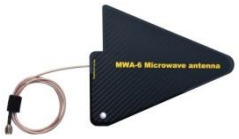
Delta X

Counter surveillance sweeping system



User Manual

For version 1.1

09.11.2017

Content

General description

Introduction

Welcome to the world of professional counter surveillance! The Delta X system will make your searches quick and easy, while providing extremely reliable results. The system's hardware incorporates a powerful spectrum analyzer which provides a super-fast speed of measurements with extreme sensitivity, while the built in RF 'switcher' extends the system's functionality. The supplied set includes the full set of equipment needed for professional bug detection: omnidirectional antenna, directed microwave antenna, multifunction probe for checking the infrared/low frequencies and wires, cables and adapters.

Features

- Quickly and reliably detects all kinds of RF listening devices, including analog, digital, constantly existing and intermittent, sending audio or video, with or without encryption
- Finds hidden surveillance devices employing the digital standards GSM, 3G, 4G/LTE, Bluetooth, Wi-Fi, DECT, etc.
- 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
- Can work in instant detection mode, guarding mode, locating mode and car tracker detection
- Has a 20-50 times higher sensitivity and detection distance compared to conventional RF detectors and near-field receivers
- Can monitor the RF environment 24 hours a day with data logging
- Capable of detecting covert bugging devices with an accumulation function and transmitters hidden within the spectrums of other signals
- Supports storage of an unlimited quantity of signals. Full information is stored in the log and can be reviewed during the detection, or at a later time. Multiple logs are supported.
- Demodulation of audio in FM, AM, USB, LSB, CW (adjustable BW 3…240 kHz)
- Alarm relay output can activate external devices when a dangerous signal is detected (turn on a CCTV system, for example)
- Comes in a protected case that allows you to place a 14" laptop inside (not included in the supplied set)
- Powered from the laptop's USB

Exclusive features of the 2000/6 Real-Time version:

- High update rate, 2000-3000 MHz per second
- Frequency range 40 kHz – 6000 MHz
- Detected signal's existence time: 2-3 seconds
- Instantly detects digital signals with short bursts
- Can detect and locate the transmitter simultaneously

Exclusive features of the 100/12 version:

- Update rate of 100 MHz per second
- Frequency range 100 kHz – 12400 MHz

- Detected signal's existence time: 60-120 seconds
- Detects digital signals with short bursts by accumulating data

Exclusive features of the 100/4 version:

- Update rate of 100 MHz per second
- Frequency range 40 kHz – 4400 MHz
- Detected signal's existence time: 45 seconds
- Detects digital signals with short bursts by accumulating data

Advantages

- What it is: a portable system controlled by a laptop computer
  - The high capacity of a laptop's hard drive enables full data logging during the detection (24/7 possible)
  - Wider screen is more convenient for analysis
  - Compatible with touch screen laptops
  - The handheld use of antennas is more convenient for locating transmitters in hard to access places

- Handling of the mobile and wireless bands GSM, CDMA, 3G, 4G/LTE, DECT, Wi-Fi, Bluetooth, etc.
  - Mobile and wireless signals are detected simultaneously with analog transmissions
  - Mobile/wireless signals are detected with the use of individual thresholds and are displayed separately from other signals
  - Activities within each band are stored as one signal with a certain danger level to avoid excessive records in the Signals table and to locate the sources with a hopping frequency
  - Additional sweepings on the 'short-burst' bands are performed to increase the probability of interception of such signals as GSM, 3G, 4G, DECT, Wi-Fi, Bluetooth, etc.
  - External interference from neighboring mobile phones and Wi-Fi routers can be rejected with the help of the thresholds
  - The supplied data files allow the operator to adjust the system to the mobile/wireless bands employed in the country of use

- Sensitivity and detection distance
  - The built-in spectrum analyzer has 20-50 times higher sensitivity and detection distance compared to conventional RF detectors and near-field receivers
  - Resistant to interference - sensitivity remains high regardless of the proximity to wireless routers, cordless phones, mobile phones, TV towers, radio broadcasting and mobile communications

- Support of the 'Known signals' table
  - The operator can easily distinguish between safe and dangerous signals
  - The TV frequencies employed in the country of use can be quickly imported from the supplied data files
  - The FM, VHF/UHF police and municipal channels can be collected and stored for further use

- Advanced signal recognition method

- The signals are automatically recognized in the spectrum traces and inserted or updated in the Signals table
- Both analogue and digital signals are captured with an assigning of a corresponding Danger level

➢ Unique algorithm of measuring the signal's Danger level
- Uses a combination of the reference trace and individual thresholds for mobile/wireless bands
- Takes into consideration both the signal's strength and bandwidth
- Works for both analogue and digital signals including transmissions with a changing frequency
- Is used during the locating procedure and provides more reliable results compared to the traditional 'signal strength' method.

➢ Low demands on the operator's level of knowledge
- The system can be prepared for detection with the help of the 'Update Masks' procedure within a few minutes
- Manual handing of spectrum traces is not necessary
- Everything is done automatically after the detection starts
- The operator is warned by an audio alarm when a dangerous signal is detected

➢ Data logging
- All the spectrum traces and alarms are logged during detection
- The situation at any given time can be reviewed and studied
- 24 hours a day logging provides detection of periodically working/remotely controlled bugging devices

➢ Tracking of the signal's activity
- The full history of each separate signal, or of all signals simultaneously, is displayed on the Alarms graph
- The events at any given time can be reviewed by simply clicking on the graph
- The operator can see the duration of an activity and as such distinguish between any interference and real danger

➢ The Waterfall and Persistence graphs
- Both the present and previous measurements at any given time can be displayed
- The displayed time interval (density) is selectable in the range of 2 minutes to 6 hours

➢ Car Tracker Detector mode
- The monitoring of mobile bands can detect signals from GPS trackers hidden within a vehicle

Functions of the software

- Rich visual representation: Spectrogram/Persistence, Waterfall, Alarms graph
- The Known Signals table allows the system to reject TV, FM and other 'friendly' signals while maintaining high sensitivity to unknown signals.
- The Detector and Locator allow the operator to perform location of a bugging device with both visual and audio notification
- The Alarm Threshold decreases the false alarm rate

- The Hold Max Danger feature selects and shows the strongest signals for their location as the system is moved during detection
- The Update Mask procedure allows the operator to quickly adjust the system to the local RF environment in order to reject safe signals
- Sorting and filtering is supported in the Signals table
- The Report function allows the operator to export all obtained information about the desired signals
- Is easily localizable to any language

Working modes

- **Stop / View Log**
  Review of the detection results stored in the log. The Signals table, Spectrogram, Waterfall and Alarms graph give full information about the detected signals and alarm events
- **Update masks**
  Quick preparation for detection – the system automatically accumulates the broadcasting and other safe signals existing in the area in order to pass over them during the subsequent detection
- **RF Sweep**
  The main detection mode. Provides maximum reaction time and the highest sensitivity. The operator can move the system or its antenna during the detection.
- **Guard 24/7**
  Rejection of short transmissions and usage of two antennas reduces false alarms in this mode. Suitable for 24 hour detection without unwanted false alarms
- **Car Tracker Detector**
  Detection of vehicle mounted GPS trackers transmitting the coordinates via mobile networks
- **Probe**
  Checking of AC, Ethernet, Telephone and Alarm wires and the infrared/low frequency for the presence of unwanted bugging signals
- **Wide-Range Analyzer**
  Manual mode for the preliminary study of the RF environment
- **Signal Analyzer**
  Analysis, demodulation and physical locating of detected signals
- **Settings**
  Includes the general settings and information about the mobile networks and wireless bands existing in the area as well as the known signals table

Specification

General

	2000/6 Real-Time	100/12	100/4
Update rate	2000-3000 MHz/sec	100 MHz/sec	100 MHz/sec
Frequency range	40 kHz - 6000 MHz	100 kHz – 12400 MHz	40 kHz – 4400 MHz
Time of detection (Minimal time of signal's existence needed for its detection)	2-3 sec	60-120 seconds	45 seconds
Spectrum resolution	9 kHz	15 kHz	15 kHz
Occupied disk space per 24 hours	12 Gb	1 Gb	0.5 Gb
Temperature Range	0°C to +65°C	0°C to +50°C	0°C to +70°C
Demands on computer	3rd gen. or newer Intel dual/quad Core i-series 1 x USB 3.0 2 x USB 2.0 Windows 7, 8 , 10 13-14" screen recommended	Intel® Atom™ N2600 or Intel® Core™ i3 2 x USB 2.0 Windows 7, 8, 10 13-14" screen recommended	
Displayed dynamic range	-90…-10 dBm		
Displayed spectrum spans	0.5, 1, 2, 5, 10, 25, 50, 100, 200, 500, 1000, 2000, 3000, 6000 MHz		
Spectrum graphs	Spectrogram, Waterfall		
Spectrogram's displayed data	Persistence, Live, Max, Threshold		
Detector's modes	Wide-Range, Signal, Selection		
Fields of 'Signals' table	Frequency, Bandwidth, Name, dbm Level, dbm Peak Level, Danger Level, Peak Danger Level		
Fields of 'Bands' table	Begin, End, Name, Type, Threshold, Priority, Tracker detection		
Fields of 'Known Signals' table	Frequency, BW, Name, Modulation		

ODA-4 omnidirectional antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Is capable of receiving the entire frequency range 40 kHz – 6000 MHz with increased sensitivity in the range of 80 MHz - 4000 MHz
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: BNC
- 80 cm cable
- Dimensions (without tripod) 20 x 3.5 x 0.6 cm
- Mode of use: receive
- Indoor use only

MWA-6 microwave antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Is particularly good for the location of GSM, CDMA, 3G, 4G (LTE, Wi-Max), Wi-Fi 2.4GHz, Bluetooth, Wi-Fi 5GHz, DECT and other digital transmissions
- Frequency range 800-6500 MHz
- Directed (log-periodic)
- Typical forward gain: 6 dBi
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: SMA
- 80 cm cable
- Dimensions (without tripod) 18 x 14.5 x 0.7 cm
- Mode of use: receive
- Indoor use only

MWA-12 microwave antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Is particularly good for locating digital transmissions above 2GHz: 4G (LTE on the upper ranges, Wi-Max), Wi-Fi 2.4GHz, Bluetooth, Wi-Fi 5GHz; For tracing other microwave sources, including bugging devices
- Frequency range 2000-12000 MHz
- Directed (log-periodic)
- Typical forward gain: 8 dBi
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: SMA
- 80 cm cable
- Dimensions (without tripod) 8 x 6 x 0.7 cm
- Mode of use: receive
- Indoor use only

The Multifunction Probe

- Detects electronics emitting an electromagnetic field, infrared signals and illegal signals in 110V/220V wires, Ethernet, telephone, alarm and other low-voltage wires
- 3 channels of detection:
    - IR – infrared (built-in sensor)
    - LF - low frequency (built-in sensor)
    - WIRE - high and low-voltage wires
- Frequency range
    - IR: 40 kHz – 4 MHz
    - LF: 40 kHz – 10 MHz
    - WIRE: 40 kHz – 100 MHz
- WIRE: Max. voltage 250V (Measurement Category II)
- IR: Spectral range of sensitivity: 740 ... 1080 nm
- Direction of sensor:
    - IR: 20°
    - LF: Omni-directed 360°
- Dimensions 145 x 82 x 30 mm
- Connectors: BNC male, IEC C7 socket

- Supplied with a high voltage cable and a low voltage 'alligator' cable

Supplied set

Item		2000/6 Real-Time	100/12	100/4
1.	Main unit with the built-in spectrum analyzer and RF switcher	1	1	1
2.	Software Delta X on the USB flash memory	1	1	1
3.	ODA-4 - omnidirectional antenna	1	1	1
4.	MWA-6 - microwave antenna	1	1	1
5.	MWA-12 - microwave antenna		1	
6.	Multifunction Probe with cables	1	1	1
7.	Coaxial low-attenuation cable 5 m	1	1	1
8.	In-line modular adapter	1	1	1
9.	Tripod convertible to handle	1	1	1
10.	Set of accessories (case's cover lock, angle USB adapters, BNC-to-SMA and SMA-to-BNC adapters)	1	1	1

1 Main unit with the built-in spectrum analyzer and RF switcher

2 Software Delta X on the USB flash memory

3 ODA-4 - omnidirectional antenna

4 MWA-6 - microwave antenna

5 MWA-12 - microwave antenna (supplied with 100/12 only)

6 Multifunction Probe with cables

7 Coaxial low-attenuation cable 5 m

8 In-line modular adapter

9 Tripod convertible to handle

10 Set of accessories (case's cover lock, angle USB adapters, BNC-to-SMA and SMA-to-BNC adapters)

Warnings

The spectrum analyzer's input attenuator and front end switches are sensitive to Electro-Static Discharge (ESD) and have a damage level just above +20 dBm peak. Cases of breakage due to this reason will not be accepted under the product's warranty.

Some common events which may lead to front end damage and the loss of warranty include:

- Applying more than +20 dBm peak power, such as an antenna exposed to a radar pulse or used near a signal exceeding 2 Watts (nonlinear junction detector, transceiver)
- ESD from a passive antenna, either from discharge to an antenna element, or from connecting a large antenna or cable which has built up a static charge
- Connecting to an active antenna which is already powered up

The general recommendations are:

- **Never connect any signals or outputs of active equipment directly into the INPUT connector of the spectrum analyzer**
- **Do not use active antennas**
- **Do not turn on 2-5 Watt VHF/UHF transceivers and NLJD (nonlinear junction detectors) in a close proximity to the antenna**

Startup

Setup

Use a laptop in accordance with the specifications above. Insufficient processing power may result in unstable operation.

- Depending on the computer being used and the Windows version select the appropriate setup file on the supplied USB flash drive and run it:
  - 64 bit: Delta X Setup x64.exe
  - 32 bit: Delta X Setup x86.exe

  The Delta X software and drivers will be installed automatically.

- In case the device driver is not installed properly, it can be set up manually with the help of the Drivers64bit.exe or Drivers32bit.exe files in the Delta X installation folder (Usually C:\Program Files\DigiScan Labs\Delta X or C:\Program Files (x86)\DigiScan Labs\Delta X). Run the file with the administrator rights (Right click on the file | Run with administrator rights)

- Disable all audio enhancements for the playback device in order to allow the Delta X software to produce sounds correctly:
  - Right-click the speaker icon in the system tray (near the clock)
  - Select 'Playback devices'
  - Click the sound device which will be used for playback (typically 'Speakers'), and then click the Properties button
  - On one of the shown tabs find the checkmark responsible for the audio enhancements and disable them. Remove the checkmark if it is 'Enable Audio Enhancements' or set it if you see 'Disable all sound effects'.
  - Click OK.

Preparation of equipment

Before starting the work, to prevent accidental closing of the case's cover insert the lock into the groove near the veil of the case's cover:

- Connect the cables to the corresponding USB slots of the computer in accordance to the color marking on the USB connectors. The blue USB 3.0 plug can be connected to corresponding USB 3.0/3.1 socket only, while the other USB 2.0 plugs can be connected to any type (2.0 or 3.0/3.1).
- Use the angle USB adapters to avoid bending of the cables
- USB 3.0 port is demanded by the '2000/6 Real-Time' version only

The front panel of the Delta X has the following connectors and indicators:

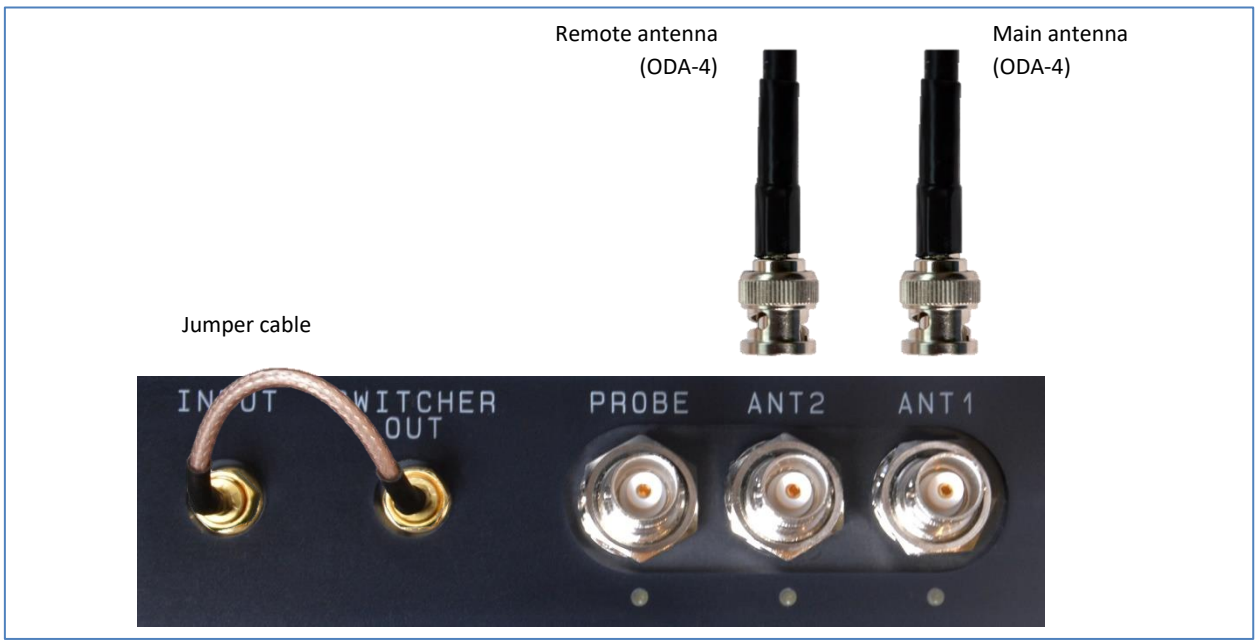
- **INPUT** – the input of the built-in spectrum analyzer. In most working modes the omnidirectional antenna ODA-4 and directed microwave antenna MWA-6 should be connected to this socket directly. In the Probe mode and the Guard 24/7 mode with 2 antennas this socket should be connected to the 'SWITCHER OUT'
- **SWITCHER OUT** – output of the RF switcher
- **PROBE** – input for the Multifunction Probe which should be connected with the help of the 5m extension cable supplied in the set
- **ANT 1** – input for the main antenna in the Guard 24/7 mode with the 2-antenna algorithm
- **ANT 2** – input for the remote antenna in the Guard 24/7 mode with the 2-antenna algorithm
- **ALARM** – indicator of a high alarm level and the relay output (normally open, max. voltage 25 V).

Connection of the antenna depends on the working mode:

- **Wide-Range Analyzer, Signal Analyzer, RF Sweep, Guard 24/7 with 1-antenna**

- **Probe**

- **Guard 24/7 (2-antenna algorithm)**



Placement of antennas

The recommended way of the antenna's placement is mounting them to the upper part of the case with the use of supplied screws. When using this method the operator can easily move the Delta X system during detection and locating:

The ODA-4 antenna

The MWA-6 antenna

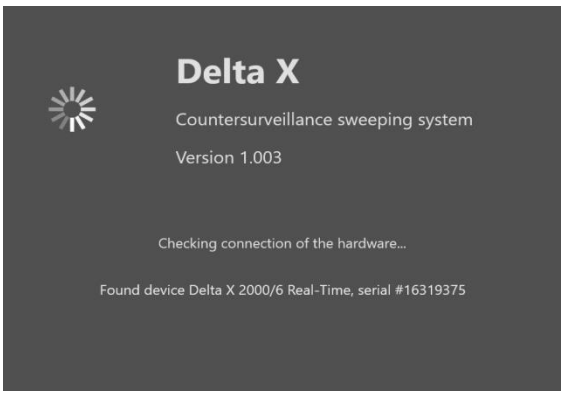
Both the omnidirectional antenna ODA-4 and directed microwave antenna MWA-6 can be mounted simultaneously and connected to the INPUT in turn depending on the needs.

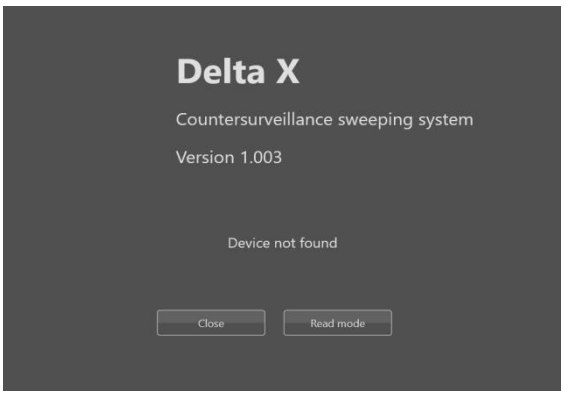
During the locating procedure the operator might need to keep the antenna in hand to probe objects and hard-to-access places more closely. For this the antenna can be mounted on the supplied tripod which easily converts to a handle.

When the Delta X systems is used in a fixed position (Guard 24/7 mode) the antenna can be mounted on the tripod.

Running the software

Start the Delta X software. The Startup window will appear on the screen and the procedure of finding the connected hardware will be performed.





In case of detecting the Delta X equipment the ‘Found device’ will appear and the main window will open.

If there is no connection, there will be a ‘Device not found’ message. The software can be closed or run in the Read mode for reviewing the logs and changing settings.

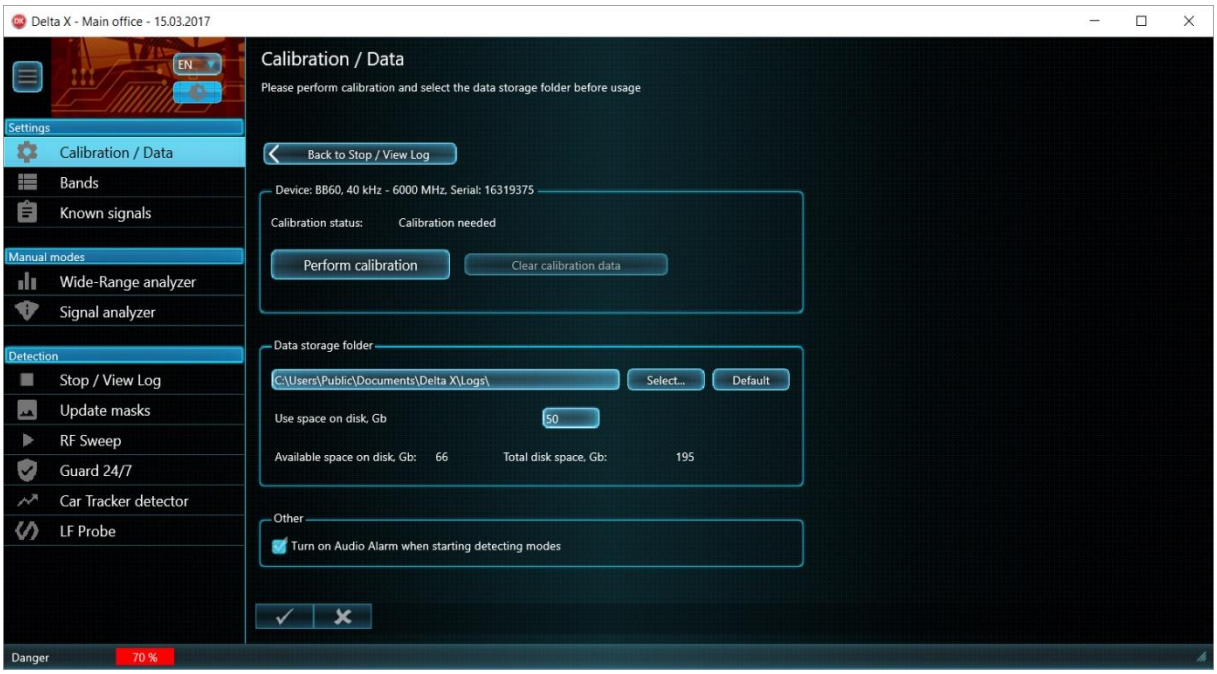
Settings

When the software is started for the first time, some required settings are missing. The application will ask the operator to perform calibration and fill the 'Bands/Known signals' tables by entering to the Settings automatically.

The settings should be changed in the following cases:

- Calibration should be performed once, for the first time
- Bands should be set individually for each country, state or region (area)
- Known signals should be set individually for each country, region (area) and city

Calibration / Data



Calibration is needed for the compensation of the changing dynamic range on different frequencies, thus making the spectrum traces smoother and more understandable.

Perform the calibration once on each computer the system is being used on.

Disconnect the antenna or cable from the spectrum analyzer's RF input (marked as INPUT) and press the **Perform calibration** button. The procedure will finish in a few minutes. The antenna should then be connected again.

If necessary, the **data storage folder** can be changed. In the case of changing the data storage path after using the system, it is recommended to manually delete the previous folder to free up disk space.

The **'Use space on disk'** allows the operator to limit the space occupied by the logs. After reaching the limit the Delta X software will automatically delete the older logs when it is in detection mode.

Take into consideration the occupied disk space per 24 hours of detection:

	2000/6 Real-Time	100/12	100/4
Occupied disk space per 24 hours	12 Gb	1 Gb	0.5 Gb

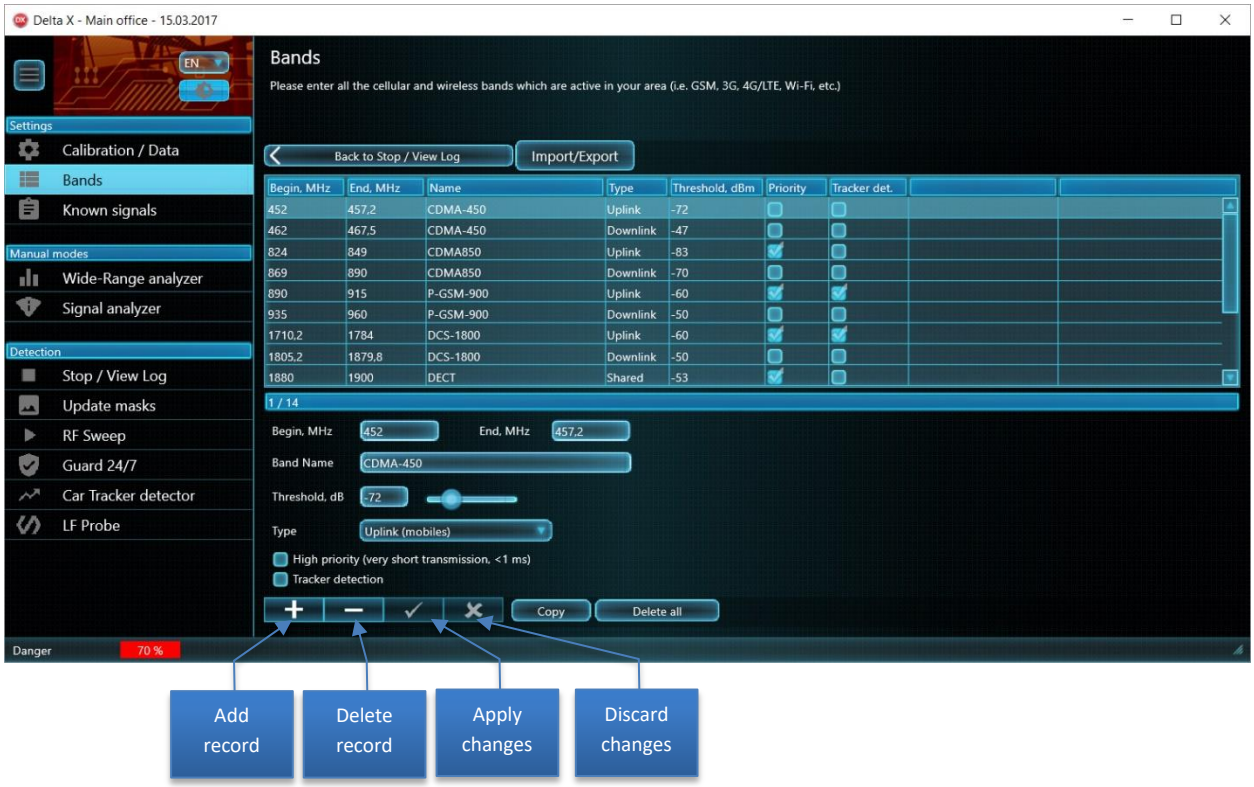
If you are planning to use the Delta X system in the Guard 24/7 mode, we suggest selecting a laptop with an increased disk space. To speed up the data writing and reading we suggest using a high speed SSD.

Please note that the logging of data during the detection may be suspended if the selected disk does not have enough free space.

With the **'Turn on audio when starting detecting modes'** on, the software will activate the Audio alarm function automatically each time the detection is started.

Bands

The Bands table contains information about the mobile and wireless bands existing in the country or region of use.



The software handles mobile and wireless bands in a special way, significantly decreasing the quantity of unwanted signals and simplifying the detection process. Therefore, the information in the table is very important for the correct operation of the system.

The mobile networks and wireless bands can be divided into the following groups:

- GSM
- CDMA/3G
- 4G/LTE
- Wireless bands and DECT

The bands can be entered and edited manually, but it is recommended to use the Import/Export function to quickly import already prepared data. The Delta X system is supplied with the data files already prepared for specific countries and the data files containing the general lists of mobile and wireless standards allowing the operator to adapt the system to any country manually.

Import of existing data file

If a country data file is present, it is recommended to use it:

1. Make sure the Bands table is empty (press the Delete All button if necessary)
2. Press the Import/Export button
3. Press the File button
4. The 'Open File' dialog box will be in the folder with the data files
5. Select the file corresponding to your country. The file's name should be of the following format: '[country] Bands'. For example, for the USA the file's name will be 'USA Bands'.
6. Open the selected file
7. Press the '<<' button to import all records
8. Press the Import/Export button to leave the import mode

Creation of the data file for your country

If there is no data file for your country, use the files listing the mobile and wireless standards and import the bands which are used in your country.

The following files are supplied with the system: 'GSM Bands', 'CDMA Bands', '3G Bands', '4G LTE Bands' and 'Wireless Bands'.

Gather information about the mobile standards and bands used in your country from the internet or by contacting the corresponding authorities and import the necessary bands into the Delta X software.

Below is an example of creating the Bands table for Poland. The internet mentions the following information about the mobile standards used in Poland:

GSM	UMTS (3G)	4G/LTE
900 (E-GSM)	Band 1 (2100)	Band 1 (2100)
1800 (DCS)	Band 8 (900)	Band 3 (1800+)

1. Clear the Bands table by pressing the Delete All button and press the Import/Export button
2. Press the File button and open the 'Wireless Bands' file. Import the 'DECT', '2.4 GHz Wi-Fi' and '5GHz Wi-Fi' bands by pressing the < button:

3. Open the 'GSM Bands' file and import the 'E-GSM' Uplink/Downlink bands and the 'DCS-1800' Uplink/Downlink bands:

4. Open the '3G Bands' and import the 'Band 1' Uplink and Downlink. It is also necessary to import the 'Band 8' Uplink and Downlink but since they completely coincide with the already existing 'E-GSM-900', rename the 'E-GSM-900' to 'E-GSM-900, 3G'. Rename both the Uplink and Downlink:

5. Open the '4G (LTE) Bands'. Since the '4G/LTE Band 1' coincide with the '3G Band 1', rename the existing '3G Band 1' to '3G/4G Band 1'. Rename both the Uplink and Downlink.
Since the '4G/LTE Band 3' coincides with the existing 'DCS-1800', rename the existing band to 'DCS-1800/4G Band 3' (both downlink and uplink). Adjust the frequency edges slightly to include both the 'DCS-1800' and '4G Band 3':

6. Press 'File' and enter 'Poland Bands' to create a new file. Then, export all the records using the >> button.

Press the 'Import/Export' to leave the mode. Now, all the collected band data for Poland is stored in the external file and is available for future use.

In case of using the Delta X in another country, the Band table's records can be quickly imported from the corresponding country data file or from the files containing all bands for each standard.

Description of the Bands table

The **Begin** and **End** fields are the edges of the band.

The **Name** field is obligatory and should be unique for each pair of bands, consisting of uplink and downlink.

The **Threshold** is the level which, when exceeded by a signal, makes this signal 'dangerous' and produces the alarm.

There are the following **types** of bands:

- **Uplinks:** Used by mobile devices for sending information to base stations
- **Downlinks:** Used by base stations for sending data to the mobile devices
- **Shared frequency**: The band is used by both sides of communication simultaneously. This technology is used by some 4G/LTE bands, Wi-Fi, Bluetooth, ZigBee and DECT.

The main task of the system is monitoring the uplinks and shared bands since they are used by potential bugging devices for transmitting. Therefore, the threshold for the 'uplinks' and 'shared' should typically be lower than for the 'downlinks' to provide a higher sensitivity. The parameter can be adjusted later in the working modes.

The **High Priority** parameter should be set for the upli

nk bands of the standards which have short transmission time or timeslots. These are GSM, 3G, 4G, DECT and Wi-Fi. When fetching the spectrum trace, the Delta X system measures the priority bands longer in order to capture the short bursts.

The **Tracker Detection** parameter should be set for the uplinks of the mobile networks so they are scanned in the Car Tracker Detector mode.

Manual editing

If manual editing in the Bands table is needed, use the corresponding **navigation buttons** to add and delete records, apply and discard changes.

There are the following rules for bands:

- Both the uplink and downlink bands should be imported or created according to the mobile standard
- Do not create nor import the bands which are absent in your country/state
- No empty records are allowed
- No empty names are allowed. At least a short description should be assigned to each pair of bands.
- No repeating of names
- Uplink and downlink's names for the same band should coincide
- The bands cannot overlap. In case of overlapping they should be combined in one record. For example, if 2 bands 1700-1750 MHz and 1700-1770 MHz are used in your country, they should be combined in one band 1700-1770 MHz.

Known signals

The Known signals table contains the signals of FM and TV broadcasting, as well as the other continuously existing signals in your area: VHF/UHF channels, police/fire/municipal, trunking, etc.

Advantages of using the Known signals table:

- Fewer false detections
- Higher general detection sensitivity
- More information for the operator

The software decreases the danger level of the known signals so they do not create unwanted alarms. As a result, weaker but potentially dangerous signals can be detected easier. Additionally, the known signals are automatically marked, so that the operator can distinguish between the known 'friendly' signals and unknown, potentially dangerous, signals.

Therefore it is strongly recommended to fill the Known signals table before starting work.

The Known Signals table is opened automatically after the software starts if it is empty.

Import of TV frequencies

The frequencies of the TV broadcasting channels do not change across the country. Therefore they can be easily imported from the supplied external files. There are some formats of video signal. For each format there is a separate data file. The data file's name describes the video format and what countries it is suitable for.

When importing, select the file which corresponds to your country. If during further work you observe the captured TV signal is not marked as 'known' (without a name), this can mean use of the incorrect data file, not suitable for your country.

To import the external data file:

1. Press the Import/Export button
2. Press the 'File' button. The Open File dialog box will be in the folder containing the corresponding data files
3. Open the data file corresponding to your country
4. Press the << button to import all the signals:

5. If the VHF and UHF channels for your country are stored in separate files, repeat the same action for the both files (open and import)
6. Close the data file by pressing the Import/Export again.

List of the data files supplied with the Delta X:

VHF television channels
TV VHF B 625 - Western Europe, Greenland and most countries in Asia, Africa and Oceania
TV VHF D 625 - Eastern Europe and Former Soviet Union
TV VHF L 625 - France

UHF television channels
TV UHF D,G,H 625 - Western Europe, Greenland, most countries in Asia and Africa, and most of Oceania
TV UHF I 625 - United Kingdom, Ireland, Hong Kong, Macau, Falkland Islands and Southern Africa
TV UHF K,L 625 - France, Eastern Europe, Former Soviet Union, French overseas territories and former French colonies in Africa

VHF+UHF television channels
TV VHF, UHF M525 and N625 - Americas, Caribbean, Taiwan, South Korea, Philippines
TV Digital ATSC - USA

Removal of unused TV channels

In each particular area not all of the TV channels are used simultaneously. If a bugging device's frequency coincides with the TV signal it will be assigned its name in the Signals table. Despite the fact that the Delta X will assign a high danger level to such a signal, the operator may be misled by the fact that the signal is 'known'. To avoid such situations the TV channels which are not used in the area can be removed from the Known Signals table.

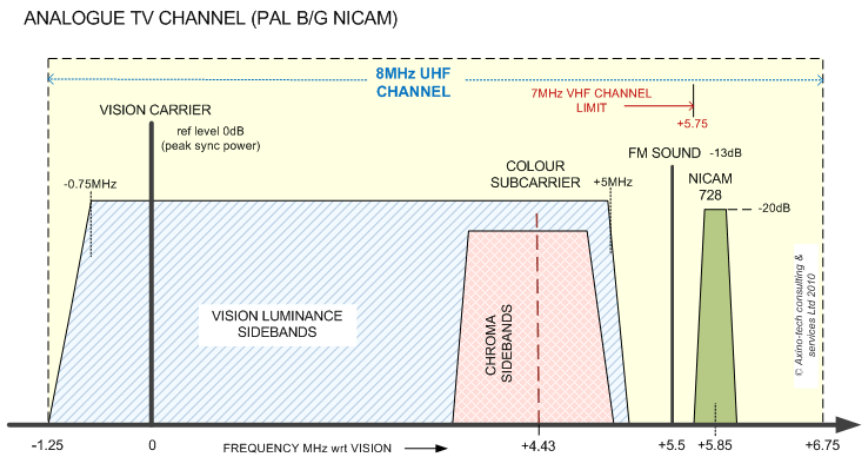
After all the TV channels are imported, it is possible to scroll through them, observe the activity on the spectrogram and remove the non-active ones. The spectrogram can be seen when the spectrum traces are obtained in advance and with the Import/Export mode closed.

1. Position the antenna near the window or outdoors to provide the best reception and update the spectrum in the Wide-Range Analyzer or RF Sweep mode a few times
2. Enter the Known Signals table again
3. Scroll through the imported TV signals while observing their spectrum in the spectrogram on the right and delete the records with empty spectrums
4. If a DTV signal is observed (one wide carrier instead of 2 video and audio carrier), remove the audio carrier and widen the video carrier so it covers the full bandwidth of the signal as described below
5. The existing records can be exported to a data file for further use in this specific area. Assigning a name describing the area is recommended. For example: 'Miami signals'.

Additionally, some 'upper' TV channels might be reassigned for the mobile communications in some countries. Therefore it is recommended to compare the imported TV channels with the Bands table and remove the records which overlap with the bands.

Analog and digital television

An analog TV signal consists of 2 carriers – video and audio, as shown in this illustration of PAL signal's spectrum below:

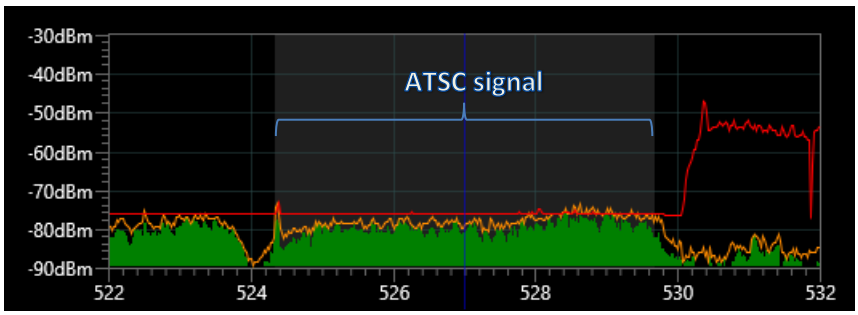


Therefore the external data file for the analogue TV system contains a pair of signals for each of the TV channels.

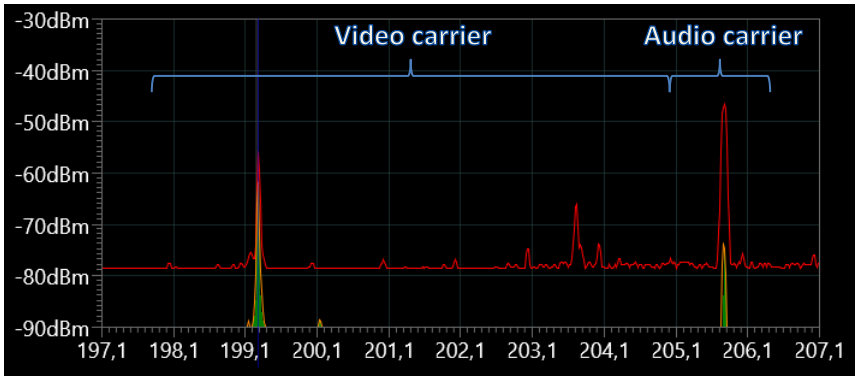
Since Digital Television (DTV) has become more widely used in many countries, some of, or all analog TV signals consisting of a pair 'video + audio carrier' are substituted with the modern digital signals occupying the entire bandwidth with one solid carrier. If you are observing the digital spectrum, the corresponding record in the Known Signals table should be modified:

- The audio carrier should be removed
- The video carrier should be widened to correspond to the bandwidth of the signal

Below is an example of a digital TV signal in the ATSC format (USA, channel 23):



The analogue TV signal (Eastern Europe, channel 9):



FM broadcasting, VHF/UHF communications and manual editing

Unlike the video and audio channels of TV broadcasting (which can be imported from the file quickly), the FM broadcasting stations and VHF/UHF channels will vary depending on the city and area, therefore it is recommended to capture them using the Wide-Range Analyzer manual mode, then to study and add to the Known Signals table in the Signal Analyzer mode. It is also possible to add and edit the known signals right in the Known Signals table using the navigation buttons: **Add record**, **Delete**, **Apply**, **Discard** and **Copy**.

The **frequency shift (+MHz)** allows the operator to create a copy with a shifted frequency. This is useful for creating lists with fixed channel spacing (TV frequencies for example).

Rules for editing the known signals:

- No repeated names
- No empty names
- The starting frequency F1 should be less than the ending frequency F2
- The bandwidth cannot be 0
- No signals overlapping with the records already in the Bands table

The known signals can be exported for subsequent use. If the Delta X is periodically used in different locations, a set of external files will help to quickly re-adjust the system each time the location is changed.

The **Show As** defines the representation of signals in the table. In the 'Central frequency and bandwidth' mode it is convenient to work with the signals having a symmetric spectrum, i.e. FM stations, VHF/UHF stations, audio signals of TV broadcasting, etc. In the 'Start and finish frequency' mode it is convenient

to work with the TV video signals since their carrier frequency is not positioned in the center of the bandwidth.

When not in the import/export mode the right side will contain the **Spectrogram**. It will show:

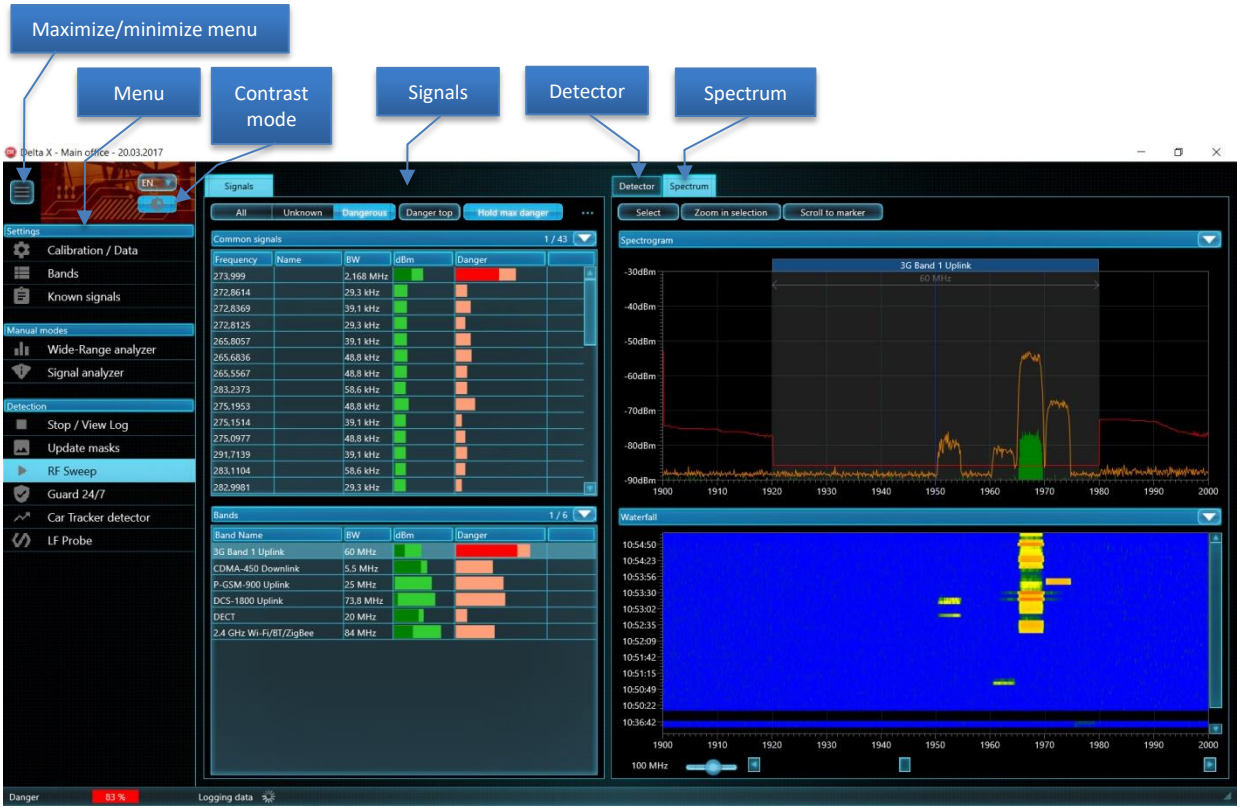
- Green and orange - the Live and Max traces
- Blue - the mask of a known signal

The spectrogram will display the updating Live and Max traces if the software is not in the Stop / View log mode.

The buttons above the spectrogram allow the operator to work with the masks: Update, Clear and Clear All. The masks are updated from the spectrum's maximums, displayed by the color orange.

Please read the Update Mask section for more details.

Controls and elements



Menu

The menu on the left side allows the operator to select the working mode. The menu can be **minimized and maximized** with the help of the button in the top left corner.

The **contrast mode** allows the operator to select the convenient color scheme of the application. By default, the high contrast mode is selected.

The current working mode stays active when the software is in Settings so some changes can be made without interruption of the current operation.

Status

The bottom 'Status' line shows the general danger level, status of logging data, errors and warnings.

Signals

The Signals table contains the detected signals. They are selected from the spectrum traces and inserted into the table automatically when the software is in the following modes: RF Sweep, Guard 24/7, Car Tracker Detector and Wide-Range Analyzer.

There are two sections in the table: Common signals and Bands.

When the system detects activities within a mobile/wireless band, they are inserted into the Signals as a band. Other activities appearing outside the bands are inserted as common signals.

Each signal consists of the following fields:

- **Frequency** – central frequency (not displayed for bands)
- **Name** – is displayed if a common signal is present in the Known signals table or **Band name** – name of a band
- **BW** – bandwidth of a common signal or band
- **dBm** – current dBm level (green bargraph) and Peak dBm level (light green bargraph). The level is measured in the range of -90 dBm (low) … -10 dBm (high)
- **Danger** – the current danger level (red bargraph) and the peak danger level (light red bargraph). The danger level appears when a signal exceeds the threshold and is measured between 0% and 100%. The danger reflects the strength and the bandwidth of a signal simultaneously.

Double-click (or press Enter) on a signal (common or band) to see its spectrum. The displayed frequency span of the spectrum graphs (Spectrogram and Waterfall) will be changed to show the signal's bandwidth fully. If the Detector is in the Signal mode, it will be assigned to the signal.

A **Click** on a signal shows it in the spectrum graphs without changing the displayed span, i.e. just scrolls to the signal. If the Detector is in the Signal mode, it will be assigned to the signal.

The **signal filtering** button allows the user to quickly select the desired signals:

- All – all signals are shown
- Unknown – only the signals absent in the Known Signals table are shown
- Dangerous – the signals with a Peak Danger of more than 0% are selected

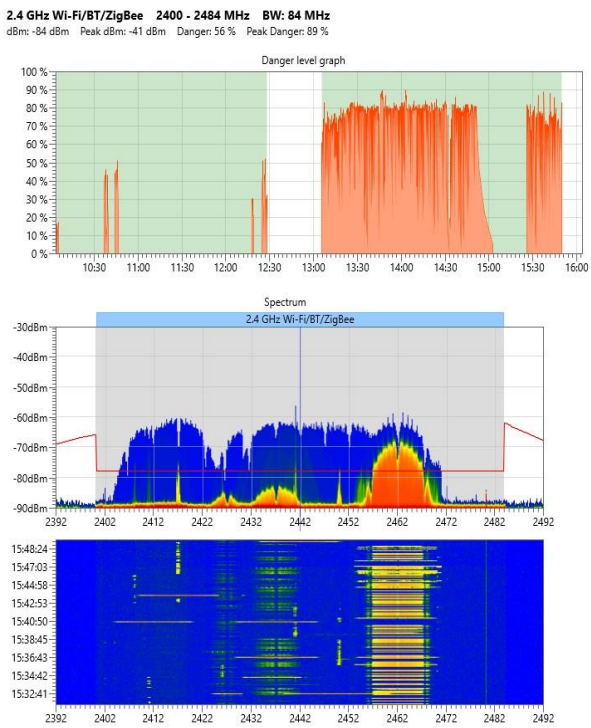
The **Danger top** button quickly adjusts sorting of the most dangerous signals to the top.

The **Hold Max Danger** function automatically tunes in the most dangerous signals during detection so that the spectrum graphs and the Detector start showing the signal. Since the Detector allows the operator to carry out the locating procedure, the function is convenient for simultaneously detecting and locating. The system is moved during the detecting (RF Sweep mode). As soon as a signal is found the Detector will instantly show the danger level changing depending on the distance.

<u>The Hold Max Danger function should be deactivated when it is necessary to scroll to and review other signals from the Signals table or other frequency ranges on the spectrum graphs. Otherwise the function will forcibly tune into the most dangerous signal again while readjusting the spectrum graphs correspondingly.</u>

The **popup menu** contains the following controls:

- **Clear Signals** – deletes all the signals from the Signals table. This function is accessible in the Wide-Range analyzer, Signal analyzer and in the Stop / View log mode.
  As standard, when you work with a log, each new launch of detection continues updating signals collected during the previous sessions. If the Clear Signals is pressed in the Stop / View Log mode the next detection will start from the empty table. If the Clear Signals is called from a manual mode (Wide-Range Analyzer or Signal Analyzer), the signals will be deleted from the memory temporarily and loaded again in the Stop / View log mode or when starting a detecting mode.
- **Report On Signal** allows the operator to generate a report on the currently selected signal and save it into a .bmp or .jpg file. Before calling this function select the desired signal and adjust the spectrum graphs if necessary (set span, density and representation mode). The report will include the textual and graphic information. Below is an example of report on a Wi-Fi signal:



- **Show values** turns on the showing of extra columns in the Signals table with the text values of dbm and danger level

The **field's headers** are used for sorting the signals. Subsequent clicks on a field's header sorts the signals in an ascending and descending order. The subsequent clicks on the dBm and Danger firstly sort by the current level (darker color) and then by the peak level (lighter color).

The common signals and bands are sorted simultaneously not depending on which header was clicked.

The **toolbar for the common signals** is shown and hidden when the section's header is clicked. It contains the following controls:

- Labels with the central frequency and name
- **Delete** – erases the current common signal
- **Add to known** – adds the current common signal to the Known Signals table. Please make sure that the signal which you are adding is safe. Signs of safety are: 1) the signal is present in different parts of city or areas; 2) the level does not rise sharply in a certain part of the premises; 3) the demodulation explains what information is being transmitted; 4) it is in the list of frequencies used by police, fire or emergency service; 5) it is in the list of FM stations for the area.
- **Update mask** – re-updates the mask of the selected known signal (please read below).

The **toolbar for the bands** is shown and hidden when the section's header is clicked. It contains the following controls:

- The **Name** of the selected band
- The **current dBm level** of the selected band

- The **threshold** for the selected band (please read the 'Test detection and adjustment of thresholds' on page 42)

Updating masks of separate known signals

What is masking?

When a signal exceeds the threshold it becomes dangerous. The threshold for the masked signal lays higher than the signal and therefore is not exceeded. As a result the masked signals do not produce danger events. The Delta X uses masking to avoid alarms from broadcasting and other safe signals.

Some known signals may become dangerous despite the fact they are masked. This can happen in areas with a good reception of broadcasting - on upper floors, in buildings facing TV towers, etc. Re-updating of a separate signal's mask changes the threshold so the signal stops being dangerous.

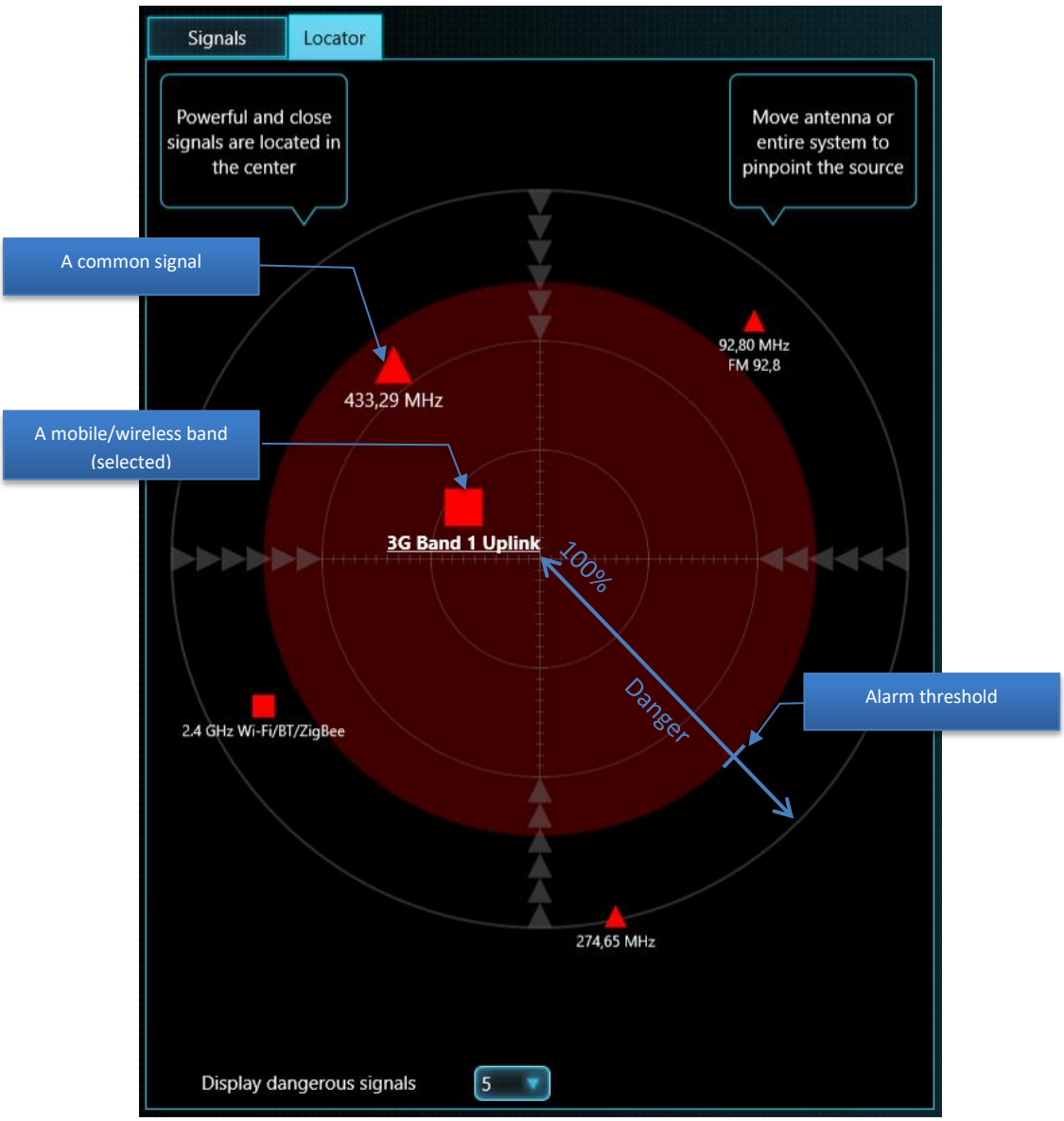
The re-updating of the mask can be done in the following modes: Wide-Range Analyzer, Signal - Analyzer, RF Sweep and Guard 24/7. If the operation is made in the target area, firstly make sure the known signal has no signs of another signal hidden within it. Inspect the known signal in the Spectrogram and Waterfall. Use the Persistence rendering mode. If the spectrum changes its form significantly, do not update the mask.

Locator

The Locator is a new feature introduced in version 1.1 of the Delta X. The Locator significantly simplifies the process of tracking the results of detection and the physical locating of transmitters.

While the Signals table lists all registered signals, including the non-active ones, the Locator displays the currently active dangerous signals only. The position of a signal on the Locator's circle is selected depending on the level of danger. Strong and close signals, with a danger level near 100%, are situated in the center, while weaker and further signals with a low level of danger are positioned near the outer edge.

Thanks to the visual ranking of the signals the operator can easily distinguish between close and far sources. As the Delta X system or its antenna is being moved the approached RF source is displayed closer to the Locator's center so that the operator can easily pinpoint it.



A mobile or wireless band is displayed by a red square, while a common signal – by a red triangle.

The signals which exceed the alarm threshold and get into the red zone are drawn by a bigger shape (please read about the alarm threshold in the next section - Detector). The signals below the alarm threshold are drawn smaller.

Display dangerous signals allows the operator to set the desired quantity of displayed signals.

Click onto the signal to select it in the Signals table and show it on the spectrum graphs. The currently selected signal is drawn underlined in the Locator. Please bear in mind the 'Hold Max Danger' function, which automatically re-selects the most dangerous signal when active.

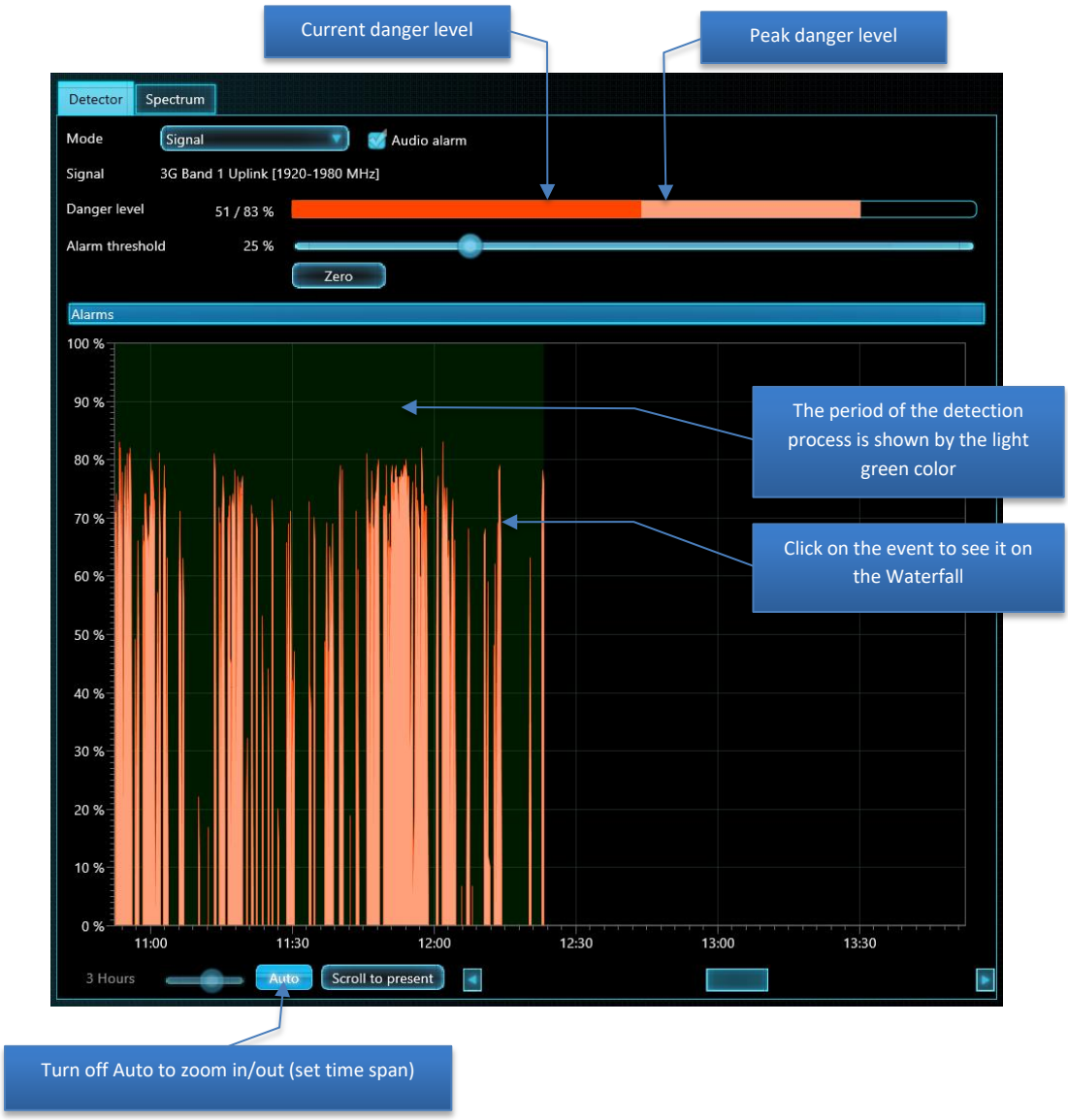
The Locator function can be engaged in any working mode. In the RF Sweep, Guard 24/7 or Car Tracker Detector mode it will display a number of dangerous signals simultaneously, while in the Signal Analyzer mode it only shows the currently selected signal. This function can also be used in the Stop / View Log mode to see how strong the signals were during detection.

Using the Locator in the Signal Analyzer mode for physical locating of the transmitter is strongly recommended. The physical locating is performed by scanning the area with the antenna and finding the place with the strongest danger level, i.e. when the signal is centered in the Locator.

Detector

The Detector is created for informing the operator about the detected danger events and locating the transmitter. It shows the current level of danger on the bargraph and notifies the operator with the audio alarm. In addition the Detector displays the history of the danger events on the Alarms graph.

The physical locating of the transmitter is performed by finding the place with the highest danger level (both the Locator and Detector can be used at the same time). The audio alarm function produces proportional sound when activated.



The Detector can work in 3 modes: Wide-Range, Signal and Selected range.

In the **Wide-Range mode** the Detector monitors all signals simultaneously. The operator can keep an eye on the general RF situation existing in the area by watching the bargraph and listening to the audio

alarm. When a new dangerous signal appears, the Detector will warn immediately. Use the Locator to observe the danger level of separate signals.

In the **Signal mode** the Detector displays the danger level of a particular signal which is currently selected in the Signals table (whether common signal or band). This mode can be used during the locating procedure, or for studying the history of a separate signal.

In the **Selected range mode** the Detector displays the danger level of a frequency range selected in the Spectrogram. This mode can be used for physical locating of:

- hopping signals thanks to the ability to monitor a number of channels at the same time;
- narrow signals existing within a mobile/wireless band, for example, Bluetooth or Zigbee

When the **Audio alarm** is on and a danger event is detected, the Detector will produce the warning clicking sound. The intensity of clicks is proportionate to the level of danger. This function is used for the physical locating of the transmitter.

The **Alarm threshold** allows the operator to adjust the level at which the Audio alarm starts producing sound. The alarm threshold helps to avoid false alarms occurring from the insignificant changes of safe signals' spectrums and is convenient during the physical locating (localizing) procedure. The default value is set to 25% in all the detection modes, except the Car Tracker Detector, where it is 10%.

The increase of the alarm threshold is helpful during physical locating since it decreases the area around the transmitter where the alarm audio appears. Increase the threshold step-by-step in order to outline the location of the transmitter.

The **Zero** button allows the operator to quickly set the audio threshold equal to the current level of danger and as such reject all weaker values. It can be also useful during the physical locating procedure.

The **Alarms graph** displays the history of the danger events:

- The **Time Span** adjustment allows the operator to select the displayed time span, when the Auto is off. The time span can also be selected with the help of the mouse wheel or by the standard gestures "Pinch" and "Spread" on the touchpad or touchscreen
- The **Auto** button automatically adjusts the time span so that all the logged danger events are displayed
- The **Scroll to Present** button scrolls to present time
- The **scrollbar** allows the operator to scroll in time in order to see the events at any desired moment (when the Auto is off).

Clicking on the Alarms graph works differently depending on the working mode of the Delta X:

- In the Stop/View Log mode a click scrolls the Waterfall to the corresponding time, loads and displays the corresponding trace on the Spectrogram and shows the dBm and Danger levels in the Signals table which existed at the moment of clicking. The Locator will show the dangerous signals which existed at the moment of clicking.
- In all other modes a click just scrolls the Waterfall to the corresponding time

Spectrum

The Spectrum page displays the graphs responsible for visual representation of spectrum:

- The **Spectrogram** in the upper part renders the frequency on the horizontal axis and the dBm level on the vertical axis.
- The **Waterfall** in the bottom part shows how the spectrum is changing in time. Its horizontal axis is the frequency, the vertical is the time and the color of pixel reflects the dBm level.

Spectrogram

The **Spectrogram** can display the following data:

- Persistence - a way of rendering the traces with color depending on the continuity (persistency) of the signal. Please see the description below.
- Live – the current trace, obtained during the last update. Shown by green color.
- Max – the maximums accumulated during the current operation. Shown by orange color
- Threshold – the reference trace used by the detection algorithm for the selection of signals from the trace and estimating their level of danger. Is shown by red color

A **click** on the Spectrogram when in the Signal Analyzer mode allows the operator to tune in the desired frequency. The **marker** (vertical line) will show the selected frequency. When the graph is scrolled to another range and the marker is not visible, the **Scroll to marker** button goes back to it.

The Spectrogram allows the user to make a **selection** with the help of the left mouse button. It is possible to zoom into the selection with the help of the **Zoom in selection** button. Thus, a desired frequency range can be quickly viewed. Please note, that when the signal is double clicked in the Signals table the selection of its bandwidth in the Spectrogram is made automatically.

The **displayed frequency span** can be selected with the help of the corresponding control. It is possible to select the convenient value of between 0.5 MHz and 6000MHz. The span of the spectrogram and waterfall is selected simultaneously. The span can also be selected with the help of the mouse wheel or by the standard gestures "Pinch" and "Spread" on the touchpad or touchscreen.

The **frequency scroll** allows the selection of the desired frequency range. The Drag gesture over the Spectrogram can be used on touchscreen computers.

In some cases the displayed span and scroll will be selected automatically:

- When a signal is double clicked in the Signals table
- When the Hold Max Danger function is activated and a more dangerous signal is detected

The **band labels** display the edges of the mobile and wireless bands which exist in the Bands table and get into the displayed frequency range.

The **toolbar for the Spectrogram** can be shown and hidden by a click on the Spectrogram's header. It contains the following controls:

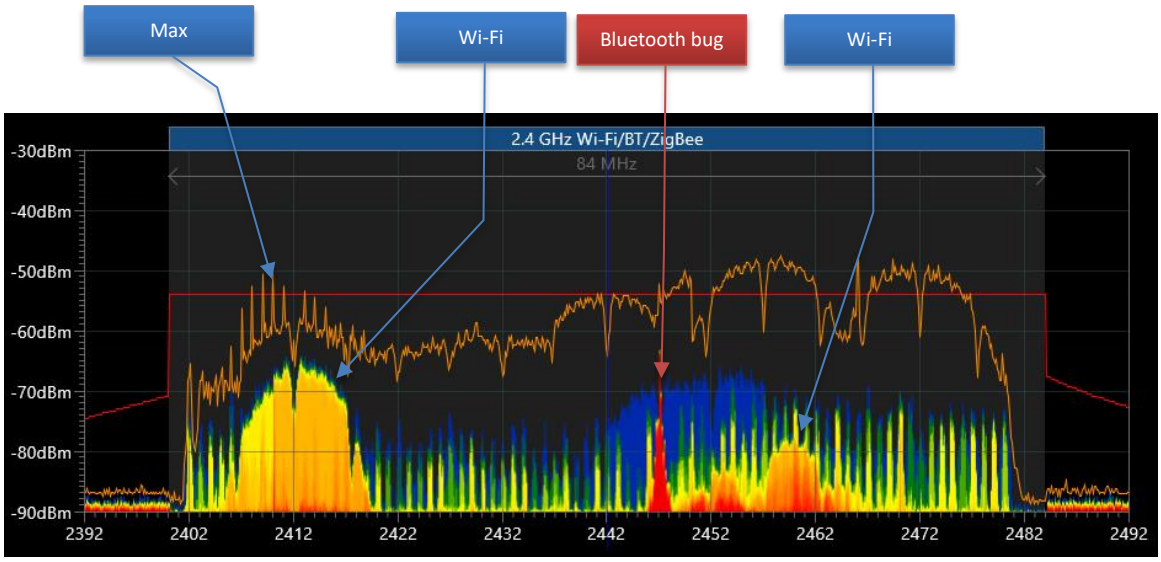
- Setting of the **Persistence**, **Live, Max** and **Threshold**
- The **Max clear** button is available in the manual modes
- The **Dynamic range** selector. The higher selection -90…-10 dBm allows the user to observe strong signals better, the moderate -90…-30 dBm suitable for most tasks, while the lowest -90…-50 dBm is suitable for viewing the weakest signals.
- The **Color scale** displays how the color in the Waterfall depends on the dBm level and the color in the Persistence depends on the activity of signal. The Color scale changes as the Point of Yellow is adjusted.
- The **Point of Yellow** sets the dBm level to be displayed by yellow in the Waterfall and the level of activity to be displayed by yellow in the Persistence

Persistence

The Persistence is the way of rendering the spectrum with color depending on the activity of the signal, i.e. how frequently it exists. As such the operator can distinguish between permanent and intermittent signals. The rare intermittent signals are drawn in blue or green color, whereas more permanent signals are shown in yellow or red.

A great advantage of the Persistence is that it allows the operator to recognize constant signals hidden under intermittent signals.

Below is an example of finding a Bluetooth bugging device hidden under the Wi-Fi signal:



The Max trace contains the maximums accumulated from the intermittent signals during a long period of time and therefore cannot be used for visual recognition of a hidden signal with a lower level. At the same time the Persistence clearly shows in red the 2447 MHz signal with more frequent existence than a blue and yellow Wi-Fi signal 'behind' it.

The Persistence uses multiple spectrum traces taken from the Waterfall; therefore the Waterfall's view and settings influence the Persistence.

The Point of Yellow controls the colors in the Persistence.

As a standard, the green 'Live' trace is displayed filled. When the Persistence is activated, the filling of the Live goes off and the trace is displayed just by a stroke.

Waterfall

The **Waterfall** displays the multiple traces obtained during a specified span of time and is extremely valuable for the detection of intermittent signals.

During detection the Waterfall displays the information accumulated in the log and scrolls as a new measurement is performed. In the Stop / View Log mode the waterfall displays the information stored in the log. In the manual modes (Wide-Range Analyzer and Signal Analyzer) the Waterfall temporarily accumulates data for the displayed frequency span.

The **density** regulates the time span displayed by the Waterfall. The density may vary between 'one trace per 10 pixel lines' up to '10 traces per one pixel line'.

When the data is loaded from the log in the detection modes or in the Stop / View Log mode a higher density setting may cause significant disk reading and a large processing of data. Therefore fetching may take longer, particularly when a wide displayed span is selected. Try to avoid maximum density with the simultaneous wide span to achieve optimal performance. After using a high density return a low value.

When in the Stop / View Log mode a **click on the waterfall** allows the user to upload and view the corresponding trace in the Live. The Signal table will display the dBm and Danger values which existed at the clicked moment.

The **time scroll** allows the operator to select the desired time shown by the waterfall. It is also possible to select the time by clicking on the Alarms graph in the Detector. Please note that when the Waterfall is scrolled to an older span of time, it does not update with a new trace received from the spectrum analyzer. Scroll to the current time in order to restore the updating.

The **color scale** near the Spectrogram allows the operator to see how the color of the Waterfall's pixels depends on the dBm level. The **point of yellow** can be shifted up in order to hide weaker signals or background noise in the Waterfall. A further increase of the yellow point will hide signals of an average level. Shifting the yellow point down will show weaker signals.

Manual modes

Wide-Range Analyzer

This mode can be used for:

- Capturing signals existing in the area in order to store them in the Known Signals table
- Test detection and adjustment of thresholds

In the Wide-Range Analyzer mode the software analyzes the entire RF spectrum, recognizes the signals and inserts them into the Signals table. The signals can be further analyzed in the Signal Analyzer mode and, when necessary, stored in the Known signals table.

The fetch time of a spectrum trace depends on the version of the system being used:

Delta X 2000/6 Real-Time	Delta X 100/12 or 100/4
1.5-3 second	1-2 minutes

Antenna connection: connect the omnidirectional antenna ODA-4 directly to the INPUT socket

Capturing known signals

Both known and unknown signals are masked during detection thanks to the Update Mask procedure. Despite this the filling of the Known Signals table has certain advantages:

- Separate known signals can be re-masked manually during the detection to reduce false alarms. The unknown signals cannot be re-masked during the detection process
- The known signals can be hidden using filtering, so more attention is paid to the unknown suspicious signals
- The operator can visually distinguish between known and unknown signals

When the system is constantly used in the same area, filling of the Known Signals table is strongly recommended.

After the first starting of the software, the Known Signals table is empty. While the TV channels can be imported from the data file, the FM, VHF/UHF and other frequencies constantly existing in the area should be captured and entered to the Known Signals table manually.

Typically the sequence of actions is as follows:

- Import of TV channels to the empty Known Signals table
- Capturing signals in Wide-Range Analyzer
- Adjustment of the dBm threshold for bands
- Studying the captured signals in the Signal Analyzer mode and adding them to the Known Signals table

When the Delta X system is moved to another location (city, state or country), the Known Signals table should be re-filled for that new area. Typically the algorithm is as follows:

- Export of the existing known signals to an external file for future use

- Clearing the table ('Delete All' button)
- Import of the TV channels to the empty Known Signals table
- Capturing signals in Wide-Range Analyzer
- Adjustment of the dBm threshold for bands
- Studying the captured signals in the Signal Analyzer mode and adding them to the Known Signals table

In the Wide-Range Analyzer the antenna should be placed so that the best reception of broadcasting is achieved. This could be done in, or near a window. Higher floors are advisable.

Stay in the Wide-Range Analyzer for a while and change the position of the antenna in order to accumulate the maximums trace. If the real-time spectrum analyzer is used (the 2000/6 model) the capturing of signals is done within few seconds, while the slower versions will need a few minutes.

To be sure that there are no potential bugging devices among the captured signals, it is recommended to collect the known signals in a place other than that of the pending sweeping.

The information is not stored in the log in this mode; therefore after capturing signals go straight to the Signal Analyzer mode to handle the results.

Test detection and adjustment of thresholds

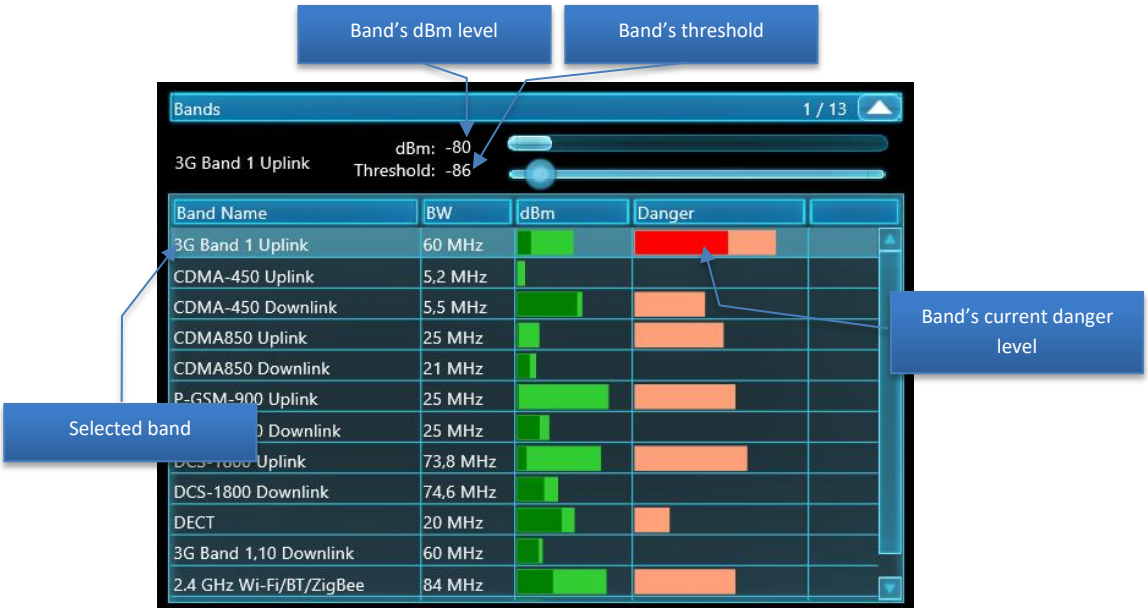
The Wide-Range Analyzer works similarly to the RF Sweep mode. Therefore it can be used for testing the RF environment, updating masks of known signals and adjusting the band's thresholds before the detection.

Press the Danger Top button in order to view the most dangerous signals in the top.

The masks for the known signals which produce danger can be updated as described in the 'Updating masks of separate known signals' on page 33.

It is also possible to use the Wide-Range Analyzer to adjust the mobile and wireless bands' thresholds before starting detection. The default values can be left without change although more precise tuning will allow better sensitivity and fewer false alarms.

Make sure the 'Hold max danger' function is inactive. Open the Band's toolbar by clicking on the 'Bands' header, select the desired band and adjust the threshold using the track bar:



The downlink bands should not normally produce alarms and therefore the threshold for them should be above the dBm level. Do not set the value too high to avoid losing sensitivity.

The uplink and 'shared' bands (without the 'uplink' or 'downlink' label) should be sensitive enough to detect the signals; therefore their threshold level should be lower. Do not set it too low 'on the floor' as the band will constantly produce alarm events and create interferences for the detection process.

While the GSM standard needs the threshold to be higher in order to limit the detection of remote devices, the CDMA, 3G and 4G/LTE should have lower threshold as they have lower dBm level.

Standard	Recommended threshold level	
	High sensitivity (longer detection distance)	Low sensitivity (Shorter detection distance)
GSM	-60 dBm	-40 dBm
CDMA, 3G, 4G/LTE	-85 dBm	-75 dBm
Wi-Fi/Bluetooth/Zigbee	-70 dBm	-40 dBm
DECT	-70 dBm	-40 dBm

A decrease of sensitivity may be needed when there are Wi-Fi, cellular or DECT signals coming from the uncontrolled neighboring premises. The higher the threshold is, the lower the sensitivity will be.

Please note that adjustment of the thresholds for the bands can be done in any mode.

Signal Analyzer

This mode was created for studying the spectrum of separate signals or bands, demodulation, adding safe signals to the Known signals table and the physical locating of any bugging devices. This mode does not capture new signals, but works with the records already stored in the Signals table.

Antenna connection: connect the ODA-4 or MWA-6 antenna directly to the INPUT socket. The antenna should be selected depending on the signal's frequency. The omnidirectional antenna ODA-4 covers the

wide frequency range and is suitable for all situations, while the directed microwave antenna MWA-6 has a coverage starting from 800 MHz and provides a higher sensitivity and directivity which simplifies the locating procedure.

In the upper part of the software there is a toolbar containing some controls specific for this mode:

The **Watch mode** defines what information is taken from the spectrum analyzer – spectrum or the demodulated sound. With the **Spectrum** selected the spectrum graphs will update continually. With the **Demodulate** selected the system allows the operator to listen to the signal and select the demodulation mode and bandwidth (BW).

The **Input** allows the operator to select the input on the RF switcher. The control is used when the antenna is connected not directly to the INPUT socket, but via the RF switcher.

Spectrum

Unlike the Wide-Range Analyzer, RF Sweep and Guard 24/7 where the entire RF spectrum is updated continually, the Signal Analyzer only updates the partial spectrum. Thanks to this a higher update rate is achieved so that the location procedure can be performed faster.

The **Update Span** defines the updated frequency range. When the **Auto** is selected, the item displayed in the spectrum graphs (Spectrogram, Waterfall) span will be updated. When the user changes the displayed span or scrolls to another frequency in the spectrum graphs, this new range is updated. Please note that the system updates the span around the marker. Therefore after scrolling to a new position the marker should be set inside the new visible area by clicking on the Spectrogram. When a signal is double-clicked or clicked in the Signals table, the marker is set automatically.

The **Number of readings** defines how many times the trace is fetched from the spectrum analyzer. Thanks to the accumulation of maximums the increased number allows the operator to track any intermittent signals with a short time of existence. For example, a Wi-Fi signal's bursts only last 5-100 microseconds so the increased number will improve the probability of capturing. Increase the number of readings for Wi-Fi, 4G/LTE, and all other non-constantly existing signals in order not to pass the activity during the locating procedure.

Please note that this setting is valid in the Signal Analyzer mode only, while the other modes fetch traces in accordance with their own algorithms.

The **Frequency** shows the tuned frequency. The marker on the Spectrogram will be positioned correspondingly. There are 3 ways to change the tuned frequency:

- Double-clicking or clicking the signal in the Signals table
- A click on the Spectrogram
- Editing the value directly using the Frequency control

Demodulation

When the watch mode is set to **Demodulate** the Delta X produces demodulated sound on the currently tuned frequency.

The toolbar in the Demodulate mode:

There are 5 **demodulation modes**: FM (frequency modulation), AM (amplitude modulation), USB (upper sideband modulation), LSB (lower sideband modulation) and CW (continuous wave modulation).

Please note that in our modern environment there are a huge number of digital signals which cannot be listened to with the help of the analogue demodulator. Mobile communications, wireless devices and encrypted VHF/UHF communication cannot be demodulated. Despite this the Delta X warns the operator about the existence of such signals, by detecting their spectrum. The subsequent locating procedure makes it possible to pinpoint the transmitter in the premises not depending on the ability to demodulate.

Analogue bugging transmitters typically use the FM modulation, although some devices sending audio through wires can use the AM or other modes. Radio broadcasting uses both the FM and AM, depending on the band. TV signals can be sent in the FM or AM, depending on the country.

The demodulation **bandwidth (BW)** can be selected in order to achieve the best quality of reception. For example 240000 Hz is suitable for the demodulation of some analogue bugging devices, FM stations and audio channels of TV stations. 15000 Hz is suitable for the reception of some analogue bugging devices and VHF/UHF communications.

It is recommended to apply different demodulations and BWs when inspecting any unknown signals.

To tune in a signal double-click or click it in the Signals table. By default the signal's central frequency is tuned in. Since the carrier of some signals is not positioned in the center (for example TV/video signals), it is recommended to change the tuned frequency within the edges of signal's spectrum in order to study the unknown signal and find possible signs of modulation and audio.

Please note the absence of audio is not a sign of a signal's safety. The more important indication is the absence of a high danger level in different parts of premises. Therefore it is recommended to move the Delta X system or its antenna in order to inspect and locate any suspicious signals.

Physical locating of the transmitter

The procedure should be accomplished in the watch mode set to Spectrum.

Both the Locator and Detector can be used during the locating procedure.

The Locator will indicate the danger level by positioning the higher values closer to the center and lower values to the outer edge. The signal's position will move to the center as the Delta X system or its antenna is being moved closer to the transmitter.

The Detector will indicate the danger level on the bargraph. The current value will be shown by red, the peak value - by light red color. The operator will be warned by the proportional sound if the Audio alarm function is activated. The signal's danger will increase as the Delta X or its antenna is closer to the transmitter and will drop at longer distances. The Audio Alarm function will produce a clicking sound with changing intensity, depending on the danger level.

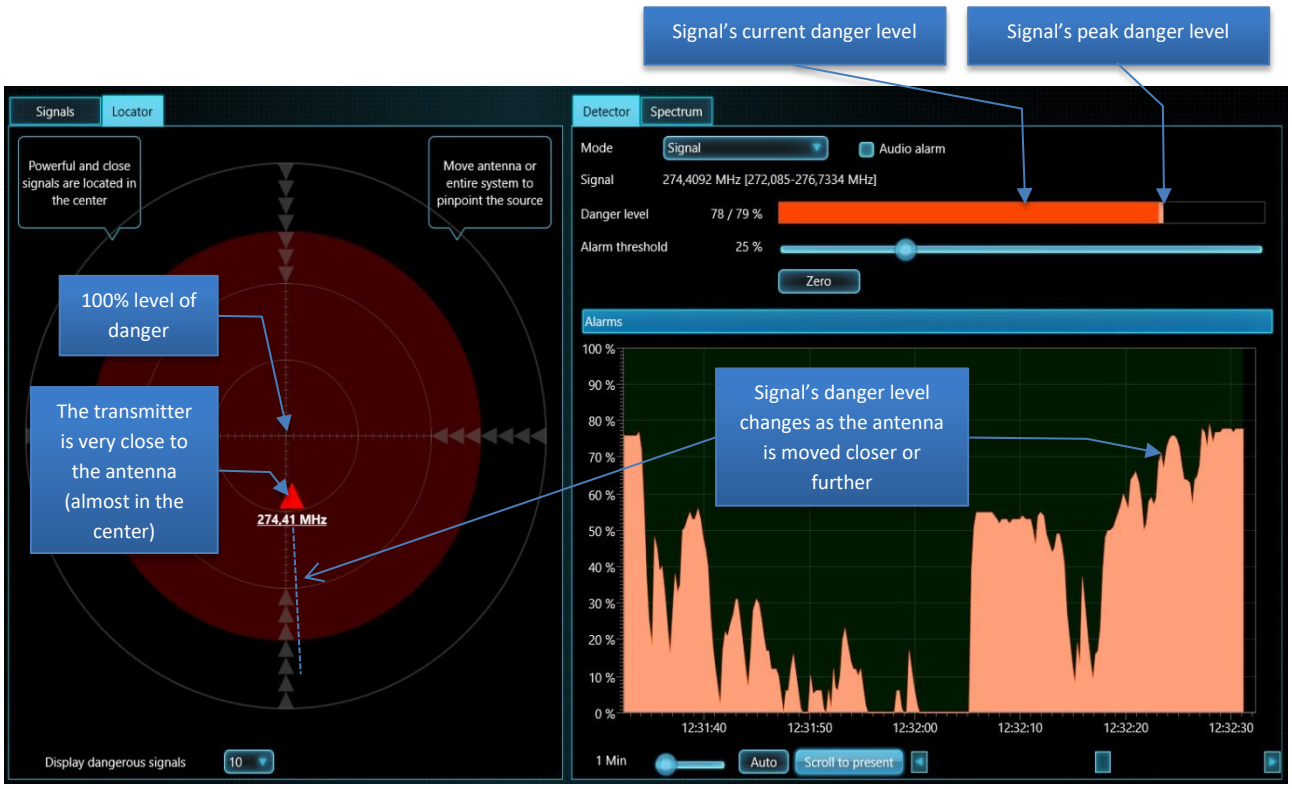
By finding the place with the highest danger level the operator can locate the transmitter.

The signal's danger level can be between 0 and 100% and is calculated from the above-threshold level and bandwidth. While the threshold for common signals is generated automatically, for bands it is set by the operator.

Algorithm of the locating procedure:

1. Start the Signal Analyzer
2. Set watch mode to Spectrum
3. Open the Detector and select its mode as Signal or Selected Range.
4. With the Detector in the Signal mode: double-click or click the desired signal in the Signals table; With the Detector in Selected range mode: select the necessary span in the Spectrogram with the help of the mouse' left button (the Select button should be in the pressed state)
5. Turn on the Audio alarm in the Detector
6. Open the Locator
7. Move the Delta X system or its antenna in order to find the place with the strongest danger level
8. The Detector and the Locator will show the changing level while the Audio alarm will produce sound of corresponding intensity. The level and intensity of the sound will grow as the antenna is moved toward the transmitter. Please note that the danger only appears when the signal exceeds the threshold. If the Detector is in the "Selected range" mode in order to locate the suspicious signal residing inside a mobile or wireless band (for example Bluetooth or Zigbee), the threshold for this band should be decreased temporarily so that the signal within the selection exceeds it. In this case the bargraph will show a non-zero level.
9. The Alarm threshold allows the operator to mute the audio for weaker levels. By increasing the alarm threshold progressively it is possible to find the area with the strongest signal and, as such, pinpoint the potential transmitter. The Zero button quickly sets the alarm threshold to the current level.

Example of locating the 274.4 MHz transmitter:



Some safe signals from broadcasting or communications might produce increased danger levels or 'false alarms'. False alarms have the following signs:

- The danger level changes insignificantly in different parts of checked premises
- The danger level rises near windows and outside the premises
- There is no sharp increase of danger in a certain part of a room
- The same signal exists in other logs obtained in other areas

At the same time, really dangerous signals have the following signs:

- A sharp increase of danger level in a certain place
- A high danger level

Please note that the mobile networks of the higher generations (3G, 4G/LTE) may use the older networks GSM/CDMA temporarily. A mobile device may change the network and frequency during the communication session. At this moment the signal may disappear from the Signal Analyzer tuned in the initial band. Testing other bands or returning to the detection will be necessary to find the new active band and to continue with the location.

Directed microwave antenna MWA-6

The supplied microwave antenna MWA-6 can help in locating any transmitters working on frequencies above 800 MHz. In addition to the increased sensitivity it can show the direction to the transmitter which simplifies the locating procedure significantly.

- To avoid losses in the RF switcher, connect the microwave antenna directly to the INPUT socket.
- Rotate the antenna in different directions to find the strongest danger level and go in that direction. The Delta X system should be carried.

- After approaching the potential location repeat finding the direction. As such, step-by-step, a precise position of the transmitter can be found.
- Proceed to the physical inspection

The following transmitters can be found with the help of the MWA-6 microwave antenna:

- CDMA, GSM
- 3G
- 4G/LTE
- Wi-Fi, Wi-Max, DECT, Bluetooth, ZigBee, wireless cameras
- All other signals above 800 MHz

Adding signals to the Known Signals table

After a signal is identified in the Signal Analyzer mode as safe, it can be added to the Known Signals table. To do this the operator should stay on the signal and press the 'Add to known' button in the Common signals' toolbar. The software will open the Known Signals table with the new record added.

It is necessary to enter the name of the new signal and specify its modulation mode. In some cases the correction of the central frequency and bandwidth will be necessary.

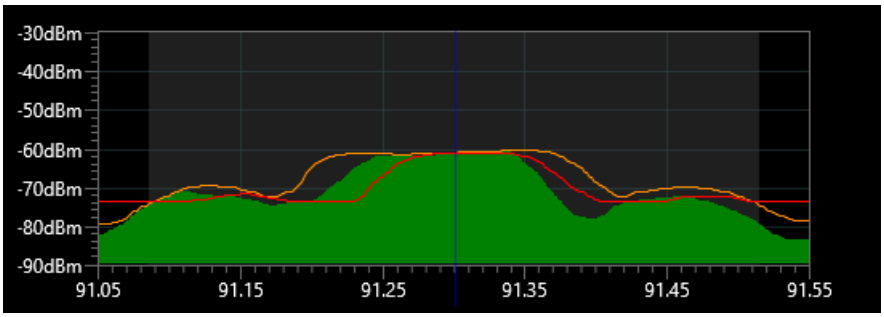
➢ **FM stations**

Since the signal's central frequency and bandwidth are detected automatically, it may be necessary to set more precise 'rounded' values before the new signal is saved.

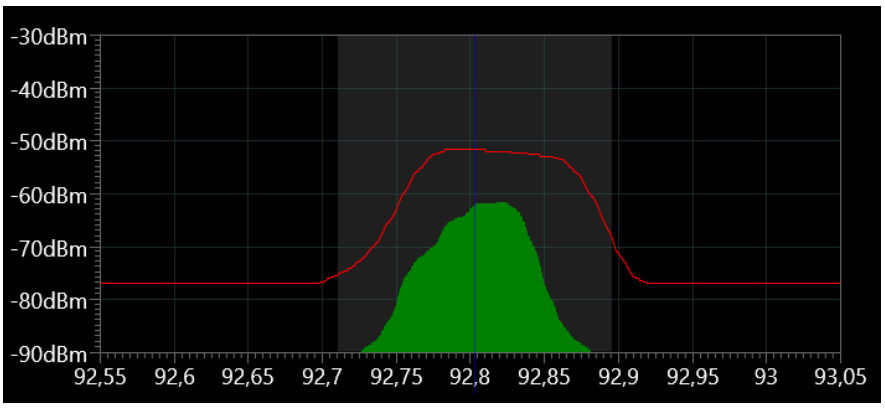
The central frequency of an FM station should be rounded to the nearest 100 kHz, while the bandwidth depends on the type of signal:

- 250 kHz for an analog FM station
- 500 kHz for a High Definition (HD) radio

Below is the example of a HD radio (USA, 91.3 MHz):



Analogue FM station (92.8 MHz):



Assign the name which precisely describes the signal. For example, the HD radio can be given name 'HD Radio 91.3 MHz' while the analog signal can be named 'FM 92.8'.

Set type of modulation 'FM'.

- **VHF/UHF signals**

  A name describing the signal should be specified. The frequency and bandwidth may be left unchanged, while the modulation should be set to 'FM'.

Press the Apply button to store the changes.

The Mask for the added signal will be updated automatically.

Press the 'Back to Signal analyzer' button on the top toolbar of the Known Signals.

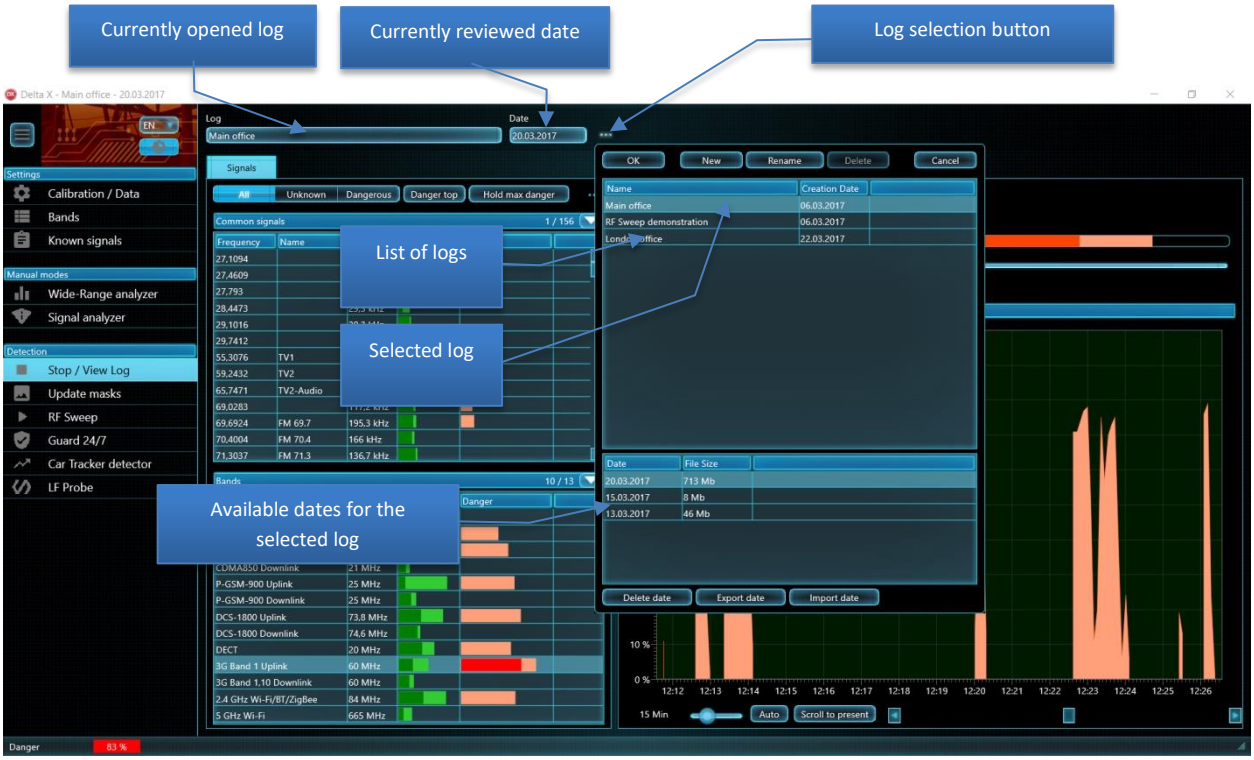
Detecting modes

Stop / View Log

A log is a database which stores data collected during the detection process. In the Stop / View Log mode the operator reviews the results of detection without performing new measurements.

Selecting log and date

The Stop / View Log can be pressed anytime during the detection so that the current log for the present date can be reviewed. At the same time, it is possible to select any other log or date later, using the **log selection button**.



The upper part of the log selection window contains the **list of logs**, whereas the bottom part displays the **list of dates** available for the selected log.

The information in the logs is split into dates. When the detection is started on another day, a new date is created. If the detection is performed continually, the Delta X system creates a set of dates. A new date is created at midnight.

Press the log selection button, select the log, date and press **OK** to open. It is also possible to open the log by double-clicking it or the desired date.

The **File Size** reflects the occupied disk space (by the date).

It is possible to delete a separate date with the help of the **Delete date** button. The entire log and all its dates can be erased at once by the **Delete** button in the upper toolbar. A currently open log and date cannot be deleted.

The **Export date** and **Import date** buttons can be used for backup and reviewing the detection results of another Delta X system.

Viewing signals and alarms

The Stop / View Log mode gives information about the detected signals to the operator. The task of the operator is to study the dangerous signals, alarms and to go to the Signal Analyzer for locating or saving the signal to the Known Signals table.

The Signals table shows the list of detected signals. All the standard operations with the signals are available in this mode: filtering, sorting, etc.

The Danger field represents the maximum danger level of the signals (light red) measured during the last detection. Use the Dangerous filter and the Danger top button to quickly select the most dangerous signals.

When the mode of the Detector is Wide-Range, the Danger level bargraph shows the maximum alarm from all the signals, while the Alarms graph shows the distribution of alarms in time.

When the mode of the Detector is Signal, the Danger level bargraph represents the maximum alarm from the selected signal, while the Alarms graph shows the distribution of alarms in time for the signal.

There are two ways of reviewing the logged information:

1) Inspection of dangerous signals in the Signals table one by one, and reviewing the alarms of each signal on the Alarms graph with the Detector in the Signal mode:
   - Set the signal's filtering as Dangerous
   - Set the Detector's mode as Signal
   - Click, or double-click, the signal in the Signals table. The Alarms graph will show the alarm events created by the signal
   - Click the events on the Alarms graph. The Waterfall and Spectrogram will show the corresponding time, while the dBm and Danger columns in the Signals table will reflect the levels which existed at the time of clicking

- A click on the Waterfall will display the corresponding measurement in the 'Live trace' on the Spectrogram

2) Inspection of the Alarms graph with the Detector in the Wide-Range mode, clicking on the alarms and reviewing what signals created them:
   - Set signal's filtering as Dangerous
   - Set the Detector's mode as Wide-Range
   - Click the alarm events on the Alarms graph. The dBm and Danger columns in the Signals table will reflect the levels which existed at the time of clicking. The Danger column will show what signals created the alarm at the moment of clicking. The Locator will display the dangerous signals at the clicked point.
   - Click, or double-click, the dangerous signals in the Signals table or Locator and review the activity in the Spectrogram and Waterfall
   - A click on the Waterfall will display the corresponding measurement in the 'Live trace' on the Spectrogram

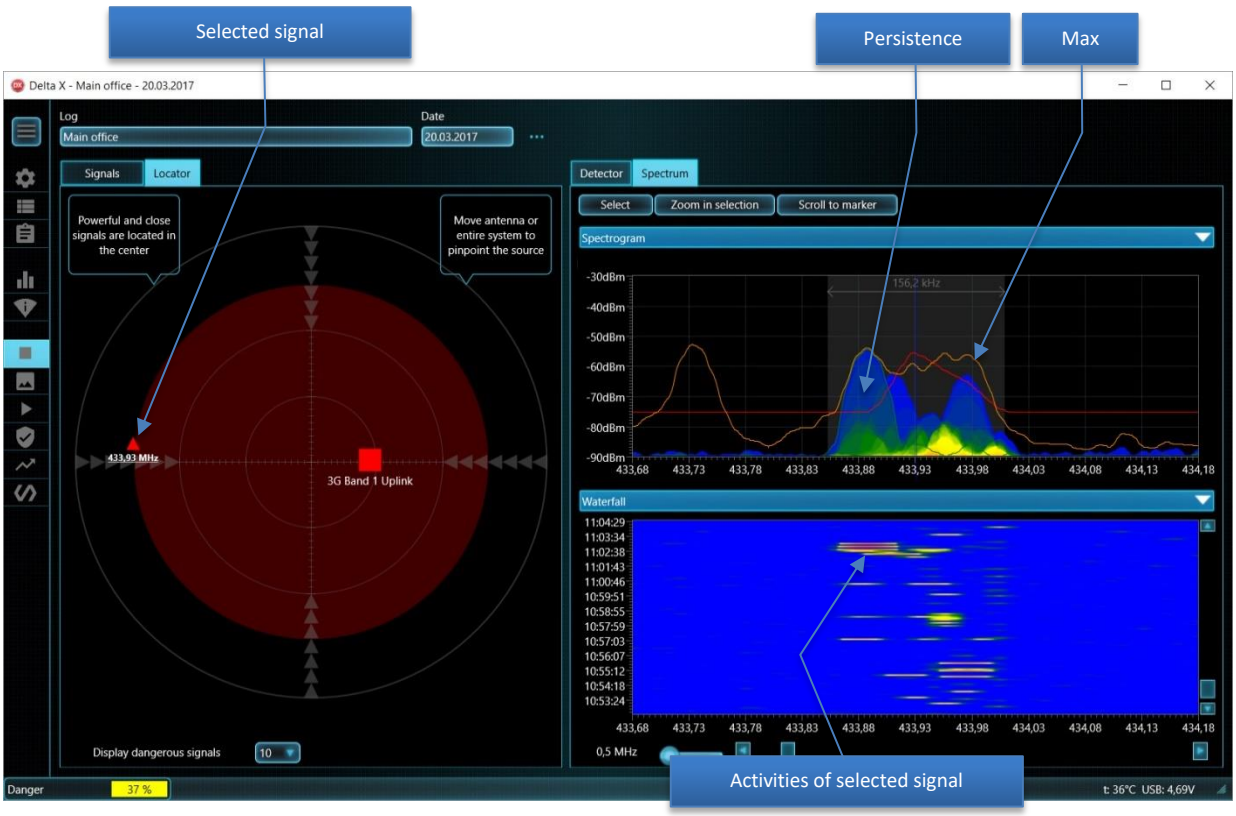
The Alarms graph can be clicked in order to select the corresponding time in the Waterfall.

Below is an example of the intermittent signal 433,9307 MHz. The bargraph is showing a 37% peak danger level, while the Alarms graph displays the moments of activity.

When the Auto button in the bottom toolbar is in the pressed position, the Alarms graph automatically changes the displayed time span to show all the available alarms.

The Locator displays the dangerous signals which were active at the moment the Alarms graph was clicked on. The Spectrum page allows the operator to see the spectral information. Below is an example

of the same 433,9307 MHz signal:



The Persistence rendering (shown on the above example) draws the spectrum by a changing color depending on the activity of signal. Depending on your needs, the Persistence or Live can be activated.

The orange Max shows the maximums accumulated during the detection. The maximums are convenient for learning intermittent signals as they keep the information even if the signal is not active at the moment of reviewing the results.

The Waterfall allows the operator to see the changes of signals in time. While the Alarms graph shows the danger level, the Waterfall displays the dBm level by color. By clicking on the Waterfall it is possible to view the spectrum trace taken at the moment corresponding to the position of the click on the vertical time scale. The Live will show the clicked trace.

Adjustment of the Waterfall's density will help to set the displayed period, while scrolling it vertically sets the starting moment. It is also possible to scroll the Waterfall by clicking the needed time in the Alarms graph (Detector page). The Waterfall data defines what is shown in the Persistence.

To inspect the signal's history during other days, open the needed date in the log selection window.

To study a signal's spectrum in the present time, demodulate and locate the transmitter use the Signal Analyzer mode.

Update Masks

In this mode the Delta X can be adapted to the current radio-frequency environment before any detection. This procedure significantly reduces false alarms and increases the general detection sensitivity since it stores spectrums of safe signals existing in the area. Both the known and unknown signals are masked.

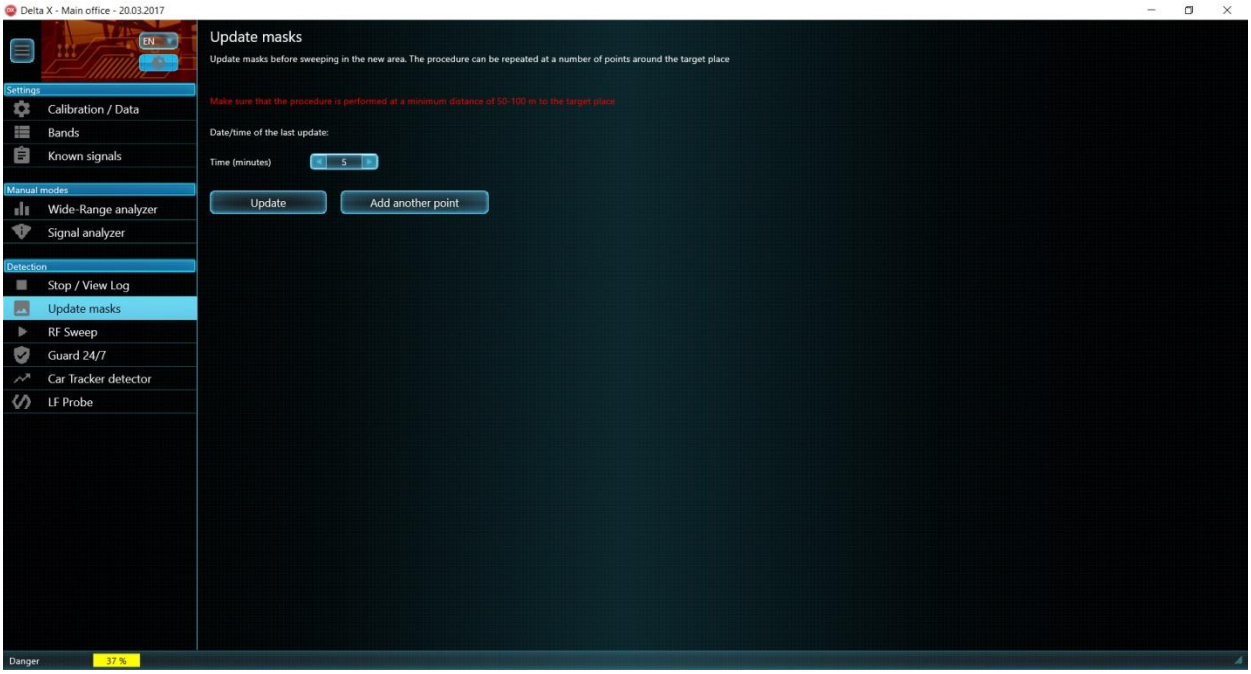
Perform the Update Masks procedure each time you are going to use the Delta X in a new location.

Antenna connection: connect the omnidirectional antenna ODA-4 directly to the INPUT socket.

Start the Delta X system and run the Update Masks mode before entering the target zone. This can be done in a car, outdoors or in another building. Higher floors are recommended since they provide better reception of broadcasting signals. Place the antenna near a window if possible. Move it in different directions and angles in order to accumulate the highest levels.

Make sure the procedure is performed at a minimum distance of 50-100 meters to the target area. It will prevent the system from masking a real danger (bugging signal). Longer distances are also possible.

If it is completely impossible to update masks at the specified distance, perform the procedure as far from the target room as possible. Select a remote room or another floor and update masks there. In case of updating in close proximity the detection distance might decrease slightly.



Select the **time** of update in minutes. With a longer time the system will have more chances to capture non-constant signals like remote controls, VHF/UHF transceivers, etc. and as such to mask them. The default value is 5 minutes.

Press **Update** to start the process. The progress bar will show the status.

Please note that the Delta X versions 100/12 and 100/4 use a slower spectrum analyzer and therefore will perform the procedure longer than shown on the progress bar.

Additional mask updates may reduce false alarms even more. Use **Add another point** to perform more measurements. Please note that the Update button clears the old masks, while the Add another point adds new data to the existing ones.

Below is the example of placement for the Update Mask in a modern city. The red spot is the target zone. The circle of 50-100 m radius is the non-recommended zone. The suggested places for updating masks are drawn by the green spots.

Target zone

Places suitable for the Update Masks procedure

The results of the Update Mask are saved automatically.

RF Sweep

This is the main detection mode, in which the Delta X detects signals, evaluates their danger level and warns the operator about any high danger. The signals, alarm events and spectrum traces are saved in the log.

The RF Sweep mode provides extremely high sensitivity thanks to the ability to omit the safe broadcasting and communication signals existing in the area and detect all other signals.

This mode is suitable for the following tasks:

- Checking premises for the presence of RF bugging (sweeping procedure)
- Checking vehicles for the presence of GPS trackers and RF bugs
- Securing conference rooms during negotiations

Preparations

The following preparations should be made before starting the RF Sweep:

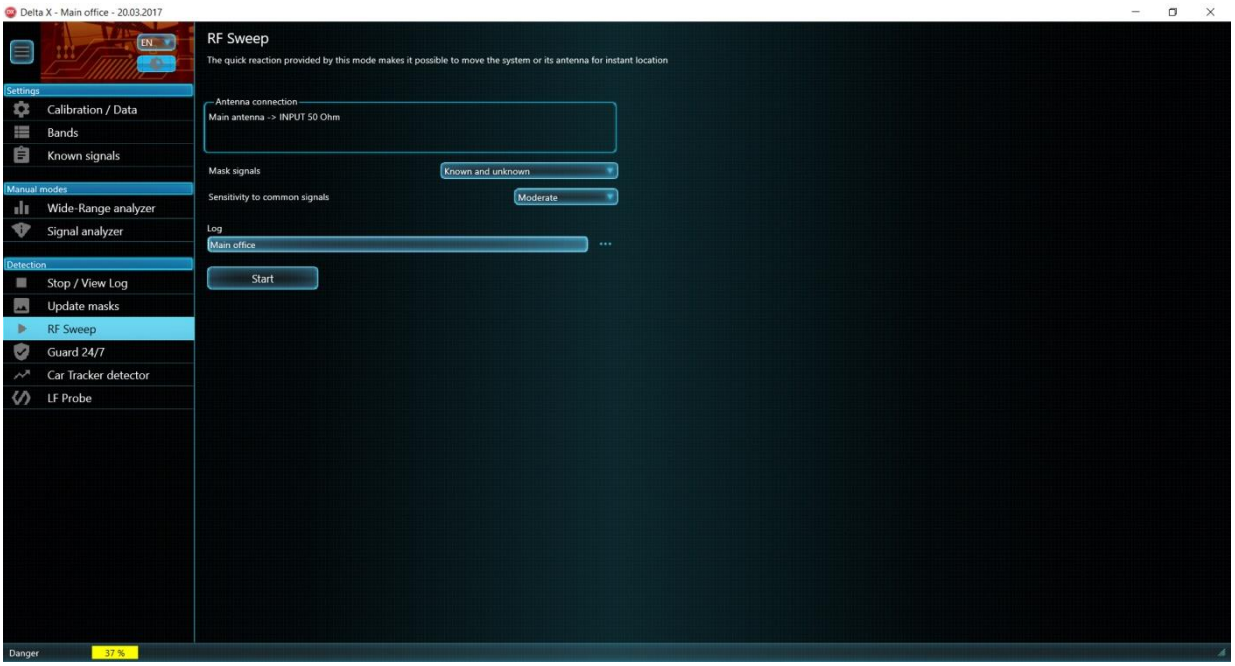
- Mobile networks and wireless bands should be specified in the Bands table
- Known signals imported or collected using the Wide-Range Analyzer and Signal Analyzer
- Personal Wi-Fi, cellular and DECT devices deactivated
- The computer running the Delta X should be in flight mode (Wi-Fi and Bluetooth off)
- The mobile/wireless thresholds adjusted
- The Update Masks procedure performed

- Sound in the checked room should be created to activate any potential bugging devices. In addition to the voice activation function present in some analogue bugs, cellular devices and bugs using the GSM, 3G, 4G/LTE increase their transmitting power and intensity when there is a sound. The laptop with the Delta X can produce music or a language tuition course for example

Antenna connection: connect the omnidirectional antenna ODA-4 directly to the INPUT socket.

Initial parameters

After selecting the RF Sweep mode the operator is asked to set the initial parameters.



Mask signals defines what signals to mask during the detection. This function will work if the Update Masks procedure was executed in advance. The masked signals do not produce any alarms so the false alarm rate decreases. **Known and unknown** will mask both types of signals, minimizing false alarms and increasing the general sensitivity. **Known only** will mask the known signals only. More alarms are usually produced in this variant.

Sensitivity to common signals defines how strong a signal should be to be detected. The position of the threshold is connected with this selection. **High** sensitivity will provide the detection of the weakest signals, but with more false alarms. **Low** minimizes false detections. **Moderate** is set by default.

Log selects to what log (database) the data will be written. Press the selection button if necessary. The log selection window will pop-up. Please see the 'Stop / View Log' section for details.

When the 100/12 version of the Delta X is being used, the user is offered to select the frequency range. There are two options: partial 100 kHz – 6000 MHz or full 100 kHz – 13000 MHz. Selection of the partial range helps to speed up the detection process by scanning the most probable bugging frequencies.

To start detecting press the **Start** button.

The Delta X will enter its working state and the Signals table, Detector and Spectrum will be shown. Within a few seconds, after initialization of the USB connection, detection will start.

Detection process

In the RF Sweep mode the software automatically recognizes the signals in the spectrum traces, adds them to the Signals table and updates the dBm and danger levels. The trace's fetch time depends on the used version of the system:

Delta X 2000/6 Real-Time	Delta X 100/12 or 100/4
1.5-3 seconds	1-2 minutes

The Signals are divided into Common signals and Bands. The Bands contain the activities registered in the mobile and wireless ranges while the rest of the signals are placed into the Common signals category.

The excess of the threshold may mean that the signal has a local origin. The aim of the Delta X is to discover all local transmitters, therefore such signals are assigned a higher danger level. The level is calculated on the above-threshold basis and takes into consideration the dBm level and the bandwidth of the signal.

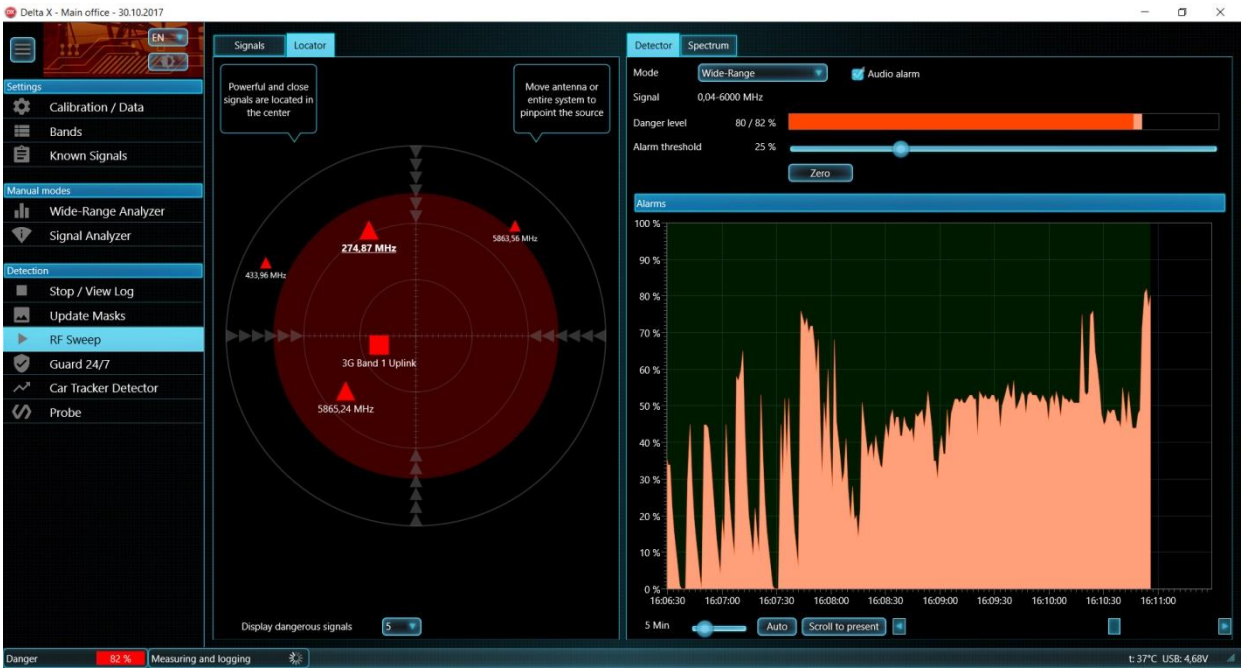
The Danger level is drawn by red and reflects the current level of danger. The Peak Danger is drawn by light red. It keeps the maximum danger level and allows the operator to observe any non-constant signals.

The 'Dangerous' filtering can be applied to select the signals with a Peak Danger above 0%

The Detector and its Audio alarm function warns the operator about the detected danger visually and with sound. The intensity of the sound changes depending on the signal's power, which makes it possible to locate the transmitter instantly. The Detector can work in the Wide-range mode, informing

the operator about all the signals simultaneously, or in the Signal mode, where the particular signal is displayed.

The Locator helps the operator to observe the results of detection by displaying dangerous signals and changing their position on the circle depending on the level of danger which reflects proximity and power. The below example shows 5 detected dangerous signals: 3G (the closest to the center, is a 3G bug with a SIM card), 5865,24 MHz (wireless camera), 274,87 MHz (audio bug), 5863,56 MHz (second signal from the wireless camera) and 433.96 MHz (wireless alarm detector).



The default value of the Alarm threshold is 25% in the RF Sweep mode. Such a value allows the operator to pass most of the false alarms while keeping the ability to capture any real danger. The red circle on the above example displays the selected threshold.

The left bottom corner of the Delta X software displays the danger status. The color of the rectangle changes depending on the danger level and is green for low values, yellow for a moderate danger level and becomes red as the level becomes higher.

When entering the RF Sweep mode the Hold max danger function is activated by default. The function places the dangerous signals on the top of the Signal table and tunes in the signal with the highest danger level.

When it is necessary to review other signals or change the displayed frequency span or scroll in the spectrum graphs, the Hold Max Danger must be turned off.

Detection distance

The detection distance depends on the transmitter and is connected with its transmission distance.

A typical bugging device sends signals over 20-200 meters and can be easily detected by the Delta X at a distance of 5-50 meters. At the same time, the 3G and 4G standards, due to the specific type of modulation can be detected at a shorter distance of 2-4 meters.

Type of signal	Detection distance
TV, FM broadcasting	5-10 km
VHF/UHF communications	0.2-2 km
VHF/UHF bug	5-50 meters
GSM bug	5-20 meters
CDMA, 3G, 4G/LTE bug	2-4 meters
DECT	5-10 meters
Wi-Fi	5-10 meters
Bluetooth, ZigBee	2-10 meters
Wireless video camera	5-20 meters

Most bugging devices can be found without the necessity of moving the system or its antenna within the room in order to scan the area. Nevertheless, to obtain the most reliable results and find all types of bugging, including the 3G/4G and the low-power devices like Bluetooth, the antenna should approach them at least 2 meters. Therefore, moving the system/antenna and scanning the area is recommended.

Scanning the area

The advantages of moving the system or the antenna are:

- Low-power transmitters and some hard-to-detect cellular signals can be detected at a closer distance
- The operator may need to decrease the sensitivity on some bands in order to avoid false alarms from neighboring Wi-Fi and cellular devices. The loss of detection sensitivity can be compensated at a closer distance
- The location of the transmitter can be discovered during the detection

When the entire system is carried, the antenna must be screwed to the cover of the case and connected directly to the INPUT.

When the Delta X is stationary and the antenna is being carried, the coaxial extension cable and the adapters from the supplied set must be used. The antenna is connected to the INPUT via the coax cable and adapters. Using the handle/tripod from the supplied set simplifies carrying the antenna.

The scanning procedure depends on the used version:

Delta X 2000/6 Real-Time	Delta X 100/12 or 100/4
Scan all areas in the room by moving the system or its antenna smoothly with the speed of 50 cm per second taking into consideration the detection distance of 2 m	Relocate the system or its antenna by 2 meters every 5 minutes until the entire room is scanned

False alarms

Since the RF environment changes in different places, some known signals may produce alarms in the RF Sweep mode despite the Update Masks procedure being performed before the detection. This may happen on higher floors, near the windows or in any premises facing broadcasting towers.

The influence of false alarms can be lowered by an increased Alarm threshold, but a more recommended measure is to re-update the individual masks for known signals which produce danger. The procedure can be done without stopping the detection process:

- Place the system or antenna where a good reception of broadcasting can be achieved (near a window)
- Deactivate the Hold max danger function
- Open the Spectrum page
- Open the Common signal's toolbar by clicking the header
- Tune in a known signal producing the danger by double clicking it in the Signals table. The known signals can be recognized as their Name field is not empty. The mask for unknown signals cannot be re-updated.
- Inspect the spectrum of the known signal. Make sure the spectrum has no signs of the presence of another signal hidden within – no sharp increases of spectrum, no other signals within the signal's edges are seen in the Persistence view.
- Press the Update Mask button in the toolbar to mask the signal. After the next fetch of the trace the threshold within the signal's edges will increase and the signal's danger level will drop.
- Repeat the same procedure a number of times for all other known signals showing danger. Some signals may need repeated updates.

False alarms may also appear on the mobile/wireless bands if their thresholds are not adjusted properly. To adjust the band's threshold open the toolbar by clicking the Bands' header.

The downlink bands should not normally produce any alarms. If this happens, firstly check the spectrum and behavior of the danger level. Since the downlink signals are coming from base stations situated outside, the danger level may grow near windows. In this case and when there is no concentration of the high danger level the band's threshold can be increased to prevent alarming.

With the uplink and shared bands a lower threshold will provide a higher detection distance. At the same time it may be necessary to set it to a certain level to reject any Wi-Fi, DECT and cellular devices creating interference from an adjacent (neighboring) premises.

After the known signal's masks are updated and the thresholds for bands are adjusted, the Alarm threshold can be minimized and the maximum sensitivity achieved.

Results of detection

The results can be reviewed in the Locator or Signals table during detection. Double-clicking or clicking the signal shows it on the spectrum graphs. When the Detector is in Signal mode, it will show the alarm events of the clicked signal on the Alarms graph.

The RF Sweep mode presumes the detection and locating simultaneously, but due to the processing of the entire frequency range the movement speed is limited. The Signal Analyzer mode can be used temporarily in order to study a suspicious signal and locate it physically. Then the RF Sweep can be continued again.

Press the Stop / View Log after the detection is completed. The information can be reviewed in this mode (page 49).

Training

Before starting the actual detection a 'test' detection with bugging devices of different types can be performed.

Some home appliances and cellular devices work similarly to real bugging devices; therefore they can be used for training in the absence of real bugs.

Bugging device	Replacement
VHF/UHF radio microphone	Body-worn 'bodypack' radio microphone used on TV
GSM bug	Mobile phone in GSM mode (with 3G off) in the conversation state. A call from a landline telephone can be made, the phone picked up and left off hook
3G bug	3G mobile phone in the conversation or data exchange state. To initiate continuous data exchange Skype or Viber software can be used or a long Youtube video watched
Wi-Fi transmitter (client)	A Wi-Fi connected mobile phone in the state of data exchange (Skype/Viber/Youtube)
Wi-Fi transmitter (server)	Wi-Fi router
Hidden wireless camera	Video baby monitor
DECT radio microphone	DECT phone in the conversation state
Bluetooth bug	Bluetooth headset or wireless mouse in the active state

Cellular devices can decrease the power or intensity of exchange when there is no conversation (no sound). When performing the test training detection, make sure there is a sound near the cellular device.

When testing the Delta X take into consideration the reaction time of the used version in the RF Sweep mode. The '2000/6 Real Time' has the fastest speed so the signal does not need to exist for so long to be detected (up to 3 seconds). The slower versions 100/12 and 100/4 need the signal to exist for at least 2 minutes to detect it. At the same time, in the Signal Analyzer mode both versions have a quick reaction time.

When testing the system with a car's remote control take into consideration that the sent signal may last less than the reaction time of the system. The detection of such signals may take up to 10 seconds.

Guard 24/7

There are a number of hidden bugging devices transmitting signals non-constantly:

- Radio microphones or video cameras activated remotely
- GSM/3G/4G/LTE bugs activated by an external request
- Bugging devices with accumulation and periodical uploading of information

Such types of bugs transmit radio signals just periodically - during an important meeting, negotiations or whenever necessary. An audio accumulating bug can store conversations during days and then upload the data within a few minutes at a pre-programmed time or under an external request.

The Guard 24/7 mode was created for the day-and-night guarding of the target zone in order to detect all types of signals including non-constant ones and provide the highest level of security.

There are some differences compared to the RF Sweep mode:

- The system has a lower alarm rate thanks to the rejection of short transmissions
- The reaction time depends on the signal's power and bandwidth
- The operator can use 2 antennas simultaneously to decrease any false alarms

Gaining experience in the RF Sweep mode isrecommended before using the Guard 24/7.

Reaction time

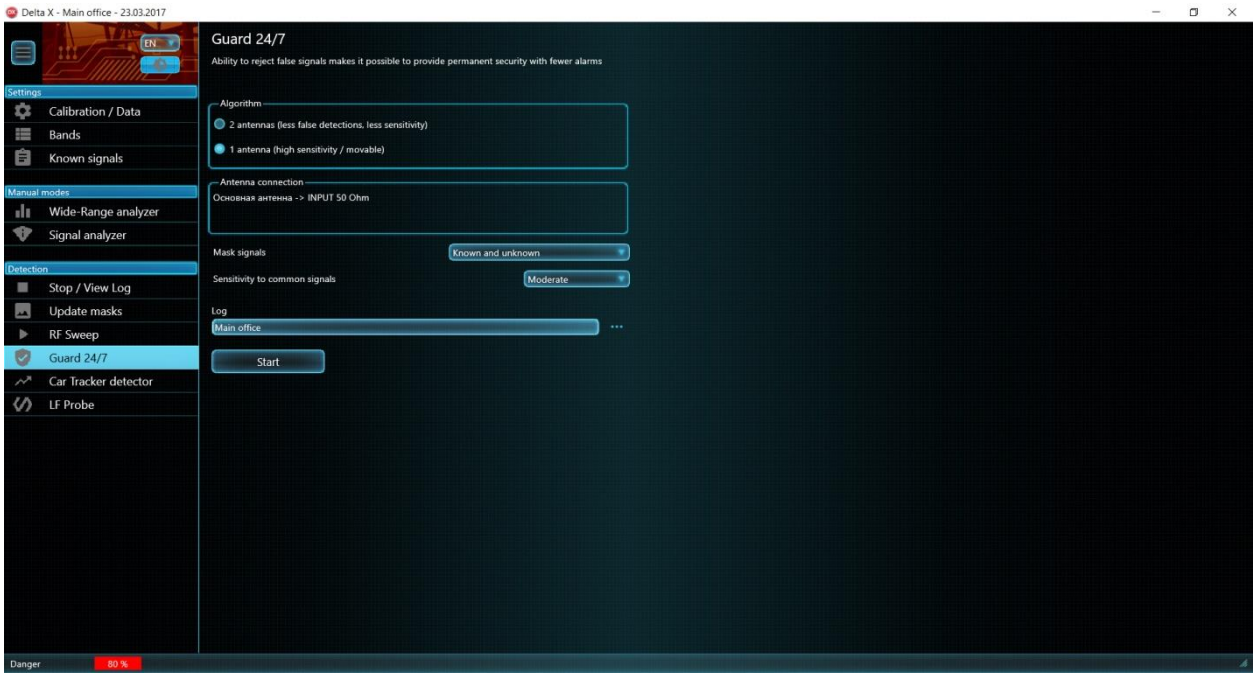
Since the short signals from remote controls, wireless alarm sensors and VHF/UHF communications are considered to be safe, the Guard 24/7 rejects them. In this mode a signal should exist and exceed the threshold during a certain time in order to become dangerous.

The reaction time depends on the signal's power and bandwidth. The stronger signals with a wider bandwidth produce an alarm faster, usually within 3-5 seconds. The weaker narrowband signals should exist for at least 5-10 seconds to produce the alarm.

Please note that the pulsing timeslot signals like DECT, Wi-Fi, GSM, 4G/LTE, etc. are detected in the Guard 24/7 mode.

Initial parameters

The parameters page appears when the Guard 24/7 mode is selected. All the options are similar to the RF Sweep mode, except the Algorithm selector:



When the **1 antenna** algorithm is selected the Delta X works the same way as in the RF Sweep mode. The system/antenna can be moved or remain fixed. The only exception is the reaction time. Please read about the 'RF Sweep' on page 55.

The **2 antenna** algorithm was created for static use. The Delta X can guard the target zone for a long time and adapt to the RF environment by updating the masks automatically. The antennas are placed inside the target room and in a remote area.

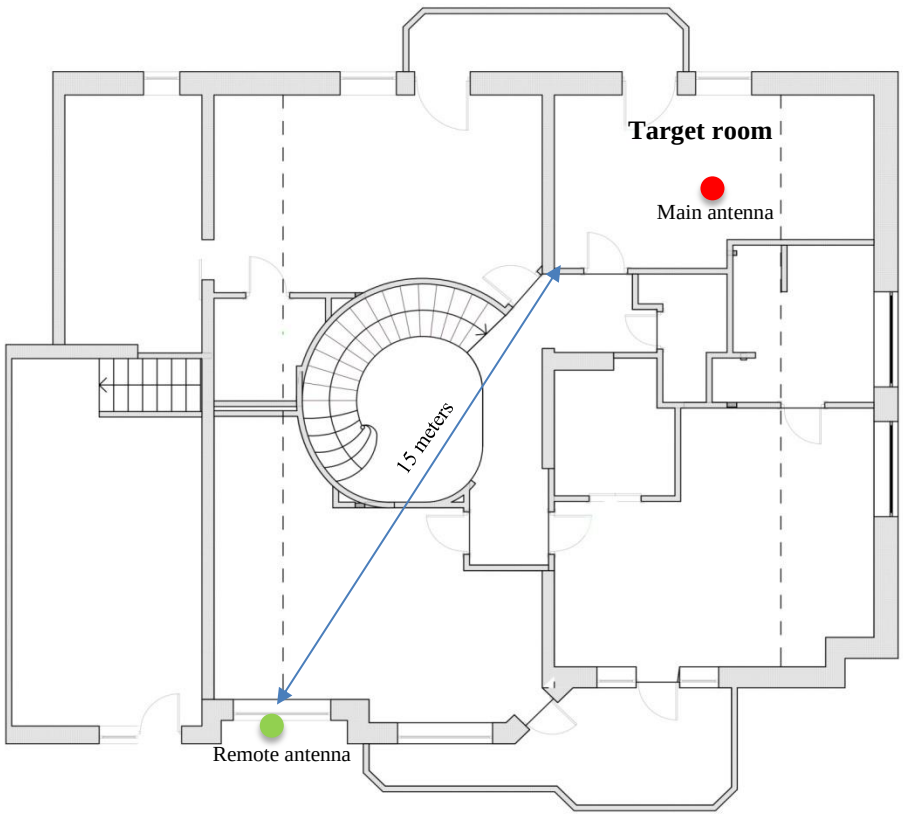
The set for 2-antenna detection mode is supplied separately (option 001). It includes one ODA-4 antenna and two 20 m extension cables.

Usage of 2 antennas

- The main antenna should be put within the target zone (in the checked room)
- The remote antenna should be as far from the target zone as possible (not closer than 15-20 meters)
- The remote antenna should be able to receive the broadcasting and other external signals with high sensitivity. The optimal placement is near a window.
- Both antennas should be used with the extension cables to equalize the attenuation, not depending on the position of the system.
- The system can be placed in any convenient place, within the target zone or in an adjacent room

In case of organizing a permanent control post and running through its own cables, use the following 50 Ohm low-attenuation cables: LMR-240, 5D-FB (6-7 mm), RG-8, RG-213, LMR-400 (10 mm), LMR-600 (14 mm).
The RG-58 and other high loss cables cannot be used.
Do not exceed 30-50 meters length. Use the same cable length for the main and remote antenna.
If possible, the remote antenna can be placed in the roof area or at least in a window to provide the best reception of broadcasting.

Example of antenna placement:



Antenna connections

When 1 antenna is used, it should be connected directly to the INPUT socket (omnidirectional antenna ODA-4).

When the 2-antenna algorithm is applied, the RF switcher is used. Before pressing **Start** make all the necessary connections:

- The RF switcher's output marked as SWITCHER OUT should be connected to the INPUT with the supplied cable
- The main antenna ODA-4 should be placed in the target zone and connected to the ANT 1 with the help of the 20 m extension cable
- The remote antenna ODA-4 should be placed in the remote area and connected to the ANT 2 with the help of the 20 m extension cable

When it is necessary to make a location procedure or study a suspicious signal, stop the detection temporarily and enter the Signal Analyzer mode. Move the main antenna to make the physical location.

Detection process

When the Guard 24/7 is started with the 2-antenna algorithm selected, the system works under the following algorithm:

- After the start, the 'Update Masks' procedure is performed automatically on the remote antenna during 1 minute
- The main antenna is selected and the spectrum traces are fetched
- If dangerous signals are detected on the main antenna, the mask updating procedure on a remote antenna is repeated with a frequency of once per 30 seconds
- Some external 'false' signals can be eliminated in this mode thanks to the quick mask updating

Car Tracker Detector

GPS trackers

A GPS tracking unit is a device, normally carried by a moving vehicle or person, that uses the Global Positioning System to determine and track its precise location, and hence that of its carrier, at intervals. The recorded location data can be stored within the tracking unit, or it may be transmitted to a central location data base, or Internet-connected computer, using a cellular (SMS or internet packets), radio, or satellite modem embedded in the unit.

Usually, a GPS tracker will fall into one of these three categories:

- Data logger. Logs the position of the device at regular intervals in its internal memory.
- Data pusher (most common type, also known as a *GPS beacon).* This kind of device sends the position of the device at regular intervals, to a determined server, which can store and instantly analyze the data.
- Data puller (also known as *GPS transponders)*. Sends the position under external request only. This technology is not in widespread use and can be used in the case where the location of the tracker will only need to be known occasionally e.g. placed in property that may be stolen, or that does not have constant source of energy to send data on a regular basis, like freights or containers.

The data pusher, sending the coordinates periodically and using the cellular networks is the most popular type of GPS tracker used nowadays. The data is sent via the GSM, 3G or 4G/LTE networks.

The Delta X can detect data pushing GPS trackers by detecting their periodical exchange with the mobile network.

Algorithm of detecting the periodical exchange

Unlike the RF Sweep mode which detects all types of signals, the Car Tracker Detector mode is concentrated on measuring activities on the cellular bands only. The other frequency ranges are not scanned. Since the spectrum analyzer does not scan other frequencies, the update rate and the probability of detection are higher and the reaction is quicker.

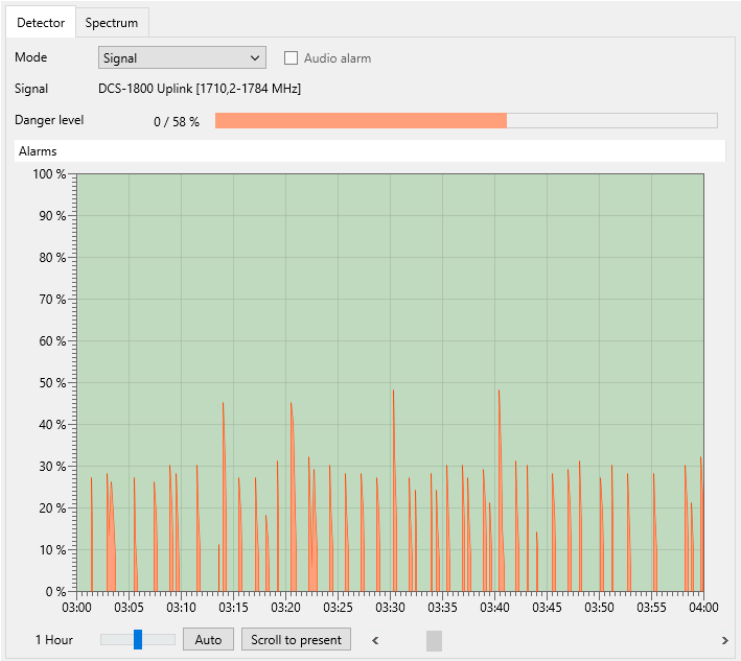
The bands to be monitored in the Car tracker detector are selected in the Settings – Bands. The 'Tracker detection' check box allows the user to include the desired bands. It is recommended to include all the cellular uplinks and exclude the downlinks and the wireless bands like Wi-Fi and DECT. The 4G/LTE bands of a 'Shared' type should be included as well.

The Delta X system must be placed inside the checked vehicles. The detection algorithm is as follows:

- All personal mobile phones and other carried cellular devices must be switched off or placed into flight mode
- All the known cellular devices built in the car (alarm systems, traffic statistics senders, etc.) should be deactivated (switched off). If necessary, contact a service center for turning them off temporarily
- Go to a secondary road in the country to avoid external interferences. Start the Car tracker detector mode. Like the other detection modes, the Car tracker detector allows the user to select the log. Press the Start button to begin.
- Typically trackers have a movement sensor; therefore the vehicle should move in order for the tracker to be detected. Drive along secondary roads omitting cities, high traffic areas or crowded places in order to avoid interferences from other external cellular devices
- Since the frequency of the coordinate's upload is unknown, driving and simultaneously measuring for at least 1-2 hours is recommended.
  <u>Note: A car's power point can be used to power the Delta X's laptop</u>
- The periodical activity in the GSM, 3G or 4G/LTE bands with a moderate to high level may be a sign of a GPS tracker. Watch the Alarms graph. The frequency of exchange may be every 10 seconds or 30 seconds or 5 minutes, for example.
- In case of a large-sized vehicle repeat the test with the Delta X or its antenna placed in another part of the car. Keep watching the danger level and the Alarms graph
- The dBm threshold for the bands can be adjusted to achieve the best balance between the sensitivity and any false detections. Typically for GSM it is not necessary to set a very high sensitivity so the threshold can be between -60...-30 dBm in order to reject any external signals. 3G or 4G/LTE will demand the setting of a higher sensitivity with the threshold's level at -85…-70 dBm.
- The Alarm threshold can be adjusted when necessary

It is also possible to analyze the results later by reviewing the log.

Below is an example of a GPS tracker sending signals on the DSC-1800 band :



Location change algorithm

There is another approach to detecting data pusher and data puller types of GPS trackers.

In addition to the periodical exchange (data pushing), the GPS tracking devices communicate with the network when they change an area. The mobile network's base stations are combined into areas with a unique code. When a cellular device enters the area with another code it issues a location update request, thereby informing the mobile provider of its new position. This allows the provider to locate the cellular device in case of an incoming call.

If the GPS tracker does not perform periodical exchanges, the presence of a strong signal when the vehicle is crossing the coded area's border may discover the tracker.

The size and the borders of the coded area are unknown, but it can be supposed that if a vehicle moves 20-50 km in one direction the probability of changing the coded area and appearing of the data exchange will be high. If there is an activity in a certain place, the test may be repeated in the reverse direction in order to check if the activity occurs again.

A high danger level may last 3-5 seconds in case of the presence of a 'hidden in the vehicle' cellular device. Presence of a cellular device may be a sign of a GPS tracker.

While the Car Tracker Detector discovers the most popular GPS trackers on the move, the RF Sweep mode can find hidden devices of other types: beacons sending data by other means (Satellite/Wi-Fi/VHF/UHF), bugs/radio-microphones, wireless cameras, etc. Additional usage of the RF Sweep mode is recommended for a full check of the vehicle.

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 bugging device of this type 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.

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.

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**

The Delta X software will have the following view in the Probe mode:

The Signals table shows the Common signals section and hides the Bands. The Spectrogram's and Waterfall's span is initially set to display the range 0 - 10 MHz, although it is possible to change the span and scroll to any frequency.

The first toolbar's line contains the same controls which are present in the Signal Analyzer mode: Watch Mode selection (Spectrum or Demodulate), Update Span selection, Number of readings and Frequency.

The second toolbar's line contains controls specific to the Probe mode.

Unlike the other detecting modes the Probe mode does not store the signals in the Signals table after work is completed. The Signals table and the Waterfall are cleared each time the Zero button is selected.

The **Zero** function rejects the background RF emissions received by the Multifunction Probe. The rejection is performed by storing the current spectrum trace for its subsequent extraction. The use of the function is described for each further input. The Signals table and the Waterfall are cleared each time the Zero button is pressed.

The **Full Range** button sets the recommended span of the spectrum graphs for the Probe mode: 0 – 10 MHz. This range is selected as the most probable for bugging. Nevertheless a wider span can be selected manually. Please note that despite the spectrum graphs display, the span starting from 0 means the actual measured range begins at 40 kHz or 100 kHz, depending on the system's version.

Like in all other modes **double clicking** on a signal in the Signals table performs tuning it in. The spectrum graphs adjust automatically to show the clicked signal fully. If the Detector is in the Signal mode it will be assigned to the clicked signal. A single click tunes in a signal without adjusting the spectrum graphs.

Clicking on the Spectrogram allows tuning in the desired frequency.

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 'SWITCHER OUT' to the INPUT with the help of the supplied jumper cable
2. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
3. Select the IR input on the probe
4. Select the Probe mode in the Delta X software
5. Cover (close) the probe's IR sensor and press the Zero button. Keep the sensor covered for few seconds
6. Create a source of sound in the room to activate any potential bugging devices
7. Point the probe's IR sensor to the place of possible bugging (for example, from outside the window to the interior and frames)
8. If an infrared signal is detected, it will be automatically inserted into the Signals table.
9. 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. 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.
10. 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.

The detection distance is up to 30 cm; therefore objects and surfaces must be probed carefully.

Algorithm

1. Connect the 'SWITCHER OUT' to the INPUT with the help of the supplied jumper cable

2. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
3. Select the LF input on the probe
4. Select the Probe mode in the Delta X software
5. Keep the probe far from the electronics and objects to be inspected and press the Zero button in the software
6. Create a source of sound in the room to activate any potential bugging devices
7. Start scanning the area (objects, surfaces, constructions, etc.) while observing the change of the danger level. The Audio alarm function will produce sound of changing intensity, depending on the level.
8. All the signals (parts of spectrum exceeding the threshold) will be inserted into the Signals table automatically. Their dBm and Danger levels will be updated during the search
9. 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.
10. 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 than 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 SWITCHER OUT to the INPUT with the help of the supplied jumper cable
2. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
3. Select the WIRE input on the probe
4. Select the Probe mode in the Delta X software
5. Connect the high voltage cable to the Multifunctional Probe.

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

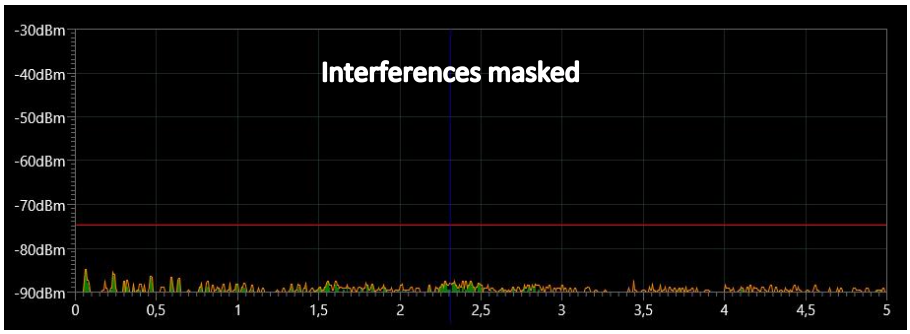
6. Create a source of sound in the room to activate any potential bugging devices and recognize them during demodulation
7. Connect the high voltage cable to the AC outlet #1 in the room
8. Press the Zero button
9. Connect the high voltage cable to the other AC outlets in the room one by one and watch 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' in Watch Mode
    - 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

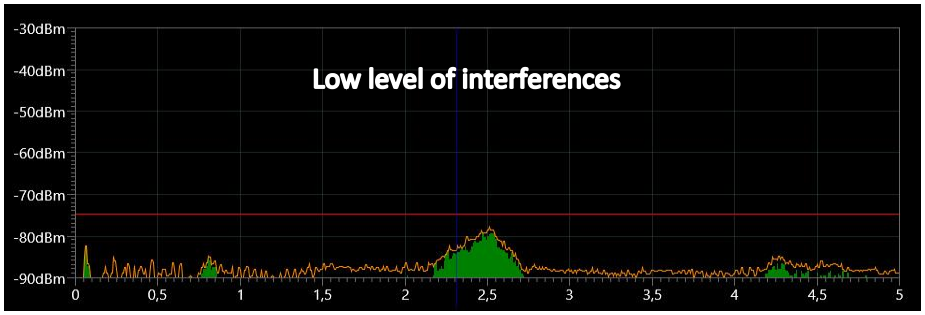
Example of detecting an audio bug sending a signal over an AC line:

AC outlet #1

AC outlet #1 after pressing Zero

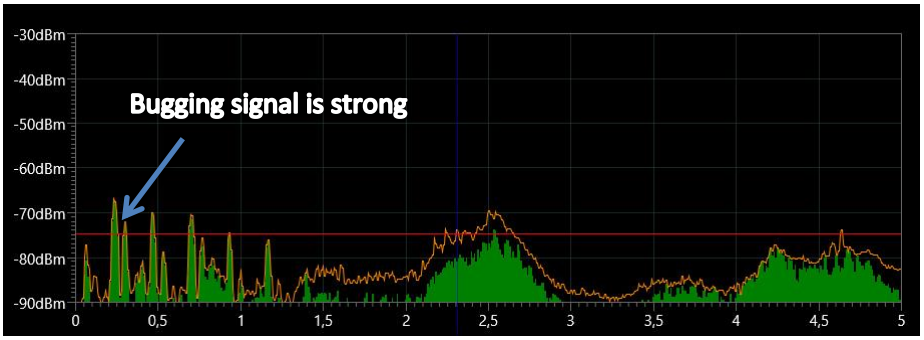


AC outlets #2…5 – no danger, low level of interferences



AC outlet #6 – the first sign of danger

AC outlet #7 - BUGGED



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	Direct	Low-voltage cable	

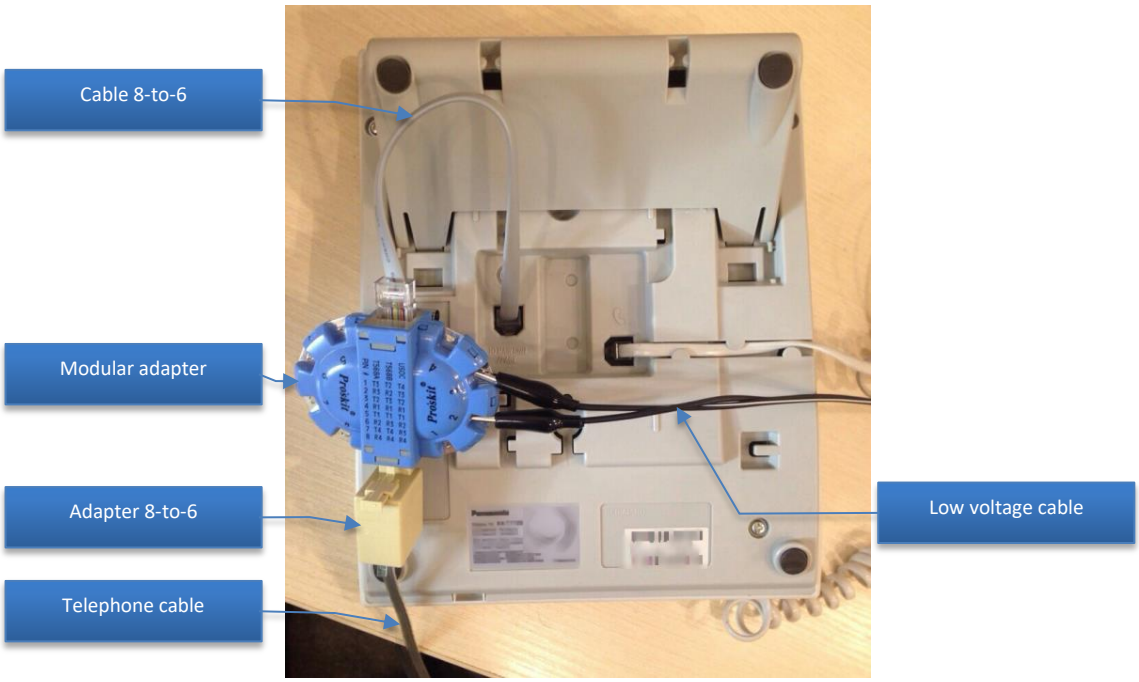
cables	(alligator connector)

Algorithm:

1. Connect the SWITCHER OUT to the INPUT with the help of the supplied jumper cable
2. Connect the Multifunction Probe to the PROBE with the help of the supplied coax cable
3. Select the WIRE input on the probe
4. Select the Probe mode in the Delta X software
5. Connect the low voltage 'alligator' cable to the Multifunctional Probe.
6. Press the Zero button in the software
7. Create a source of sound in the room to activate any potential bugging devices and recognize them during the demodulation
8. Connect the low-voltage 'alligator' cable to the wire. If necessary use the in-line modular adapter and accessories:

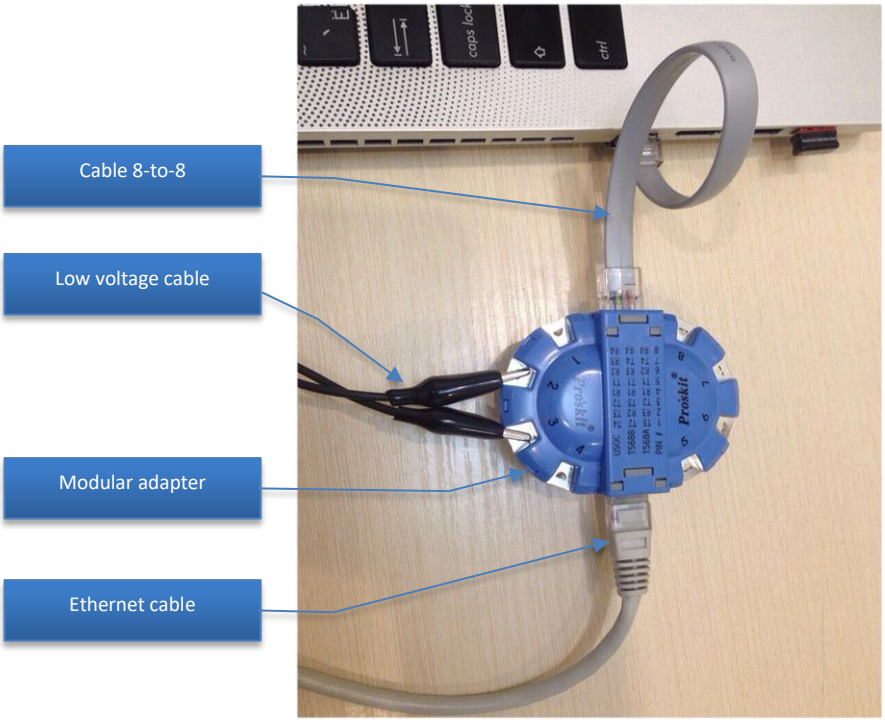
Landline phone

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:



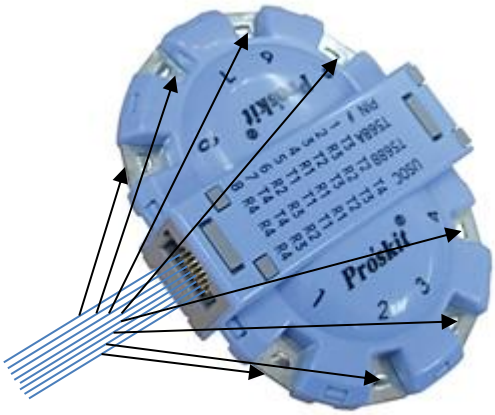
Alarm and other low-voltage wires

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's movement detector should be disassembled in order to reach the terminals. The procedure can be made on the control panel as well.

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.

9. 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.

10. 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.

11. 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 in the Watch Mode
    - 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.

      <u>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.</u>

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

12. If you are checking the phone line, perform the test off-hook and hung up
13. Repeat the test for all the combinations of pairs on the modular adapter, reconnecting the alligators as necessary
14. 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.

Advanced possibilities for experienced users

Auxiliary receiver

Since the spectrum analyzer cannot measure the spectrum and demodulate simultaneously, the Delta X system allows the operator to connect an auxiliary wide-band receiver in order to listen to a signal simultaneously with the detection or location.

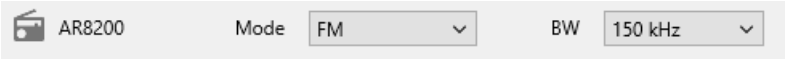
Like the spectrum analyzer, the receiver cannot demodulate digital signals (bands). The great advantage of the Delta X system is that it can identify local transmissions and help to physically locate them without demodulation. But the ability to demodulate allows the operator to identify the unknown analogue signals faster.

The AOR AR8200MK3/AR8200D is a compatible model of receiver.

While the AR8200D has a built-in USB interface, it is necessary to have the separate interface cable for the AR8200MK3.

Connect the receiver to the USB port, turn it on and start the Delta X software. After detection of the spectrum analyzer the software will detect the receiver and display the corresponding message in the startup window:

In the main window the receiver's control toolbar will appear:



The **Mode** allows the operator to select the demodulation mode, while the **BW** setting selects the bandwidth.

The auxiliary receiver will be tuned into a signal in the following cases:

- When the Hold Max Danger function is active and a dangerous signal is detected
- When the signal in the Signals table is clicked
- When the operator clicks on the Spectrogram or selects the frequency in the Signal Analyzer mode

The demodulation mode is not changed when a new signal is tuned in. It might be necessary to change the mode and BW in order to hear the signal with the best quality.

The Hold Max Danger function should be deactivated in order to allow the Delta X and the auxiliary receiver stay on the manually selected signal during the detection.

Localizing the interface

The Delta X software can be localized to any language by creating the corresponding translation file.

The translation file should be placed in the application's folder (Usually C:\Program Files\DigiScan Labs\Delta X or C:\Program Files (x86)\DigiScan Labs\Delta X).

The translation file should have the following name: InterfaceXX.txt, where XX is the abbreviation for the language. For example, the translation file for Poland should have the name InterfacePL.txt.

The file must contain the translation strings in the following format:

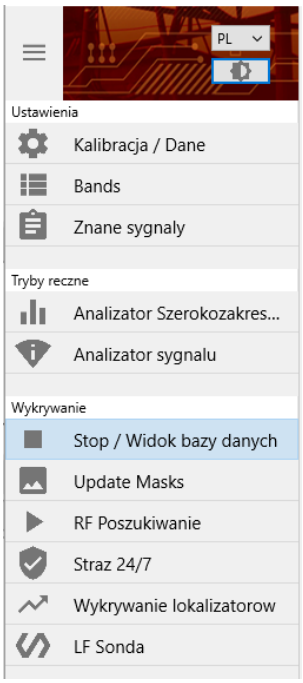
Sentence in English1=Translated sentence1
Sentence in English2=Translated sentence2

…

The length of the translated sentence should not significantly exceed the original to avoid the concatenations. Use shortenings where necessary.

Below is the example of the translation file for Poland and the result:

Settings=Ustawienia
Calibration / Data=Kalibracja / Dane
Known signals=Znane sygnaly
Manual modes=Tryby reczne
Wide-Range analyzer=Analizator Szerokozakresowy
Signal analyzer=Analizator sygnalu
Detection=Wykrywanie
Stop / View Log=Stop / Widok bazy danych
RF Sweep=RF Poszukiwanie
Guard 24/7=Straz 24/7
Car Tracker detector=Wykrywanie lokalizatorow
LF Probe=LF Sonda
…



An already existent translation file can be found in the application’s folder and used as a blank.