



2013 Conference

Covert Audio Technical Surveillance

BURST & TMVWB Systems

Why this presentation ?

A typical example of ex. Gov Stuff

- ▶ State level threat some years ago. Now Corporate level
- ▶ Very good quality
- ▶ They aren't brand new, so widely spread in Europe
- ▶ Affordable and available on the commercial market
- ▶ Easy to detect with proper tools and procedures

Introducing

- ▶ The need for new designed equipment in TSCM
- ▶ A new approach in TSCM procedure

1/ AURORA

Pulse Audio Monitoring System



Aurora presentation

Type

- ▶ Digital UHF TX - RX kit remotly controlled
- ▶ Buffer & Burst transmission system
- ▶ Low Probability of Interception
- ▶ Low power consumption

Origin

- ▶ Russia
- ▶ Manufactured by SET-1 (www.set-1.ru)

Complete set

Transmitter



Extern. Microphone



Remote Control



Receiver



Aurora system

Operating principle

- ▶ Audio information is picked up by external microphone
- ▶ Transmission of audio intelligence via radio channel
- ▶ TX. Step by step accumulation of audiodata in the internal RAM followed by rapid rate packed RF transmission of the stored datas.
- ▶ RX. Reception of data packets, error correction, packet merging and digital to analog conversion.
- ▶ RC. Control over transmitting power, sampling rate, duration and packet reoccurrence interval.

Tech. Specifications

TX ref RMI 400



- ▶ Carrier freq. of data channel: 1000 - 1200 MHz
- ▶ Output power (selectable): 50 - 350 mW,
- ▶ Modulation: GMSK - BW: 12 MHz (-20dB)
- ▶ Packet duration (selectable): 30 - 250 milliseconds
- ▶ Packet reoccurrence interval (selectable): 1,2 - 26 s.
- ▶ Power supply: 3,6 - 4,6 v
- ▶ Current consumption: standby: 250 μ A, storage: 15mA, packet transmission (max output); 500 mA
- ▶ Dimensions: 137 x 30 x 10 mm

RX ref PRI 400

- ▶ **Sensitivity: No less than 10 μ V**
- ▶ **Power supply: 4 x AA or extern. supply**
- ▶ **Current consumption: > 180 mA**
- ▶ **Dimensions: 170 x 70 x 35 mm**
- ▶ **Connexions for :**
 - **Antenna**
 - **Headphone**
 - **External power supply (9 V, 300 mA)**
 - **Recorder**



RC ref DPK 010

- ▶ **Output power: + 22 dBm**
- ▶ **Quantity of instructions: 17**
- ▶ **Carrier frequency: 433,920 +/- 100 KHz**
- ▶ **Power supply: 4 x AAA**
- ▶ **Dimensions: 100 x 51 x 18 mm**



Operation modes

Set by the Remote Control

	D1	D2	D3	D4	Packet Duration
L1	1,2	1,6	4,4	3,2	30 mS
L2	2,4	3,2	4,7	6,5	58 mS
L3	4,7	6,5	9,4	13	116 mS
L4	9,4	13	18,8	26	231 mS
Sampling Rate	22 KHz	16 KHz	11 KHz	8 KHz	

L: Packet Duration (ms)

D: Sampling rate of the A-D converter

xx: Packet succession period (s)

P: Tx output (250 - 450 mW)

Detection

Methods and Means

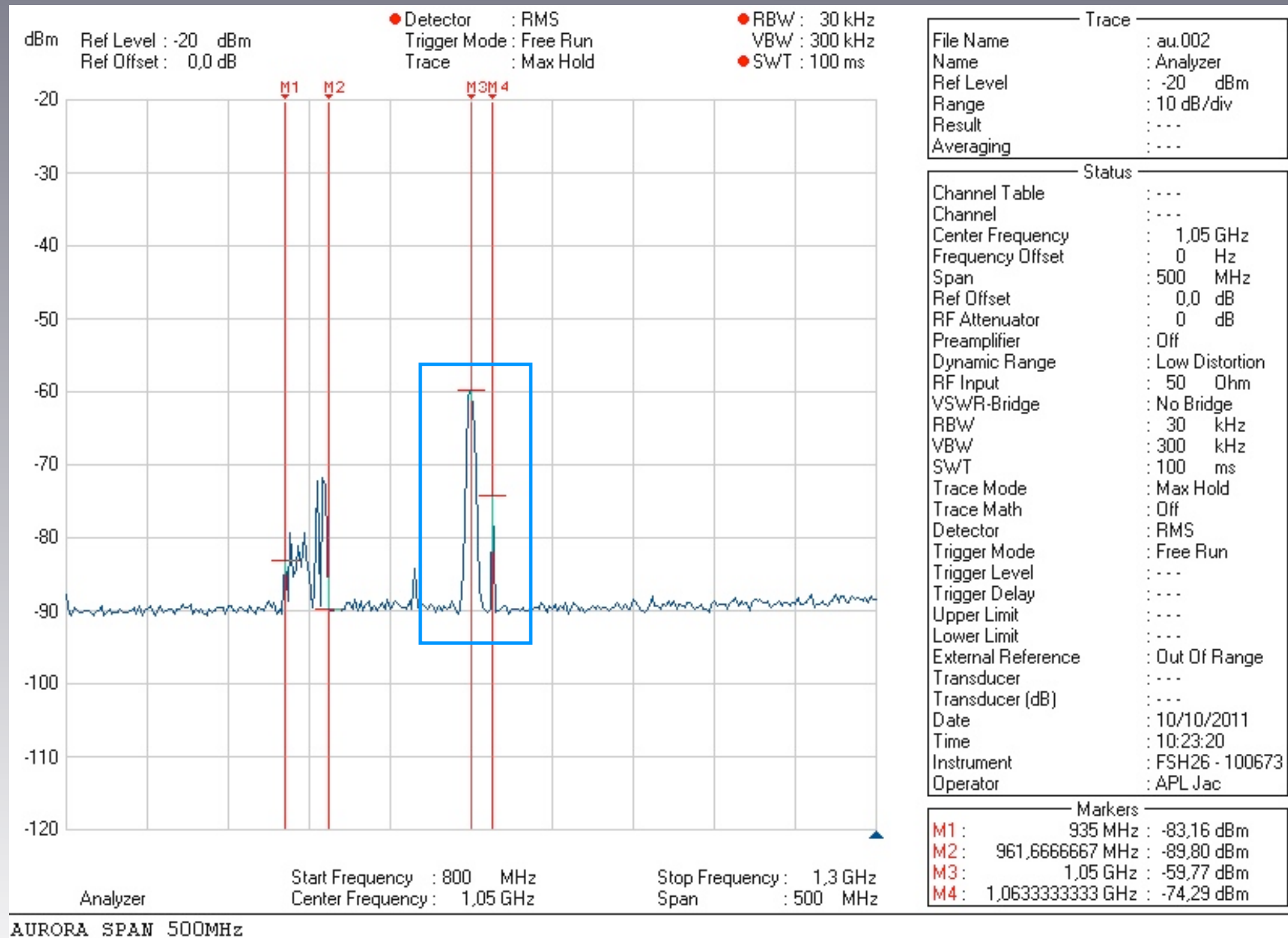
▶ **RF Capture & Analysis**

- **Spectrum Analysers (Maxhold configuration)**
- **RF wide band & fast receivers with waterfall display**
- **TSCM dedicated equipments - Oscors, Raptor, Merlin 3, SDR ?**
- **Fast near field detectors (Close to the active TX)**

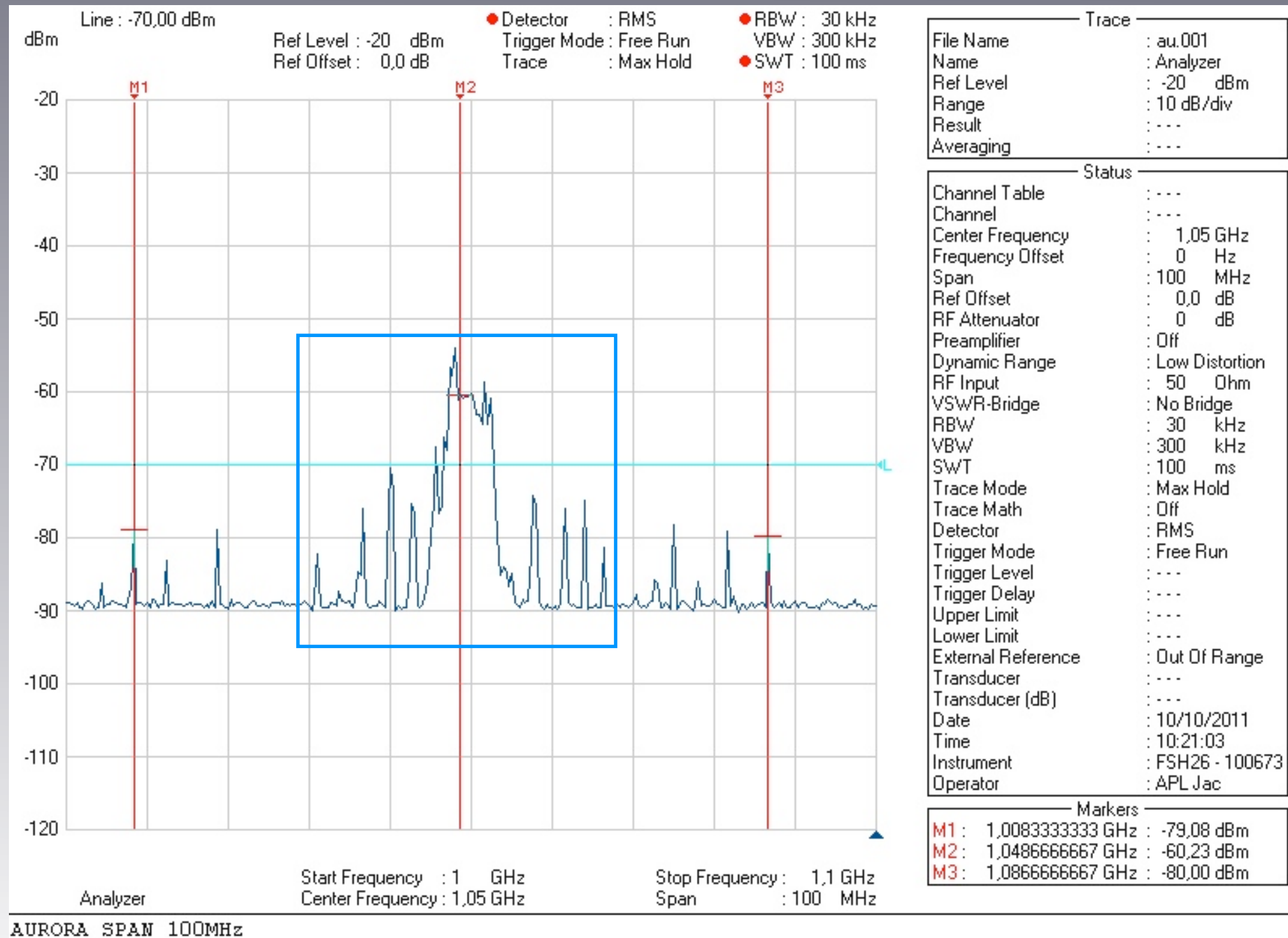
▶ **Physical & Electronic search**

- **Visual & optimal search**
- **NLJD**
- **ASMD (if the TX mic is active - powered)**

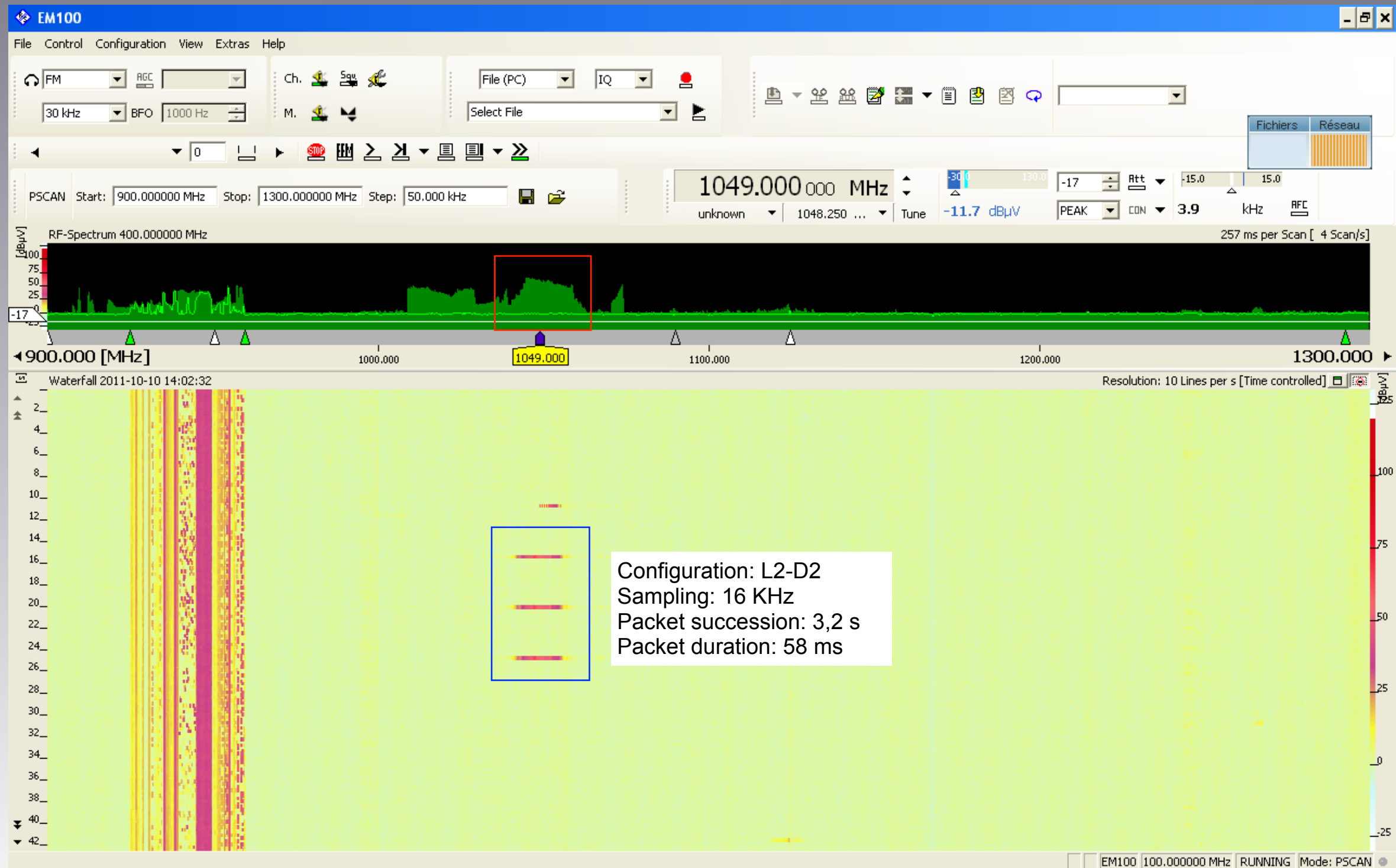
RF Capture (SA - R&S / FSH-6 Screenshots)

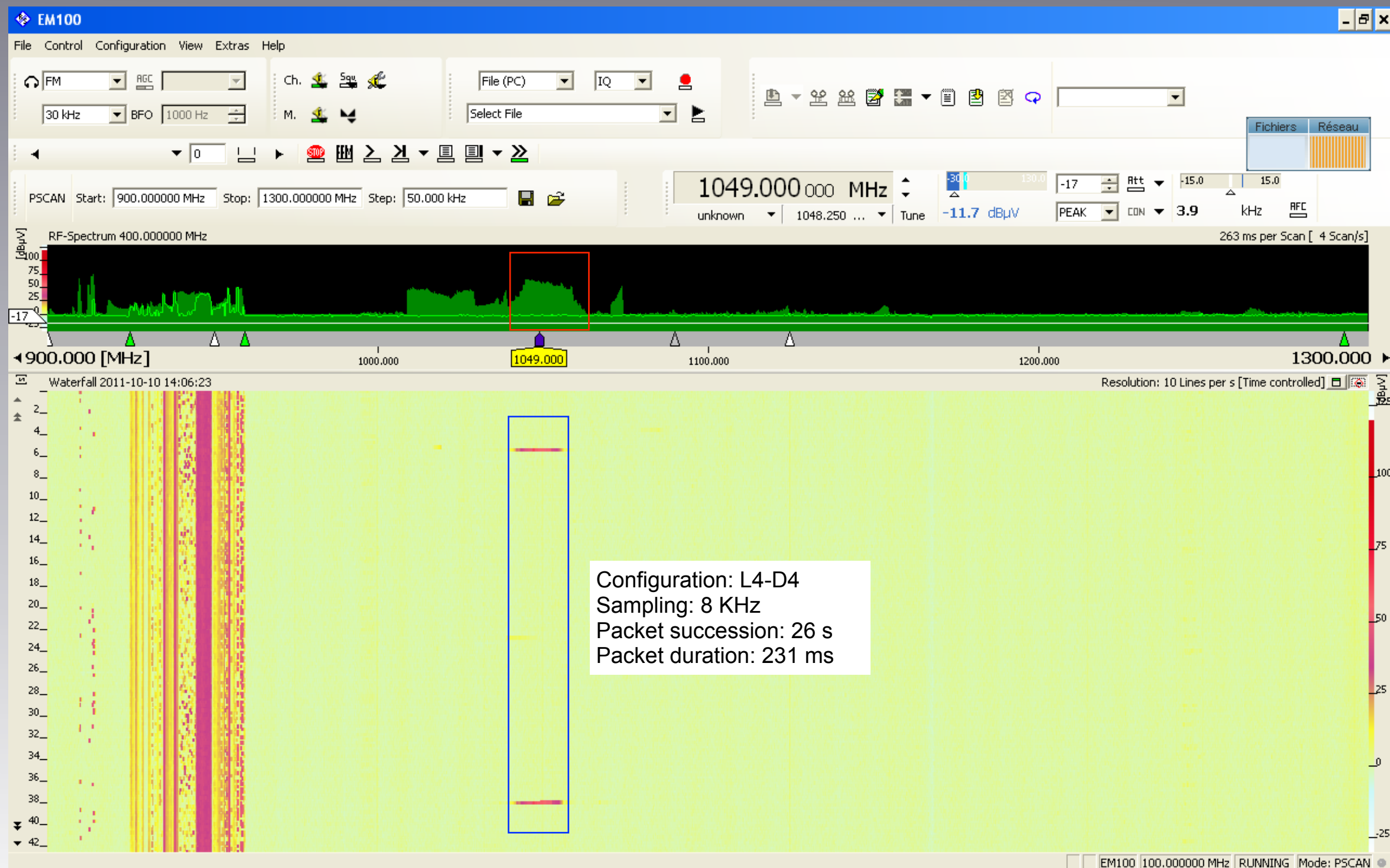


RF Capture (SA - R&S / FSH-6 Screenshots)



RF Capture & Analysis (EM-100 Screenshots)





2/ OMEGA-1T

TMVWB Audio Monitoring System



OMEGA-1 Présentation

Type

- ▶ Digital UHF TX - RX kit remotely controlled
- ▶ Time Modulation Very Wide Band transmission system
- ▶ Low Probability of Interception
- ▶ Versatile and modular by rerouting the signal
- ▶ Extremely low power consumption (1 x 9 V batt. = 500 h)
- ▶ «Old» product, widely distributed. Constantly upgraded

Origin

- ▶ Italy
- ▶ Manufactured by BEA (www.bea.net.it)

Complete Set

GSM Repeater



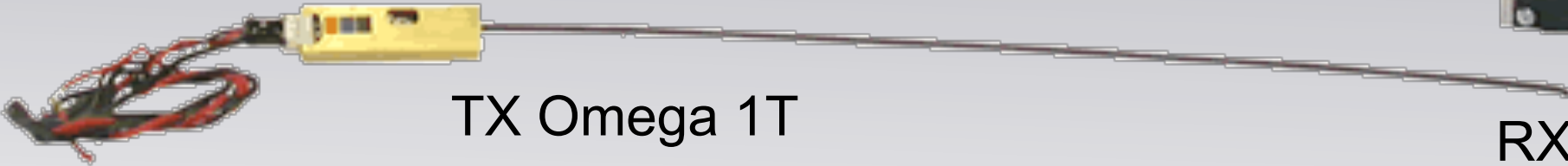
Omega 1 Master
Docking station



RF Repeater



Phone Line
Interface



TX Omega 1T

RX Modulo

OMEGA-1 System

Operating principle

- ▶ Audio information is picked up by external microphone
- ▶ Transmission of audio intelligence via radio channel
- ▶ TX. UHF, TMVWB transmitter with RC receiver
- ▶ RX. Local listening base. Docking station for RX modules
- ▶ RC. Control over On/ Off, power adjust., mic tone & gain
- ▶ Complementary options for rerouting the signal
 - Phone line interface server
 - RF repeater
 - Cellular network interface

Tech. Specifications

TX - Omega 1 T

- ▶ Frequency range: 300 - 390 MHz
- ▶ Output power: 04 - 200 mW
- ▶ Audio dynamic range: 60 dB
- ▶ Power supply: 4 - 12 V or external power supply (12V)
- ▶ Consumption: standby:0,5 mA, transmit:depend of power
- ▶ Dimensions: 41 x 17 x 7 mm without antenna



Voltage	Output power	Range	Consumption
4 V	04 mW	X	1,1 mA
6 V	16 mW	2X	1,5 mA
9 V	50 mW	3X	2,0 mA
12 V	200 mW	5X	3,0 mA

RX - Modulo F Module

- ▶ **Frequency range: 300 - 399,9 MHz**
- ▶ **Tuning steps: 100 KHz**
- ▶ **Sensitivity: - 90 dBm**
- ▶ **Audio bandwidth: 50 Hz - 5 KHz**
- ▶ **Freq. Shift compensation (± 3 MHz) + Notch filter**
- ▶ **Power supply: 8 - 14 VDC**
- ▶ **Current consumption: 50 mA**
- ▶ **Dimensions: 73 x 45 x 10 mm without antenna**
- ▶ **To be integrated into the docking station Omega Master**



RX - Omega 1 Master

- ▶ **Listening and docking station for the Modulo**
- ▶ **Front panel indications: RSSI (dBm), BF (mV), Vlin (V)**
- ▶ **Control adjustment: Volume, REC and VOX gain**
- ▶ **Power supply: 1,5 Ah rechargeable batt. or extern. supply**
- ▶ **Current consumption: > 180 mA**
- ▶ **Dimensions: 130 x 90 x 40 mm**
- ▶ **Connexions and control knobs for :**
 - **Headphone, recorder and phone line**
 - **External power supply (100-240 VAC - 12 VDC)**



RC - TC 2002

- ▶ **Carrier frequency: 433,9 mhz**
- ▶ **Output power: 2 W**
- ▶ **Quantity of code: 99**
- ▶ **Features control :**
 - **Mic ON/Off**
 - **Tone transmission quality and mic. preamplification**
 - **Mic output power**
- ▶ **Remotable functions: Via DTMF tones**
- ▶ **Power supply: 1,5 Ah rechargeable batt. or extern. supply**
- ▶ **Dimensions: 80 x 58 x 27 mm**

Complementary rerouting options

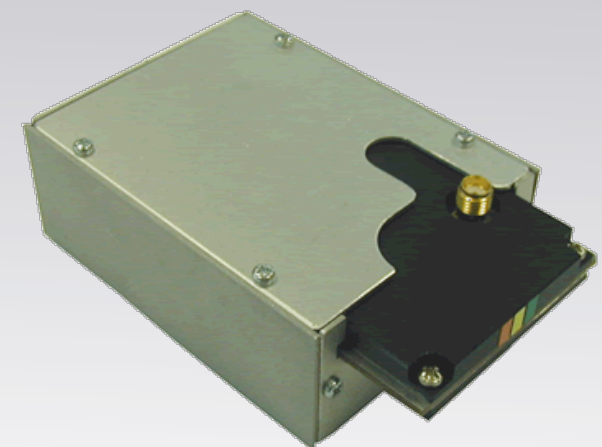
RF repeater - Omega 1 Ponte

- ▶ Extend the RF transmission range
- ▶ Output power: 1 W
- ▶ RX sensitivity: - 90 dBm
- ▶ Dimensions: 80 x 58 x 27



Phone line interface - Omega Server

- ▶ Repeat the signal through a dedicated phone line
- ▶ Power supply: 18 - 60 V
- ▶ Line isolation: > 20 M Ω
- ▶ Dimensions: 80 x 58 x 27



GSM repeater - TFG08C

- ▶ Re-launch the signal over the cellular network
- ▶ Securely programmed using SMS or DTFM tones
- ▶ Many features can be programmed (Vox, motion detec ...)
- ▶ Power supply: 6 - 36 V
- ▶ Consumption: 250 mA - 12 V
- ▶ Dimensions: 123 x 64 x 30 mm



Detection

Methods and Means

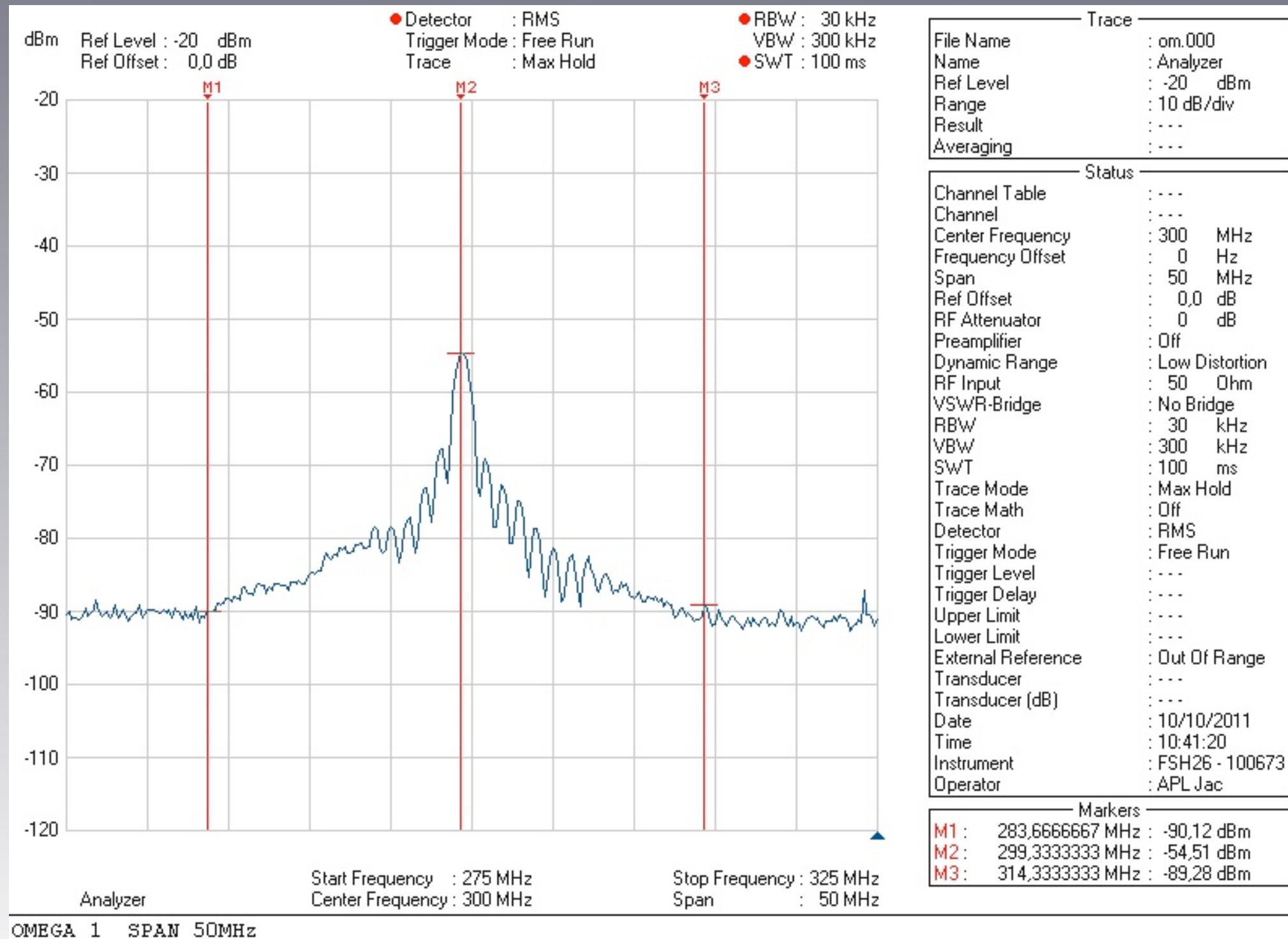
▶ **RF Capture & Analysis**

- **Spectrum Analysers (Maxhold configuration)**
- **RF wide band & fast receivers with waterfall display**
- **TSCM dedicated equipments - Oscors, Raptor, Merlin 3, SDR ?**
- **Fast near field detectors (Close to the active TX)**

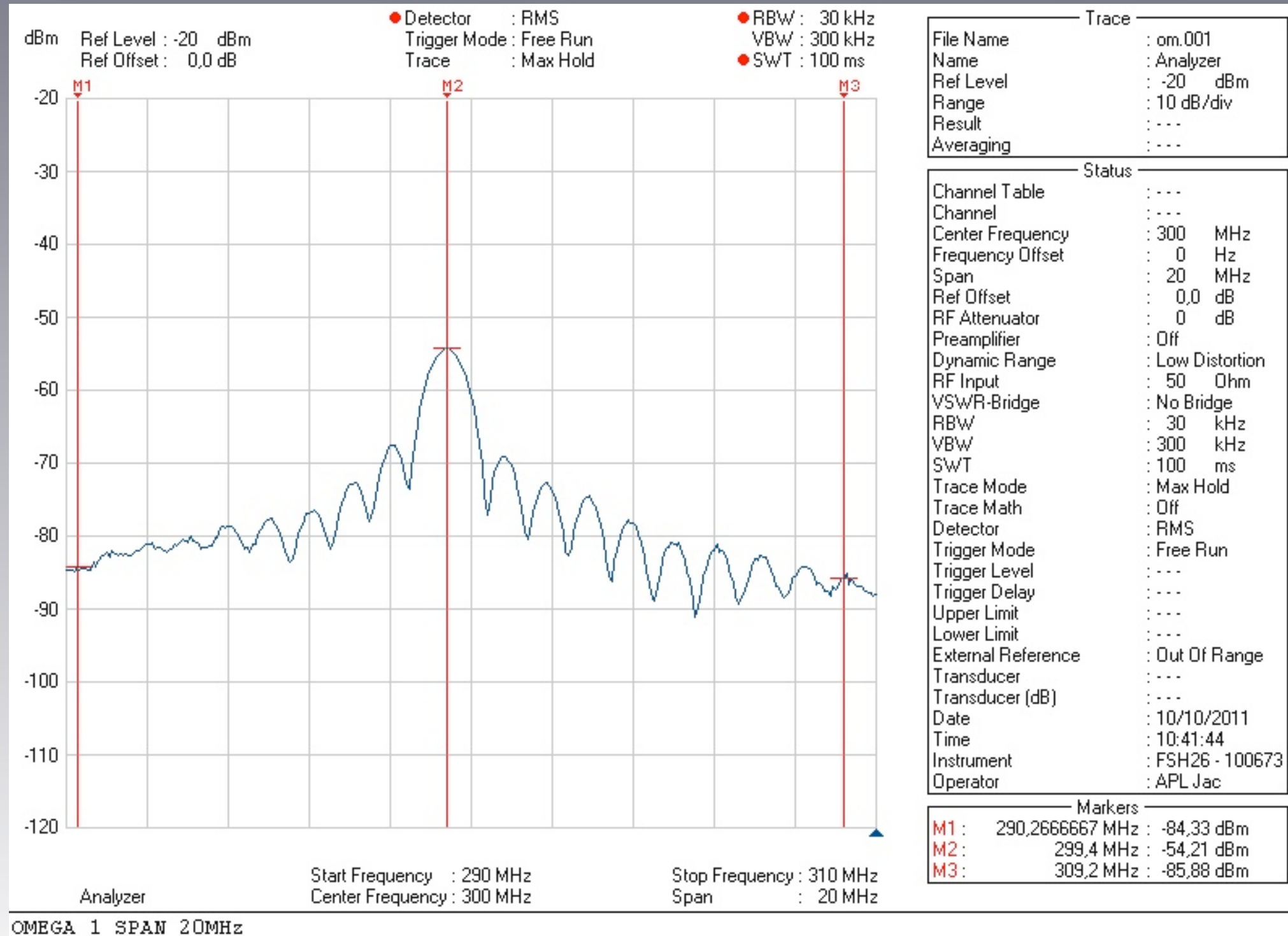
▶ **Physical & Electronic search**

- **Visual & Optical search**
- **NLJD**
- **ASMD (if the TX mic is active - powered)**

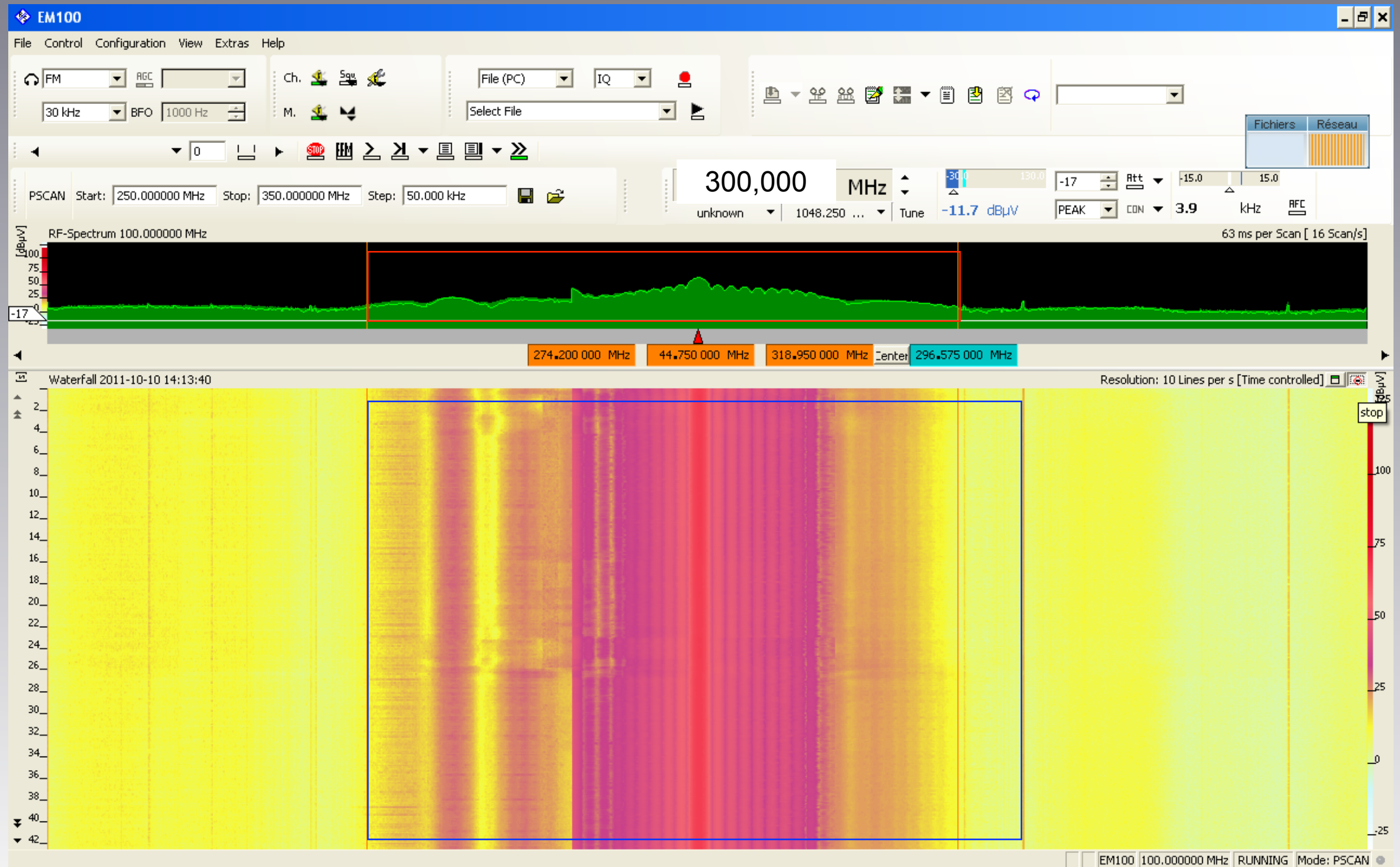
RF Capture (SA-R&S FSH-6 Screenshots)

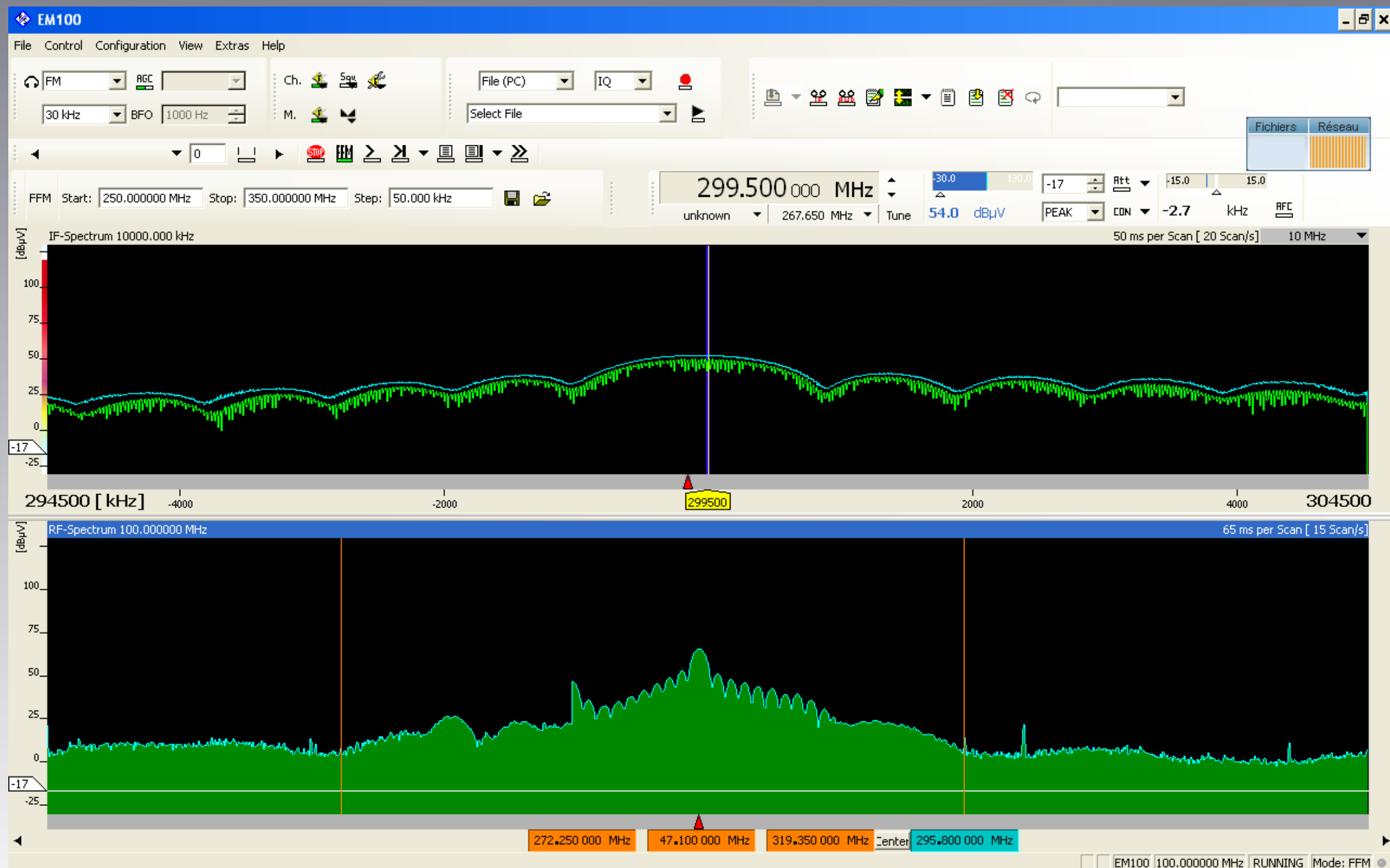


(SA-R&S FSH-6 Screenshots)



RF Capture & Analysis (EM-100 Screenshots)





Conclusion - The introduction to :

The need for specially designed systems which:

- ▶ Cover high frequency range
- ▶ Scan very quickly with good selectivity and sensitivity
- ▶ Record data for replay with time & frequency read out
- ▶ An analysis capability to identify/classify particular signals
- ▶ Can be remotely controlled (Ethernet, wireless networks)

The need to adapt our procedures

- ▶ A capability to analyse in differ mode
- ▶ A capability to analyse from a remote place (big challenge!)
- ▶ A capability to face new threats - GSM, Wifi, Bluetooth bugs



**« Thanks for your time &
attention »**