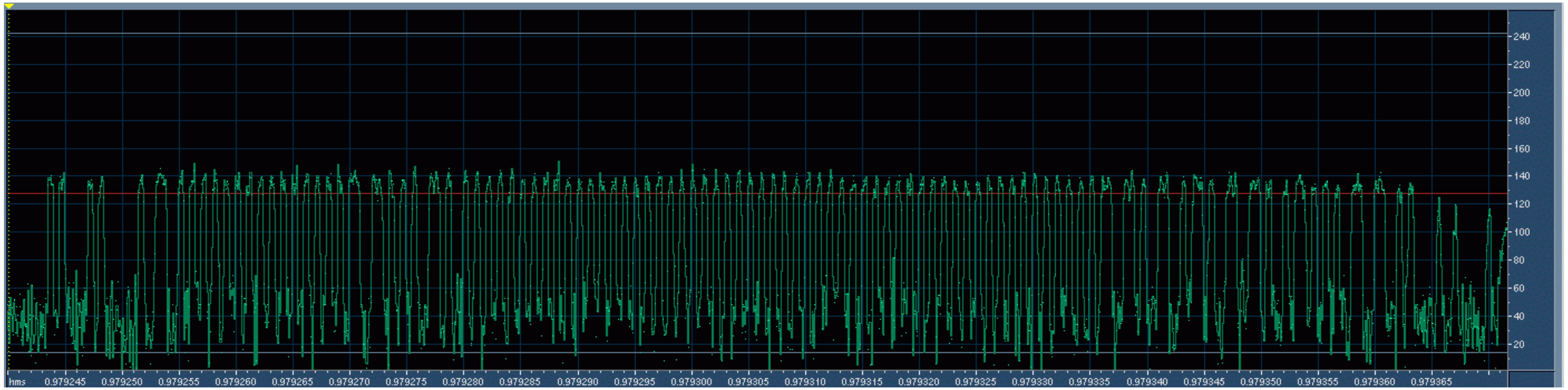
  0x60: heading and speed report

1090MHz Radio Channel Users

1. Mode-S (56 Bit frame)



2. Mode-S (112 Bit frame)

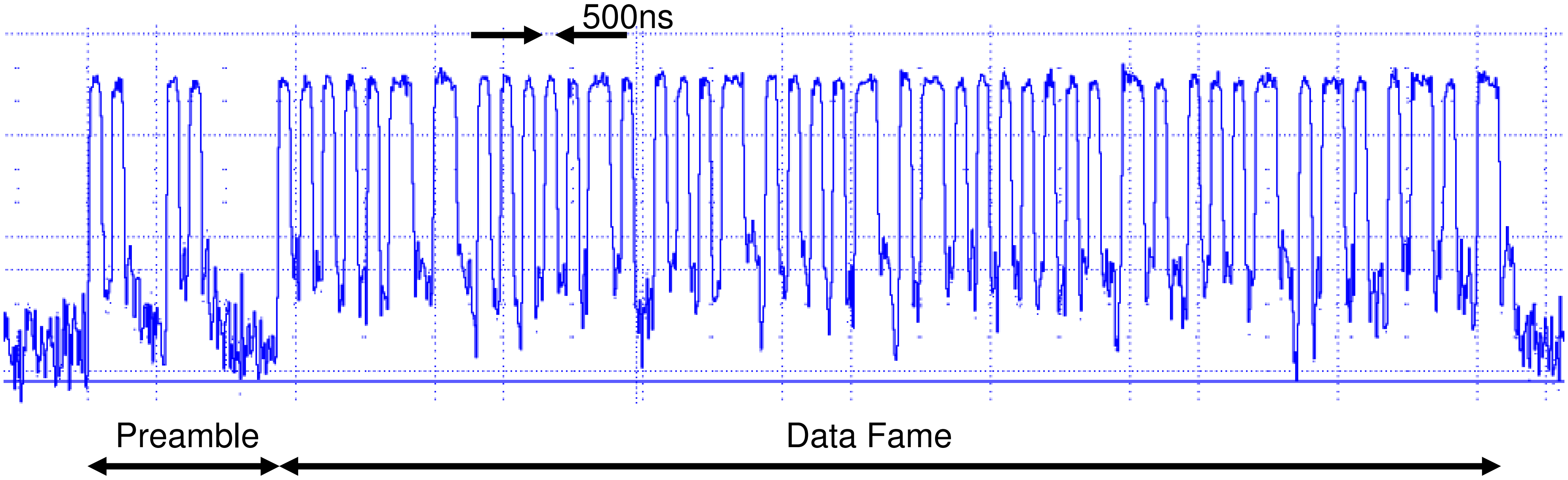


Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

The ADS-B Signal

The ADSB-B data frame consists

1) of a 8µs long preamble with 4 pulses of 500ns
2) data signal is Manchester coded with 1MBit/sec



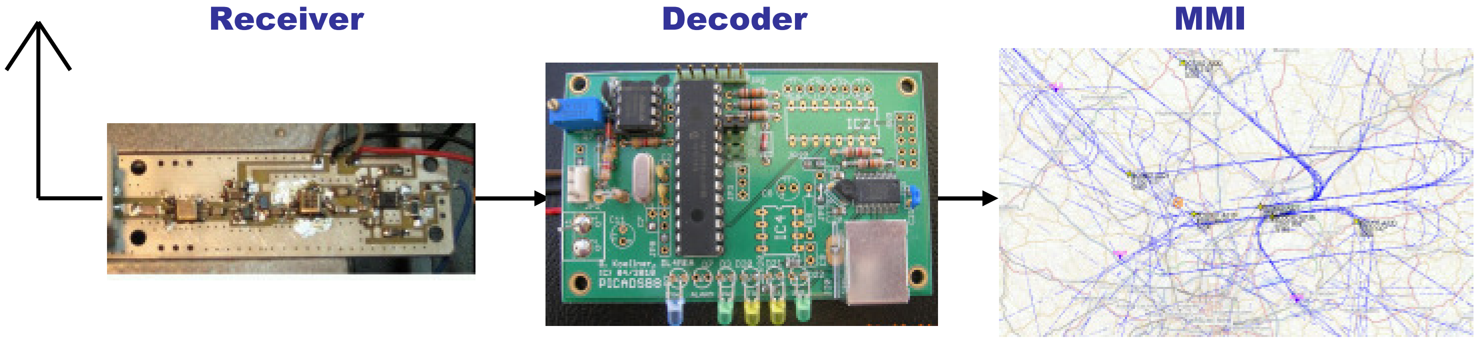
(self captured frame)

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

First reproducible non-commercial system

Based on some hobby projects, a homemade system could have been built:

- miniADSB receiver from Andy Kruse, Hamburg
- PICADSB receiver developed by Bertrand Velle, France
- PlanePlotter software from Bev M. Ewen-Smith, Portugal



I joined the open project and contributed

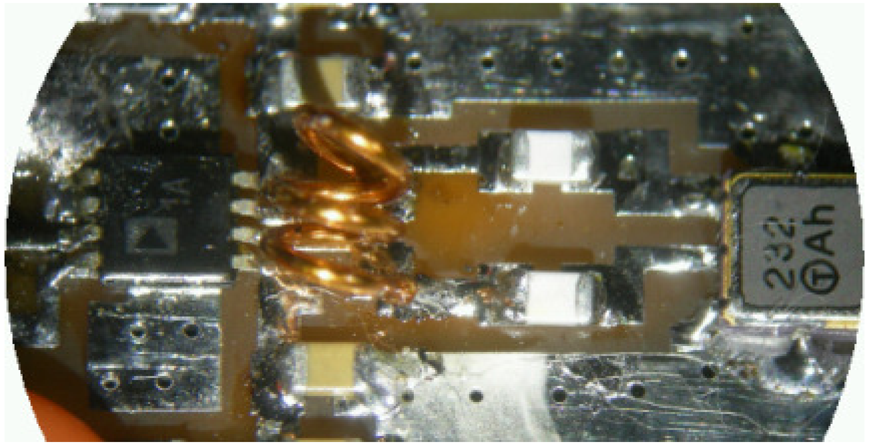
- RF improvement of the receiver: about 2dB more sensitivity
- Software debugging
- PICADSB commercial PCB with USB serial interface and power over USB

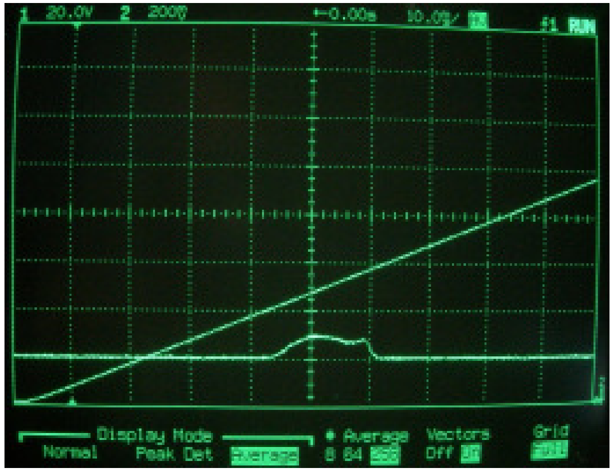
Optimization of the miniADSB Receiver

- The miniADSB receiver basically is a reverse engineering of the receiver that is used in SBS-1
- The AD8313 (chip on the left side of the picture marked '1A') is a wideband logarithmic detector
- With the wideband matching, a 53 Ohm resistor terminates in a wide frequency range, which is not needed when only used on 1090MHz, so I used a LC circuit to match it for narrow band.

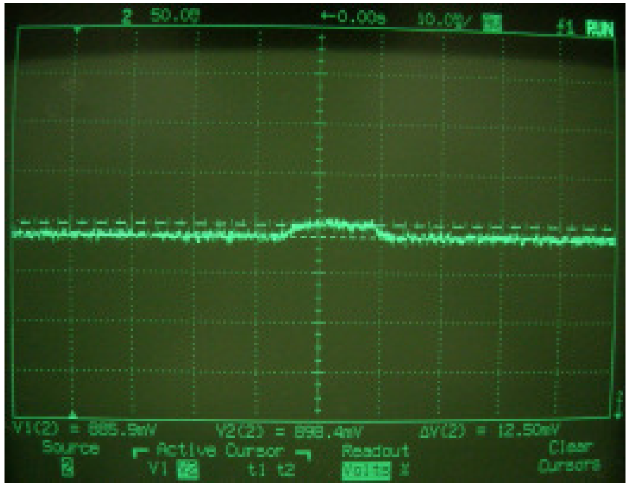
Result:

- Gain increased by app. 6dB (see left)
- Sensitivity increased by 2dB (experience)





Wideband Matching -90dBm
100mV above noise
Scale 200mV/10dB →-100dBm not detectable



Narrow Band Matching -100dBm
12.5mV above noise

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Doughnut Effect

The AD8313 “power off” edge is slow.

With a fixed level comparator as it was used in previous circuits (grey line) it does at the output not provide a 50% duty cycle signal.

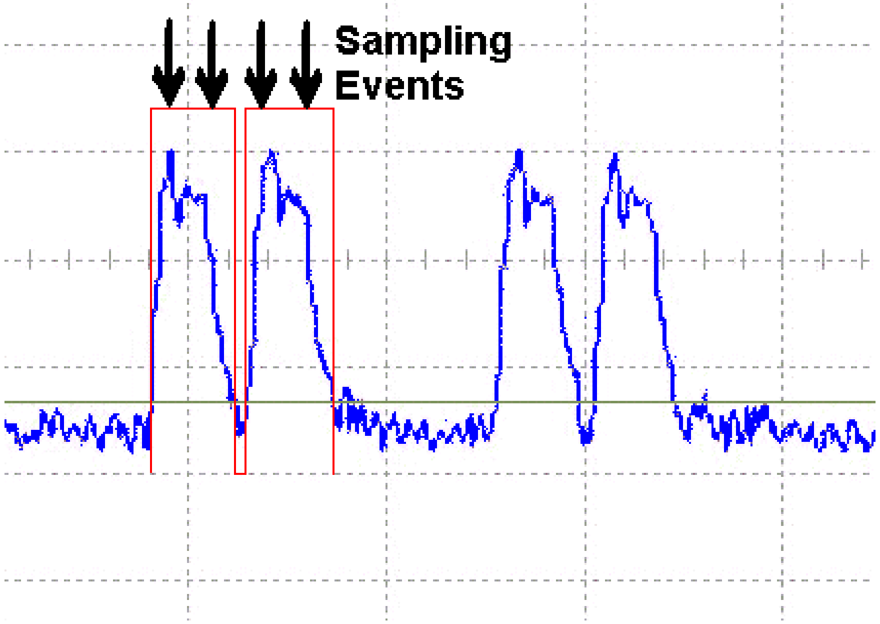
→The microprocessor reads “11” in this case.

→ Strong signals are not decoded correctly

Otherwise, if comparator level is set to high level, weak signals would not be decoded.

→Required is a fast adapting comparator level

(Even some of the cheaper professional units suffer from this problem)



Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

My solution:

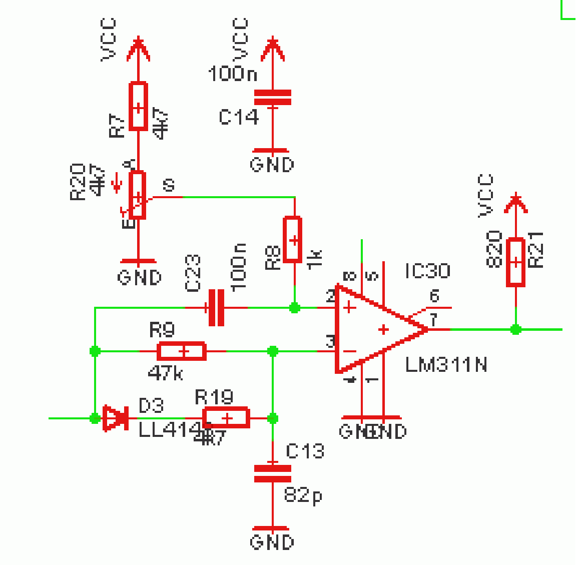
Asymmetric lowpass adapts the comparator reference to the signal strength.

Circuit:

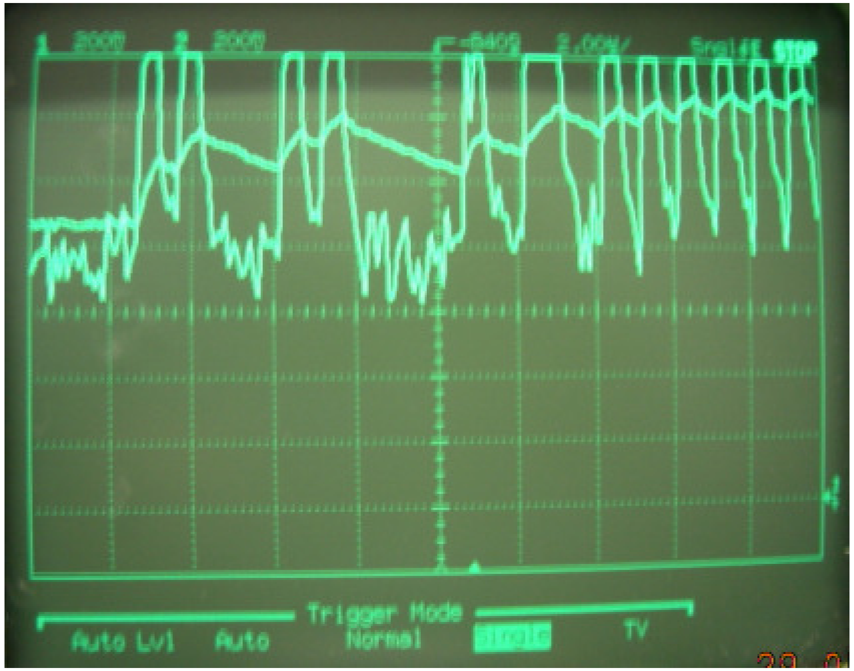
Charge quickly via diode D3/R19

Discharge slowly via resistor R9

Diode also ensures required offset to peak



Verification:

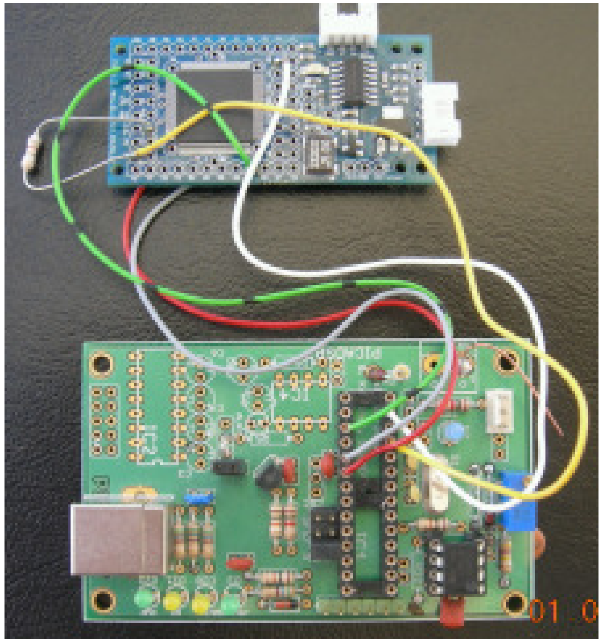


The line in the middle is the comparator level as it adapts to the signal level with each pulse.

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Development in VHDL

- For my own training, I also developed an ADS-B decoder, based on the current available hardware, just replacing the PIC by a small Altera Cyclone development board



- **Development:**
  - Completely done in ModelSim, worked immediately in real HW

Advantages of an FPGA

- Any microprocessor has only one processing unit
  - It can only do one thing at a time (at least smaller ones like ATMEL or PIC:
    - Signal sampling (anyway, as non interruptible task only)
    - CRC calculation
    - Output interface handling
  - while the FPGA builds up dedicated hardware for each function
    - a FPGA is like wiring standard gates from the shelf in order to reach the functionality. Each block is working for its own

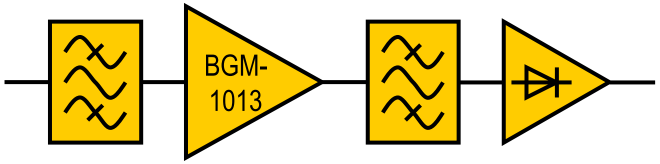
- Faster Speed:
  - The FPGA can provide logic signals up to around 120MHz, depending on the programming.
    - For example, internal processing is done based on 64 MHz
    - While a microprocessor can just do 2 samples per microseconds, as it is necessary for the 1MBit signal, the FPGA does 16 samples in the same time, and even those each with 8 bits from the ADC

- Simulation Capability (better say: essentiality?)
  - All tasks inside the FPGA can (must) be verified with simulation
    - Verification of the whole decoding process
    - Verification of the cause of errors

    ➔ I am even so far that I can verify the cause of single bit errors.

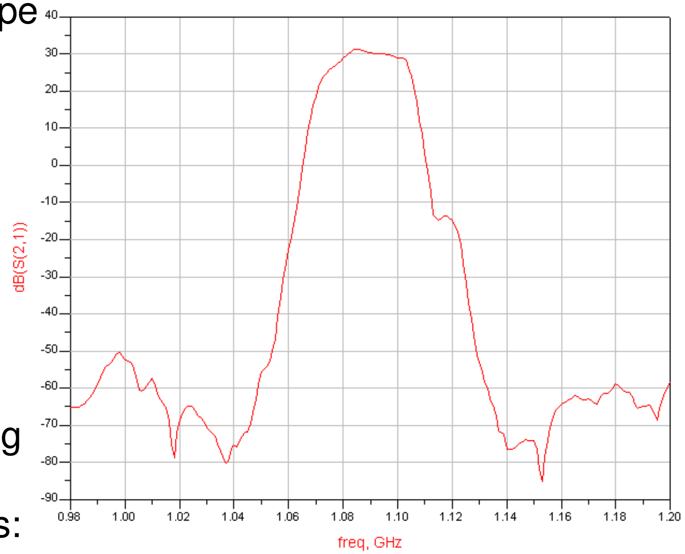
2nd Phase of Receiver Improvement

miniADSB receiver:



- attenuation of 1st band pass adds to noise figure of receiver
- non matched filters misshape the pass band curve

without matching

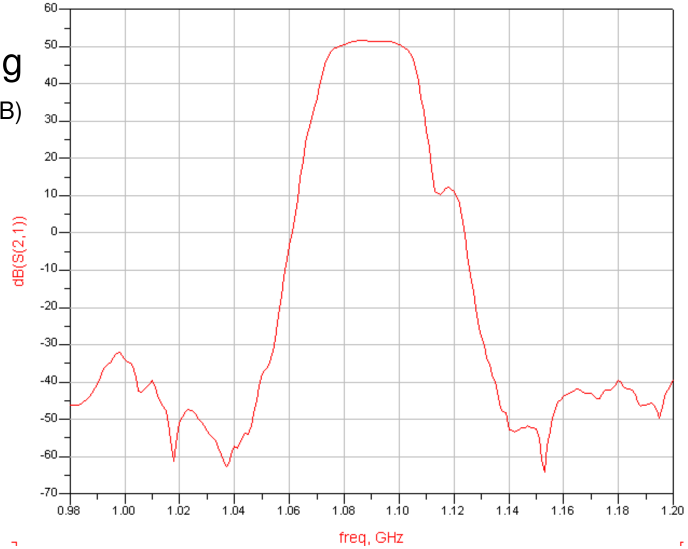


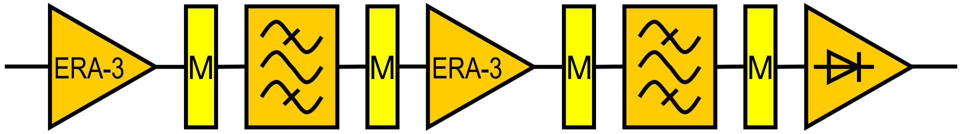
HFSS Simulation Results:

Integrated receiver with matching sections:
(done by Luis Cupido, CT1DMK)

with matching

(scale shifted by 30dB)





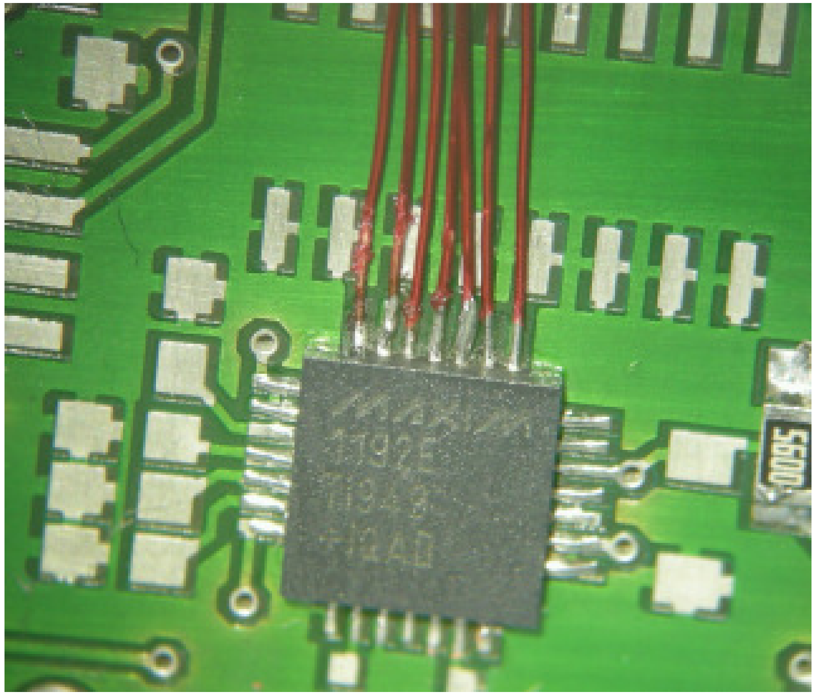
Total gain was split into two devices in order to avoid noise figure degradation in first filter. A high IP3 amplifier is used for safety against intermodulation from GSM, radar, DVB-T and others

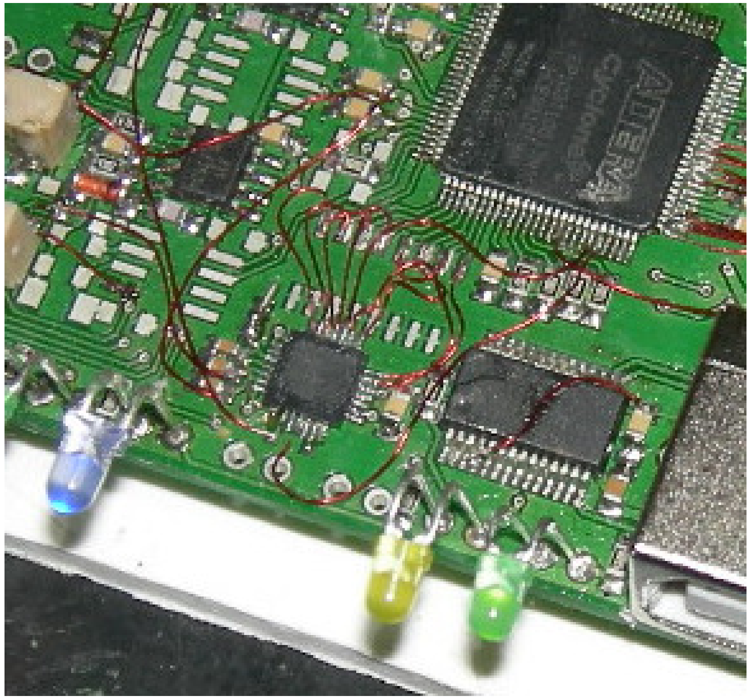
Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Upgrade using a MAX1192 ADC

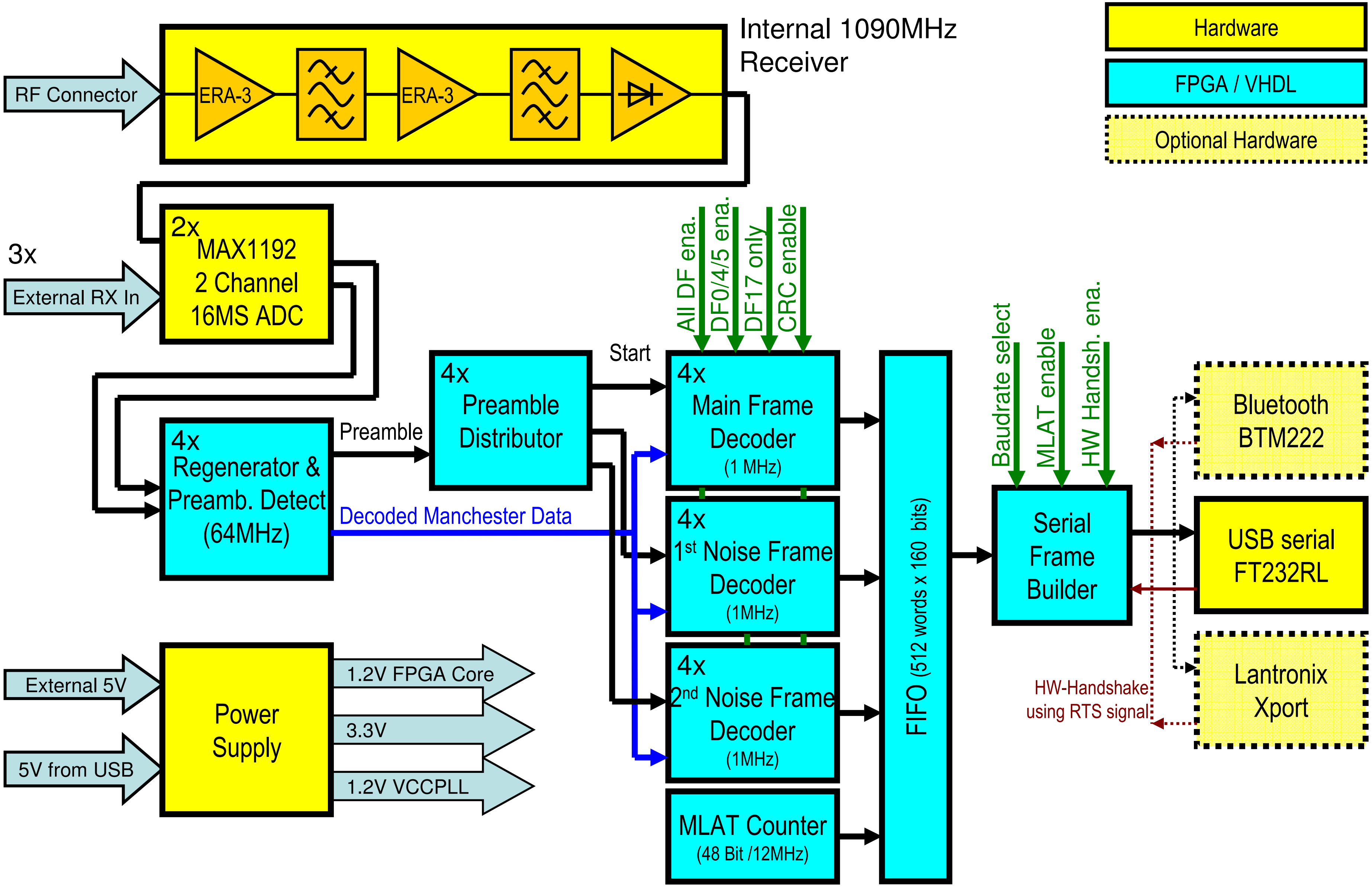
- Place to solder was already foreseen for proper grounding and power supply
  - Manual wiring of signals with thin wires (this weird wiring has at least less crosstalk)

- ADC is providing 16MSample/sec (1st generation used 10MSample/sec)
  - 8 samples per chip → easy to average
  - no other ADS-B receiver is known using such a high sampling rate





Block Diagramm (Version 1.0)

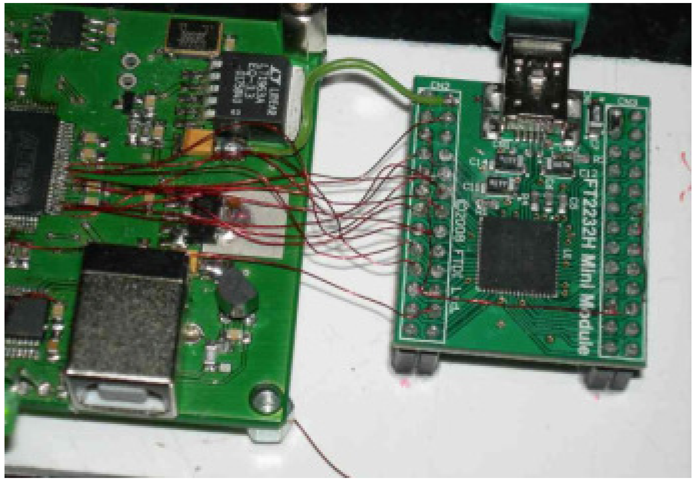


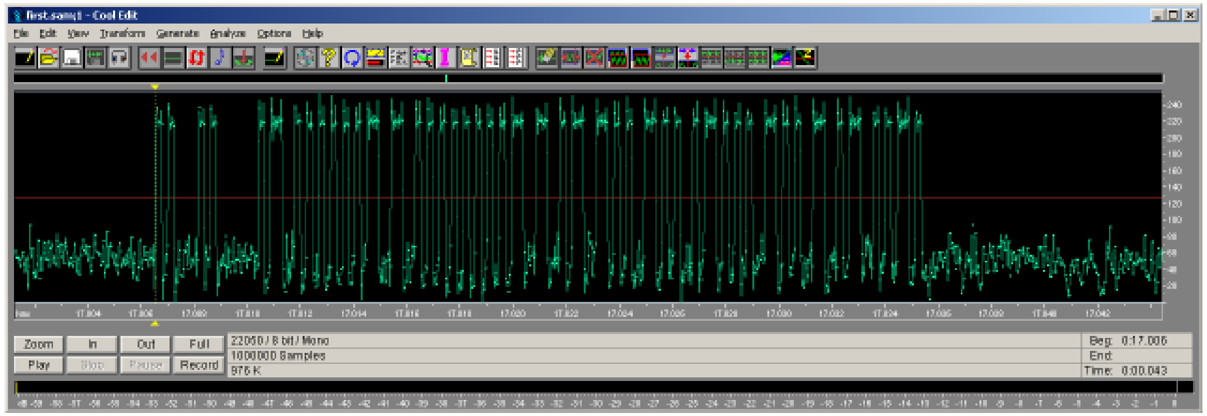
Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

AD Data Capturing

- For offline analysis and simulation with comparable input data, a capture port was implemented.
  - 16 MByte/sec towards the PC using USB 2.0 High Speed
    - Cypress FX2 was tried but found as too complicated to implement
    - FTDI FT2232 provides up to 16MByte/sec in asynchronous, up to 40MByte/sec in synchronous mode, and is available as “FT2232 mini module”
  - Simple Capture Tool in DOS on PC

- CoolEdit96 is able to display raw sample files after minor data format conversion





22050 / 8 bit / Mono
1000000 Samples
976 K

Beg: 0:17.006
End:
Time: 0:00.043

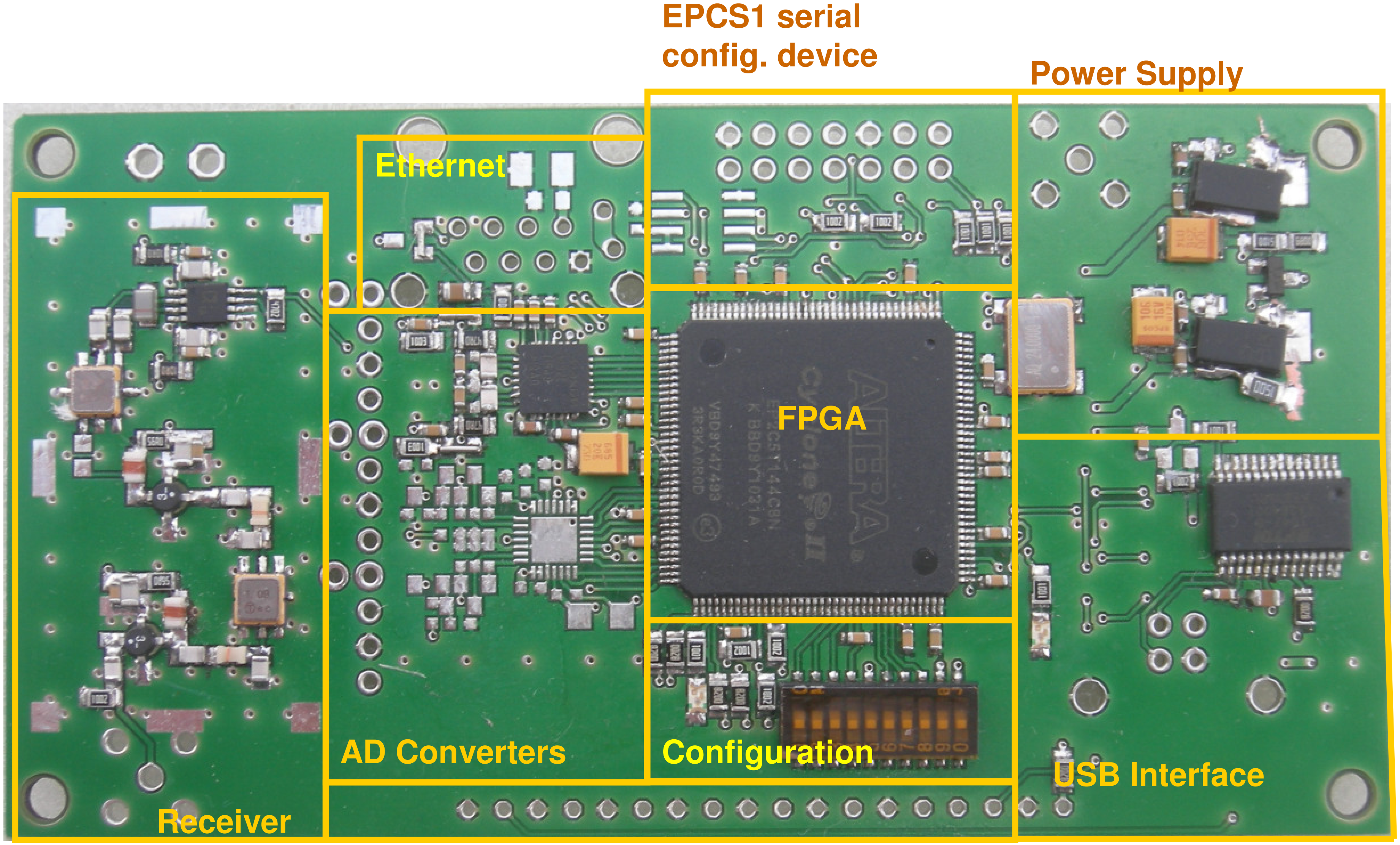
Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Simulation Using Captured Data

- Captured data can be read in ModelSim VHDL simulator and are undergoing the same sequence as in real hardware
  - Options
    - Analysis of frames that were aborted
    - Impression how the decoder handles weak frames
    - Simulation of 1 sec in reality needs around 5 minutes in simulation

➔ Results in simulation and reality are very close together

PCB made with Eagle (10mil technology)



EPCS1 serial
config. device

Power Supply

Ethernet

Receiver

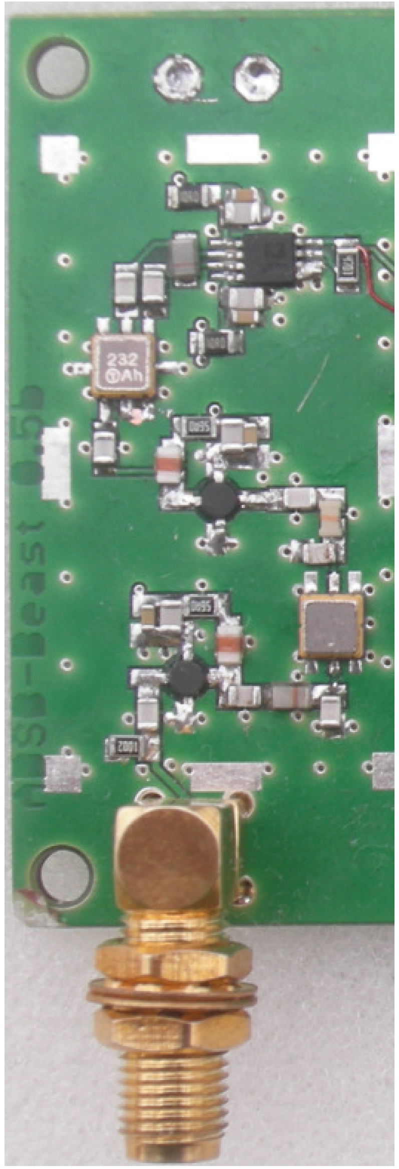
AD Converters

FPGA

Configuration

USB Interface

Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen



PCB Layout - RF part

Challenge:

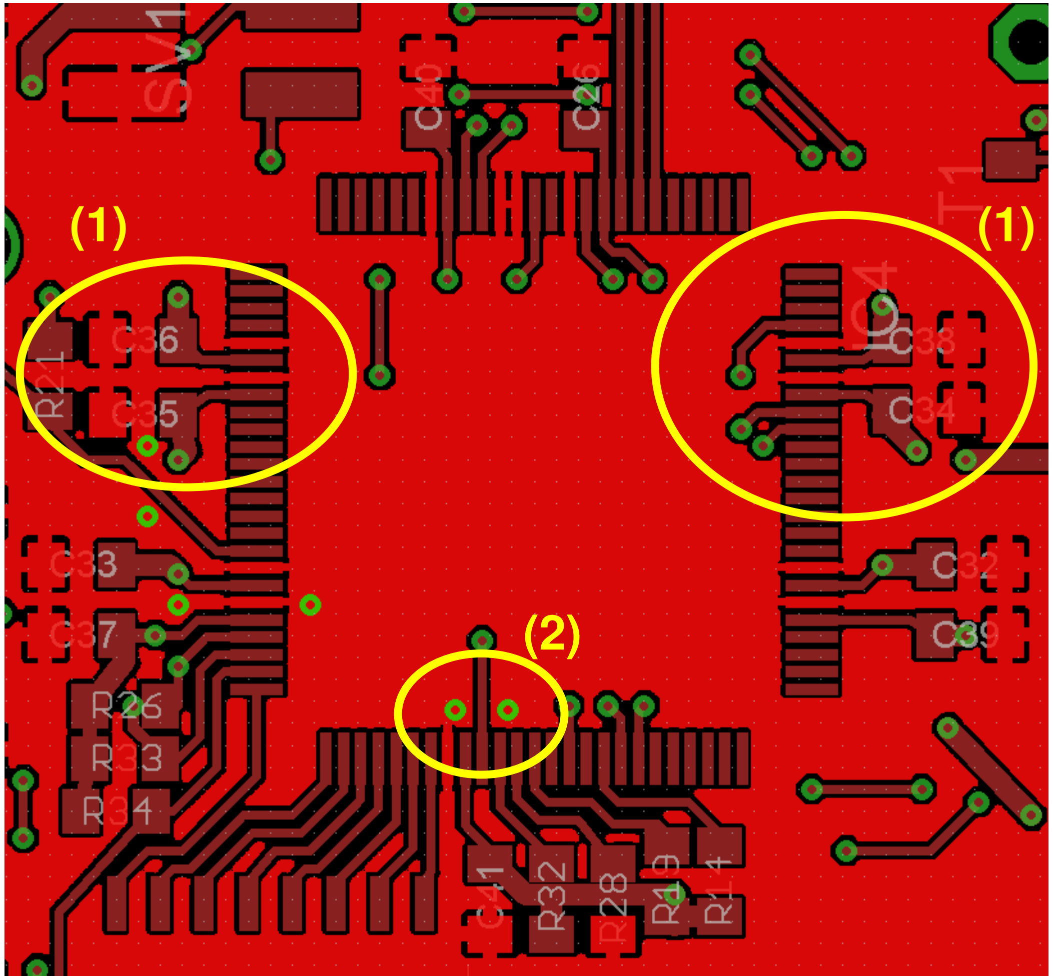
Sensitive receiver (actually only a power detector) on same PCB with **Bluetooth transmitter**. Even when frequencies are different, there might be remains

Solution:

- Receiver uses a solid ground plane without thermals, a solid ground plane on reverse side and an option for shielding cover
- Receiver and Bluetooth on different sides and also opposite layers on PCB
- Bluetooth antenna externally connected

→ Result: While bluetooth is active just 10% degradation

PCB Layout - FPGA



Light red is ground plane

Challenge: Layout with only 2 layers due to costs

Solution:

- All FPGA ground pins connected from 2 sides (1)
- Power supplied from bottom
- Bridging of ground plane slots on bottom (2)
- Shortest connection between blocking capacitor and power pins

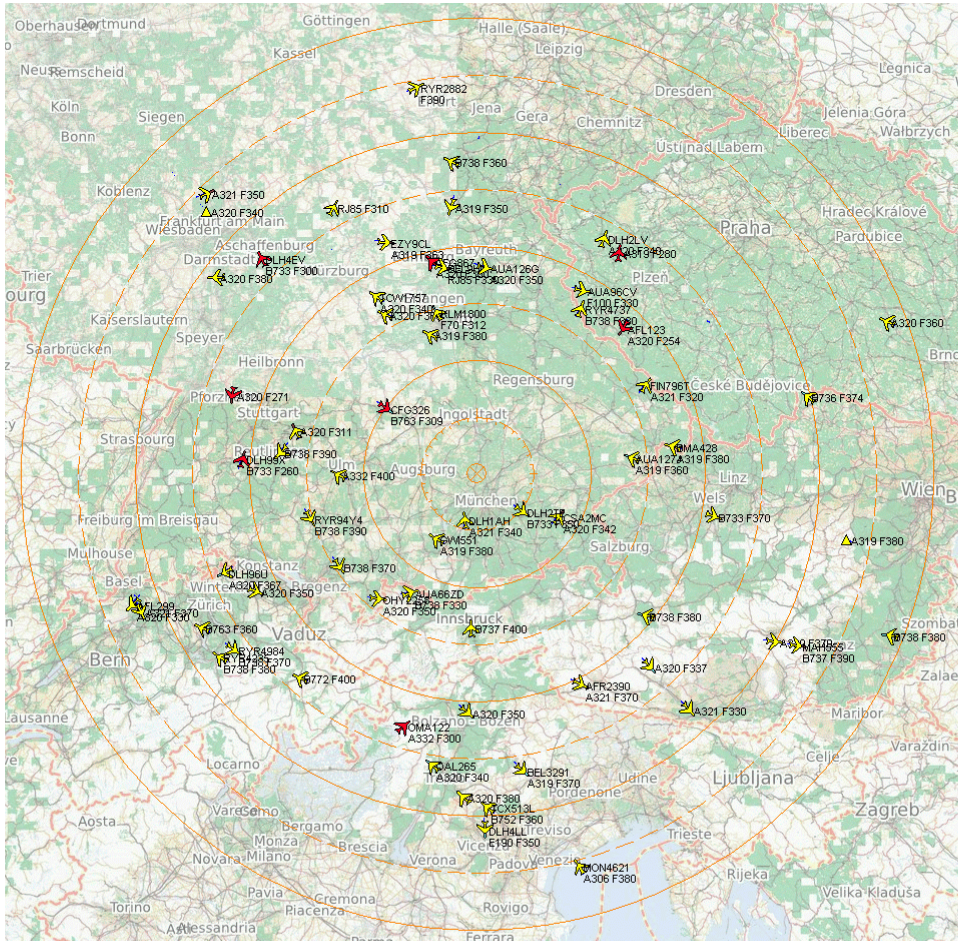
→ Result:

No problems with FPGA

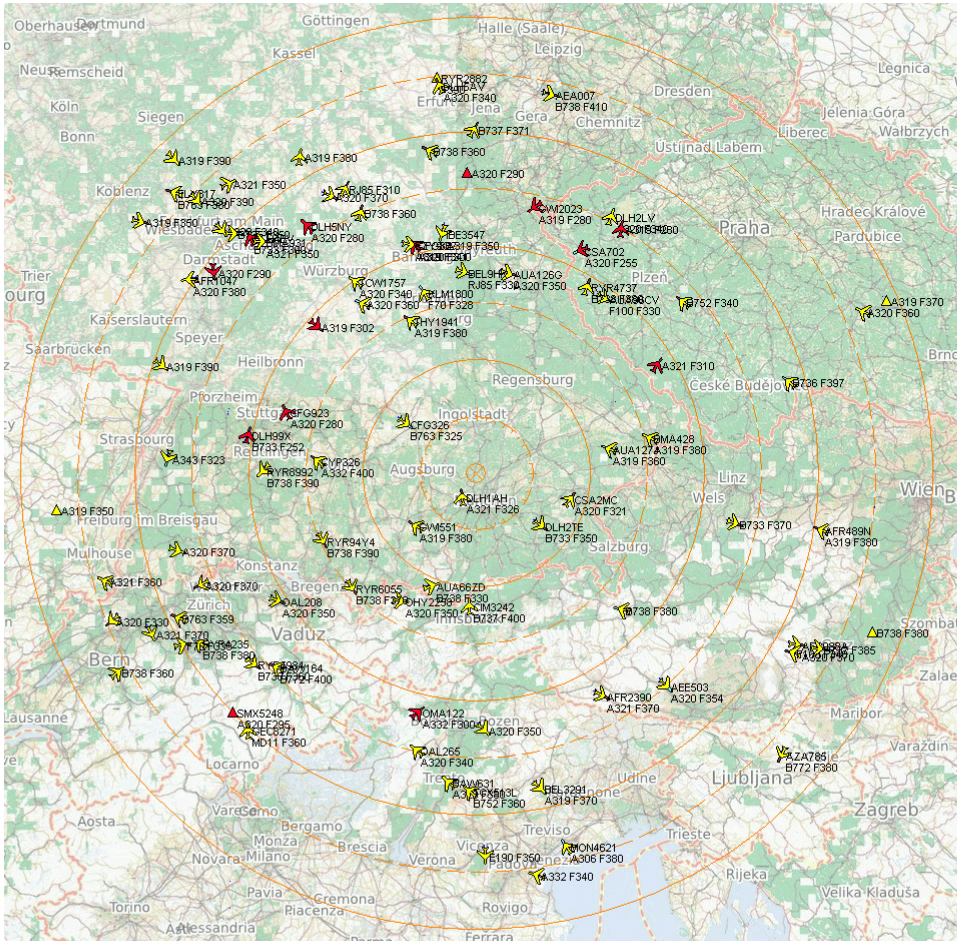
Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Performance of the Mode-S Beast → aircraft beeing shown

Flagship running for 30sec



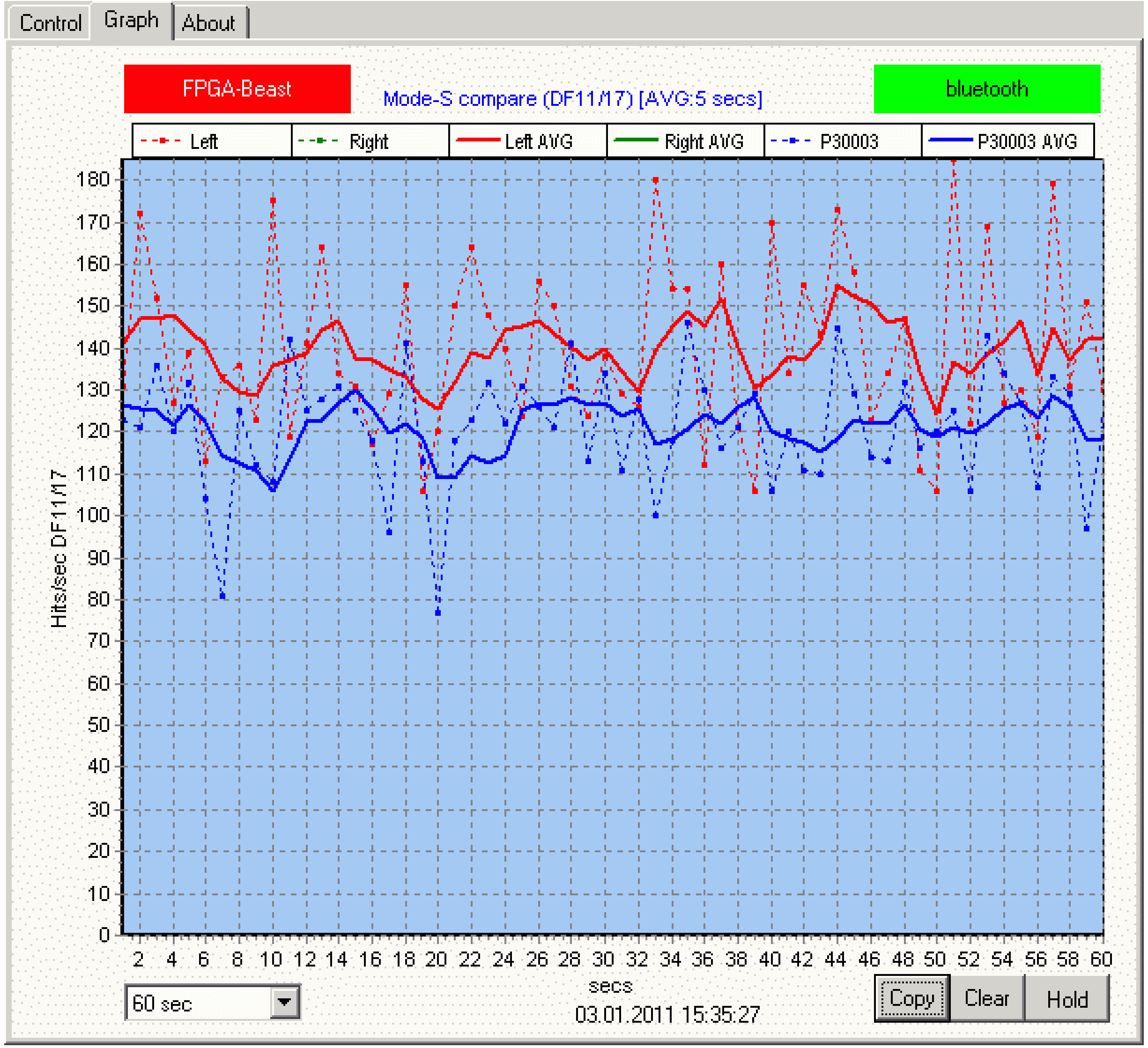
Mode-S Beast running for 30sec



Performance of the Mode-S Beast → frame rate

Red: Mode-S Beast

Blue: Flagship



Günter Köllner, DL4MEA, Am Rain 24, 85256 Vierkirchen

Further Development Planning

- MatLab processing of captured data
  - Cancelled: I do actually not believe that there is any possible gain from this in aspects like performance increase and saving FPGA resources

- Further improvement of RF receiver
  - faster detector using a diode → would drastically help decoding overlapping frames
  - lower noise figure → cancelled since there is no further improvement from 2dB down to 1dB on a terrestrial antenna

- Postprocessing of data frames using an embedded core
  - Currently done using a PC software driver
  - Offline post processing of corrupted frames has shown that around 25% of the erroneous frames suffer from just a single bit error (13% with 2 bit errors) which can be corrected.

- Decoding of
  - Mode-A/C frames
  - frames with FRUIT (FRUIT: „False Replies Unsynchronised in Time“)
  - Overlapping frames (as far as possible with AD8313 detector)

Further Information

- Web Site:

  http://www.qsl.net/dl4mea/fpgaadsb/modesbeast.htm

- Youtube:

  http://www.youtube.com/watch?v=Re0FT606GEY&feature=recentlik