ST154

RF MONITORING SYSTEM

TECHNICAL DESCRIPTION AND OPERATION MANUAL

TABLE OF CONTENTS

Introduction

This manual contains information required for proper "ST154" operation.

Before starting your work with “ST154” carefully read this instruction and save it for further use as a handbook.

Any information in this manual can be changed fully or partially without further notice.

Manufacturer reserves the right to make changes to the device which will not affect its characteristics.

1 Description and operation

1.1 Purpose of the device

Main purposes of the ST154 RF Monitoring System:

- detection of unauthorized transmission within the supervised area, which is carried out by special radio transmitting devices as well as legally operate radio communication devices such as cell phones and modems CDMA450, GSM 900, 1800, 3G, 4G, WLAN 2.4 and 5 GHz, BLUETOOTH and DECT;
- detection and further measurements of analog radio signals (signal level, frequency);

- localization of emission:
  - through procession of signal levels data gathered from no less than 3 Control modules;
  - using the Search module ST154.S (**SM**)

24/7 monitoring of radio environment with creation of event log.

1.2 TECHNICAL SPECIFICATIONS

1.2.1 Technical specifications of the Control module **CM** (ST154.A, ST154.W, ST154.E and ST154.E+POE)

1.2.1.1 Frequency range, MHz	25-6000
1.2.1.2 Sensitivity threshold, dBm	
100 MHz	-90
1000 MHz	-95
2000 MHz	-95
4000 MHz	-85
5000 MHz	-75
1.2.1.3 Maximum input signal level, dBm	+5
1.2.1.4 Detected types of wireless data transfer standards	CDMA 450, GSM 900, GSM 1800, 3G, 4G, WLAN 2.4 and 5 GHz, BLUETOOTH, DECT
1.2.1.5 Bandwidth of analysis, MHz	0.1 - 20
1.2.1.6 Interfaces	USB, WLAN (for ST154.W), ETHERNET (for ST154.E and ST154.E+POE)
1.2.1.7 Power supply	5V AC adapter 2200 mA/h built-in Li-Pol batt (for ST154.A and ST154.W)
1.2.1.8 Current consumption, mA, no more than	500
1.2.1.9 Dimensions with no antenna, mm	109x60x27

1.2.2 Technical specifications of the Search module ST154.S

1.2.2.1 Frequency range, МГц	25-6000
1.2.2.2 Sensitivity threshold, dBm	
100 MHz	-90
1000 MHz	-95
2000 MHz	-95
4000 MHz	-85
5000 MHz	-75
1.2.2.3 Maximum input signal level, dBm	+5
1.2.2.4 Interfaces	USB
1.2.2.5 Indication	OLED display 160X128
1.2.2.6 Power supply	2200 mA/h built-in Li-Pol battery
1.2.2.7 Current consumption, mA, no more than	500
1.2.2.8 Dimensions with no antenna, mm	109x60x27

1.3 CONTENTS

1 Control module (ST154.A, ST154.W, ST154.E or ST154.E+POE)*

2 Search module ST154.S**

3 Antenna №1*

4 Antenna №2*

5 Power supply 5V 1A ***

6 Flash drive with software and operation manual

7 USB cable****

* Amount varies depending on the size of controlled area.

** Optional. One per system.

*** For all **CM** with no POE feature (ST154.A, ST154.W and ST154.E).

**** One per system

1.4 DEVICE AND OPERATION

1.4.1 General Description

Main unit of the system is a **CM** which identifies unauthorized radio transmissions in its range.

CM's effective work range depends on many factors. On the average this range can vary from 10 to 50 m^2. If used in open space, effective range is larger.

CM can transmit alarm signal on Control Center or it can work in **Offline** mode with sound and light alarm indication.

Control Center is a PC, laptop or Windows compatible tablet with installed ST154NET software.

Alarm signal is transmitted via ETHERNET or WLAN connection.

To localize the radio transmitting device it is possible to use:

- Search module **SM** (ST154.S). This module is designed for the fast detection of emission location. It works by getting data from Control module through Control Center USB connection and further detection of signal source by controlling signal level on **SM** screen.

- Procession of signal levels data gathered from no less than 3 Control **CM**s.

1.4.2 CM

There are 4 available modifications of the **CM** available. They are different by the way of alarm transmission: WLAN or ETHERNET. All modifications have 2 SMA sockets, LED alarm indication and radiator.

ST154.A – Standalone **CM**.

Alarm indication carried out by sound and light alarms which are located on the **CM**. Pre-installation parameters are set via USB port. This type of **CM** is intended primarily for the control within the one room.

Power supply is provided by a built-in Li Pol battery or AC adapter.

ST154.W = ST154.A+ transmitting via WLAN to the PC.
Power supply is provided by a built-in Li Pol battery or AC adapter.

ST154.E - ST154.A+ transmitting via ETHERNET to the PC.
The power supply is provided by 5V 1A Power supply.

ST154.E+POE = ST154.A+ transmitting via ETHERNET with POE to the PC.
The power supply is provided by network equipment with the support of POE feature.

1.4.3 System's configuration options

- **Minimal available configuration is one CM**
  It uses LED and sound indication for alarm.

This configuration is suitable to control one room.

- There are **CM** designed with remote alarm transmission through **WLAN or ETHERNET** (ST154.W, ST154.E or ST154.E+POE) for control of area varying from one room up to the whole building.

1.4.4 ETHERNET Connection

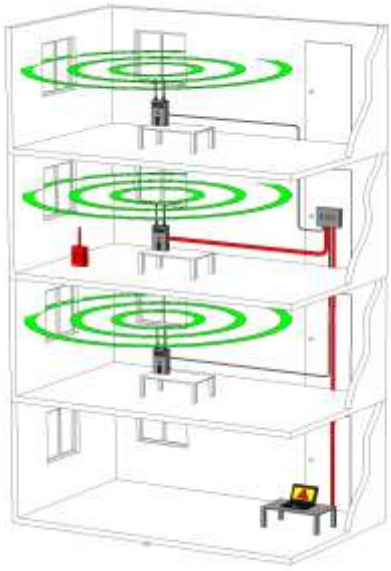
It is possible to connect **CM** to already existing or specifically created network.

Amount of maximum **CM** depends on the availability of ports in your network equipment.

It is possible to connect **CM** to PC directly or through available network equipment using «RJ-45».

To provide maximum reliable connection distance it is recommended to use ETHERNET cable of category 5 or better. Maximum possible length is no less than 100 m.

Maximum amount of connected **CM** is restricted by the number of free ports on network equipment.

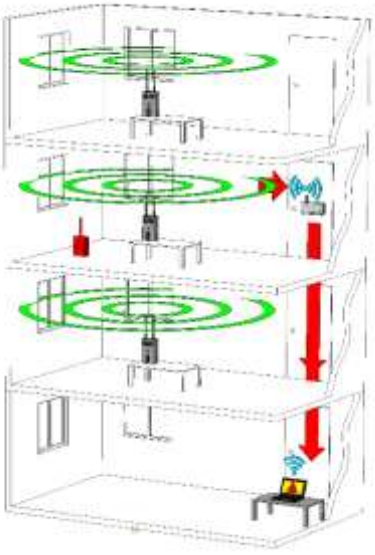


1.4.5 WLAN Connection

It is possible to connect **CM** to already existing network or new specially created wireless network.

Amount of connected **CM**s is restricted by WLAN range limitations.

To create your own network it is required to connect and configure WLAN router.



2. ST154NET SOFTWARE

ST154NET software is designed for preliminary setting of the **CM** and further monitoring of radio environment with creation of event log (only for Control **CMs** with remote alarm transmission through **WLAN or ETHERNET**).

2.1 Minimum PC requirements

OS: Windows 2000/XP/7/8/10
CPU: Pentium 4 or better
Memory: 1GB RAM
Screen resolution: not less than 1280X1024.

2.2 ST154NET Installation

Installation of «ST154NET» is done from the Flash drive which comes with device. Follow on screen instructions to proceed with installation.

When program is initialized for the first time (This instruction is for Windows 7, on other OS steps can differ) when prompted you should select the network which will be used and "Allow connection"

If selection was not made, it is possible to Allow/Deny connection to network through the Control Panel: Start -> Control Panel -> System and Maintenance -> Allow an app through Windows Firewall --> ST154NET.

2.3 User Interface

After program initialization there will be empty window with menu, toolbar and status bar. Main menu contains 3 items: **View, Settings and Help**.

View menu contains 2 items: **Event Log** (further description in 2.6) and **Rearrange Modules** — arranges **CM**S in consecutive order in top part of window.

Settings menu contains 3 items: **Options** (2.7), **Configuration** (2.8) – individual **Module** configuration, **Localization** (2.9) and **Default** – for factory settings.

Help menu contains 2 items: **Manual** – opens this manual, **About** – contains software version information.

2.4 Configuration

Configuration is a creation of common network for all **CM** in system. This can be done two ways:

- Setting PC's IP address with installed ST154NET software in each **CM** in system. This method is main and will be described in next paragraphs.
- Setting fixed IP address to PC with installed ST154NET software and then assigning this IP to each **CM** in system. This method is secondary and need for it will be described in Ch. 2.4.3

Configuration is done for each CM via USB connection

2.4.1 ETHERNET SETTINGS

These settings are required for station to work in network via ETHERNET.

Final target of these settings is saving IP address of Control Center in each **CM**.

It is important to notice that it is possible to integrate **CM** in already existing network as well as create new one.

To identify local IP address of your PC select **Start -> Control Panel -> Network and Internet -> View network status and tasks**. Next you should select your Local Area Network Connection.

If there is no local area connections in the list you should connect your PC to the network via ETHERNET cable and wait for network to appear in this window.

After selection of network you will see window

Pressing the **Details...** button will allow you to see your local IP address in **IPv4 Address** graph.

This address should be set in ST154NET software in **Settings -> Configuration -> ETHERNET Settings** submenu as **Server address.** To finalize this setting you should press **Send to device**. If you want to know what **Server address** device is currently using you can press **Request from device** button.

Disconnect USB cable from **CM** and connect ETHERNET cable to **CM** directly from or through networking devices. You will observe appearance of **CM** indicator in main window of ST154NET (few minutes delay is possible).

2.4.2 WLAN settings

These settings are required for station to work via WLAN network.

Final target of these settings is saving IP address of Control Center in each **CM**.

To start with, we need to check the condition of **CM**'s WLAN. In order to do this, we need to type **AT** in **Sending string** and press **Send** button. Device should respond with **OK** in the **Receiving string**. This means that **CM** is fine and we can start configuration of Wi-Fi.

Next we must fill **Wi-Fi Settings**:

«SSID» - name of the WLAN

«Security type» - selection of the WLAN security type (default is OK in most cases)

«Password» - connection's password

«Server address» - local IP address of Control Center.

To identify local IP address of your PC, select **Start -> Control Panel -> Network and Internet -> View network status and tasks**. Next you should select your Wireless Connection.

Pressing the **Details...** button will allow you to see your local IP address in **IPv4 Address** graph.

After everything is set and the button **Send to device** was pressed, information about data exchange with **CM**'s WLAN adapter will appear in **Receiving string**

If you want to know WLAN settings device is currently using, you can press **Request from device** button.

Disconnect USB cable from **CM** and observe appearance of **CM** indicator in main window of ST154NET (few minutes delay is possible).

If **CM** is configured it will automatically read this data from memory and attempt to connect to Wi-Fi, ETHERNET or USB.

If **Offline** mode was turned on, **CM** will proceed directly to work.

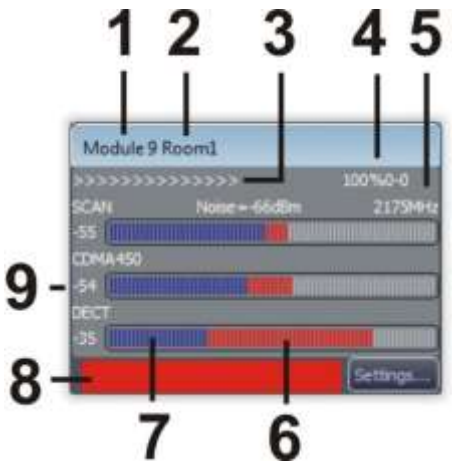
2.4.3 IP address selection problem when using ST154NET.

WLAN and ETHERNET usually feature automatic IP address assignment to all participants of the network so there is possibility that IP address of the PC with ST154NET will be changed without user interference (for example when new devices connect to the network while PC is off). If such thing happens all **CM**s will be not visible for PC.

To avoid this it is recommended to assign your PC fixed IP address (high value is preferred). By default ST154NET suggests IP address 192.168.1.64 (in few cases this address may differ).

To manually set this address you need to select **Start -> Control Panel -> Network and Internet -> View network status and tasks** then you have to identify the adapter and network you are using and select it in **Connection** line. Then you have to select **Properties -> IPv4 -> Properties** then tick **Use the following IP address** and in write "192.168.1.64" in IP address and "255.255.0.0" in DNS and press OK.

2.5 The CM Indication



When connection with **CM** is established you will see indicator of this **CM** in main window.

Title shows name of the **CM**. Factory number is shown by default (**1**).

It is possible to assign name to each **CM** by Right-Clicking window and selecting **Rename** option. Assigned name will appear after the factory number (**2**).

Cycle length indicator (**3**) allows to estimate time required to analyze selected channels. Less channels - faster cycle. Time for one cycle is the time of one arrow appearance. (2.4.1).

Data transfer from **CM** to PC is done independently for each **CM** after it finishes data procession cycle (**CM** are not synchronized with each other).

For analog signals data about signal will be transmitted only if signal is present for 5+ cycles.

In main part of the window, three signals with highest signal levels are shown. There are Title, Signal level in dBm (**9**) and 2-color graphical indication. Red color indicates excess of set signal level threshold (**6**). Blue color indicates the signal level over the noise level (**7**).

Full indicator means than the signal level is more than -20 dBm. Further increasing the level displays only in numerical value (**9**).

In case of 3G, 4G, WLAN or analog signal there will be available signal frequency (**5**). This information allows to identify cellular service provider and the WLAN channel number.

Red rectangle (**8**) indicates excess of set threshold for any signal type.

Additionally there is numeric service information of current state of connection (**4**).

Indication options are available in **Options** menu. **CM** windows are draggable and position is saved for the next sessions

2.5.1 Channel assessment time

Maximum time – 20 seconds with all channels are selected, maximum range for analog signals is set and minimum bandwidth (2 MHz).

With maximum bandwidth (20 MHz) – three seconds.

With only cell channels – less than one second.

Time required to transfer data from **CM** to PC is insignificant and slightly depends on amount of working **CM**s.

2.6 CM Settings

It is possible to adjust **CM**'s settings individually by clicking **«Settings…»** in **CM**'s window.

This window contains all channels available for assessment (Pic.4).

Each channel or group can be toggled by selecting/deselecting it.

At least one channel must be selected or software will automatically set GSM 900.

It is possible to set activation threshold for each channel.

Next to each channel there is tick box **"For ALL"**. If it is ticked channel setting will be applied for all **CM**s in network. Setting will become effective after few seconds.

Channels are divided on four main subcategories:

2.6.1 Cellular – contains standards for cellular and microcellular network.

2.6.2 2.4 & 5 GHz – unlicensed frequency range (ISM) in 2.4 and 5 GHz range. WLAN and BLUETOOTH networks are represented here.

It is possible to monitor intensity of data transfer in these networks. This channel DOES NOT display signal level. Result is displayed in range from 0% to 99%. Values less than 10% means insignificant amount of transferred data. 20% and more corresponds to big amounts of data.

2.6.3 Jammers

Cellular and GPS signal jammers are present in this subcategory.
Detection of GSM jammers is based on their ability to emit wideband signals at least in two frequency ranges (900 and 1800 MHz).
Detection of GPS (GLONASS) jammers is based on the analysis of emission in this standard's range.

2.6.4 Scan

It is possible to set conditions (Squelch level; start, end and step frequencies) for detection of analog signals in this subcategory.

Squelch is set relatively to noise level in range from 0 to 30 dB. If this threshold is set too low it increases chance of false positive alarm (detection of signals, with sources outside of controlled area), however lower threshold means that the chance of detection of weak signals is higher.

Step freq is equal to the analysis bandwidth. It is possible to select in range from 0.1 to 20 MHz. Selection should be made based on the requirements of scan detail. With wider band analysis is faster but the level of noise is higher (lower chance of weak signals detection).

After analysis **CM**'s indicator will display strongest signal, its frequency and level of noise in selected range.

2.6.4.1 Scan-pause option

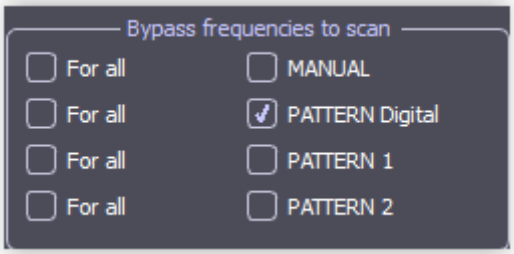
This category allows capture (input) and analysis of signal level of one frequency for one or all **CM**s. It is possible to input frequency two ways:

- Automatic capture with **"AUTO fill frequency"**. In this mode, frequency detected during the scan mode is set automatically.

- Manual input of frequency in window: **"Frequency, MHz"**

To pause on the selected frequency, you need to tick **"PAUSE"**.
Setting bandwidth in **"Band, MHz"** in this mode changes sensitivity threshold. Higher value – lower sensitivity.

2.6.4.2 Excluded Frequencies

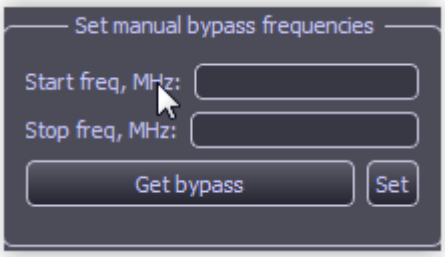


Because there are plenty of legal signals present in every area there is option allowing manual and automatic skip of certain frequencies using ready or user-made presets.

Those frequencies include cellular network base stations, television channels, radio station and different radio signals of industrial, military or other origin.

Automatic frequency skip is supported for cellular network frequencies (phones and base stations) and 2.4 and 5 GHz range. It is required to tick **"PATTERN Digital"** (Set by default) for these features to work.

2.6.4.3 Manual frequency skip



This window is purposed to create your own list of frequencies excluded from analysis.

Created list can be used during current session or use it as a base for a preset which can be used later in future at any time with any configuration of system and working conditions.

For immediate use you need to tick "Manual" in **"Bypass frequencies to scan"**.

To select frequency band you need to set start frequency (**"Start freq"**) and end frequency (**"Stop freq"**).

Manual exclusion of single signal is possible by two ways:

- Setting same value for the **"Start freq"** and **"Stop freq"** and pressing **"Set"**. If frequencies are set correctly info window with confirmation will appear.

- Select in event log (ch.5) signal which must be excluded, right-click it and select **"Bypass this frequency"** or **"Bypass this frequency for all"**.

To browse list of excluded signals you can press **"Get bypass"** button.
If you select only **"PATTERN Digital"**, you will only see frequencies of cellular network excluded from analysis.

If **"MANUAL"** is selected, list will show list of frequencies created by user.
If you select both option you will see all excluded frequency ranges as well as single frequencies.
To delete frequency or range from this list, select it and then right-click your selection.

It is possible to create individual list of skipped frequencies and save it as **PATTERN1** or **PATTERN2**.
You should first create list in **MANUAL** mode. If there is data present you can save it with **"SAVE"** under any name for later use and then delete any present data with **"By default"** button.
After new list was created in window "**Set manual bypass frequencies**" press **"Get bypass"** - **"SAVE"** and pick a file name to save on your PC

Loading excluded frequencies

Loading file with required list of frequencies is done in window **"Load bypass frequencies to..."**
When **"Load"** button is pressed you will see files with saved lists on the computer.
After selection of file with frequency list it will load into **PATTERN1** or **PATTERN2** which was selected before pressing **"Load".**

2.6.5 Defaults

To return to factory settings you should press **"Settings"**.

After pressing **"Bypass frequencies"** all lists of excluded frequencies except for **"PATTERN Digital"** are deleted.

2.6.6 Identification Disable (Only for testing purposes) - ticking it turns off identification of digital protocols.

Identification of signal in this system is done by analyzing fixed frequency ranges and temporary parameters of detected signals.

For GSM, DECT and BLUETOOTH signals it will be displayed only if frequency band correlates with timing parameters of signal.

2.6.7 "Device indication and offline mode"
In window **"Device indication and offline mode (out of network)"** you can switch your **CM** in offline mode and set parameters for LED and sound indication on **CM**.

Option of light indication:

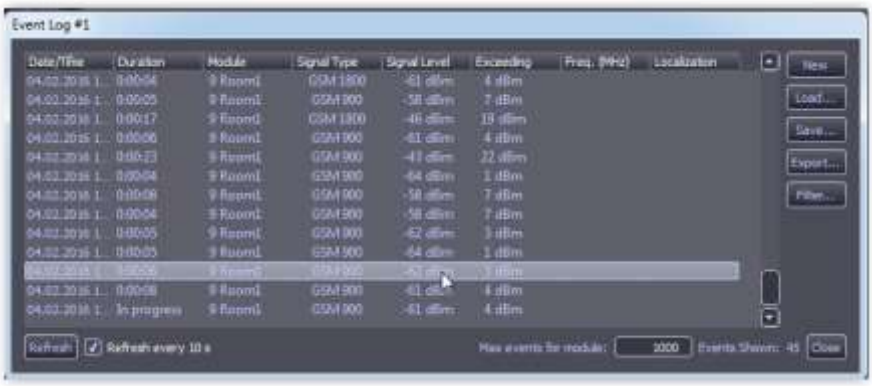
- **"Power + Link"** - permanent light and switches off for the time of data transmission with PC (by USB, ETHERNET or WLAN). If **CM** is in offline mode light is always ON.
- **"Diagnostic"** - one blink every 30 seconds. This indication is used to acknowledge **CM**'s working condition.
- **"Alarm"** - one blink per second if alarm conditions are met.
- **"Alarm + Diagnostic"** - one blink per second if alarm conditions are met + blinks every 30 seconds.

If sound indication it will only be active during alarm.

Parameters of acoustic and light indication are active immediately after selection.

To switch **CM** in offline mode you need to tick **"Enable offline mode"** and press "OK".

2.7 Event log



Event log is always recorded, regardless other settings.

Event log is possible to open in **View** and also by using according button on toolbar.

It is possible to open and work with multiple event logs at the same time (just open it again).

Event log always contains 7 columns. When you hover cursor over name of column and press left-click it will sort all log according to this column. If you click more than one time it switches sort order Ascending\Descending.

Event log shows events from all **CM**s. By default event log is entirely refreshed every 10 seconds. For convenience of the analysis auto-refresh is possible to turn off in the bottom of the window and refresh list manually by pressing **"Refresh"**.

By default event log can't contain more than 1000 events for each **CM**. After limit is reached oldest data will be deleted to create free space.

Maximum number of events on **CM** is changeable. After changing value you should confirm selection by pressing Enter on your keyboard.

Pressing **"New"** button allows creation of new event log. After confirmation **"Do you want to clear the log?"** existing data is erased.

Pressing **"Load..."** button allows to load event log saved earlier.

Pressing **"Save..."** buttons allows to save event log in your PC's drive for later use in this software.

Pressing **"Export..."** button allows to save event log in PC's drive in "HTM" format for later view of event log outside of designated software. In this case it is not possible to sort event log by desired columns.

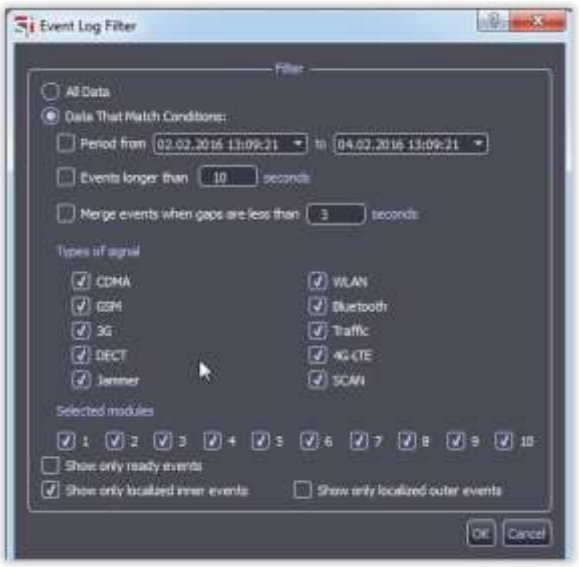
Event log always contains all available data about event.

"Filter..." button allows to filter event by such conditions as: time of event, length of event, signal type, **CM**s.

It is possible to merge very short events together.

While working with event log you need to be aware of **CM** assessment cycle length. It varies from less than one second (when working with digital signal) up to 20 seconds for the most precise analysis. So for example in the last case it is rational to set **"Events longer than"** 20 sec and **"Merge events when gaps are less than"** 20 secs.

If **"Show only localized inner/outer events"** options are selected, only localized signal will be shown (for three or more **CM**s).



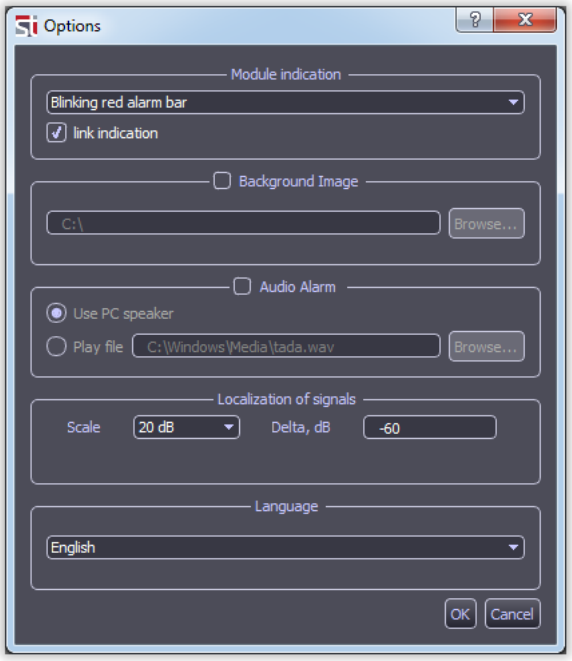
Number of unfiltered events during the day for all **CM**s can reach and surpass 10000. With filtering by proper criteria this number can be 10 and more times lower.

When you select required signal, you can right-click your selection for a wider variety of options such as:

- Add this frequency in list of excluded frequencies (Ch. 2.6.4.2 **Manual frequency skip**)
- Add this frequency in list of excluded frequencies for all **CM**s
- Transmit this frequency on external receiver via USB

2.8 Options

Options window is possible to call from **Settings** menu. In this window it is possible to:



- Selection of additional alarm indication options (Pic.3 Pos.7)
- Allowing indication of analysis cycle length
- Setting background for main window of program (floorplan of building etc.). Size of image must be selected accordingly to the screen resolution.
- Trigger of sound alarm on PC when threshold is exceeded. It is also possible to select alarm sound.
- Selection of localization speed. Lower value corresponds to faster move.
- Language selection: English or Russian.

2.9 Localization.

If number of **CM**s in system is more than three it is possible to use **"Localization"** function by pressing according button. It will automatically localize signal and indicate supposed location as a circle. Diameter of circle and accuracy of localization depends on the number of **CM**s and their position related to signal source.

Localization requires for target signal to be detected by three or more **CM**s.

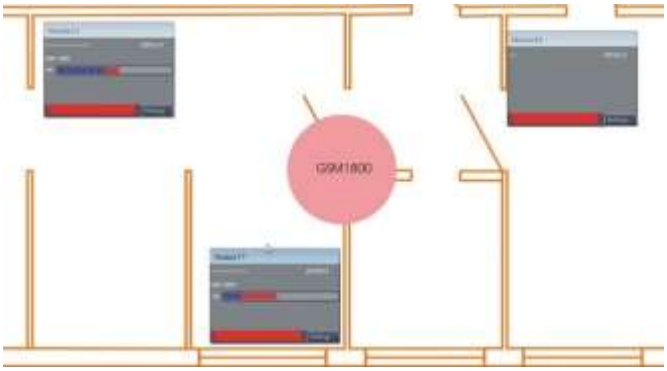
The less circle diameter, the more accuracy of localization.

The best arrangement of **CM**s is in the corners of an equilateral triangle. The worst arrangement is on one line.

Moving activity of circle can be set in **"Options – Localization of signals - Scale"** (Ch. 2.8). The option **"Delta"** allows to determine inner and outer signal during localization process. When selecting this setting you have to consider two conditions. The maximum possible localization accuracy of inner signals and ignoring outer signals.

So, to fulfill the first condition, the value **"Delta"** should be minimal, for the second condition should be maximal. The choice is a compromise between these terms.

On the picture we can see GSM 1800 cell phone being localized.



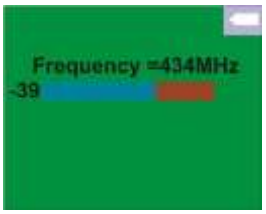
3. SEARCH MODULE ST154.S

The search module ST154.S (**SM**) is designed to determine the exact location of the radio source.

Working with the SM is divided into two stages:

- Transfer the signal frequency or data transfer mode into the SM;
- Physical localization of the radio signal source.

Connect the SM to the PC via USB cable and launch the ST154.NET program to get data to be transferred. In the event log (Ch. 2.7), select the desired signal and click the right mouse button then select the line: **"Send this frequency/item to the external receiver via USB"** and confirm. If successful, the signal level is shown as a numerical value and a multi-segment scale.



The physical localization is performed by moving inside the searching area in the direction of increasing the displayed signal level. The greater signal strength, the closer the source of radio.

3.1 Power supply of ST154.S

Power supply is provided by a built-in Li Pol battery or AC adapter.

The battery charge level is displayed in the upper right corner of the screen. Fully colored icon corresponds to the full battery, empty icon corresponds a fully discharge.

To charge the battery, connect the AC adapter. Position of the power switch does not matter. The "CHRG" indicator, located on the side of the SM, shows the charge is active. At the end of the charge of the indicator turns off. A full charge takes about six hours.

4 WORK WITH SYSTEM

4.1 Recommendations

Before setting up system on spot it is highly recommended to check it for special technical means (STM) of eavesdropping. One of reason is that this system only detects radio emitting STM. Other classes of STM (for example wired microphones, dictaphone, infrared transmitters etc.) are not detected by this system.

It is common practice to use STM with different ways of data transfer (wired and radio transmission for example).

It is also possible that there is STM with high emitting power used as decoy and can be "easily" found to draw attention away from other STMs.

4.2 Installation the CM on the working place.

To make a decision of placement of the **CM**s, the possible coverage area of STM devices should be examined first. As usual the microphone sensitivity of the STM is about 10 meters and common places of the installed STMs are inside meeting tables or nearby.

Thus, if the only **CM** is considered to be installed in one room, it must be located in the center of the working area.

The presence of external signals from the lower and upper floors should be taken into consideration.

When three or more **CM**s are being installed, make sure their arrangement in view of features of the localization possibility.

4.3 Antennas.

The supplied RF antenna is not optimal for the entire frequency range of the **CM**. Using it is justified in the case of requirement minimum dimensions and value-based pricing.

If specific requirements are taken place, the narrowband and appropriate antennas should be used, for example, the receiving antenna for particular cellular band. It will improve detectability of these particular signals.

The greatest effect is achieved by using a directional antenna, which allows to exclude or minimize influence the signals out of working area as well as to improve detection possibilities. The effect of using these kind of antennas is enhanced in the **Localization** mode.

4.4 Work with EVENT LOG.

In real time the PC screen may be displayed multiple alarms caused by transient signals, which do not pose as danger signals. Therefore it is recommended to use the event log for reviewing the detection results. Using the filter option in the event log is an important factor.

For example, the option **"Merge events when gaps are less than … seconds"** allows to reduce the list of log significantly.

When the **Localization** option in use and the **"Show only localized inner events"** option selected, the event log will be reduced even more.

4.5 Using the USB connection.

The USB connection provides:

- Operation of any **CM** with the ST154NET program, including the **CM** configuration for standalone work (Ch. 2.6).

- Configuring the ST154E, ST154E+POE and ST154W for ETHERNET and WLAN networks (Ch. 2.4).

4.6 Getting started.

4.6.1 The CM ST154.A

Connect ST154.A to the PC via USB cable and launch the ST154.NET program to configure this device. After appearing in the main window appropriate small indicator window (Pic. 3), make configuring detection conditions in according to chapter 2.6 and recommendations in the current chapter. Upon completion of the settings, disconnect the PC from the **CM**.

4.6.2 The CMs ST154.E, ST154.E+POE, ST154.W

Connect the **CM** to the PC via USB cable and launch the ST154.NET program to configure this device. After appearing in the main window appropriate small indicator window (Pic. 3), make configuring for working in the specified network (ETHERNET or WLAN).

Upon completion of the network settings, disconnect the PC from the **CM**. If network configuration has been done properly, in a minute after disappearing small indicator window this window will be shown again with the data transferred through the network.

4.7 Detection of cell phone and STM using cellular network standards

Possible ways of exploitaition:

- Visitor having phone on. It uses to get information of conversation in real time. Low sensitivity of cell phone's microphone is main restricting factor.

- "Forgotten" phone method is used to get instant information regarding meeting after which the phone was "forgotten"

- Specially manufactured STM with high battery capacity, extremely sensitive microphone and working in all frequency ranges.

Such devices feature remote ON\OFF toggle so they only active during required time (during meeting, negotiations etc.).

Modern cell phone transmits only:

- If sound signal is present after establishing connection.
- During data transfer (i.e. SMS)
- When connecting to the base station.
- All other time cell phone is only works for reception. It is not possible to detect device unless it transmits.

Detection range depends on emission power of cell phone and range to the closest base station. Emission power is higher if base station is further away. Emission power of GSM900\1800 phone can be up to 33 dBm (2W) with maximum distance to the base station and about 10 dBm (10mW) when station is up close.

Approximate range of detection GSM900\1800 standard in the city is about 10 meters (this estimation does not includes walls, reflection and absorption).

3G-2100 channels differ by significantly lower level of signal emission. In city environment it varies from +14 to -30 dBm (from 25mW to 1μW). Therefore, this channel requires most accurate configuration. System possesses designated antennas to increase maximum sensitivity in 3G channel. It works in range from -100 to -75 dBm. If selected threshold is -75 dBm main antenna will be used for 3G analysis.

In microcell connection DECT for eavesdropping and data transmission can be used phone modes with function of ambient listening or baby phones.

4G - noise-like signal with emission power counting tens of mW

4.7.1 The CM settings

Select only **"Cellular"** in **"Settings..."** You can do it for all **CM**s at the same time.

Turn off all cellular devices on controlled area for the time of setup.

Set sensitivity threshold about 5 dB higher than the ambient noise level. When selecting the threshold, ignore short term indication (these are usually random signal from long distances). If there is a constant signal for tens of minutes and signal level more than -60dBm (Pic.3 Pos.8), that tells about work of GSM modem or STM with GSM channel of data transfer. For the fast result you can set threshold level of **CM** with the highest level of noise for all **CM**s by ticking "For All". You can later alter threshold individually for every **CM**.

4.8 Detection of devices using WLAN+BLUETOOTH standards

4.8.1 WLAN

This standard can be used for:

- Unauthorized data transmission from PC. Time and amount of data is unidentifiable.
- Video snooping by using WLAN video camera.

System has no ability to distinguish between legal or illegal networks but it can detect data transmission. This means that indication of signal level and traffic there must be present data transmission (download is data reception and is not detected by system). System shows signal level and traffic from all networks in controlled area. Usual level of traffic when browsing internet

is around 10%. Depending on the WLAN camera and image dynamics traffic can vary from 10 to 100%.

It is also important to notice that if camera transmits data to the PC in the same WLAN it will show traffic increase from two sources - from camera and from wireless router which retransmits data to PC. This can make search for camera more complicated.

4.8.2 BLUETOOTH

When using this standard there are few ways for unauthorized data transmission:

- Data transfer from PC, cellphone's contact list and other data.
- Reception and transfer of audio data from Bluetooth headset.

Emission power of devices using this standard is changing drastically because of current usage. From tens of μW (Bluetooth headset) to tens of mW (data transmission).

System identifies establishing of the Bluetooth connection between devices.

This is short term event and to find it in the event log minimum time must be less than one second. Range of detection is <1m.

4.8.3 The CM settings

In **"Settings…"** select only **"2.4 & 5 GHz"** and set minimum levels of detected signals and traffic (All sliders in left position).

Set alarm threshold about 5 dB more than indicated level and 5% more for traffic.

4.9 Analog signal detection

Analog signals are constant signals with wide or short band frequency modulation. There are numerous STMs which use this kind of transmission.

They differ by emission power, power supplies and remote on\off toggle feature.

Emission power defines maximum range of data transmission from this device and usually varies from mWs to Ws (there are few exotic devices with higher emission power). Minimum power is corresponds to transmission through the wall and maximum to hundreds of meters.

4.9.1 The CM settings

Turn this channel ON for all **CM**s with maxed out slider - minimum squelch level, maximum frequency range and minimum step. Turn all other channels off in settings (uncheck).

These settings give value of minimum noise level on the **CM**'s placement and their threshold sensitivity. In future, this will allow us to properly distinguish STM detection range. On pic. 10 noise level (pos.2) is -90 dBm (7μW).

To speed up signal detection (up to 5 times faster) tick **Identification Disable (Only for testing purposes)** (Ch. 2.6.6).

Information about ability of system to detect signals is presented in Table 1. It contains dependency between emission power of radio transmitting device, placed on different range from **CM** and level of signal indicated on **CM**. Data is recorded at 1000 MHz frequency. This data is for reference only and not formal measurements.

Table 1

Distance, m	0.1 mW	1 mW	10 mW	100 mW
1	-50	-40	-30	-20
5	-60	-50	-45	-25
7	-70	-60	-40	-30
10	-80	-70	-60	-35

Frequency range selection is done accordingly to supposed STM frequencies. Because of specific of radio waves spreading and cost most popular frequencies among STM are from 100 MHz to 2 GHz. This setting also affect analysis time.

In range from 20 to 6000 MHz and 2 MHz step it takes about 13 sec to assess area, 100-2000 MHz is about 5 secs. When selecting 20 MHz step it takes less than 1 second.

When you increase analysis step value to the maximum (20 MHz), noise value increases up to -80dBm (22μW) but it drastically increases analysis speed. It is recommended to have medium value – 10 MHz

Create manual list of legal frequencies (ch.2.4.3 Scanning)

When you are creating list use "Attachment 1" which includes frequencies of TV channels. If found frequency overlaps with central frequency (+/- 2 MHz) of image or sound from attachment you should add this frequency to the list. Regardless bandwidth of image being 6 MHz recording is done as single frequency.

In case of detection of unidentified frequency you need to localize its source. One of the information source is the difference between signal levels on different **CM**s. It is recommended "Scan pause options" for this.

After finishing the setup you should untick **Identification Disable (Only for testing purposes).**

5 MANUFACTURER'S WARRANTY

5.1 The manufacturer guarantees that each manufactured product meets all requirements of the specifications for a period of 12 months from the date of sale.

5.2 The manufacturer shall, within the warranty period if free of repairs are required, its subsidiary and other parts, until replaced by the instrument as a whole, if it is during this time will be damaged or its performance will be lower standards specifications.

5.3 Covers free repair (control) or replacement shall be made only when the user observes the rules of operation, transportation and storage, in the absence of mechanical damage to the device itself and its parts, as well as the presence of a correctly completed warranty card.

5.4 The warranty applies to each of the products only in the presentation of a consumer with a warranty card stamped manufacturer and its dealers to sell, certified by an official round stamp standard pattern.

6 CERTIFICATE OF ACCEPTANCE

ST154 device №_____

meets specifications and is fit for use.

Release Date _____

COUPON № 1 For warranty repair (maintenance) of ST154

number _____ Made _____

Seal of the manufacturer

Sold _____ (Trade name of the company)

Date of sale _____ 201__Seller_____ Vendor Seal (signature) of commercial

enterprise_____
_____

Spine ticket number 1 for warranty repairs (maintenance) of the ST154 № _____ seized the

contractor _____
(surname, personal signature)