delta S
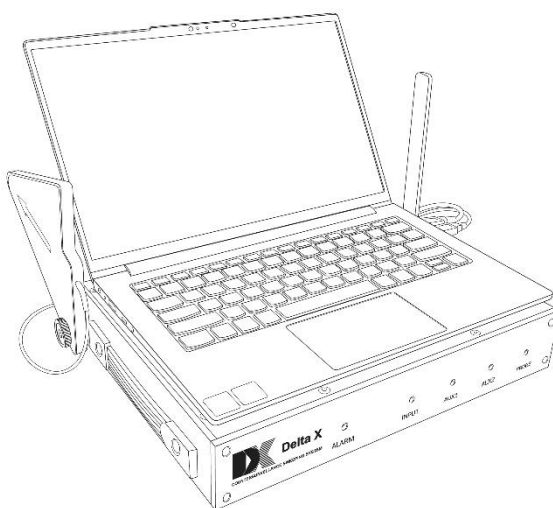
Delta X

Countersurveillance sweeping systems
(with "Breeze RF" software)

User manual

Content

About the systems

Welcome to the world of professional counter surveillance! The Delta S and Delta X analyzers will make your bug sweeps quick and easy, while providing extremely reliable results. Their hardware provides a super-fast speed of measurements, while the built in antenna switching system gives the ability to achieve extreme sensitivity in the entire frequency range.

Unlike other spectrum analyzers the Delta S and Delta X retain their ability to detect all signals not depending on what span is being viewed on the spectrum graph. While the operator inspects the suspicious signal, the analyzer continues to detect threats in the full frequency range.

The Delta S and Delta X automatically divide the spectrum into bands according to the local frequency allocation and thus inform the operator about the probable type of signal, whether it is a 4G, Wi-Fi, Bluetooth or another transmitter.

The great advantage of the Delta S and Delta X is their high sensitivity and immunity to interference. While near-field receivers and detectors lose their sensitivity either significantly, or fully, near strong transmitters such as cellular towers, communication antennas, broadcasting stations, Wi-Fi access points, and wireless phones etc. the Delta S and X retain their ability to detect RF bugs at a significant distance.

There is a class of eavesdropping devices that do not broadcast continuously, accumulating information and transmitting it on an external request or according to a schedule. To detect such threats, it is necessary to conduct long-term radio-monitoring with full registration of the RF environment and subsequent analysis. The Delta S and Delta X can monitor the RF environment 24/7 with full data logging to the SSD drive of the laptop or tablet.

The Delta S and Delta X mate with a laptop, or tablet, with the help of magnetic holders. They hold the computer reliably in all situations giving the operator the ability to move and tilt the system during sweeping.

General features

- Both easy to learn and a powerful sweeping system
- Quickly and reliably detects all types of RF surveillance devices in the range up to 6 GHz (12GHz), including analog, digital, working continuously and periodically, transmitting audio or video, with or without encryption
- Finds and identifies covert surveillance devices which use the digital standards GSM, 3G, 4G / LTE, 5G, Bluetooth, Wi-Fi, DECT and others in the range up to 6 (12) GHz
- Analyzes Wi-Fi 2.4 GHz, Wi-Fi 5 GHz, Bluetooth, "Bluetooth LE" and "Bluetooth LE Advertising" channels
- Detects RF signal jammers on all bands, including mobile uplinks and downlinks, bands of Global Navigation Satellite System (GPS, GLONASS, GALILEO, etc.), Wi-Fi/Bluetooth, etc.
- Spectral analysis provides high sensitivity and a long detection distance, exceeding the performance of typical RF detectors and near-field receivers by 10-20 times
- The background masking feature allows you to reject friendly signals such as television, radio, mobile base stations, etc., and focus on finding local signals that pose a danger

- Can monitor the RF environment 24 hours a day with full data logging (spectrum traces, alarms). Unlimited number of logs, each can contain an unlimited history of events
- Can be quickly adjusted to the local frequency allocation in the country of use (mobile and wireless bands)
- High-speed spectrum updating and wide real-time bandwidth (RTBW) provide the ability to register short-burst signals
- Search modes include: "All Signals", "Mobile/GPS trackers", "Wireless/ISM", "Downlinks/Navigation" and "Custom", as well as two additional modes for the inspection of suspicious bands or signals
- Several antenna inputs and built-in antenna switch provide maximum sensitivity over the entire frequency range
- "Threat Mark" feature shows dangerous signals on a spectrum graph
- "Burst Hunt" feature improves detection of such burst signals as Wi-Fi, Bluetooth, 5G, etc.
- The audio alarm warns the user about the presence of danger with a sound of variable intensity
- The attenuator simplifies location of powerful transmitters
- The "Hold maximum danger" feature automatically displays the most dangerous band or signal
- Demodulation of audio in AM/FM mode
- Works with, and is powered by, a laptop or tablet. Is reliably mated with the laptop or tablet and moved during the detecting and locating process. Has convenient magnetic system for attaching the laptop / tablet to the main unit.
- Side handles are used for carrying. All antennas are fixed to the main unit
- Carrying case is in the supplied set

Unique features of the Delta X

- Wide frequency range:
  ◦ Delta X G2/6:   9 kHz - 6 GHz
  ◦ Delta X G2/12:   9 kHz - 12 GHz
- Detects illegal information transmission in AC, telephone, Ethernet, alarm and other wires as well as in the infrared range with the help of the supplied Multifunction Probe
- Based on the dBm-calibrated spectrum analyzer providing the precise measurements
- Wider dynamic range thanks to the 14 bits bitrate of the spectrum analyzer's ADC
- Alarm indicator on the front panel
- Alarm relay output can activate external devices when a dangerous signal is detected
- The frequency distribution between the antennas can be changed by the operator

Unique features of the Delta S

- Frequency range 60 MHz – 6 GHz
- Affordable, light weighted and easy-to-use detecting system
- Fixed frequency distribution between the antenna inputs (INPUT 1: 60 – 2000 MHz, INPUT 2: 2000-6000 MHz)
- High sensitivity and fast scanning speed provides detection of all types of threats

Specification

	Delta S	Delta X
Frequency range	60 MHz - 6000 MHz	G2/6: 9 kHz - 6000 MHz G2/12: 9kHz – 12000 MHz
Sweeping speed - with Burst Hunt - w/o Burst Hunt	8 GHz per second 10 GHz per second	7 GHz per second 11 GHz per second
ADC resolution	12 bits	14 bits
Spectrum resolution	11 kHz / 21.9 kHz	9.8 kHz
Unit of measurement	dB	dBm
Sensitivity - standard gain - high gain	-85 dB -95 dB	-85 dBm - 95 dBm
Dynamic range	72 dB	84 dB
Attenuator	20 dB	10 dB
Displayed signal level - standard gain - high gain	-90...-20 dB -100...-20 dB (to 0dBm in auto)	-90...-20 dB -100...-20 dB (to 0dBm in auto)
Real-time bandwidth (RTBW)	24 / 27 MHz	27 MHz
Format	Handheld unit	Handheld unit
Platform	SDR by Analog Device	Spectrum Analyzer
Antenna inputs	INPUT 1: 60-2000 MHz INPUT 2: 2000-6000 MHz	INPUT: 9 kHz – 3000 MHz AUX1: 3000-6000 MHz AUX2: 6000-12000 MHz (G2/12 only)
Searching modes and time of update	• All signals (~0.8 s) • Mobile/GPS trackers (~0.2 s) • Wireless/ISM (~0.3 s) • "Downlinks/Navigation" (~0.3 s) • Inspect band/signal (~0.1-0.2 s)	• All signals (0.9-1.1 s) • Mobile/GPS trackers (~0.2 s) • Wireless/ISM (~0.3 s) • "Downlinks/Navigation" (~0.3 s) • Inspect band/signal (~0.1-0.2 s)
Visual elements (panels)	• Level • Spectrum + Waterfall • Alarms	
Demodulation	AM and FM with bandwidth 5, 15, 30, 100 and 200 kHz (in the range 70-6000 MHz)	AM, FM, CW, USB, LSB with bandwidth 2, 5, 15, 50, 100 and 200 kHz
Demands on laptop / tablet	Intel Core i3 / AMD Ryzen 3 or better (recommended Intel Core i5 / AMD Ryzen 5) 2 USB ports, one should be of SuperSpeed type (USB 3.0/3.1/3.2 or USB Type C) RAM 8 Gb or more	

	SSD 128 Gb or more Windows 10,11 or newer Screen size 12-14"	
Powered	by USB-port of laptop / tablet	
Battery resource	1-1.5 hour	
Duration of work from AC	Unlimited	
Displayed spectrum span	2 - 6000 MHz	2 – 12000 MHz
Peak trace modes	Off, fast, moderate, slow, forever	
Range of working temperature	-5°C...+45°C / 23°F … 113°F	
Dimensions of main unit (w/o antennas)	33.5 x 26 x 6 cm / 13.2 x 10.2 x 2.4"	
Dimensions of packaging	50 x 40 x 20 см / 19.7 x 15.8 x 7.9"	
Weight of main unit with antennas (w/o computer)	3 kg	3.5 kg
Weight in packaging	8.5 kg	10.5 kg

Functions and features

Search modes
- In the "All signals" mode the system analyzes the spectrum in the full frequency range and detects signals of all types. In addition to mobile and wireless signals, bugging surveillance devices are successfully detected on other frequencies, such as VHF / UHF radio microphones, 900/1200 MHz wireless cameras, and all other RF transmitters up to 6 GHz.
- In the "Mobile/GPS trackers" mode the system detects mobile devices of all standards, including GPS beacons (trackers) that are installed on vehicles and transmit coordinates via mobile networks. Quickly and reliably detects embedded devices (hidden cameras and microphones) that transmit information via mobile GSM, 3G, 4G / LTE and 5G networks (up to 6 GHz).
- In the "Wireless/ISM" mode the Delta S/Delta X quickly detects Wi-Fi, Bluetooth, ZigBee, DECT, LoRa and other radio frequency devices operating on the ISM bands, such as remote controls, smart home components, wireless sensors, etc.
- In the " Downlinks/Navigation " mode the system scans the downlink bands of mobile networks and bands of Global Navigation Satellite System. With the active "Detect RF jamming" feature the interferences and anomalies created by RF signal jammers will be detected and displayed on the bargraph. Additionally, a special warning sound will be produced.

Bands
- Information about the RF environment is displayed on the bargraphs, each responsible for a separate frequency band
- By default, the frequency range is divided into several basic bands, in addition to which a number of mobile and wireless bands are added according to the local frequency allocation
- The table of bands can be easily adjusted to the frequency allocation of the country of use
- It is possible to edit and add new bands, including 4G / LTE and 5G in case of change of frequency allocation

- Each band has an individual threshold which defines the sensitivity and detection distance
- For each band the following information is displayed: name, frequency, current dB level, peak dB level, maximum dB level, threshold, number of dangerous signals and frequency of the most dangerous signal. Additionally, the jammer level is shown when the "Detect RF jamming" feature is active
- The band's bargraph changes color to red when the threshold is exceeded
- The alarm history for each of the bands is stored in the log and displayed on the graph
- The user can inspect separate bands, view the list of signals in it and perform location of the transmitter

Signals
- Signals are automatically recognized in spectral traces, added to the signal list, and then automatically updated
- The list of signals is available in the band's inspection mode
- The frequency, band, channel, current, peak, and maximum recorded level are displayed for each signal
- The alarm history for each signal is stored in the log and can be displayed on the alarms graph
- The user can proceed to the inspection of a single signal

Masking of background
- The "Mask Background" procedure allows the operator to collect and mask external signals, such as TV signals, radio signals, mobile base stations, etc. and thus, focus on identifying only those transmitters that are located in the target area.
- Background signals are ignored with the help of spectral mask, which makes it impossible to hide a bugging device within the TV or radio channel
- This procedure is only required for the "All signals" searching mode
- Signals outside of the mobile and wireless bands are subject to masking only
- The duration of measurement can be selected
- Background masking can be performed at several points around the target zone
- Offset of spectral mask (sensitivity) is set by a threshold

Analysis of Wi-Fi and Bluetooth
- Level of each active Wi-Fi channel is displayed separately when the bands 2.4 GHz and 5 GHz are inspected. Each channel can be studied individually. Interferences of Bluetooth are rejected
- Levels of Bluetooth, Bluetooth LE and Bluetooth LE Advertising are displayed separately. Each type can be inspected separately. Interferences of Wi-Fi are rejected.
- A list of Wi-Fi access points and not paired BLE devices with their attributes and levels can be displayed in the Devices list and on the spectrum

Threshold and warning about alarm
- Each band has an individual threshold which can be defined by user
- The color of the bargraph changes to red when the threshold level is exceeded
- Signals which exceed the threshold are automatically recognized and stored in the log
- The "Audio alarm" feature warns the operator when the threshold is exceeded. The intensity of the alarm increases as the level rises, which facilitates locating the transmitter
- Full alarm history is stored for each band and signal during the search

- Alarm history of a signal or band can be displayed on the graph for any period

Detecting of RF signal jammers

- Delta S/Delta X can scan bands where the RF signal jammers may operate - mobile downlinks and bands of Global Navigation Satellite System (GNSS)
- The "Detect RF jamming" feature activates measurement of noise level on all active bands and a special audio alarm
- The feature can be active in all searching modes
- When the presence of an RF signal jammer is discovered, the operator can accomplish finding the source of interference by using the "noise level" bargraph and audio
- In addition to mobile downlinks and GNSS, all other bands can be scanned for the presence of jamming signals

Spectrum

- Traces "Live", "Peak" and "Threshold"
- Persistence mode
- Dangerous signals are marked on the spectrum (ThreatMarks feature)
- Waterfall function
- Convenient scrolling and zooming
- Compatibility with touch screens
- Able to zoom in on any part of the spectrum while continuing to search in the entire range
- Buttons for quick selection of the displayed span: "Full" – sets entire range; "Band" – displays the selected band; "Signal" – displays the selected signal.

Supplied set

#	Item	Delta S	Delta X
1.	Main unit Delta S or Delta X	1	1
2.	Carry case	1	1
3.	USB drive with software and user manual	1	1
4.	Omni-directed wideband antenna ODA-4	1	1
5.	Microwave antenna MWA-6	1	1
6.	Microwave antenna LPDA-12	1	1
7.	Magnetic sticker for laptop or tablet	4	4
8.	Adapter USB type C – USB type A	2	2
9.	Multifunction Probe with cables (high-voltage cable, low-voltage cable, 2m coaxial cable)	-	1
10.	In-line modular adapter	-	1
11.	Angle USB adapter	-	2
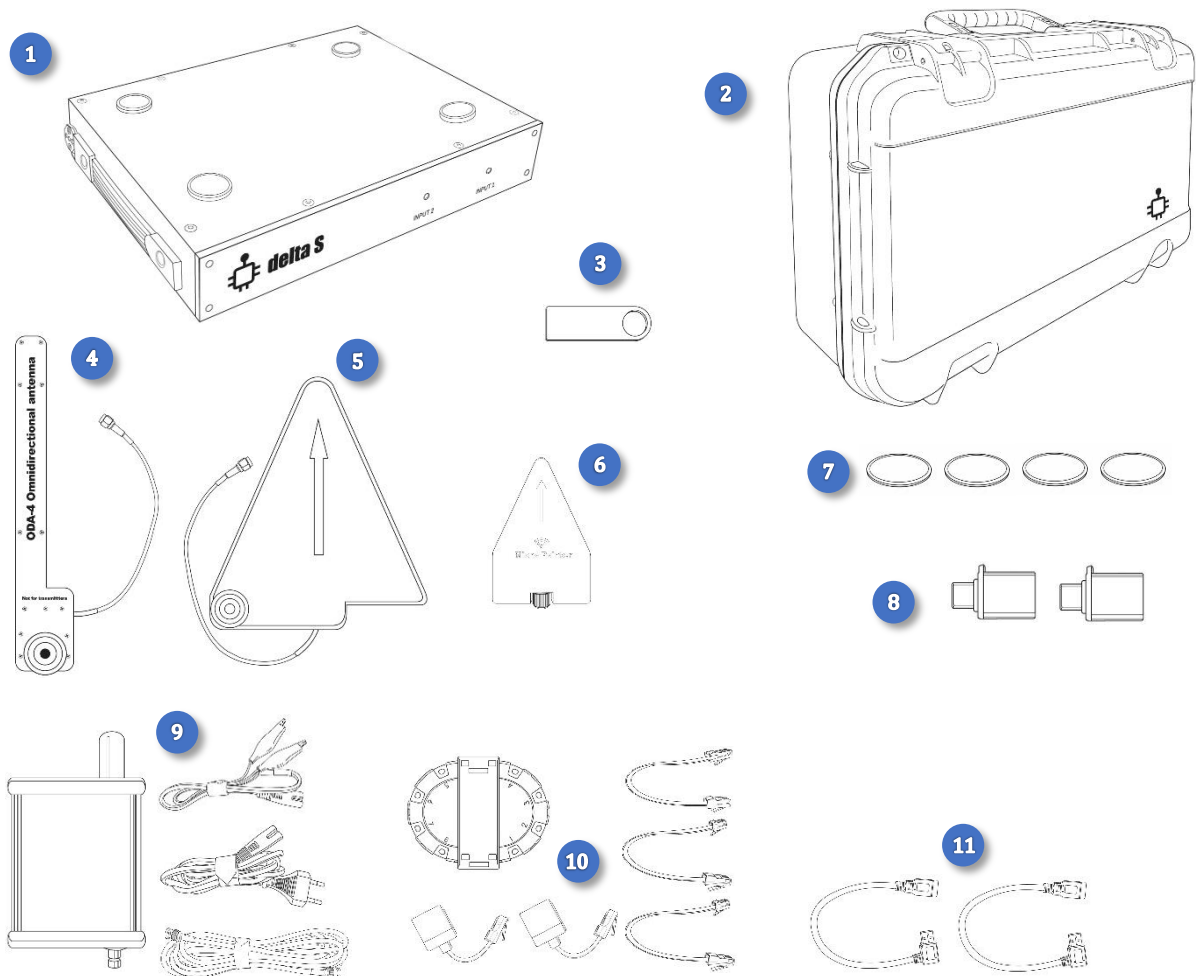
Preparation

Warnings

- Do not apply signals exceeding 0 dBm directly to the inputs of the device
- Avoid operation near strong transmitters such as transceivers or non-linear junction detectors; avoid directing the device's antennas to them.
- Do not direct antennas of powerful transmitters toward the device
- Do not use antennas with non-isolated parts to avoid the electrostatic discharge (ESD)
- Protect input connectors against ESD
- Do not turn on the device immediately after its storage or transporting in a cold environment

Installation

Make sure you are using a computer which corresponds to the specification. Since the system demands significant processing power and performs a high-speed transfer of data, a configuration with a weaker parameter may lead to incorrect work. If possible, deactivate the "USB Suspend" mode in the energy saving settings.

Setup the software from the supplied USB drive. Wait for installation of all components and re-start the computer. Use the start menu or find the shortcut on the desktop to start the software.

Attaching of a laptop or tablet

The Delta S/Delta X system is designed in the form of a portable unit which holds the laptop or tablet with the help of magnetic holders on its upper side. The counter magnetic stickers are included in the supplied set and must be stuck to the underside of the laptop or tablet before the system is used. Once the stickers are fixed on the bottom side, the laptop or tablet can be attached to or de-attached from the unit when necessary.

**Attaching of magnetic stickers:**
1. Clean the bottom side of the laptop/tablet with an anti-grease cleaning wipe
2. Temporarily screw the ODA-4 wide-band antenna to the holder on the right side of the main unit and position it vertically.

Put your laptop or tablet on the Delta S/Delta X unit, connect the power cable to it, connect the USB cables and adapters as described in section "USB connections" and find the best location for the laptop/tablet, keeping in mind the following suggestions:

- The laptop or tablet should not protrude beyond the edges of the main unit
- Protrusion of the USB cables can be minimized by shifting the laptop/tablet to the opposite side to the USB sockets
- Interference between the cables and antennas can be avoided by shifting the laptop/tablet back-or-forth
- If a tablet is being used make sure the magnetic holders do not interfere with the tablet's magnetic sensors of "closed cover". If the screen turns off, or a

sleep mode is entered suddenly when the tablet is on the holders, it is necessary to change the position of tablet.

- Areas on the laptop's bottom side which touch the magnets must be flat and without any legs or ventilation slots (the stickers will be fixed there). Change the position of laptop if necessary
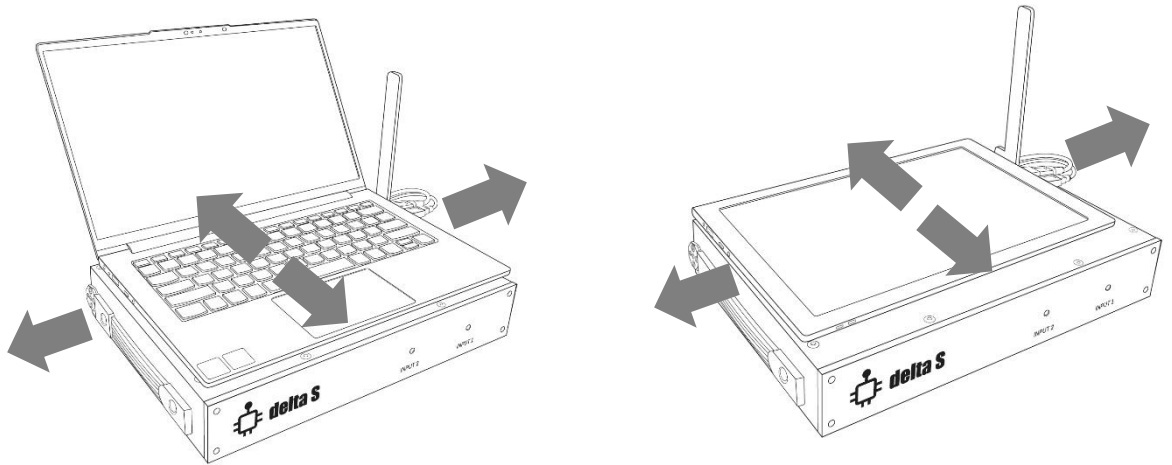
3. Remember the selected location and remove the laptop/tablet
4. Put 4 magnetic stickers on the holders with the adhesive side up and protective film removed. Align the centers
5. Keep the laptop/tablet above the main unit in the desired location, then lower and press it firmly to the stickers. Hold for a minute or two, then lift the laptop by raising its corners in turn. The stickers will be fixed to the bottom side of the laptop/tablet. Allow the glue layer to dry, and avoid multiple mating during the first 24 hours.
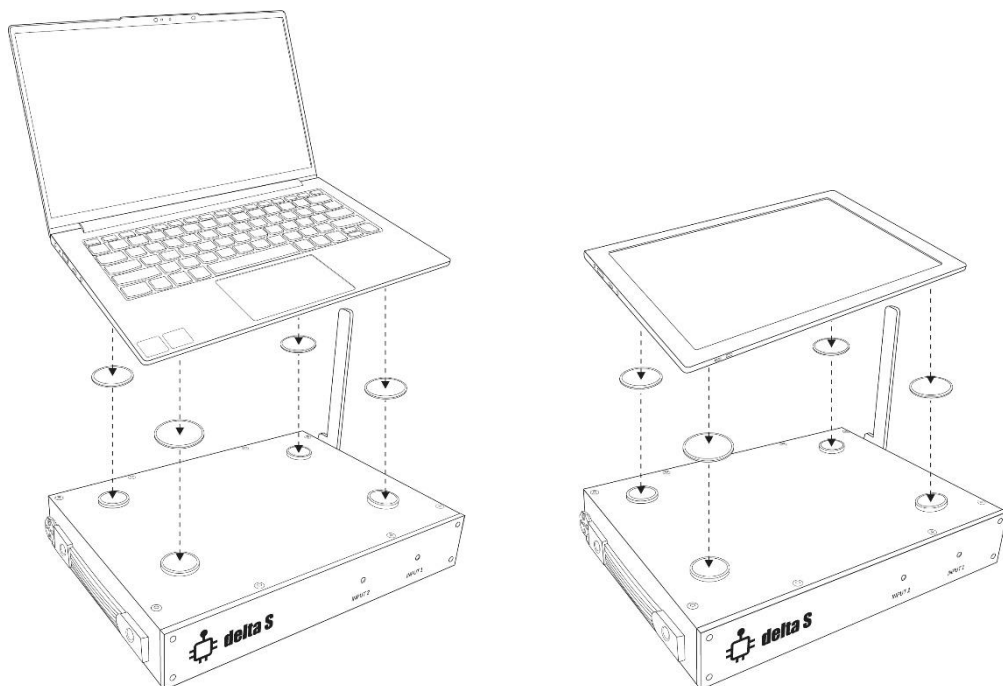
USB connections

The Delta S/Delta X system has 2 USB cables which should be connected to the USB slots of the laptop or tablet:
- The cable marked "SS" (SuperSpeed) is used for controlling and exchanging data with the receiver. It demands a superspeed port USB 3.0, 3.1 or 3.2 with the similar "SS" label. If such port is absent on your computer, use the Type C port and adapter from the supplied set.
- Another USB cable (without SS marking) can be connected to any USB port directly or via the USB Type C adapter
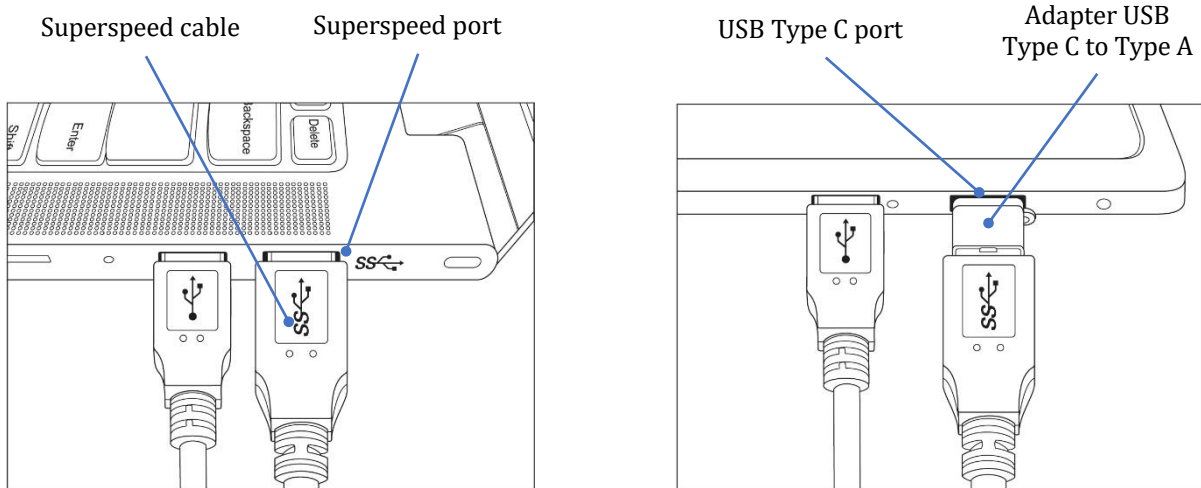
Selecting and connecting of antennas

The Delta S/Delta X is supplied with 3 antennas:

Antenna	Delta S	Delta X
ODA-4 – omni-directed wideband antenna	INPUT 1	INPUT
MWA-6 – directed microwave antenna 800 MHz- 6 GHz	INPUT 1	AUX1
LPDA-12 – directed microwave antenna 2-12 GHz	INPUT 2	AUX2

The ODA-4 antenna has a wide frequency range and circular sensitivity; therefore, is well suited for all searching modes, including "All signals".

Thanks to its high sensitivity the **MWA-6 antenna** provides longer detection distance on the upper part of the spectrum and is therefore well suited for scanning the mobile / wireless signals ("Mobile/GPS trackers", "Wireless/ISM" modes). In addition to the increased sensitivity, the MWA-6 antenna speeds up the locating process in the band/signal inspection mode thanks to the ability to point in the direction of the transmitter.

The LPDA-12 antenna is used for scanning the span of 6-12 GHz in the Delta X and the span of 2-6 GHz in the Delta S.

Delta S:
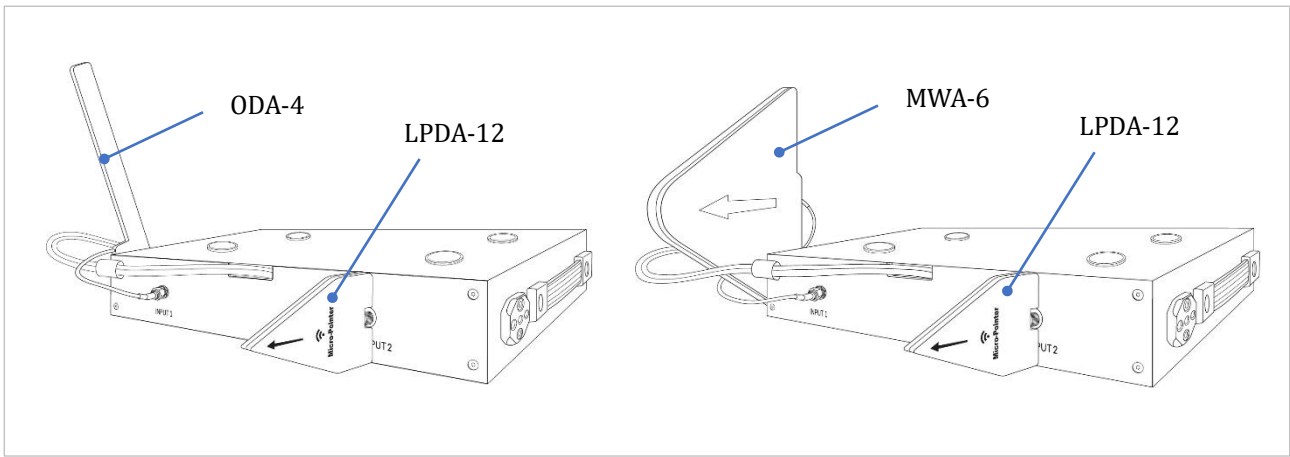
INPUT 1 (frequency range 60-2000 MHz)

Connect the ODA-4 antenna to the INPUT1 in all searching modes. When inspecting a truck or oversized cargo in the "Mobile/GPS trackers" mode an extended detection diagram is necessary. In this case use the MWA-6 antenna instead of the ODA-4. The ODA-4 or MWA-6 antenna should be fixed on the right side of the device.

INPUT 2 (frequency range 2000-6000 MHz)

Connect the LPDA-12 antenna directly to INPUT 2.

Delta X G2/6 and Delta X G2/12:
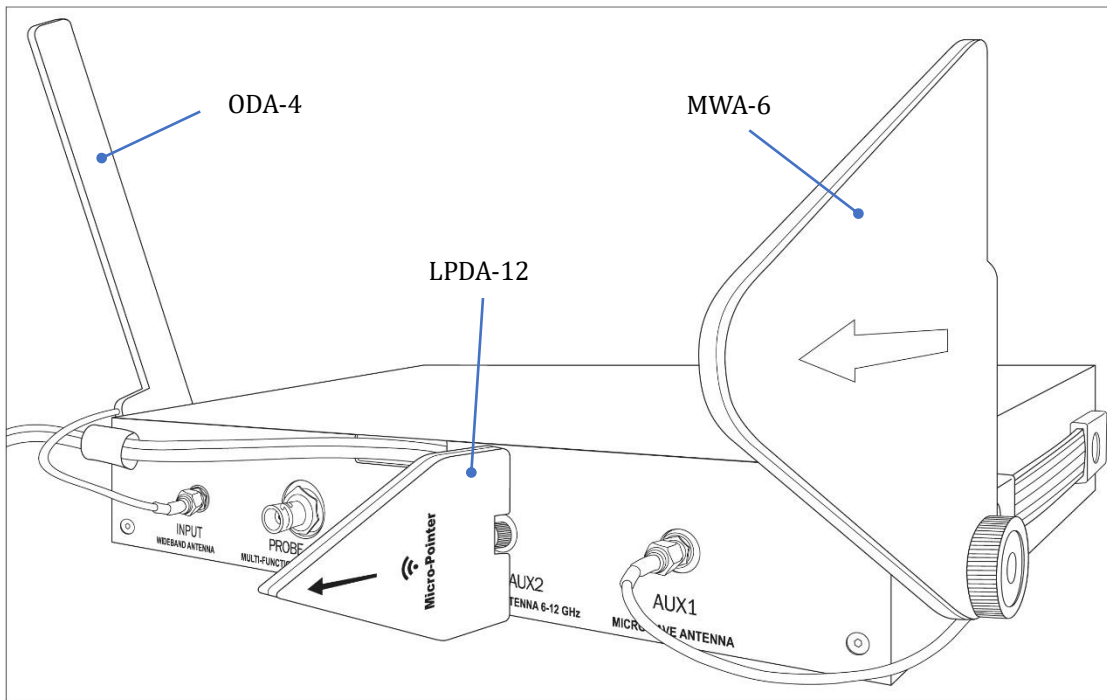
INPUT (frequency range 9 kHz - 3000 MHz*)

The ODA-4 wide-band antenna must be screwed vertically to the holder on the right side of the device with the help of the ¼" bolt from the supplied set. Connect the cable to the INPUT socket on the rear panel.

AUX1 (frequency range 3000 MHz*- 6000 MHz)

14

Screw the MWA-6 microwave antenna to the holder on the left side of the device with the help of the ¼" bolt from the supplied set. Position the antenna by its "back" and cable directed to the operator. Connect the cable to the AUX1 socket on the rear panel.

* 3000 MHz is a default value. The frequency distribution can be changed by the operator.

AUX2 (Delta X G2/12 only)
Screw the LPDA-12 antenna directly to the AUX2 socket on the rear panel of the unit

Starting the software

Start the "Breeze RF" software using the icon on the desktop or in the Start menu. As the main window opens the software will check the USB ports for the connection of the device. If both USB cables are connected, the program will recognize the device and begin its initialization, displaying a corresponding message in the status bar.

After initialization, all software's functions become available. When the device is not connected, some features of the application remain unavailable.

Problems with the device's recognition can occur because of the following reasons:
- The drivers are not installed
- The high-speed USB cable of the device is inserted into a slow, not high-speed USB slot of the computer or is poorly inserted
- The computer's battery is low
- The computer configuration, particularly the processing power and type of port, is insufficient.

The program recognizes the connection of the device during operation.

If you have started the software for the first time or have changed the country, it is necessary to adjust the bands table to the frequency allocation of the country of use. To do this, use the menu: Settings | Bands | Country. You can read more about this in section "Settings - Bands".

If you have started the software for the first time on the computer, it is necessary to cancel noise: menu "Settings – Device" – "Device" – "Cancel noise"

Elements of software and their use

Main menu

The menu button [icon] in the top left corner opens gives access to the functions and commands:
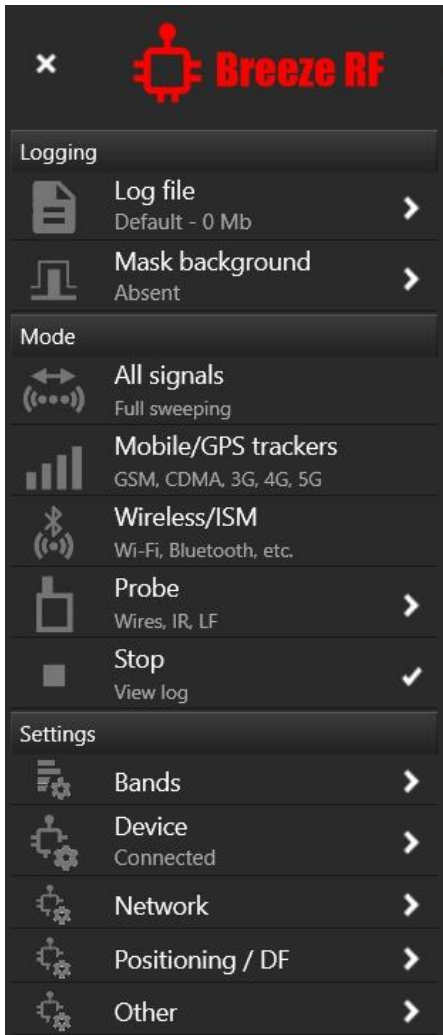
Logging – Log file. Operations with the log file.

Logging – Mask background. Masking the RF background and saving it in the current log file allows the system to avoid detection of safe background signals in the "All signals" and "Downlinks/Navigation" modes.

Mode. Selection of the working mode. Some modes can be activated simultaneously. Please read their description below.

Settings – Bands. Adjustment of the band's list – selection of the frequency allocation for the country of use, editing the bands, etc.

Settings – Device. Information about the device and its status.

Settings – Network, Positioning / DF. These functions are reserved for another type of hardware and not used with the Delta S or Delta X

Settings – Other. Other settings.

Close the menu to expand the window's area and increase the "Spectrum" and "Alarms" panels.

Logging of data

Logs store the following information: detected signals, spectrum traces, history of alarms and masked background. The stored spectrum traces can be reviewed on the Waterfall and the Spectrum graph, while the alarms are displayed on the Alarms graph.

We recommend that you keep a separate log for each search location and reopen it when you work there again.

Go to the "Log file" menu to work with the log.
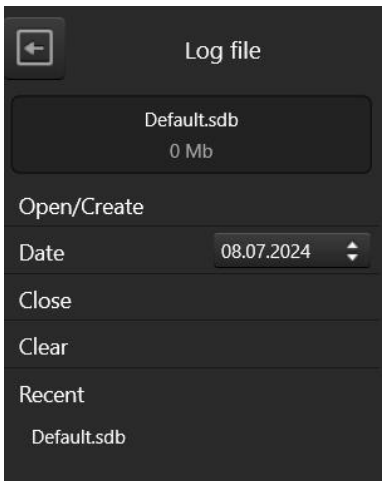
Open/Create

Opens the "Open/Create log file" window. If you want to create a new file, select the desired folder and enter a name for the new file. You will be prompted to create a new file.

Date

Allows to select a date for review in the Stop mode. The dates are created automatically when the logging function is active during the search.

Close

Closes the current log. Features of the software are limited when the log file is closed.

Clear

Fully removes all information from the current log.

Recent

Quick selection of a previous file.

Press the "Back" button to return to the main menu.

Masking background

Masking of the background is an important stage when searching for hidden bugging devices. It allows you to exclude safe background signals existing in the area, such as TV and radio broadcasting, radio communication, mobile base stations, repeaters, etc. Under normal circumstances a significant number of such "friendly" signals would be detected and distract the operator from finding real danger. Thanks to the masking, the Delta S/Delta X rejects the background and quickly finds only dangerous signals, i.e., those that exist in the target zone.

Masking of the background is required before using the "All signals" and "Downlinks/Navigation" modes only. It is not required before searching in the "Mobile/GPS trackers" and "Wireless/ISM" modes, as detection is performed by the threshold method in these bands.

The procedure of masking the background is quick and convenient. Before entering the target room, place the system where external signals will be well received, but not too close to the target room. This can be a window sill of a remote room or corridor, located at a distance of at least 10 meters from the target room. You can also stay outside the building, for example in a car.
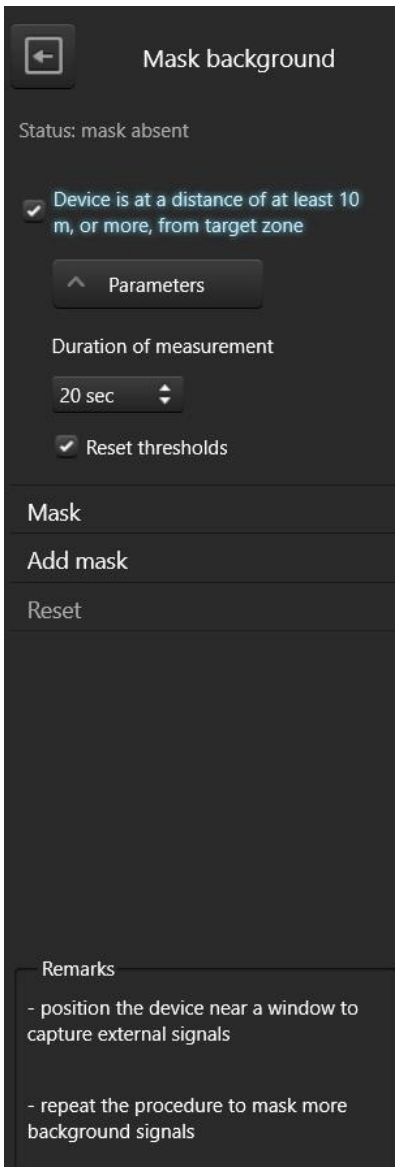
Enter the **"Mask background"** menu and confirm the correct placement by setting the checkbox "**Device is at a distance of least 10 m, or more, from target zone**". Then click "**Mask**" and wait for the result.

"**Add mask**" allows you to add a new measurement to the previous one and thus improve masking. You can repeat the masking at several locations by doing "Mask" in the first location and then **"Add Mask"** in several other locations.

After the procedure, the measurement results are saved in the current log file. Now you can place yourself in the target room and start searching in the "All signals" mode.

"Reset" allows you to erase the results of background masking.

The **"Parameters"** button opens some additional settings for advanced users:
- **"Duration of measurement"** - allows you to increase the measurement time in order to capture more non-constant signals and minimize false alarms
- **"Reset thresholds"** - sets the thresholds of mobile and wireless bands to the default values when masking the background

Searching modes

All signals

In this mode, the system searches for all types of RF bugging devices in the full frequency range:
- signals of all mobile standards (GSM, CDMA, 3G, 4G/LTE and 5G);
- wireless signals Wi-Fi, Bluetooth, LoRa, DECT, etc.;
- all other transmitters such as radio microphones, wireless video cameras, remote control systems, components of "smart home" systems, wireless sensors, etc. in the full frequency range.

All categories of bands are scanned - "Basic", "Mobile", "Wireless/ISM" and "Downlinks / Navigation".

Signals that exist within the mobile or wireless bands are displayed as mobile or wireless. Transmitters operating on frequencies outside the mobile and wireless bands are displayed in the "Basic" category.

Background masking must be performed before working in the "All Signals" mode. Results of masking are applied to the parts of spectrum which are outside of the mobile and wireless bands only.

The sensitivity and, accordingly, the detection distance can be regulated by thresholds. It is possible to set the threshold for each individual band, for a category of bands or for all bands at once. Thresholds of the basic bands in the presence of background masking work as offsets of masks.

For details, please refer to the "Search recommendations".

Mobile/GPS trackers

The use of mobile communication has several advantages for eavesdropping/covert surveillance:
1. Broadband channel allows you to transmit audio or video with high quality
2. No need in organizing a control post near the surveillance object. Data is transferred through the Internet. A cloud service can be used
3. Remote control of the surveillance device is possible
4. A convenient way for transmitting the position of the vehicle (GPS trackers)
5. The possibility of accumulating information with fast upload on schedule, or upon request
6. Typical signal of mobile communication attracts less attention during the search

The "Mobile/GPS trackers" mode allows you to search for all types of mobile devices including GSM, CDMA, 3G, 4G/LTE and 5G on frequencies up to 6 (12) GHz. In this mode only the "Mobile" category of bands is being scanned and displayed.

Reducing the measurement interval increases the speed and probability of detecting burst signals. Therefore, this mode is well suited and recommended for tasks related to the search of mobile signals. In addition to detection of trackers the mode can be used during sweeping in the building to maximize the probability of detecting specific types of bugging devices.

The sensitivity and, accordingly, the detection distance are set by thresholds. It is possible to set the threshold for each individual band or for the entire category "Mobile".

For details, please refer to the "Search recommendations".

Wireless/ISM

Like mobile communications, wireless standards can be used to transmit audio or video information. Their advantages are:
1. Ease of development and creation of a bugging surveillance device - the market is saturated with the necessary components
2. The bandwidth is sufficient to transmit audio or video with high quality
3. Remote control of the surveillance device is possible
4. The possibility of accumulating information with fast upload on schedule or upon request
5. A typical wireless signal attracts less attention during the search

In the "Wireless/ISM" mode, the system scans bands of only one category. Reducing the bandwidth leads to an increase in the probability of detection, which is important for detecting burst signals. Therefore, this mode can be used for finding Wi-Fi, Bluetooth, LoRa, DECT and other transmitters of this category as reliably and quickly as possible.

The sensitivity and, accordingly, the detection distance are set by thresholds. It is possible to set the threshold for each individual band or for the entire category "Wireless/ISM".

For details, please refer to the "Search recommendations".

Downlinks/Navigation

Cellular jammers create interference on downlink bands, i.e., on those parts of the spectrum where the data from a base station to a mobile device is sent. The so called "GPS jammers" create interference on frequencies of satellites in order to mask their signals and prevent navigation devices from receiving the information needed for calculating coordinates.

Therefore, to detect and find a jammer it is necessary to monitor downlink bands of mobile communication and bands of Global Navigation Satellite Systems, such as GPS, GLONASS and GALILEO.

The Breeze RF software is supplied with a data file containing frequency allocation for many countries, including the mobile downlinks and bands of Global Navigation Satellite System (GNSS). As standard the downlink and GNSS bands are not added to the band list when the user selects the country of use.

To add the downlink and GNSS bands mark the corresponding checkboxes in the "Settings – Bands | Country" and then press "Apply" to re-fill the list. When the downlink and GNSS bands are added to the list, the "Downlinks/Navigation" mode becomes visible and enabled.

Please read section "Detecting RF signal jammers and anomalies".

For details, please refer to the "Search recommendations".

Custom

The Breeze RF software allows the operator to create any number of own bands and to scan them selectively. In this mode only the "Custom" category of bands is being scanned and displayed. The mode is visible when there are "Custom" bands in the list.

Probe

This mode is available for the Delta X only. The Delta X can detect the following threats:

- Line carrier bugging devices on the AC, telephone and Ethernet wires
- Infrared transmitters
- Emissions from the planted electronics in the low-frequency range

For details, please refer to the "**Ошибка! Источник ссылки не найден.**".

Stop

In this mode the operator can work with the log file, change settings, mask background and review the results of search.

Settings- Bands
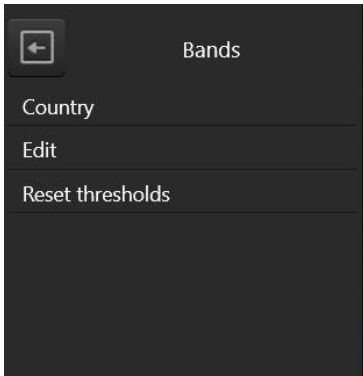
For the successful operation of the system, it is very important that the table of bands corresponds to the allocation of mobile and wireless bands that exist in the place of use. Fortunately, the "Breeze RF" software includes a data file that carries information about the frequency allocation in many countries and regions.

Country
Allows you to fill the table of bands with the frequency allocation of the place of use.

Edit
Allows you to enter the bands editing mode (is recommended for advanced users).

Reset thresholds
Allows you to reset the thresholds of all bands to the default level. This command is usually executed automatically when masking the background.

Selecting the country of use

Press the "Country" item in the Bands menu. A subpanel with a list of countries will appear at the top of the "Levels" panel.
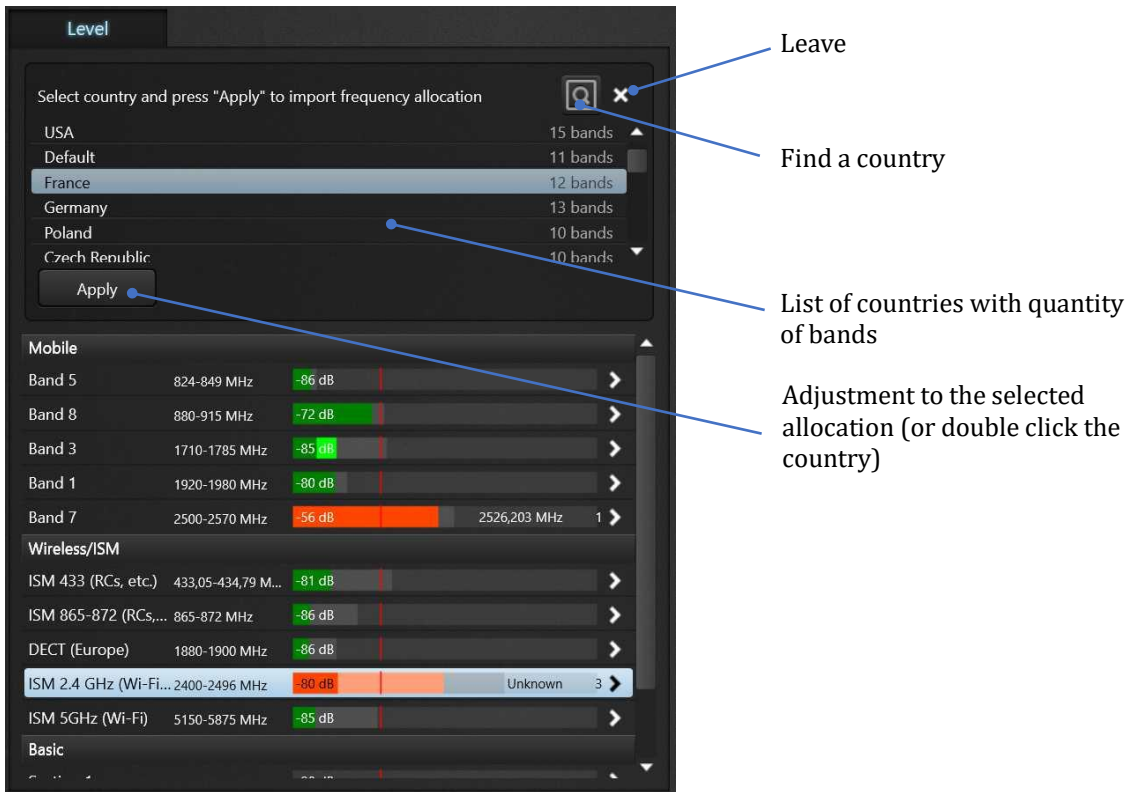
Select your country and press Apply (or double-click the country in the list). The table of bands will be filled in with the data. Perform this operation during the first starting of the software or after changing the country.

If your country is absent in the list, you can select the Default entry and, if necessary, edit the table of bands in the Edit mode. Use the internet resources to check the list of mobile bands allocated in your country and edit the list if necessary.

Editing bands

Press "Edit" in the Bands menu. The sub-panel at the top of the Levels will allow you to edit the bands.

Add a band

Or select already existing
band to edit
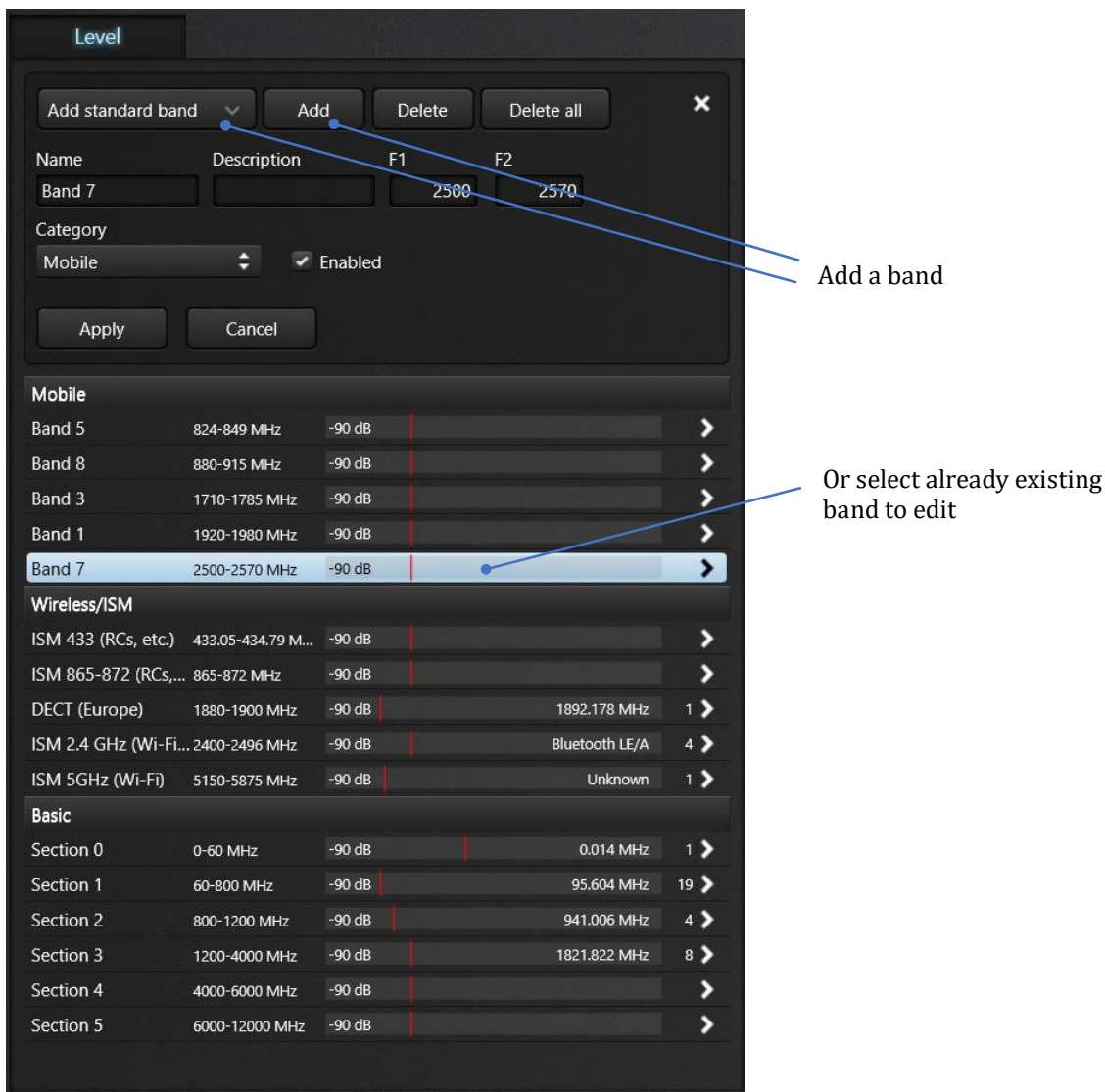
Add standard band
Opens the list of the standard mobile and wireless bands in a pop-up menu. Find the necessary
band and press "Add" to add it to the list or use the "close" button to cancel the action. Then
press Apply to store the band.

Add
Adds an empty band to the list. Enter the **Name**, **Description**, the frequencies **F1**, **F2** and press
"Apply". By default, the added band belongs to the "Custom" **category** but it can be changed by
the operator.

Delete
Deletes the currently selected band.

Delete All
Clears the list of the bands. All the bands will be removed except the basic bands.

When editing the bands make sure that mobile and wireless bands do not overlap (overlapping
with basic bands is normal).

Basic bands are built into the configuration and cannot be edited.

Settings – Device

Information about the device and its status is listed here:
- name of the connected device
- serial number
- firmware version
- temperature
- frequency range
- update time.

The **Update time** represent the duration of sweep in the current searching mode. In "All signals" searching mode the duration is the longest as the full range of the analyzer is being scanned. In other modes and during inspection of a separate band/signal the scanned span is narrower, so the Update time decreases.

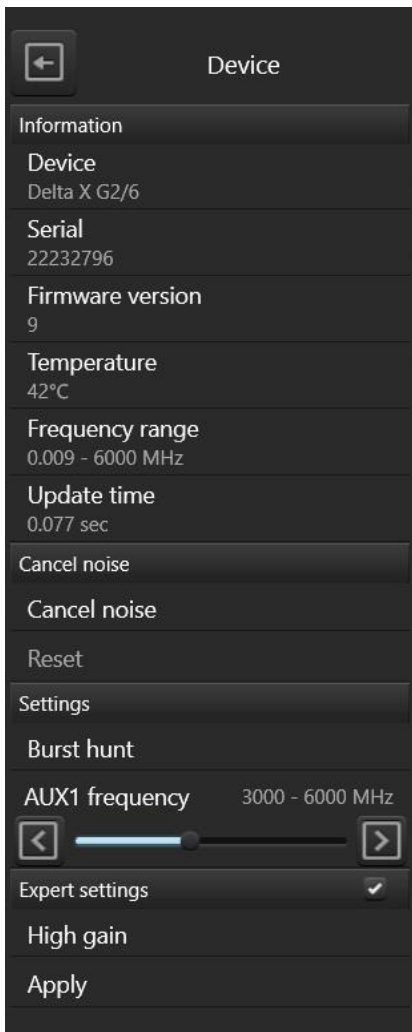**Cancel noise** allows the hardware to minimize own noises and compensate the changing dynamic range, thus making the spectrum traces smoother and more understandable. Cancel noise once on each computer the system is being used on.

Settings - Burst Hunt
When this feature is enabled the probability of detection of burst signals on the wireless and mobile bands increases. This option is applicable to the "All signals" mode only. The sweeping speed decreases slightly when it is activated.

Settings - AUX1 frequency (Delta X only)
Controls the frequency distribution for the MWA-6 antenna. In the Delta X, by default, the part of range below 3000 MHz is scanned by the ODA-4 antenna and above 3000 MHz – by the MWA-6 antenna. Lowering the AUX1 frequency may give the following advantages:
- increase sensitivity to the mobile and wireless signals
- speed up the process of locating the transmitter
- extend the detection diagram

Expert settings
These settings are hidden by default to avoid accidental changing.

Expert settings – High Gain (Delta X only)
Sets the higher sensitivity of the device. Suits very specific tasks and may lead to overloading. It is not recommended to activate this feature. The standard sensitivity of the Delta X suits well all the searching situations.

Expert settings – Apply
Applies the changes made in the Expert settings.

Settings – Other
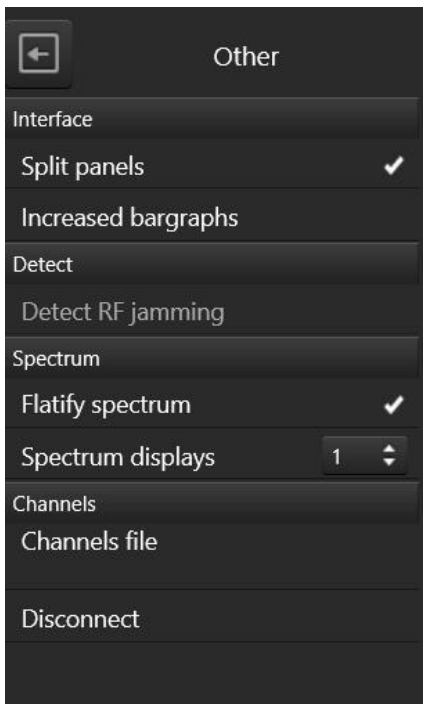
Interface - Split panels
Selection of how the main window is displayed. Splitting the window gives ability to see two panels at the same time. Without splitting, panels occupy a wide area and can show more detailed information.

Interface – Increased bargraphs
Allows you to increase the size of the bargraphs in the Level panel. Suits well for large high-DPI screens.

Detect - Detect RF jamming
This feature enables additional "Noise level" bargraphs and a special audio alarm sound. Please read section "Detecting RF signal jammers and anomalies".

Spectrum – Flatify spectrum
Additional processing of spectrum obtained from the receiver for a better representation (Delta S only).

Spectrum – Spectrum displays
Allows the operator to enable up to 3 spectrum displays in the Spectrum panel. Can be recommended for large high-DPI screens only.

Channels
This feature is not used with the Delta S or Delta X.

Toolbar

The toolbar at the top of main window contains a number of features.

Perform logging
This feature is active when the button is in the pressed state. The spectrum traces and the alarm events are recorded in the log file and subsequently displayed in the Waterfall and in the Alarms graph.

Without logging the waterfall is cleared each time the operator scrolls or zooms the spectrum graph. Then the waterfall starts to accumulate the spectrum traces again and does so until the next change of the span.

When the spectrum is scrolled or zoomed with the logging feature active the Waterfall will be automatically filled in with the spectrum data obtained earlier.

Similarly, the Alarms graph will read and display the alarm events after each scrolling or zooming if the logging is active.

Audio alarm

Sound warning for the operator about the presence of a threat (exceeding the threshold). The intensity of the clicking sound grows as the danger level increases.

Hold max danger

When this feature is active the Delta S / Delta X automatically tunes in the most dangerous band or signal and shows its spectrum. The function is convenient when inspecting large areas as it instantly draws the operator's attention to a new event. Among the dangerous bands or signals the system selects the one with the highest 'above-threshold' level. Turn this function off when you want to stop at some particular band or signal, for example when adjusting the threshold.

Attenuator

Use this function to reduce the sensitivity when locating a strong signal. If the signal level reaches -25...-20 dB and the spectrum distortion appears on the adjacent frequencies, temporarily use an attenuator.

The function is only available during inspecting a band or signal and is automatically disabled when exiting the mode.

Demodulation

Allows you to listen to analog signals such as FM radio stations or analog TV audio channels. Digital signals such as mobile or Wi-Fi cannot be heard, although they may have some characteristic sound such as buzzing or crackling. BW is the demodulator bandwidth, selectable from 5 to 200 kHz. Set the cursor to the desired frequency in the spectrum with the mouse or with your finger when on a touch screen.

The function is only available during inspecting a band or signal and is automatically disabled when exiting the mode.

On-screen keyboard (right side)

Is used on touch screens for automatic opening of the on-screen keyboard when a control requiring text input is focused. Set this button to a pressed state on tablets before entering or editing text, for example, naming a band.

Theme (right side)

Selects dark or light interface mode. Dark mode is safer for the eyes and is set by default.

Language (right side)

Choose the desired language.

Panel "Level"

One of the important advantages of the Breeze RF software is the automatic processing of spectral data coming from the Delta S / Delta X devices. These are recognition of signals, their storage in the log and measurement of level of bands and signals.

The results of spectrum processing are displayed in the Level panel as an easy-to-understand list of bands with level bargraphs. The list allows the operator, without delving into the manual study of the spectrum, to monitor the entire picture as a whole and quickly move to dangerous areas. The bargraph level increases when a new signal appears within the band or the device is moved closer to the transmitter. When the threshold is exceeded, the color of the bargraph changes from green to red.

Category — Level — Threshold — Band — Inspect band — Threshold — Frequency of the strongest signal — Number of dangerous signals in the band — Level of band

Mobile
Band 5	824-849 MHz	-85 dB		›
Band 8	880-915 MHz	-86 dB		›
Band 3	1710-1785 MHz	-86 dB		›
Band 1	1920-1980 MHz	-86 dB		›
Band 7	2500-2570 MHz	-80 dB		›

Wireless/ISM
ISM 433 (RCs, etc.)	433,05-434,79 M...	-86 dB		›
ISM 865-872 (RCs,...	865-872 MHz	-87 dB		›
DECT (Europe)	1880-1900 MHz	-86 dB	1881,806 MHz	2 ›
ISM 2.4 GHz (Wi-Fi...	2400-2496 MHz	-54 dB	Wi-Fi 6	2 ›
ISM 5GHz (Wi-Fi)	5150-5875 MHz	-85 dB		›

Basic
Section 1	57-1000 MHz	-78 dB		›
Section 2	1000-4000 MHz	-81 dB		›
Section 3	4000-6000 MHz	-86 dB		›

The operator can inspect the dangerous band by pressing the **Band** button or the arrow near the band. When the Level panel is in the band inspection mode, it displays the level of the selected band and a list of signals in the band. A bargraph is displayed for each of the signals. It changes color when the threshold is exceeded. The user can select a dangerous signal and proceed to its inspection.

Multi-band measurement ⟷ Inspect band — List of signals is displayed ⟷ Inspect signal
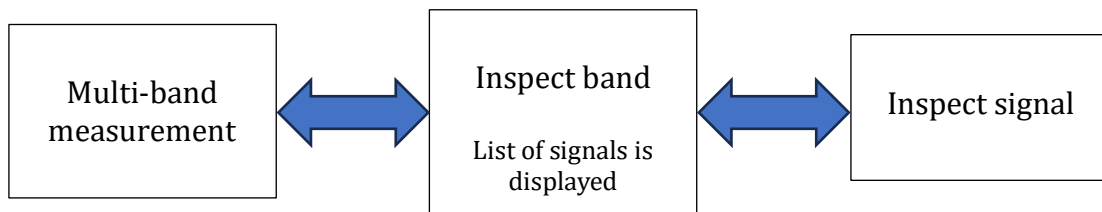
In this way, the user sees the whole picture at once and can easily switch to individual bands or signals that pose a danger. When switching to a band or signal, the spectrum graph is automatically adjusted to display the corresponding span.

The mobile and wireless bands stand above the basic bands. When the level of the basic band is measured, the spans of mobile and wireless bands are not taken into account. Thus, they do not affect the bargraphs of the basic bands and are only displayed in their own categories "Mobile" and "Wireless/ISM". So, the bargraphs of the basic bands only show signals outside the cellular and wireless bands.

Three kinds of level are displayed for the bands and signals:
- Current (instantaneous rise and instant fall) – bright green or bright red

- Peak (rises instantly, falls slowly) – light green or light red
- Maximum registered (remembers the maximum level) - gray

The band's threshold can be adjusted within -85...-20 dB or -95...-20 depending on the selected gain.

Multi-band measurement
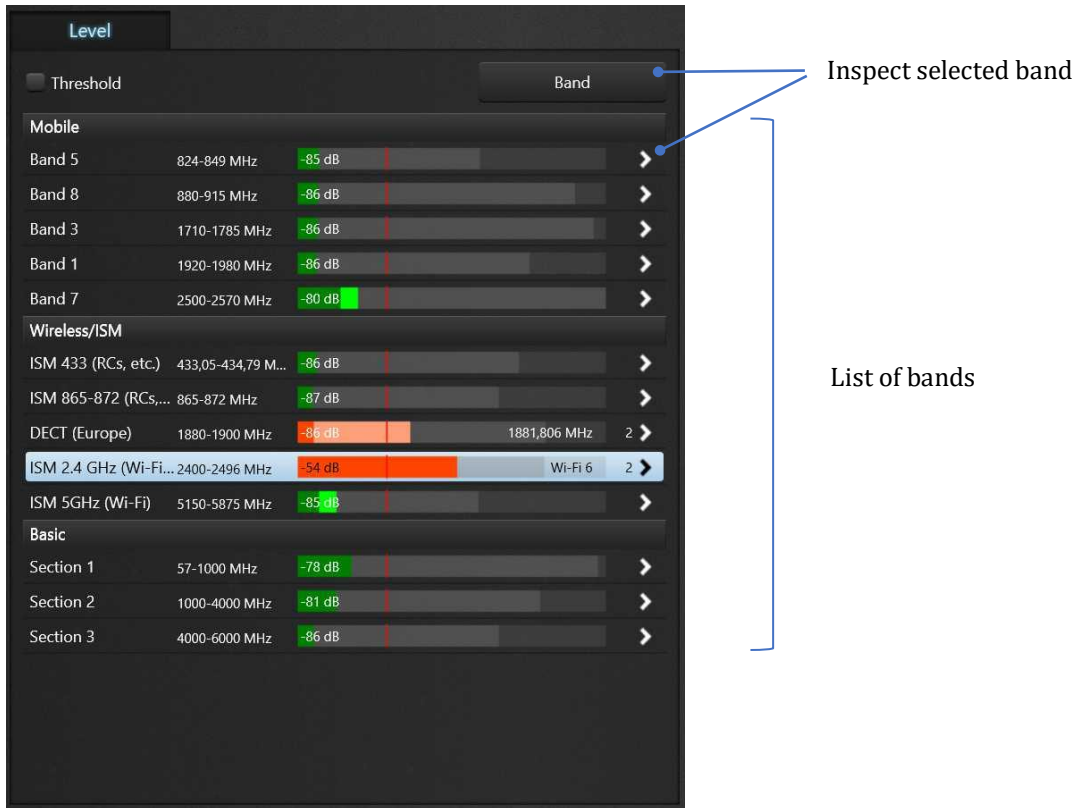
All bands according to the selected mode are scanned and displayed on the panel. The name, description, frequency, level (current, peak, and maximum recorded), as well as the number of dangerous signals and the most dangerous signal are displayed for each band. Bands are grouped by category.

Double-clicking on a band adjusts the spectrum graph to show the band's span.

Mark the "**Threshold**" checkbox to adjust the threshold. The threshold can be set for one band, a category of bands, or all bands at once.

Inspection of band

Select the band you are interested in and **click on the arrow** next to it or press the "**Band**" button. You will enter the band's inspection mode. The "Level" panel will have the following look:

Inspect signal

List of signals in the inspected band
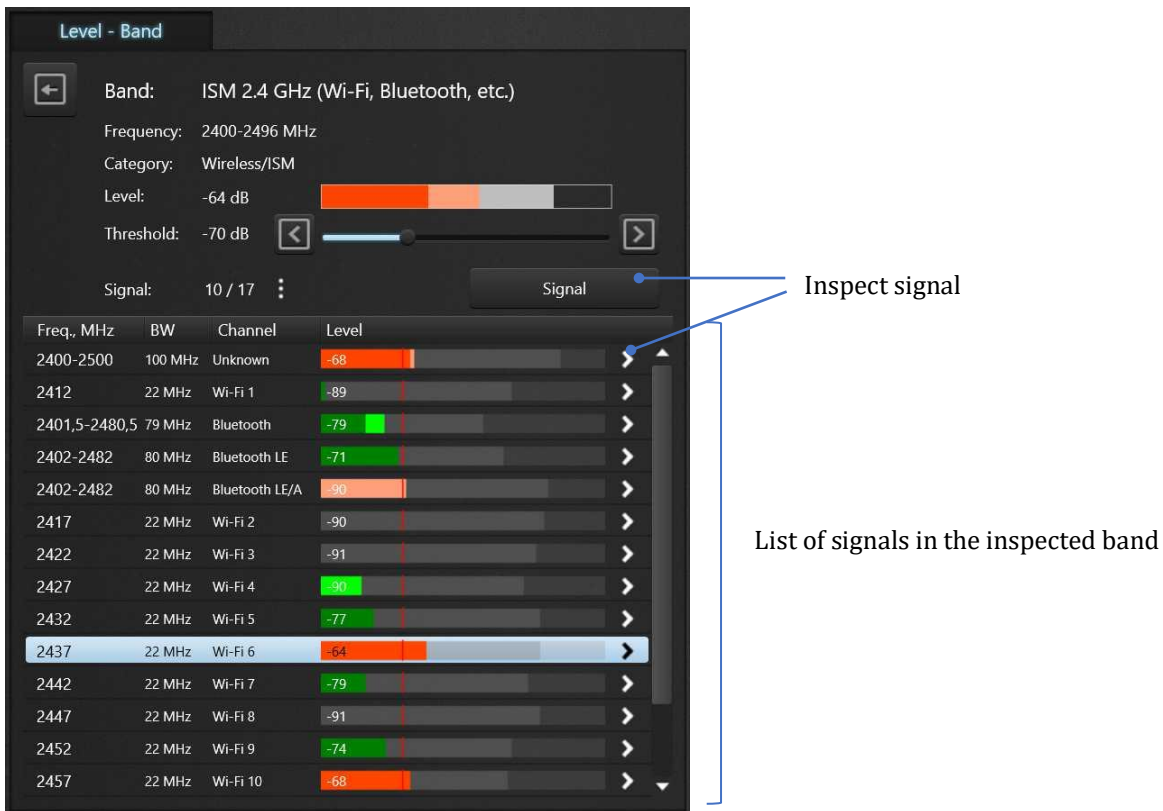
In this mode, only the selected band is scanned, its parameters and the list of signals within the band are displayed. For each of the signals, the frequency, band, channel name, current, peak, and maximum registered level are displayed.

Use this mode to see exactly which signals within the band pose a threat and to select one for a subsequent inspection. You can stay in this mode if you want to locate several signals at once or if the signal changes frequency frequently. Compared to the standard multi-band mode, a smaller part of the spectrum is measured in the band inspection mode, which increases the probability of detecting short-burst signals.

A **single click on a signal** will rewind the spectrum graph to it.
Double-clicking on a signal adjusts the spectrum graph's span and rewinds to it.

Adjust the band's threshold if necessary.

The number of the currently selected signal, total quantity of signals, as well as a button to open an additional menu, is displayed above the list of signals. The following commands are available in this menu:
- **"Delete signal"**
- **"Delete all signals within band"**
- **"Delete all signals"**

Deleting a signal or all signals may be necessary to reset the signal fusion resulting from the operation of the signal recognition algorithm. After removing from the list, all active signals will be automatically recognized and re-added. Be careful not to lose the measurement results of a suspicious signal.

Press the "**Back**" button to exit the mode.

29

Inspection of signal

Select the signal you are interested in and **click on the arrow next to it** or click the **"Signal"** button to enter the signal inspection mode. The "Level" panel will have the following look:
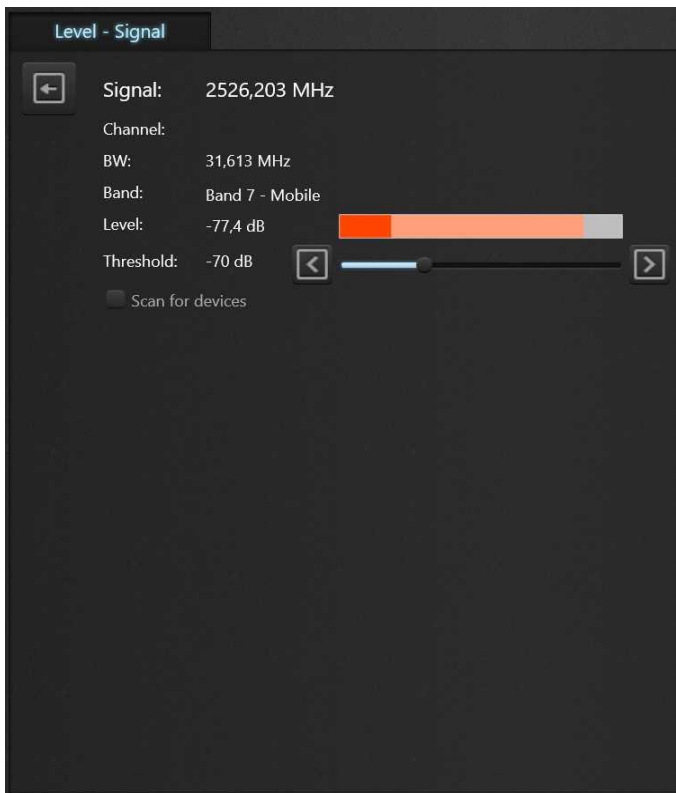
In this mode a separate signal is scanned. Use the signal inspection mode to study and locate the transmitter if it has a fixed frequency.

In this mode, the measured spectral span is minimal and the probability of registering a short-burst signal is maximal. The signal inspection mode is well suited for studying and locating short-burst pulse signals, such as channels of Wi-Fi, 4G/LTE, 5G, etc.

Adjust the band's threshold if necessary.

Press the **"Back"** button to exit the mode.

Inspection of Wi-Fi and Bluetooth

The Breeze RF and the Level panel work differently when the inspecting the "ISM 2.4 GHz (Wi-Fi)" or "ISM 5 GHz (Wi-Fi)" band.

The Wi-Fi channels, Bluetooth, Bluetooth LE and Bluetooth LE Advertising are added to the list of signals when they exceed the threshold. Decrease the band's threshold to automatically add channels with a lower level.

Each active Wi-Fi channel is displayed in the signal list as a separate signal.

The channels of the protocols which use the frequency hopping are measured together and displayed in the signal list as one signal:

- All channels of Bluetooth classic (0…78) are displayed as "Bluetooth"
- All channels of Bluetooth LE (0…36) as "Bluetooth LE"
- The advertising channels of Bluetooth LE (37, 38, 39) as "Bluetooth LE/A"

The corresponding channel marks for the selected protocol are displayed on the spectrum graph.

Each entry of the signal list can be inspected in the signal inspection mode.
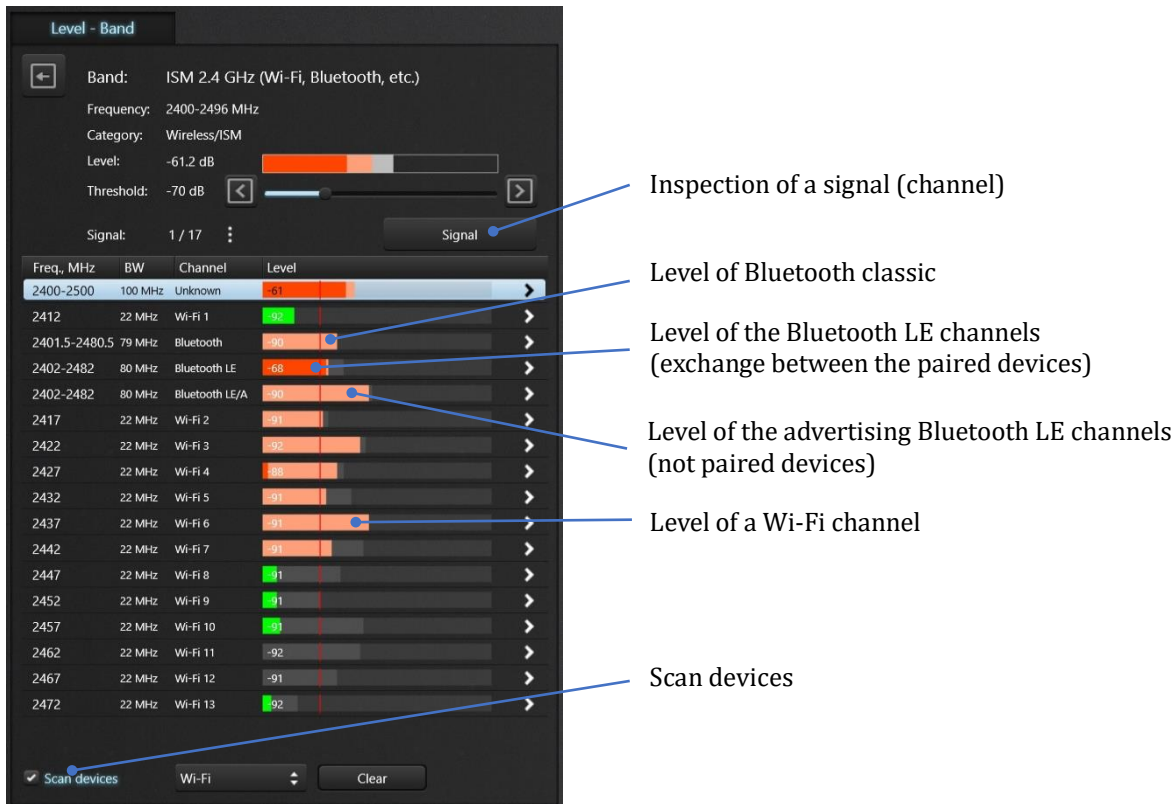
The Wi-Fi access points and not paired BLE devices can be scanned with the help of the computer's hardware and can be displayed on the spectrum graph and in the list.

The **"Scan devices"** enables the scanning of Wi-Fi access points or Bluetooth LE. The combo box right to it allows the operator to select the type of the scanned protocol. It is recommended to select the signal in the list corresponding the scanned protocol, so the spectrum graph displays the corresponding "channels" marks.

Each time the scanning is finished the devices are displayed on the spectrogram in the form of round blue icons with a caption corresponding to their SSID or MAC address. The vertical position of the icons will correspond to the device's signal level which was measured by the network card.

Icons of Wi-Fi devices
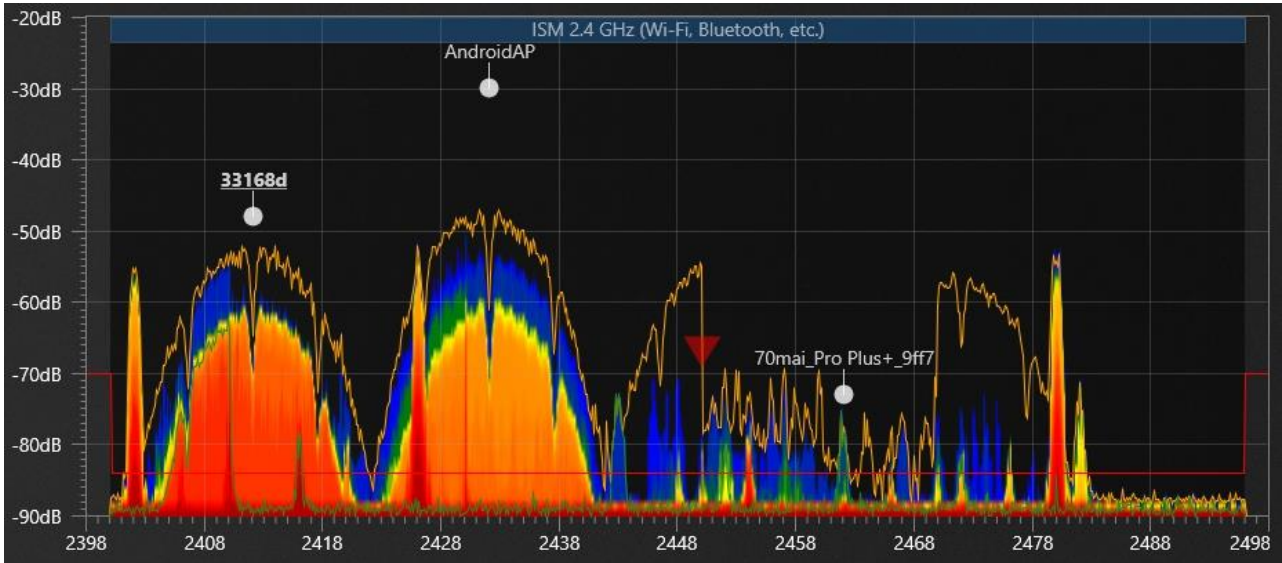
Icons of BLE devices
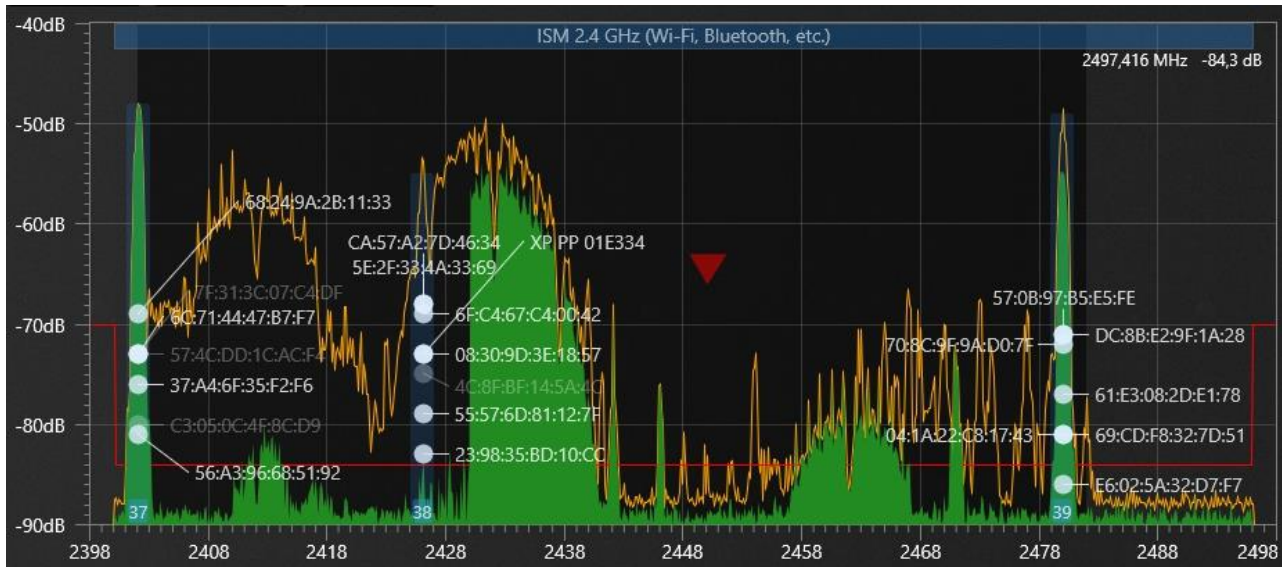
The device's level will change when the system is moved. Comparing the change in the spectral level with the change in the position of the blue icon can provide additional information about the signal. Simultaneous increase of both values will indicate that you are approaching the access point. If only the spectral level increases, and the level of the blue icon decreases or remains unchanged, you might be approaching a device that is a client of a distant access point.

The level measured by the network card (vertical position of the blue icon) may not correspond to the spectral level of the Delta S/Delta X, as the measurement is made by a separate device. Observe the relative position of both levels.

When scanning for the Wi-Fi access points the network card of the laptop or tablet sends the "probing" requests on all the channels of the band. In order to avoid the interference, the measurement of the spectrum in the Breeze RF is suspended for these short periods. Therefore, to avoid delays, it is possible to activate scanning of the Wi-Fi devices for a limited period of time.

The "**Clear**" button allows to clear the list of devices and remove them from the spectrum graph.

> *To enable scanning for devices the Wi-Fi and Bluetooth functions should be activated in the computer*

After capturing the active signals in the band inspection mode, you can proceed to inspection of separate signals. Press the 'arrow' button near the signal or the **Signal** button to inspect it.

In the signal inspection mode, the Level bargraph of the Level panel will display the strength of the currently selected channel, while the audio alarm will produce the sound according to this strength. In this way, the process of locating of the signal or channel is made easier.

If the "Scan devices" feature has been activated during the band inspection, the Level panel in the signal inspection mode will display the list of the devices. It will list the devices according to the type of the inspected signal.

Inspected signal is a Wi-Fi channel — Level of the channel — Blue round icons show the Wi-Fi devices

List of devices (access points)
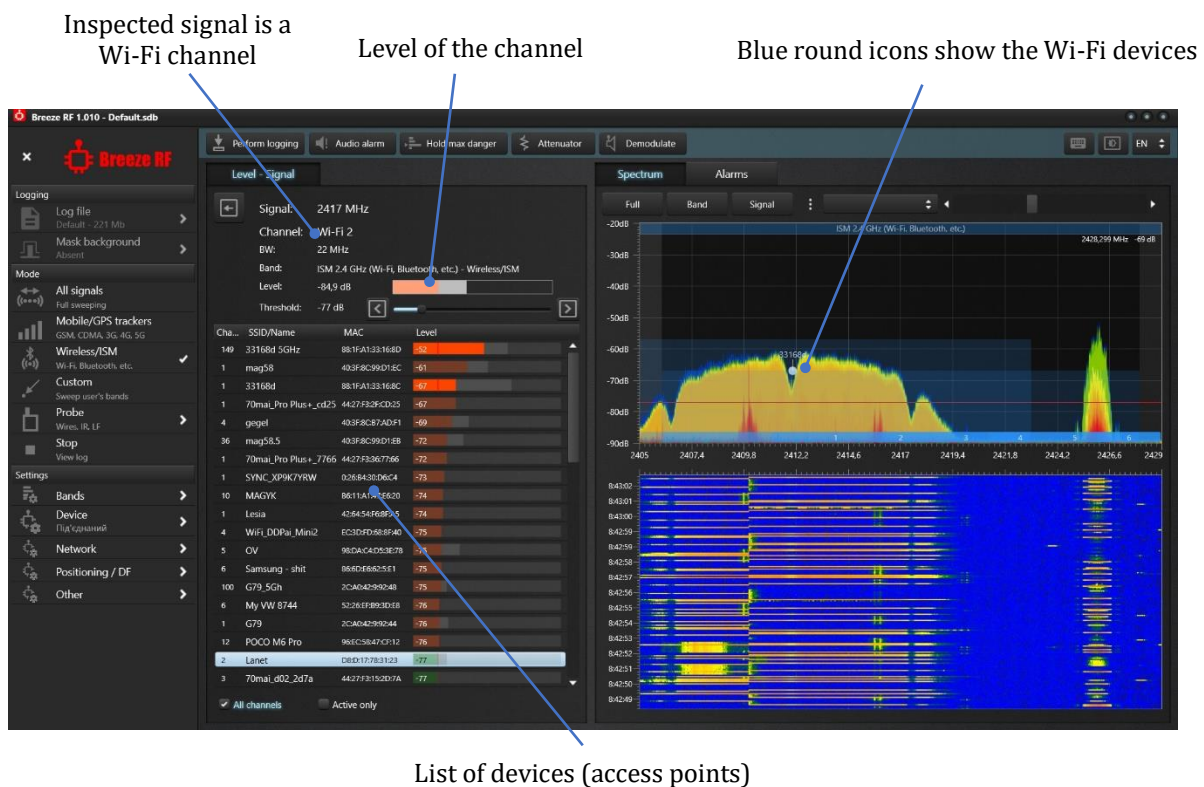
"All channels" shows all found access points, without selection by the inspected W-Fi channel.

"Active only" hides non-active devices.

After exiting the signal inspection mode using the "Back" button, the user can inspect another signal.

Adjustment of thresholds

The bands' thresholds determine the sensitivity of detection. When the signal's level exceeds the threshold, an alarm event occurs. At this moment, the bargraph turns red, an audible alarm is generated, and the event is recorded in the log.

The lower the threshold, the weaker signals are detected by the system. With a lower threshold, the detection distance increases, and with a higher threshold the distance drops.

The Delta S system allows the operator to set an individual threshold for each band and thus adjust the detection distance for each type of signals. The allowed values are from -85 dB to -20 dB (-95...-20 dB)

To adjust the threshold:
- When the Level panel is in multi-band measurement, mark the Threshold checkbox in the upper left corner
- Select the desired band
- Change the threshold using the trackbar or arrow buttons
- Select another band and repeat the settings
- You can change the threshold for the entire category or for all bands at once if you select the appropriate scope of setting
- When the system is in the band's or signal's inspection mode, the threshold controls are always available at the top of the panel

You have the option to reset the thresholds of all bands to their default values using the "Reset thresholds" command from the "Settings | Bands" menu. When developing the system, the optimal threshold values were selected as default. They provide normal sensitivity and minimize false alarms from distant transmitters: -75 dB for the basic bands and -70 dB for all other bands.

Recommendations:
- Avoid setting a too low threshold near -85..-80 dB. This may produce an excessive number of alarms from distant transmitters from outside of the area. It is recommended to set a higher threshold in order to limit the detection distance by several meters and minimize false responses. An exception may be made to the "3G 1920-1980 MHz" band often containing signals with a relatively low level. Its threshold can be set to -82..-75 dB
- Do not set a too high threshold at -40...-20 dB. This can cause loss of sensitivity and inability to detect signals

The correspondence of threshold and detection distance can be established experimentally. For this, you can use a mobile phone or a "known" Wi-Fi access point. By gradually changing the distance to the device that is active at the time of the test, you can determine how the signal level changes and determine the threshold required for the distance which you wish to achieve. Make sure the test device is active during testing. A reliable way to keep your mobile phone active is on-hook call mode (voice channel) or a call via a messenger such as WhatsApp (data transfer). When the phone's Wi-Fi is turned on and there is a connection to the access point, the data will go through the Wi-Fi. When Wi-Fi is turned off, data will go through the mobile Internet.

Approximate correspondence between the threshold and detection distance of an average mobile signal or Wi-Fi signal:

Signal level (level of threshold)	Distance
-80 dBm	5-20 meters
-70 dBm	4-10 meters
-60 dBm	3-8 meters
-50 dBm	2-5 meters
-40 dBm	1-3 meters
-30 dBm	<2 meters

Thresholds of the basic bands

Thresholds of the basic bands in the presence of background masking work as the offset for the mask. Increasing the threshold will shift the mask up and accordingly decrease the sensitivity. Decreasing the threshold will increase the sensitivity accordingly.

Panel "Spectrum"

The Spectrum panel displays a spectrum graph and a Waterfall graph. With the help of these graphs, the operator can study the signal and get information about its level, frequency of existence, bandwidth, duration of operation, etc.
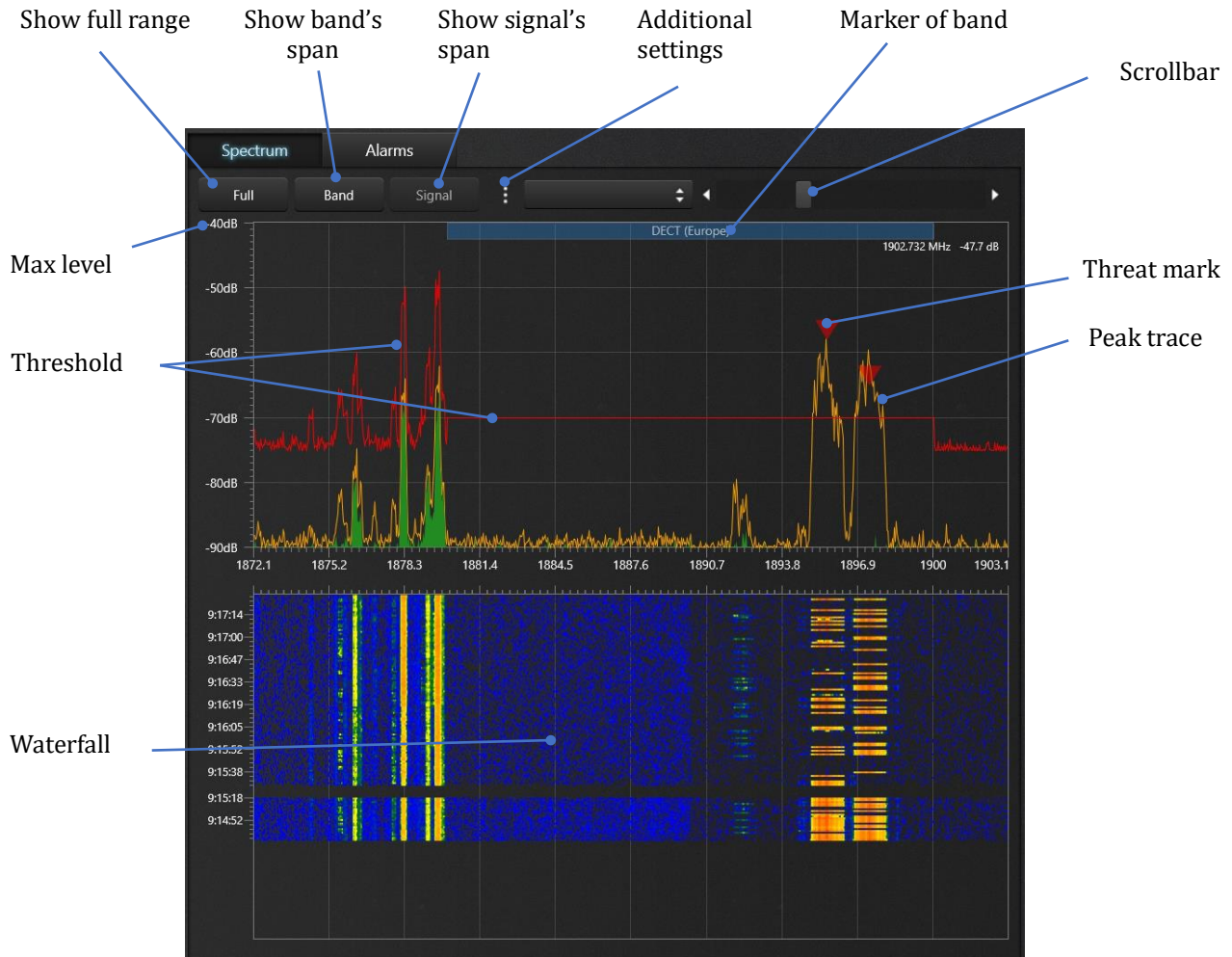
On the spectrum graph, the user can view any area, for example, the entire frequency range covered by the device, a band or a separate signal.

Signal levels from -90 to -20 dBm or -100...-20 dBm are displayed depending on the selected gain. The spectrum graph can automatically adjust its vertical scale to the maximum level being displayed. In this mode levels up to 0 dBm can be displayed. The unit of measurement depends on the version of the used system and is "dBm" for the Delta X and "dB" for the Delta S.

"Full" sets the graph to display the entire frequency range of the system.
"Band" scrolls to and sets the graph to display the span of the currently selected band.
"Signal" scrolls to and displays the span of the currently selected signal (available only in the band/signal inspection mode).

The **current (instant) spectrum trace** is drawn by green on the graph. The **threshold** is drawn in red.

The spectrum graph supports **scrolling**. In addition to the scroll bar, it is possible to press the left mouse button above the graph and drag it to the left or right without releasing the button. The graph will be scrolled to the desired section. The same can be done on touch screen devices - touch the spectrum graph with your finger or stylus and drag it left or right.

The spectrum graph supports convenient **zooming in and out**. To zoom in/out, click on the spectrum with the mouse (or finger) and press the "increase" or "decrease" button. You can **zoom to selection** if you select the desired span in advance.

To make a selection press and hold the mouse's right button over the start frequency and move the mouse to the finish frequency, then release the button. The selection of a signal is made automatically when you double-click it in the Level panel.

The **waterfall** displays the spectrum over a period of time. Each horizontal line in it represents one trace of spectrum measurement. The level is displayed by color, where blue is a low level, green is slightly higher, yellow is a medium level, and red is a high signal level. During the measurement, older traces float down, and newer traces are placed at the top. Timestamps are displayed on the left. The operator can use the waterfall to see non-constant signals and track their frequency.

The additional settings button opens the popup menu:
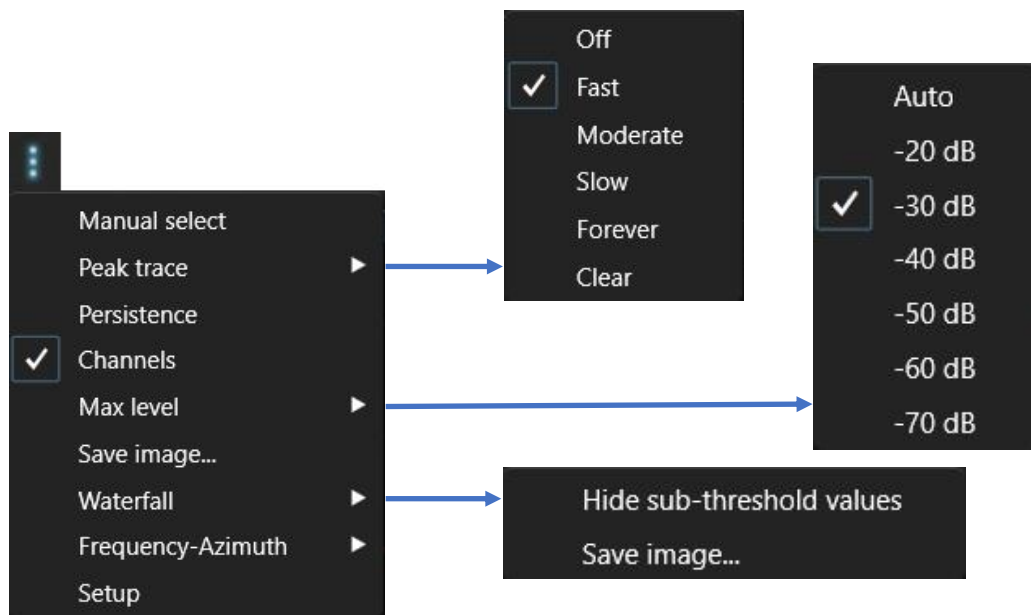
Manual select
Allows the operator to make selection in the spectrum graph with the help of the mouse's left button. That is convenient on the sensor (touch) screens. As standard it is necessary to press and hold the right button to select a span.

Peak trace
Thanks to the property of holding the maximum value of the spectrum, the peak trace allows the operator to see any short events such as short-time (burst) signals. The peak trace is drawn by the orange color on the spectrum graph.
- **Fast, Moderate, Slow, Forever -** enable the peak trace and allow the operator to set the integration time of the peak trace. "Forever" starts the constant integration

- **Off** – disables the peak trace
- **Clear** resets the peak trace and restarts the accumulation.

Persistence. This feature uses changing colors to display signals with different activity rates. The more often the signal occurs, the warmer the color on the graph is. Single occurrences are displayed in blue, more frequent activities are green, and very frequent or constant signals are yellow or red. Use this mode to study bands where many overlapping signals exist, such as 2.4 GHz ISM band.

Low persistence   High persistence
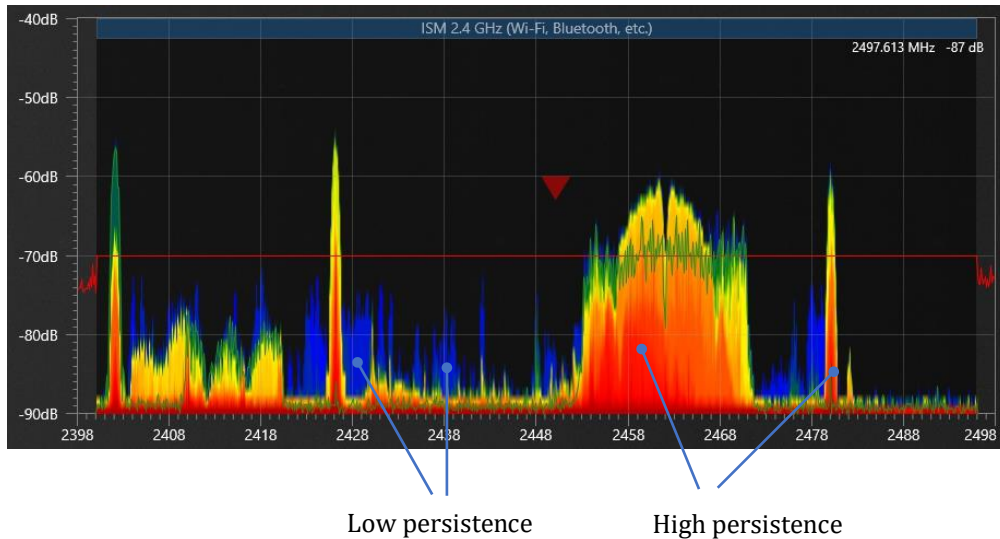
Max level. Sets the upper limit of the vertical scale of the spectrum graph. Choose a higher value to display stronger signals, and a lower value for better visual identification of weaker signals. Valid values are from -70 dB to -20 dB or "Auto". When using "Auto", the spectrum graph will adjust its vertical scale automatically.

Save image… - exports the image of the spectrum graph to a .jpeg or .bmp file.

Waterfall | Hide sub-threshold values - allows yo u to hide areas of the waterfall that have a low level and thus highlight areas with a high level (above the threshold).

Waterfall | Save image… - exports the image of the waterfall to a .jpeg or .bmp file.

Pressing **Setup** will open two additional controls:
- The vertical trackpad right to the spectrum graph helps to **customize the colors** of the waterfall and the persistence graph. By shifting the level of yellow the operator shifts the colors displaying different levels in the waterfall or the levels of persistence.
- **"Pixels per measurement"** under the waterfall allows the operator to set the desired number of pixels per one measurement. Bigger values may increase the readability but will make the waterfall shift faster and hold a shorter period of time. The default value is 2.

Panel "Alarms"

This panel displays information about the detected danger in real time during the search or in the Stop mode.
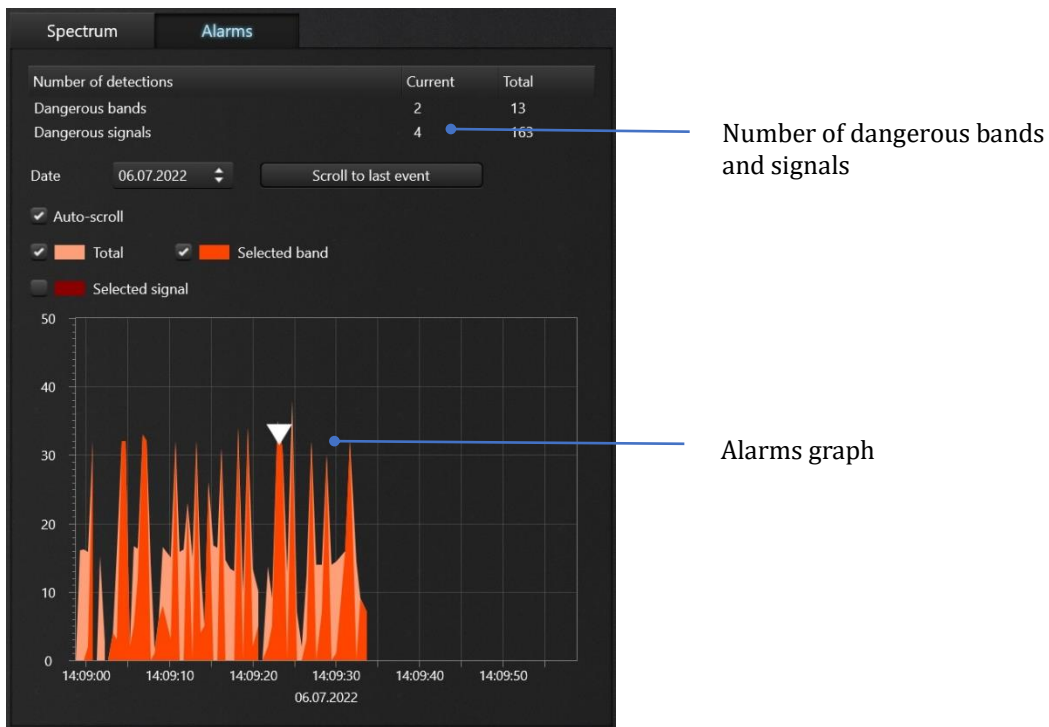
The "Number of detections" table shows the number of dangerous bands and signals at the given moment and for the entire period.

A situation when the band's or signal's level exceeds the threshold during the search is considered as an alarm event which is subject to logging. The number of such events over a long period of time can be significant because of constantly repeating short-time measurements. The alarm graph is the convenient way for displaying these multiple events.

The alarm graph allows you to display the alarm events that were registered in the selected time interval. It is possible to view all events or select them by a certain band or signal. The vertical scale of the graph is the danger level i.e. the above-threshold level of signal in dB. For example, when the signal level is -42 dB, and the threshold is -60 dB, then the danger level on the graph will be 60-42=18 dB.

It is possible to configure what is displayed on the graph:
- **"Total"** – general level of danger on all bands. Is displayed in light red
- **"Selected band"** – level of danger of the selected band. Is displayed in bright red
- **"Selected signal"** – level of danger of the selected signal. Is displayed in dark red.

"Auto-scroll" forces scrolling to the newest measurements during the search.

If auto-scroll is disabled, the alarm graph **can be scrolled** manually to any time. To do this, click the left mouse button on the graph and, without releasing the button, drag the cursor to the left or right. You can do the same with your finger or stylus on a touch screen.

If you want **to increase or decrease the displayed period (zoom in or out)**, click on the graph with the left mouse button and use the "increase" and "decrease" buttons. You can also use the mouse wheel.

In the "Stop" mode the user has access to some additional actions:
- Choose a **date**
- Scroll to the last event in the log using the **"Scroll to last event"** button
- Review the level of bands and signals by **clicking the desired time on the graph**. The "Level" panel will show the level of bands and signals at the selected time. Only dangerous bands and signals can be reviewed.

Search recommendations

Preparation

Searching mode

Decide what searching mode suits your tasks:

- **To check the premises for the presence of hidden bugging devices**, use the "All signals" mode

- **To search for trackers (beacons) on cars**, use the "Mobile/GPS-trackers" mode

- **To detect and find RF signal jammers** use the "Downlinks/Navigation" mode and/or other modes with active "Detect RF jammers" feature

- **For specific tasks**, such as detecting of Wi-Fi devices or wireless devices, use the "Wireless/ISM" mode.

> *Use the mode that best suits your task. A slower update rate reduces the probability of detecting burst signals, so we recommend avoiding "All Signals" mode for finding GPS trackers or wireless signals.*
>
> *The "Mobile/GPS trackers" and "Wireless/ISM" modes can be temporarily used after working in the "All Signals" mode to increase the probability of detecting mobile and wireless signals.*

Antennas

Delta S
Select the antenna for INPUT 1:
- The ODA-4 is a multi-purpose antenna and suits all detection modes including "All signals".
- The MWA-6 antenna provides a longer detection distance and simplifies locating thanks to its directivity but has a limited frequency range. The operator may prefer to use it when inspecting a truck or oversized cargo in the "Mobile/GPS trackers" mode with an extended detection diagram or temporarily during locating of a transmitter

Connect the LPDA-12 antenna to the INPUT2.

Delta X
Connect the ODA-4 to INPUT and the MWA-6 to AUX1. If you use the Delta X G2/12, connect the LPDA-12 to AUX2.

Change the frequency distribution between the ODA-4 and MWA-6 antenna if necessary: Settings - Device – Settings - AUX1 frequency. By default, the ODA-4 is assigned 9kHz – 3000 MHz and the MWA-6 – 3000-6000 MHz.

It may be necessary to change the AUX1 frequency when:
- the operator prefers to use the directivity of the MWA-6 during locating of a transmitter
- it is necessary to extend the sensitivity pattern in long rooms during long-time monitoring without moving the Delta X system
- inspecting a truck or oversized cargo in the "Mobile/GPS trackers" mode with an extended detection diagram

The minimum allowed value of the AUX1 frequency is 800 MHz which corresponds the MWA-6' frequency coverage.

Log file

Create a separate log file for the planned place of search. You will be able to open the file later again to add new data to it when performing a new sweep.

Masking background

The "All signals" and "Downlinks/Navigation" modes requires preliminary masking of the background outside the target room. Select a remote place and perform masking. To minimize false alarms, set a longer duration of measurement and repeat masking at several points around the target area (but not inside). The masking of background is not required for the "Mobile/GPS trackers" and "Wireless/ISM" modes.

Thresholds

Consider the distance of detection which you wish to achieve. The Delta S and Delta X systems have extremely high sensitivity and are able to detect signals from tens or hundreds of meters. For the countersurveillance sweeping it is recommended to have a shorter detection distance in order to avoid multiple alarms and to simplify the locating process. It is better to consistently move in the area, detect and locate the signals one by one than to detect many signals at the same time without understanding where they come from.

The Breeze RF software sets the optimal default thresholds to the bands. They provide the detection distance of several meters for the mobile and wireless signals and a longer distance for other, out-of-bands signals.

To decrease the detection distance, increase the thresholds. This may be necessary in the following cases:

- to avoid an interference coming from an adjacent room and creating a false positive
- when it is necessary to decrease the sensitivity on a specific band or on all bands
- during locating a transmitter, the operator approaches the source and increases the thresholds step by step

To increase the detection distance, lower the thresholds. This may be necessary:

- when you wish to perform long-time monitoring without moving the system
- if you wish to inspect big area without moving
- if you wish to inspect a vehicle in the "Mobile/GPS Trackers" mode

For details, please refer to "Adjustment of thresholds".

Avoiding false alarms

Disable all RF devices which are active in the place of the search, including mobile phones, computers, access points, wireless devices (headset, headphones, watches, etc.), other Bluetooth devices, Wi-Fi, etc. Minimizing false positives will speed up the search and make its results more reliable.

Audio background

Some listening devices are activated only in the presence of sound. To activate them, create a background sound in the room.

Target premises (place of search). Create sound background

Place for masking of background. Select distance not less than 10 m to the target place

Can be made outside
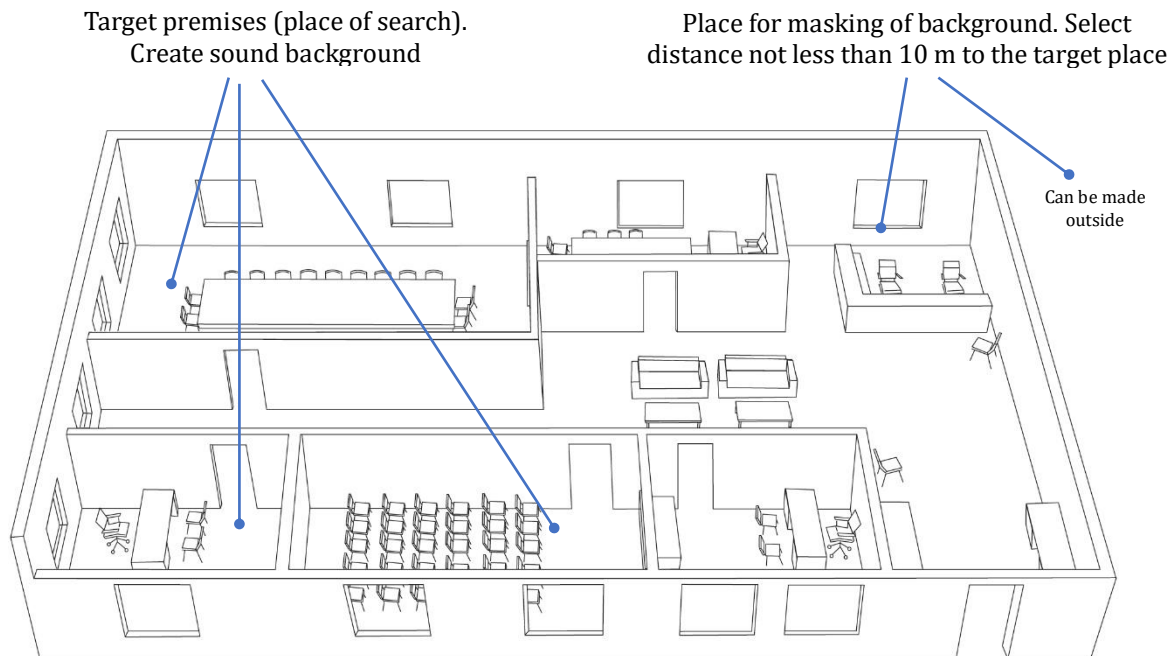
Search

1. Start the selected searching mode. The "Cellular/GPS trackers" and "Wireless/ISM" modes can be enabled together.

2. Turn on the audio alarm to make it easier to monitor the situation. Use the function "Hold max. danger." to automatically tune in the most dangerous band.

3. Check the premises by parts, for example room by room. Scan each room with a view to the detection distance of the weakest signal that could theoretically exist. For example, if at the current thresholds the minimum guaranteed distance is 1-2 meters, then it is necessary to scan the room dividing it into "strips" of 2 meters width. Move at a speed of no faster than half a meter per second, turning the system in different directions. Watch the Alarms graph, the Level panel and listen to the alarm audio.
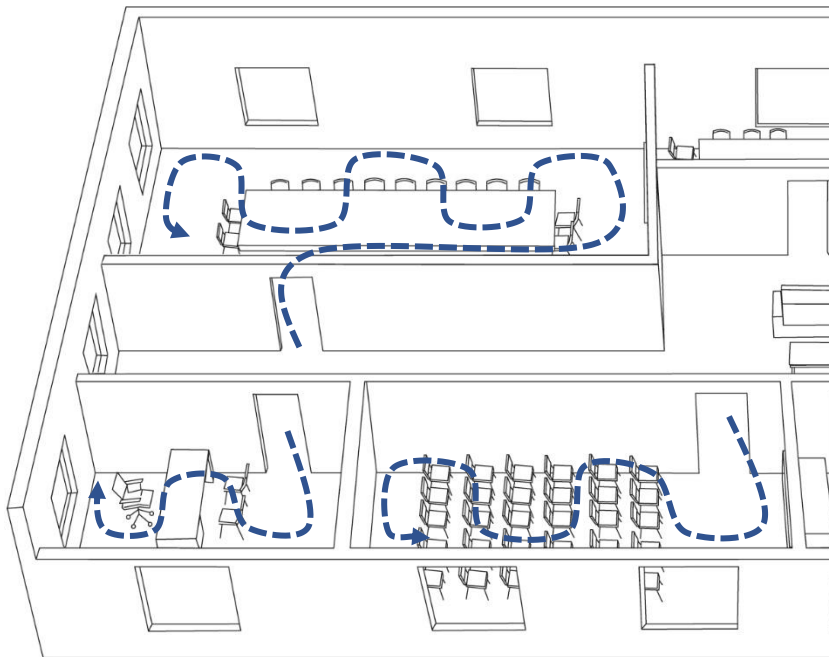
Inspect the entire space of the room evenly

Finding a transmitter's location

1. After starting the search, the Level panel will be in the multi-band measurement mode. If a threat is detected, the operator proceeds to inspecting the dangerous band (enters the band). This narrows the measured part of spectrum, increases the speed and probability of detection which is useful for locating the transmitter. It is also possible to enter a single signal's inspection mode to further narrow the measurement span.

> *LTE/4G and 5G mobile standards can dynamically change the frequency band. If the level on a band has dropped, return to the multi-band measurement and note where the high level appeared. You can proceed to inspection of a new band or locate the transmitter staying in the multi-band measurement of the "Mobile/GPS Trackers" mode.*

2. Start the search for the location of the transmitter. To do this, move or rotate the system and find the maximum signal level. Watch the level displayed on the bargraph and spectrum and go where the signal is growing. The closer the antenna is to the transmitter, the higher the level will be. LEDs on the front panel will help you determine which antenna is in use. During locating, you can gradually increase the threshold to reduce the search circle (but remember to return to the original value afterwards).

3. If the signal level reaches -25...-20 dB and spectrum distortion appears at the adjacent frequencies, temporarily use an attenuator.

4. When you have found a place with the highest signal level, start the physical search of the transmitter.

5. External signals coming from adjacent areas can cause false alarms. Such disturbances are usually located (have a maximum level) near windows, walls, floor or ceiling and their level decreases in other parts of the room.

6. After inspecting an individual band or signal, remember to return the Level panel to the multi-band measurement mode.

Long-time monitoring and studying results

The Delta S / Delta X system can record spectrum traces and danger events over a long period of time, such as a day or week. This makes it possible to detect RF bugging devices that do not transmit continuously and upload data by schedule or by a signal from a remote control.

> *To ensure that the logging is active check that the "Perform logging" button is in the pressed state during the search.*

If you wish to study the result of a search, select the "Stop" mode and open the "Alarms" panel and examine the alarm events that have been registered.
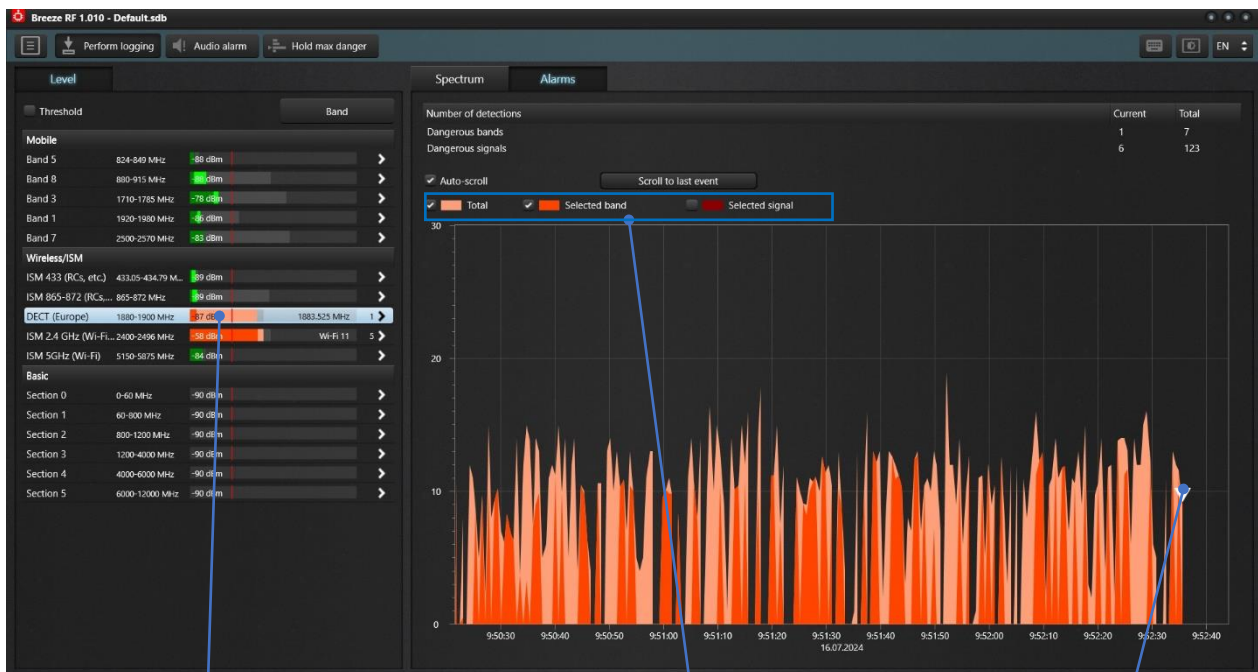
The band which was dangerous at the selected moment   Drawing mode of the graph   Selected moment

1. In the "Log file" menu, select the desired date. In the Alarms graph rewind the time to the beginning of the date, where the first event occurs.

2. If necessary, set a convenient period by zooming in or out (click the mouse, select "increase" or "decrease" several times).

3. Choose the studied moment by clicking on the alarm graph in a place with a high level of danger. The position of the white triangular cursor will show the selected moment. On the "Level" panel, the bands that created danger at the selected moment will have a red bargraph. Just like during the search, the number of dangerous signals and the frequency of the most dangerous signal will be shown next to the bargraph.

4. Select the first dangerous band in the "Level" panel, and then enable drawing of its alarms by setting the "Selected band" checkbox in the "Alarms" panel. On the alarm graph, you will be able to see the level of danger for the selected band in bright red. By analyzing this graph, you can find out how strong the band was and how long the transmission lasted.

5. The Spectrum panel displays the recorded spectrum traces on the waterfall.

When a band or signal is double-clicked on the Level panel in the Stop mode, the spectrum graph and the waterfall automatically adjust their edges to display the corresponding span.

By clicking an event on the Alarms graph the operator can scroll the waterfall to this event. Thus, he can review the spectrum of a band or signal at the selected moment.

It is possible to scroll the waterfall vertically using the scrollbar which appears after the waterfall is clicked.

It is possible to review any momentary trace on the spectrum graph by clicking the corresponding moment on the waterfall in the Stop mode. The green "live" trace will display the spectrum trace which existed at the clicked moment.

6. It is possible to inspect the band in the "Level" panel just like during the search. After pressing the "Band" button you will be able to see a list of signals that existed within the band. Those signals that were dangerous at the selected moment will have a red level bargraph. By selecting a signal with a red bargraph and checking the "Selected signal" in the "Alarms" panel, you can see the alarm graph for the selected signal. By analyzing the alarm graph for a single signal, you can find out how strong it was and how long it lasted.

7. Return to the list of bands in the Level panel and explore other dangerous bands.

8. Repeat clicking on the alarm graph at another time where high danger also existed and explore the dangerous ranges.

9. You can also study the activity of each band in turn by selecting a band and studying its history on the graph (with the "Selected band" checkbox enabled). Don't forget to rewind or zoom the alarm graph to see all events

If you find a suspicious signal that periodically exists in your premises, has a high level and a sufficiently long existence, try to find where it comes from. Study room by room, leaving the system in each room for 24h and analyzing the results. Make sure that this is not a false alarm and that the signal does not come from outside by performing measurements outside the premises.
You can leave the system in the band inspection mode to increase the probability of registering short-burst events.
Find the room with the highest level and try to predict the operating time of the transmitter. Try to locate the transmitter at this moment.

Searching for GPS trackers (beacons)

GPS trackers (beacons) can be divided into three types:
1. Those that accumulate coordinates and do not transmit them
2. Those that accumulate coordinates and transmit them upon request
3. Those which regularly transmit coordinates

Trackers of the second and third type usually use mobile networks to transmit data. To detect these mobile devices, the Delta S / Delta X system must be in the moving and maneuvering vehicle.

Provide power to the computer if you plan to work for more than one hour. You can use an inverter or powerbank.

1. It is recommended to carry out the sweeping procedure in places with minimal interference from other mobile devices. Urban environments are very saturated with

means of mobile communication and makes it impossible to correctly interpret the results. Move to an empty road in the countryside, without settlements and other transport.

2. Place the system in the middle of the vehicle

3. Delta S: If you want to provide a circular pattern, use an ODA-4 antenna for INPUT 1. If you are testing a long vehicle (such as a long size truck), the MWA-6 antenna at INPUT 1 will provide you with an extended detection distance (the system must be positioned at the edge of the target zone and pointed to it). INPUT 2 always works with the LPDA-12 antenna.

   Delta X: If you demand an extended detection diagram, such as during testing a long vehicle, it is recommended to change the frequency distribution and assign the MWA-6 to lower frequencies: Settings – Device – Settings – AUX1 frequency. Set the AUX1 frequency to 800 MHz to guarantee the use of MWA6 from 800 MHz and higher.

4. Create a log file

5. Start "Mobile/GPS trackers" mode

6. Set the desired bands' thresholds or reset them to the default values

7. Start the engine and start driving. Some tracking devices will periodically transmit information about the coordinates of the vehicle, and some also about engine start/stop and change of direction of movement. Drive for at least half an hour, periodically changing direction, stopping and starting the engine. Keep an eye on the alarm graph, level bargraphs and audio alarm at all times.

8. In the "Mobile/GPS trackers" mode, the system scans all mobile bands and displays the cumulative threat level on the alarm graph. Trackers (beacons) are characterized by short periodic exchanges with the mobile network. The alarm graph makes it possible not to miss such short-term signals and to catch their periodicity. The presence of signals can inform about a mobile device that is nearby.

9. If a suspicious signal is detected, try to find a connection between its appearance and the behavior of the car - start-stop the engine, start moving, stop, make a turn, etc.

10. If you see a signal, proceed to locating of the transmitter as described earlier. Changing the position of the system and its direction will allow you to find the direction of the signal. The MWA-6 antenna in the INPUT 1 input speeds up the result. Rare periodic signals may require more time to study.

Detecting RF signal jammers and anomalies

The web-site of the Federal Communication Commission of the U.S. informs the following:
"Federal law prohibits the operation, marketing, or sale of any type of jamming equipment that interferes with authorized radio communications, including cellular and Personal Communication Services (PCS), police radar, and Global Positioning Systems (GPS).
Signal jamming devices can prevent you and others from making 9-1-1 and other emergency calls and pose serious risks to public safety communications, as well as interfere with other forms of day-to-day communications.
The use of a phone jammer, GPS blocker, or other signal jamming device designed to intentionally block, jam, or interfere with authorized radio communications is a violation of federal law. There are no exemptions for use within a business, classroom, residence, or vehicle. Local law enforcement agencies do not have independent authority to use jamming equipment; in certain

limited exceptions use by Federal law enforcement agencies is authorized in accordance with applicable statutes.
It is also unlawful to advertise, sell, distribute, import, or otherwise market jamming devices to consumers in the United States."

Despite this, RF signal jammers can be found, especially in countries without criminal penalties for their use. Cellular GSM/3G/4G/5G jammers are used in a relatively lawful manner for creating free-of-coverage zones or with a criminal aim - by burglars for suppressing the alarm systems when breaking into the premises or hijacking a car. GPS jammers are frequently used by drivers when they do not wish the company to know the location or route of the vehicle and at the same time – by hijackers when stealing a car.

Sources of interference can create serious problems for neighbors – loss or low quality of mobile communication, decreased speed of Internet, non-working navigation or incorrect GPS coordinates, etc.

The Delta S / Delta X system can be used for detecting and finding RF signal jammers and anomalies.

It is known that cellular jammers create interference on downlink bands, i.e., where the data from the network to mobile device is sent. When there is a noise on these frequencies, the mobile terminal cannot receive signals from the base station and becomes "out-of-network". The so called "GPS signal blockers" or "GPS jammers" create interference on frequencies of satellites in order to mask their signals and prevent navigation devices from receiving information needed for calculating coordinates.

Therefore, to detect and find a jammer it is necessary to monitor downlink bands of mobile communication and bands of Global Navigation Satellite Systems, such as GPS, GLONASS and GALILEO. An increased level of noise will inform of the presence of a jamming device nearby.

1. The Breeze RF software is supplied with a data file containing the frequency allocation for many countries, including the mobile downlinks and bands of Global Navigation Satellite System (GNSS). As standard the downlink and GNSS bands are not added to the band list when the user selects the country of use. To add the downlink and GNSS bands mark the corresponding checkboxes in the "Settings – Bands | Country" and then press "Apply" to re-fill the list. When the downlink and GNSS bands are added to the list, the "Downlinks/Navigation" mode becomes visible and enabled.

2. Background masking in a remote and free-of-interference place may be performed before searching. Results of masking will be applied to the downlink and GNSS bands. As a result: 1) the existing signals, such as mobile base stations or satellite signals, will not create alarms; 2) any significant changes in the existing pattern (anomalies) will be detected. Anomalies may occur as a result of changes in the mobile network made by the provider or as a result of unauthorized intrusion in the mobile network or satellite system (interception, spoofing, IMSI-catching, etc.).

3. Activate the "Detect RF jamming" function in the "Settings – Other" menu. Enable "Audio alarm" on the toolbar.

4. Start the "Downlinks/Navigation" mode. You can also activate the "Mobile/GPS trackers" mode to scan all mobile bands, including those without downlinks (TDD bands of 4G/5G).

In order to detect Wi-Fi jammers, activate the "Wireless/ISM" mode. It is also possible to simply use the "All signals" mode, which is slightly slower but scans all categories of bands at once.

5. When the "Detect RF jamming" is active, the Level panel displays an additional blue bargraph near each band. It represents the level of noise. When there is no jammer, the level of noise stays low (less than -70dB). When a jammer appears, the blue bargraph grows. When it exceeds the threshold, the Audio alarm will produce a special beeping sound (if active).

Below is an example of detecting a multi-band jammer:

Level of noise

No jammer   With working jammer

6. It is possible to use the threshold to adjust the sensitivity and, accordingly, the detection distance. The "Downlinks/Navigation" bands are maskable, so when there is a mask the band's threshold will act as an offset.

7. When a jamming signal is discovered, the operator can accomplish finding the source of interference by using the blue bargraph and audio alarm. When the system is approached to the source of interference, the noise level bargraph will grow and the beeping sound will become more intense. Scan the area in the same way as when searching for a bugging device. Enter the band inspection mode and use the Attenuator function if the level of noise (blue bargraph) becomes too high (2/3 or more). With attenuator the sensitivity becomes lower and you can approach the transmitter closer. Do not approach closer when the level is high again with the Attenuator. An excessive level of signal may be dangerous for the receiver.

8. Anomalies (significant changes in the spectrum of downlink bands and GNSS bands) will produce usual alarms similar to that of bugging devices. The green bargraph will grow and become red when exceeding the threshold. The standard clicking sound will be produced. The signals will be added to the signal list with the possibility of reviewing

them in the band inspection mode. Perform standard locating procedure to find the source of signal.

Multi-function probe

The transmission of information through wires is supposed to be more covert since there are no easy-to-detect radio waves produced. Practically any wire lying within, or crossing the target room and further going outside the area can be used for surveillance as a transmission means. A line carrier bugging device will consist of 2 units: a transmitter located within the target area and connected to the wire and a receiver outside the target area connected to the same wire. The transmitter picks up the audio within the room, converts it up to a higher frequency and sends the signal via the wire. The receiver picks up the signal from the wire, converts it down and passes the audio to the voice recorder or monitoring post. The signal can be sent via any type of wire while leaving it operable.

In addition to the law enforcement grade line carrier bugs, it is necessary to take into consideration the powerline networking technology. A simple but hard-to detect bugging device can be built from an IP video camera with audio and an affordable powerline adapter streaming data over an AC outside the premises. Then the external powerline adapter picks up the sent information. The HomePlug AV/AV2 standards provide data throughput up to 500 Mbps and occupies the range between 2 and 86 MHz.

Infrared rays are invisible and distribute relatively long distances; therefore, they can be used for surveillance too.

Some surveillance devices, or their parts, may emit electromagnetic waves: AC powered transmitters, video cameras, etc.

The Delta X can detect the above-mentioned ways of surveillance with the help of the Multifunction Probe which is supplied in the standard set.

Multifunction Probe:

The probe has 3 inputs:

Input	What is detected
IR	Hidden infrared transmitters
LF	Electromagnetic emissions from bugging devices
WIRE	Bugging devices sending information over: • AC wires • Ethernet • Landline telephone wires • Alarm cables • Other low-voltage cables

To enter the Probe mode, press the Probe in the main menu. The Breeze RF software will have the following view in the Probe mode:
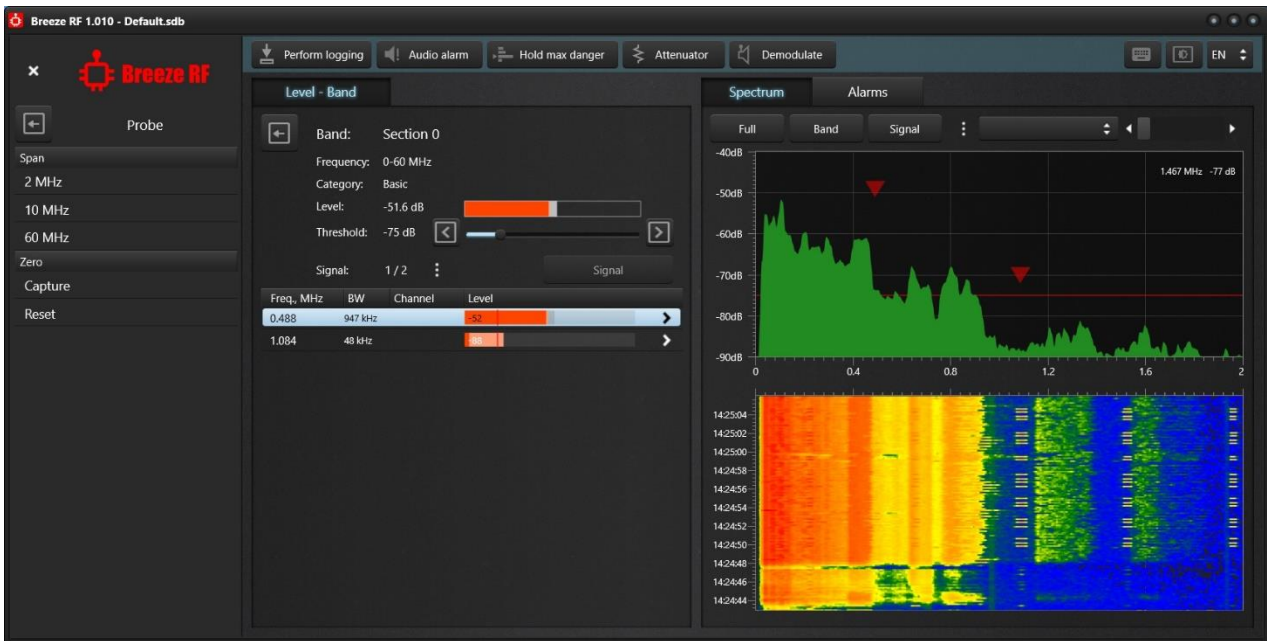
The Level panel will be in the inspection mode of the basic band "Section 0". Three spans are available:
- 2 MHz: is recommended for the IR and LF input
- 10 MHz: is recommended for the WIRE input
- 60 MHz: is recommended for the WIRE input when it is necessary to inspect the line in a wider frequency range

The **"Zero – Capture"** function can be used to capture the current spectrum trace for its subsequent extraction

The "Attenuator" function can be used when a strong signal is met.

Like in all other modes **double clicking** on a signal in the Signals table adjusts edges of the spectrum graph to fully show the signal. A single click selects the signal without adjusting the spectrum graphs.

The Persistence view of the Spectrogram, when activated, allows the user to distinguish between the continuous and non-constant signals.

Infrared (IR)

Since infrared rays have a directed nature, the potential IR bug will be directed to the place of the signal's reception. The most likely direction will be the outer area near the building or a remote part of the room. The detection should be performed inside the room and in the windows' area, with the Multifunction Probe pointed to the interior of the room, window frames and the area near the frames.

The detection distance of the probe's IR sensor depends on the transmitter's power and can be 1-5 meters, on the condition of being pointed to the source.

Algorithm
1. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
2. Select the IR input on the probe
3. Select the Probe mode in the Delta X software
4. Clear the signal list with the help of the "Delete all signals within band" command in the menu of the Level panel
5. Create a source of sound in the room to activate any potential bugging devices
6. Point the probe's IR sensor to the place of possible bugging (for example, from outside the window to the interior and frames)
7. If an infrared signal is detected, it will be automatically inserted into the Signals table.
8. In case of finding a signal, rotate the probe in different directions in order to find the strongest level, which will mean that the sensor is directed to the transmitter. Move the probe closer to the supposed source while observing the change of level. Try to find the place with the highest danger level. The Audio alarm function will change the intensity of sound correspondingly (if activated). In the place where the strongest level is found start a physical inspection. If the entire area produces a low to average level of danger, and there is no one place with a strong signal, it may mean just the presence of interference.
9. Repeat the test near other windows and parts of the room

Low frequency (LF)

The LF sensor of the Multifunction Probe allows the operator to find signs of hidden working electronics by detecting radio-frequency emissions.
T
he detection distance is up to 30 cm; therefore, objects and surfaces must be probed carefully.

Algorithm
1. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
2. Select the LF input on the probe
3. Select the Probe mode in the Delta X software
4. Clear the signal list with the help of the "Delete all signals within band" command in the menu of the Level panel
5. Create a source of sound in the room to activate any potential bugging devices

6. Start scanning the area (objects, surfaces, constructions, etc.) while observing the change of the danger level. The Audio alarm function, if activated, will produce sound of changing intensity, depending on the level.

7. All the signals (parts of spectrum exceeding the threshold) will be inserted into the Signals table automatically. Their levels will be updated during the search

8. Try to find the source of the highest signal by moving the probe in different directions. High current-consuming electronics in a working state will create a high level with a specific spectrum form. It is normal that metallic objects and construction re-emit the RF fields, sometimes producing a danger level.

9. Use the demodulation when it is necessary to inspect a suspicious signal. To do so select the signal in the Signals table or click the peak on the Spectrogram. The probe should stay near the source during this operation. Some electronic devices can have recognizable sound helpful for detection.

AC wires (WIRE)

Since the AC wire is an antenna itself, it receives a lot of RF emissions present in modern environments. The different method described below helps to avoid the sophisticated process of finding a suspicious signal among a huge number of interferences. With this method the Delta X stores the RF environment measured in the first AC outlet and extracts it further from the others. When probing other outlets the operator will observe the difference. Therefore, if a bugging transmitter is present somewhere on the AC line, its signal will grow as the Multifunction Probe is moved closer to it. This different method helps to detect signals by probing a series of AC outlets connected to the same AC wire.

Algorithm:
1. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
2. Select the WIRE input on the probe
3. Select the Probe mode in the Delta X software
4. Connect the high voltage cable to the Multifunctional Probe.

   Warning: NEVER USE THE LOW-VOLTAGE "ALLIGATOR" CABLE FOR PROBING AC WIRES.

5. Create a source of sound in the room to activate any potential bugging devices and recognize them during demodulation
6. Connect the high voltage cable to the AC outlet #1 in the room
7. Press **Zero - Capture**
8. Clear the signal list with the help of the "Delete all signals within band" command in the menu of the Level panel
9. Connect the high voltage cable to the other AC outlets in the room one by one and watch for any new signals. Interference signals typically do not have a strong peak or occupy a wider span and may be present in a number of outlets, while a real transmitter will have a stronger level only on the separate outlets.
10. Observe and learn the detected signals:
    - Double-click or click the signals in order to review them in the spectrum graphs

- Select "Demodulate"
- Click on all peaks within the Spectrogram in order to tune in precisely and listen to the signal. Try to recognize signs of modulation. Change the demodulation mode and bandwidth if necessary. Change the frequency slightly.
- In case of finding a modulated signal within the audio of the room, or a signal with an untypically strong level, start a physical inspection along the suspicious wire.
11. To avoid masking a bug, if it is present in outlet#1, repeat steps 7-10 selecting another outlet as #1 and probing all others once again

Low-voltage wires- Telephone, Ethernet and alarm (WIRE)

The Delta X is supplied with the following accessories allowing the operator to test low-voltage wires:
- Low-voltage cable with "alligator" connectors
- In-line modular adapter
- Adapter "8 pin male to 6 pin female"
- Adapter "8 pin male to 4 pin female"
- Connection cable "8 pin to 8 pin"
- Connection cable "8 pin to 6 pin"
- Connection cable "8 pin to 4 pin"

For each type of wire a specific adapter should be used:

| Wire	Connection type	Needed accessory	Terminals
Landline phone	RJ-11 (6 positions, 4 conductors)	Low-voltage cable, modular adapter, cable 8-to-6, adapter 8-to-6	1…4
Landline system phone	RJ-12 (6 positions, 6 conductors)	Low-voltage cable, modular adapter, cable 8-to-6, adapter 8-to-6	1…6
Ethernet cable	RJ-45 (8 positions, 8 conductors)	Low-voltage cable, modular adapter, cable 8-to-8, adapter 8-to-8	1…8
Alarm cables	Direct (alligator connector)	Low-voltage cable	
Other low-voltage cables	Direct (alligator connector)	Low-voltage cable	

Algorithm:
1. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
2. Select the WIRE input on the probe
3. Select the Probe mode in the Delta X software
4. Clear the signal list with the help of the "Delete all signals within band" command in the menu of the Level panel

5. Connect the low voltage "alligator" cable to the Multifunctional Probe.
6. Create a source of sound in the room to activate any potential bugging devices and recognize them during the demodulation
7. Connect the low-voltage "alligator" cable to the wire. If necessary use the in-line modular adapter and accessories:

Landline phone

The connection to the telephone can be made either at the phone set side or near the wall socket, depending on accessibility. Insert the male-to-female adapter into the modular adapter tightly to provide the proper connection. Make sure the telephone stays operable after the modular adapter is connected in-line. Below is an example of probing the phone line near the phone set.
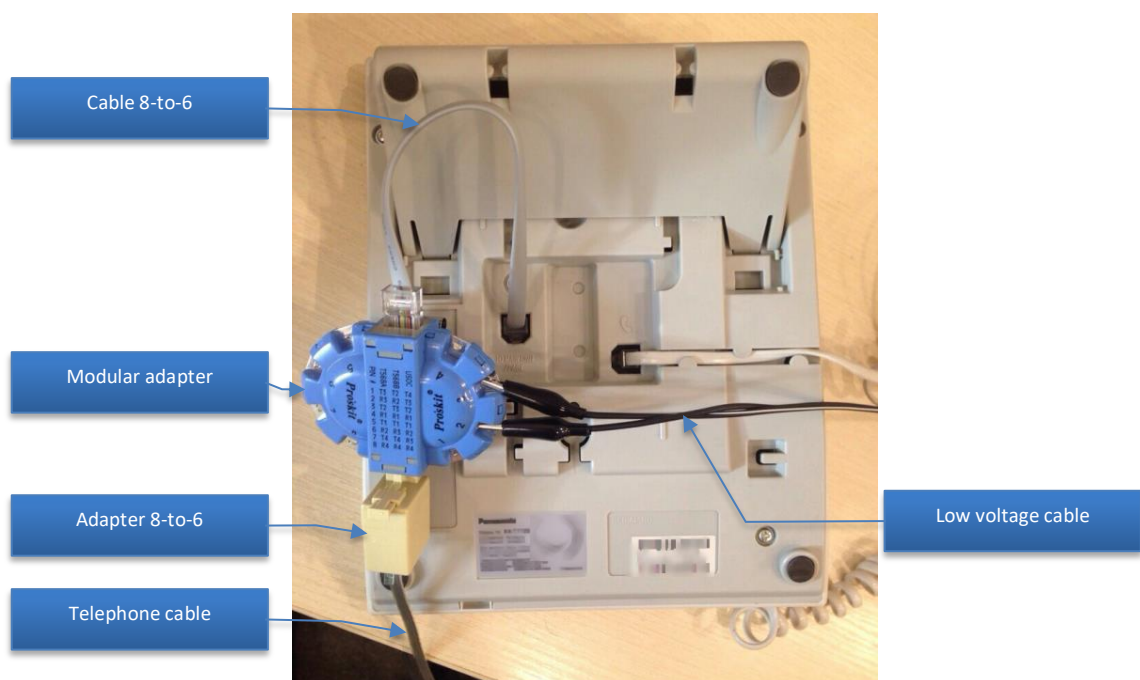
Ethernet

The connection to the Ethernet can be made near the computer, wall socket or near the network equipment (switch/router). Insert the male-to-female adapter into the modular adapter tightly to provide the proper connection. Make sure the network stays operable after the modular adapter is connected in-line. Below is an example of probing the Ethernet at the computer:

Cable 8-to-8

Low voltage cable

Modular adapter

Ethernet cable
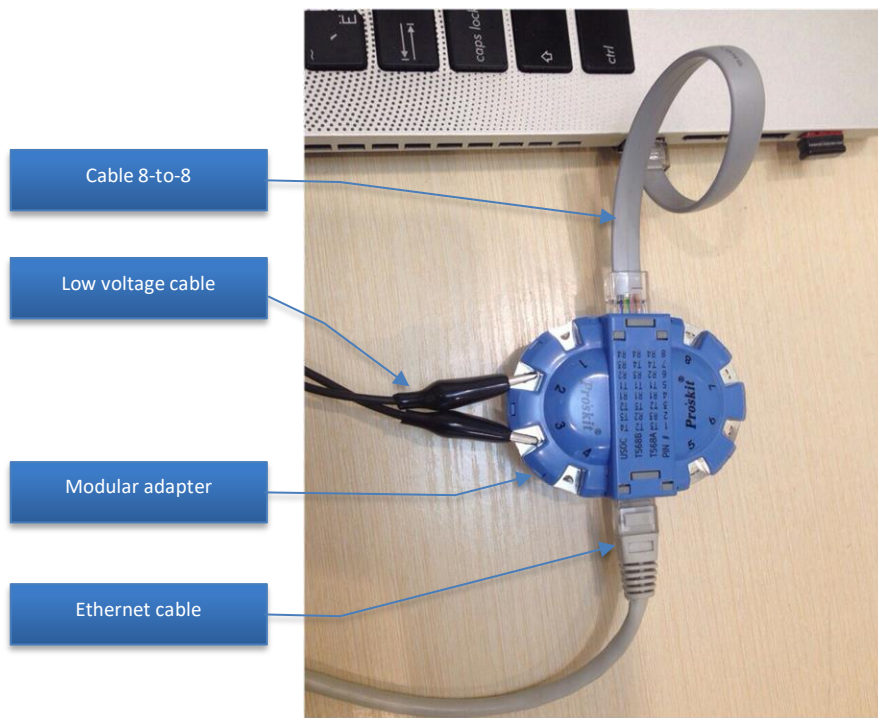
**<u>Alarm and other low-voltage wires</u>**

Connection to other low-voltage lines, including alarm systems should be made with the help of the low-voltage cable with alligator connectors.
The alarm movement detector should be disassembled in order to reach the terminals. The procedure can be made on the control panel as well.

<u>Please note, that alarm detectors, fire detectors and control panels are mostly tamperproof, i.e. they alert the alarm monitoring center about disassembly. The procedure should be agreed with the central monitoring station and performed with the presence of a technician.</u>

8. Connect the alligator connectors to the terminals on the modular adapter in accordance with the quantity of used conductors. The telephone lines may use 2, 4 or 6 conductors, while the Ethernet employs 4 conductors from the 8 present in the twisted pair cable.

The modular adapter uses the following numeration of the terminals:
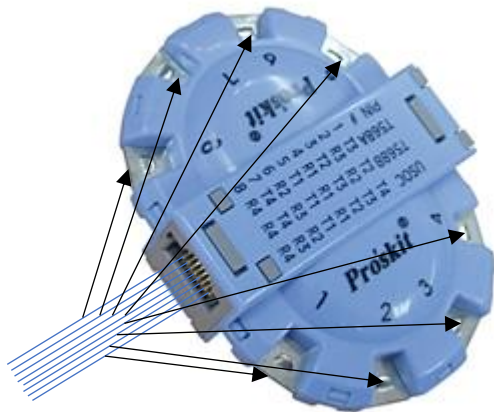
Since it is often unclear what particular conductors are used, all the combinations of the alligators can be used for checking the line: 1 and 2, 2 and 3, 3 and 4, 1 and 3, 1 and 4, etc. The spectrum may coinside in some pairs.

9. After connecting the alligators the measurement will start. The signals exceeding the threshold will be automatically inserted into the Signals table. Turn off the Audio alarm function if necessary or adjust the Alarm threshold.

10. Observe and learn the results of detection:
    - Double-click or click the signals in order to review them in the spectrum graphs
    - Select the Demodulate
    - Click on all peaks within the Spectrogram in order to tune in precisely and listen to the signal. Try to recognize signs of modulation. Change the demodulation mode and bandwidth if necessary. Change the frequency slightly.

        Please note that since the wire is an antenna itself it receives a lot of RF emissions present in our modern environment. Detection of interference signals is a normal situation. The task of the operator is to study all the signals in the Signals table and the spectral peaks in the Spectrogram, analyze the levels, demodulate and make a decision about their safety.

    - In case of finding a modulated signal with the audio of room or a signal with an un-typically strong level start a physical inspection of the suspicious wire.

11. If you are checking the phone line, perform the test off-hook and hung up
12. Repeat the test for all the combinations of pairs on the modular adapter, reconnecting the alligators as necessary
13. Repeat the test for other telephone lines/Ethernet sockets present in the target room and in the adjacent rooms.
    - The interference signals might have approximately the same spectrum and strength on all lines, while the bugged line will have different spectrum view and signal strength

- If a bugging signal is transmitted in a digital representation, it cannot be demodulated. At the same time, a strong signal and an untypical form of spectrum might point to danger.

Since the normal, non-dangerous signals are passed through the telephone and Ethernet wires the process of detecting danger among the normal signals may be difficult. It can be significantly simplified with the help of the differential method. In this case the normal signals can be eliminated so that the operator can easily detect only the new suspicious component in the line. To do so, make measurements in a number of lines of the same type and belonging to the same PBX or switch. For example, if there are a number of telephone sockets in the room, you can measure them in line to find the difference. Or this can be Ethernet sockets.

Use the "Zero" when probing the first line to capture the RF environment in it. Then proceed with measurements on the other lines to detect the difference. Since telephone and Ethernet cables contain more than 2 conductors, make sure that the same pair of conductors is measured on the other lines.

Absence of new components is a normal situation, while the presence of new signal is a suspicious sign. In this case it is necessary to study the line and equipment connected to it.