Alarm module
with GSM/GPRS communicator

MICRA

CE

Firmware version 3.03

micra_en 04/18

SATEL sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
POLAND
tel. + 48 58 320 94 00
www.satel.eu

WARNINGS

The device should only be installed by qualified personnel.

Read carefully this manual before proceeding to installation.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

CAUTION!

It is not allowed to connect a fully discharged battery (with voltage across unloaded terminals less than 11 V) to the module. In order to avoid any damage to the equipment, if the battery is fully discharged, precharge it by means of a suitable charger.

The batteries contain lead. When used-up, the batteries must not be thrown away, but disposed of as required by the existing regulations (European Directives 91/157/EEC and 93/86/EEC).

Due to the specific character of data transmission using GPRS technology and possible costs involved, it is advisable to install in the module a SIM card with tariff plan providing for at least 10 MB monthly data transfer.

SATEL's goal is to continually improve the quality of its products, which may result in alterations of their technical specifications and firmware. Current information on the introduced modifications is available on our website.
Please visit us at:
http://www.satel.eu

**Hereby, SATEL sp. z o.o., declares that this module is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
The declaration of conformity may be consulted at www.satel.eu/ce**

The following symbols may be used in this manual:

- note;
- caution.

Changes made to firmware version 3.03

Wireless devices	Support for MPT-350 keyfobs.
Telephone settings	Capability to select the operator of the GSM network the module is to log into.
Reporting	Possibility to send events to the monitoring stations using the following formats: – SATEL IP, – SIA-IP. New parameters for SIA-IP format: – SIA-IP account no., – Test transm. every.
Event log	Possibility of printing / exporting event log to file.

CONTENTS

1. MODULE FEATURES

- 4 individually programmable hardwired zones with optional operation in digital (NO, NC, EOL) or analog mode (voltage measurement 0...16.56 V).
- Additional TMP hardwired zone to supervise NO or NC wiring type:
  – acting as a tamper loop input in communication device mode,
  – programmable in alarm device mode.
- 2 programmable NO or NC type relay outputs.
- OC type output serving as indicator of GSM network logging problems, or as armed mode indicator.
- High-current (0.5 A) output, with polymer fuse, to perform the function of power supply output (optionally, it can perform the power input function).
- Ability to remotely control the relay outputs with the CLIP service.
- Built-in radio waves superheterodyne receiver:
  – support for up to eight 433 MHz keyfobs manufactured by SATEL;
  – support for up to eight 433 MHz wireless detectors manufactured by SATEL;
  – support for MKP-300 wireless keypad.
- Non-volatile 1024 event log buffer.
- Information on the status of supervised equipment and module through reporting in Contact ID format (GPRS, SMS) or messaging (SMS, CLIP).
- Encrypted transmission of events sent with the use of GPRS technology (TCP or UDP protocol) and SATEL IP or SIA-IP format.
- Capability to automatically replace the GPRS transmission with SMS message, if there are problems with GPRS transmission.
- Periodical test transmissions for checking availability of the module:
  – to selected telephone numbers (with the use of SMS message or CLIP service);
  – to monitoring stations.
- Capability of generating additional test transmissions:
  – after identification of the calling party's telephone number (CLIP service);
  – after receiving command from the GPRS-SOFT program.
- Capability of arming / disarming the premises by means of CLIP service.
- Option to check the status of available resources and account validity of the SIM card installed in the module.
- Listen-in feature for alarm verification by means of a telephone (external microphone required).
- Remote control capability by means of the MICRA CONTROL application.
- Module configuration:
  – locally – through the RS-232 (TTL) port;
  – remotely – through the GSM network (GPRS technology);
  – remotely – using SMS messages.
- Capability of remotely updating the module firmware by means of GPRS (units with built-in GSM u-blox LEON-G100 telephone).
- Indicator of GSM signal level received by industrial cellular telephone and an indicator of troubles connected with logging into the GSM network.
- Capability to select the operator of the GSM network the module is to log into..
- Automatic module restart capability.

- Switching mode power supply, output current 2 A with short-circuit protection, provided with battery status monitoring and low battery disconnection circuit.
- Powered with 18 V AC (±10%).
- Possibility to power with 12 V DC.

2. DESCRIPTION OF ELECTRONICS BOARD

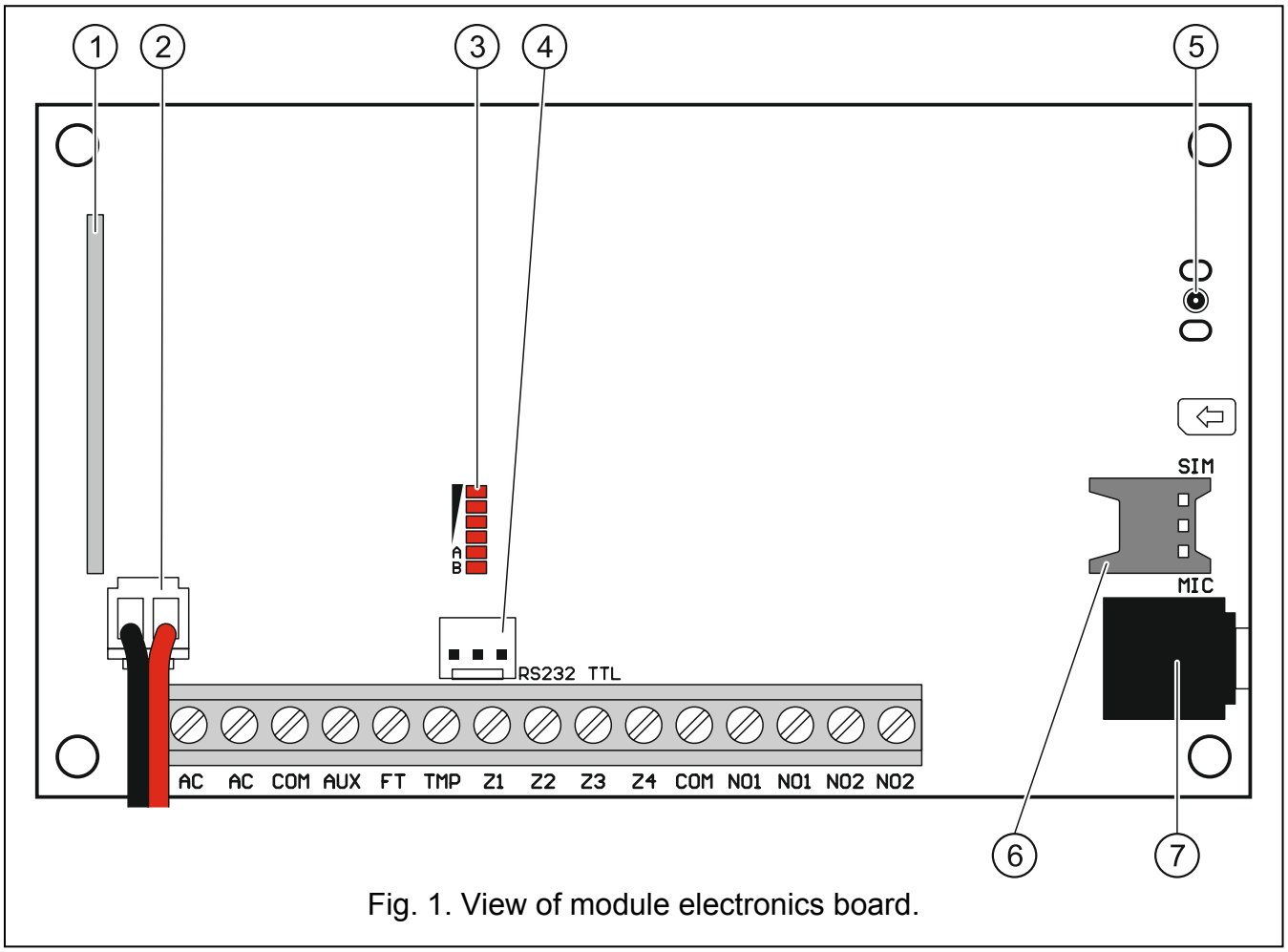


Fig. 1. View of module electronics board.

Explanations for Figure 1:

(1) **superheterodyne receiver**, high sensitivity, immune to spurious signals.

(2) **battery connection cables**.

(3) **LEDs** indicating the module status. LED A is blinking when GPRS transmission is going on. LED B is blinking when SMS message is being sent or the module is calling (CLIP test transmission). The other LEDs indicate the level of signal received by the GSM telephone. LEDs A and B blinking simultaneously indicate logging into the GSM network. In case of an unsuccessful GSM network login, blinking of the other LEDs provides information on the troubles (see: Fig. 2).

(4) **port RS-232 (standard TTL)** enables local programming by means of the GPRS-SOFT program (connection can be made using the USB-RS converter offered by SATEL).

(5) **antenna socket**. Be careful when connecting the antenna so as not to damage the socket.

(6) **nano-SIM card socket.** It is not recommended to insert the SIM card into its socket before programming the card PIN code in the module (if the card requires entering the

PIN code). If the event codes are to be sent with the use of GPRS technology, the GPRS service must be activated for the SIM card installed in the module.

⑦ **microphone socket.** The microphone enables the listen-in feature (it is recommended to use an electret microphone, e.g. a typical computer microphone).

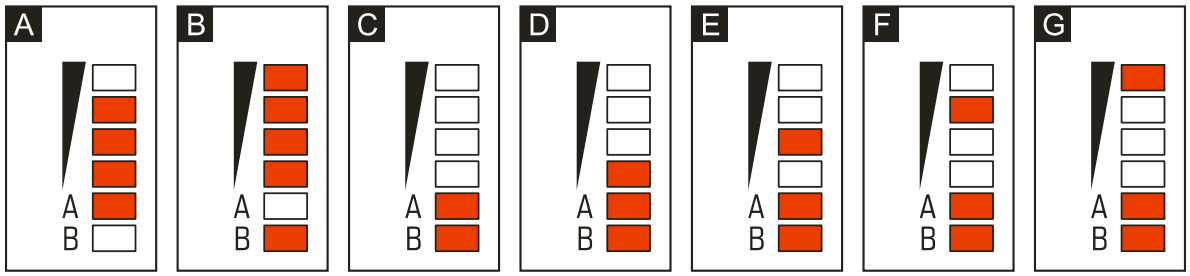


Fig. 2. Examples of LED indicated statuses.

Explanations for Figure 2:

A (LED A is blinking, the other LEDs are lit up) – GPRS transmission is going on; signal level: 3.

B (LED B is blinking, the other LEDs are lit up) – SMS message is being sent or module is calling (CLIP test transmission); signal level: 4.

C (LEDs are blinking) – logging into GSM network.

D (LEDs are blinking) – logging into GSM network has failed; missing SIM card.

E (LEDs are blinking) – logging into GSM network has failed; missing PIN code.

F (LEDs are blinking) – logging into GSM network has failed; invalid PIN code.

G (LEDs are blinking) – logging into GSM network has failed; SIM card has been blocked after three attempts to use an invalid PIN code (PUK code must be used to unblock the SIM card).

Description of terminals:

AC - power supply inputs (18 V AC ±10%).

COM - common ground.

AUX - power supply output / input (12 V DC ±15%).

FT - OC type output (shorted to ground when active) to work as an indicator of problems with logging into GSM network (it activates approx. 2 minutes of the problem occurrence) or an armed mode indicator (with the ARM STATUS ON FT OUTPUT option enabled). The problem with logging into the GSM network can be caused by:

- unavailability of GSM network (out of range),
- missing or damaged antenna,
- entering an invalid PIN code,
- missing SIM card.

Some additional information can be provided by LEDs on the electronics board (see: Fig. 2).

TMP - tamper zone (it can supervise the tamper contact of module enclosure, detectors, sirens, etc.).

Z1 ÷ Z4 - zones.

NO1 - relay output 1 terminals.

NO2 - relay output 2 terminals.

3. INSTALLATION

Disconnect power before making any electrical connections.

Before connecting the power supply source (battery, alternating voltage from transformer), you should first complete all the installation work.

The following tools will be useful during installation:

- blade screwdriver 2.5 mm,
- Phillips screwdriver,
- precision pliers,
- flat nose pliers,
- drill with a set of drill bits.

3.1 INSTALLATION PLAN

If the module is to be a component of alarm system, the installation should be preceded by preparing a plan of arrangement in the premises of all devices to be included in such a system, i.e. MICRA module, detectors, keypad and sirens.

3.2 ESTIMATION OF CURRENT CONSUMPTION

Before proceeding to installation, sum up the currents consumed by all devices to be power supplied by the module (the calculation should also take into account the battery charging current.). The sum of such currents must not exceed the current output of the built-in power supply. If the sum of currents exceeds the power supply current output, an additional power supply unit must be used.

When planning connection of devices to power output, remember that the sum of currents consumed by these devices must not exceed the maximum current-carrying capacity of this output.

3.3 CABLING

It is recommended that straight unscreened cable be used for making electric connections (using the twisted pair type of cable, e.g. UTP, STP, FTP is not advisable). Select cross-section of the power supply wires so that the supply voltage drop between the power supply and the supplied device should not exceed 1 V as against the output voltage.

When making the cabling, remember that there must be sufficient distance between the low-voltage wires and the 230 V AC power supply wires. Avoid running the signal cables in parallel to the 230 V AC supply cables, in close vicinity of them.

3.4 THE MICRA MODULE INSTALLATION

The module PCB contains electronic components sensitive to electric charges.

The MICRA module should be installed indoors, in spaces with normal air humidity. The installation place should be inaccessible to unauthorized persons. When selecting the installation place, take into consideration that thick walls, metal partitions, etc. will reduce the radio signal range. Installation in close vicinity of electrical systems is not recommended, as it may adversely affect the device performance.

An unswitched 230 V AC supply must be available at the module installation place. The power supply circuit should be protected with a proper safety device.

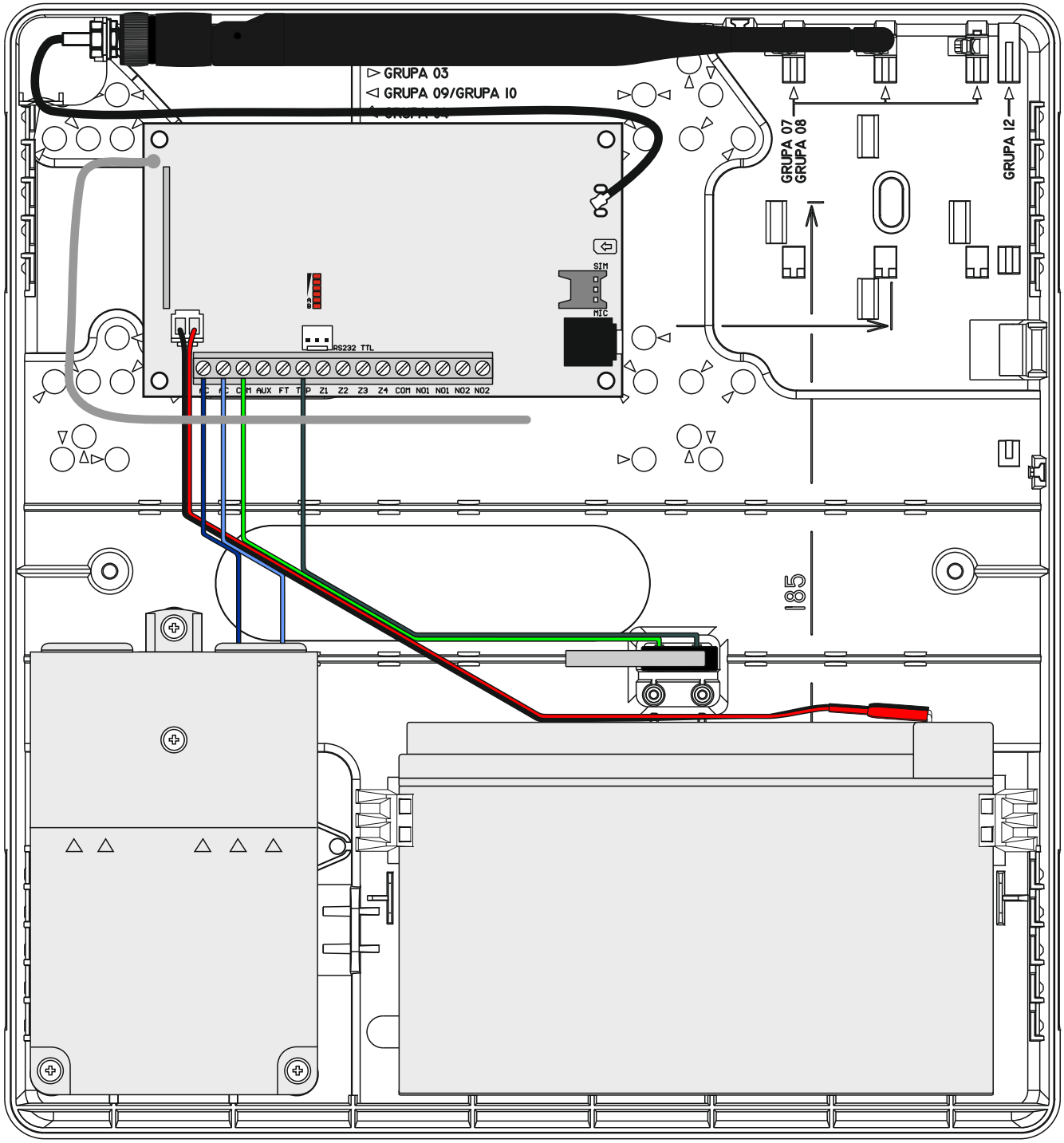


Fig. 3. MICRA module with connected antenna, battery and transformer, installed in OPU-4 P enclosure.

3.5 CONNECTING DETECTORS AND OTHER DEVICES TO ZONES

The module zones can work as:

- digital, NC type – to supervise a device with normally closed contacts,
- digital, NO type – to supervise a device with normally closed contacts,
- digital, EOL type [only in alarm device mode] – to supervise a device with normally open or closed contacts, where an 2,2 kΩ EOL resistor is used,
- analog [only in communication device mode] – to handle analog signals from devices used in automation (measurement of temperature, pressure, rotation, etc.).

The devices to be connected to the zones can be supplied directly from the module (AUX output) or from an additional power supply unit. The choice of the power supply source should be made conditional upon the previous estimation of current consumption.

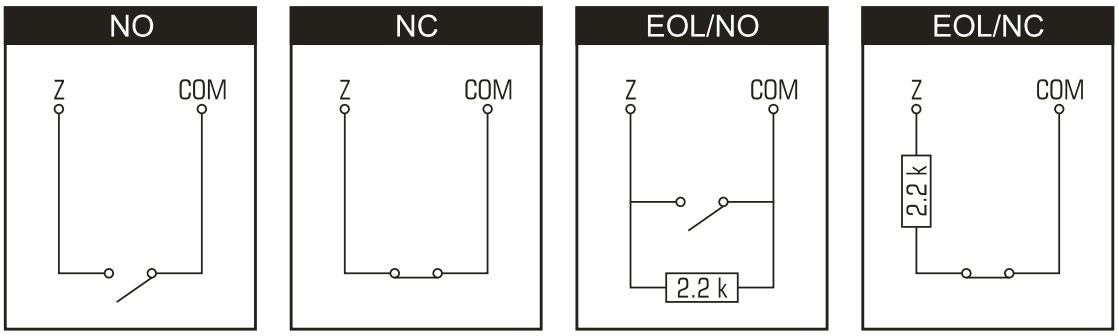


Fig. 4. The ways of connecting detectors to the alarm module.

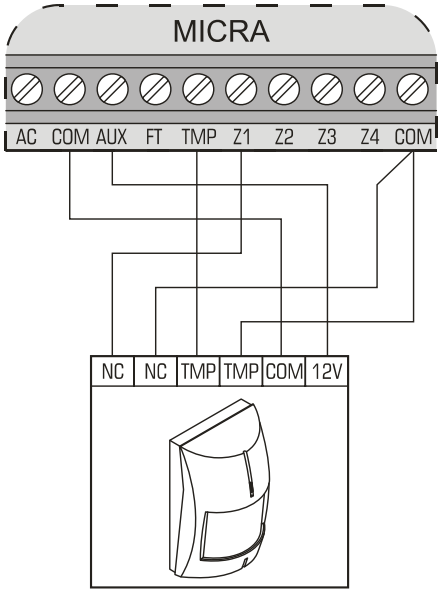


Fig. 5. An example of connecting NC type detector to the MICRA module (NO type detector is to be connected in the same way).

3.6 CONNECTING SIREN

Relay outputs should be used to control a siren. The way in which the siren will be power supplied should depend on an assessment of current consumption, which should be made beforehand. The siren can be powered from the module AUX output, if the current consumption by the siren does not exceed the output rating.

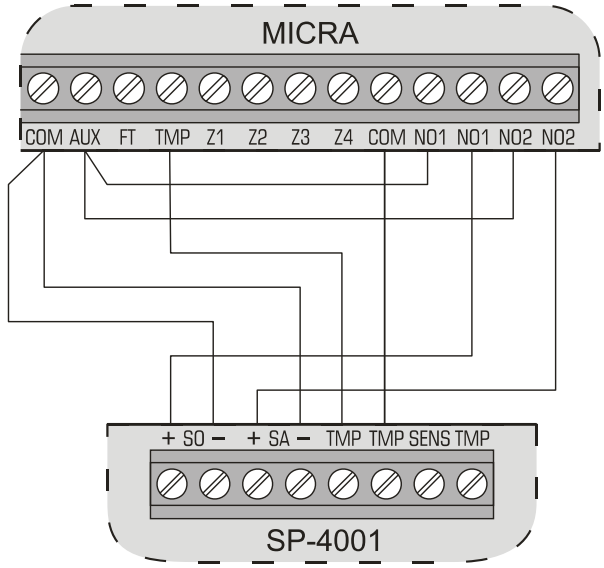


Fig. 6. Connection of the siren without own power supply (by example of SP-4001).

3.7 CONNECTING POWER SUPPLY AND STARTING THE MODULE

It is not recommended to power-up the unit with disconnected antenna.

Never connect two devices with power supply unit to one transformer.

Before adding transformer to a circuit from which it will be powered, make sure the circuit is de-energized.

It is not allowed to connect a fully discharged battery (with voltage across unloaded terminals less than 11 V) to the module. In order to avoid any damage to the equipment, if the battery is fully discharged, precharge it by means of a suitable charger.

The MICRA module must be supplied with 18 V (±10%) alternating voltage. Use the transformer secondary winding to power the module. It is recommended that a transformer with at least 40 VA rating be used. The transformer should be permanently connected to the 230 V AC mains. Before you make the cabling, familiarize yourself with the electrical installation of the facility. Make sure that the circuit you choose for powering the module will be always alive. The power supply circuit should be protected with a proper safety device. The owner or user of the module should be instructed on how to disconnect the transformer from the mains (e.g. by indicating the circuit breaker which protects the module supply circuit).

A 12 V / 7 Ah battery should be connected to the MICRA module as backup power supply.

If the battery voltage drops below 11 V for longer than 12 minutes (3 battery tests), the module may report battery failure. When the voltage goes down to approx. 10.5 V, the battery will be disconnected.

The module should be started in the following order:

1. Make sure that the antenna is connected to its socket on the electronics board.
2. Deenergize the 230 V AC circuit to which the transformer is to be connected.
3. Connect the 230 V alternating voltage wires to the terminals of transformer primary winding.

4. Connect the terminals of transformer secondary winding to the AC terminals on module electronics board.
5. Connect the battery to the dedicated leads (red one to the battery “plus”, black one to “minus”). **The module will not start after connecting the battery alone.** The battery cable ends must not be cut off.
6. Turn on 230 V AC power supply in the circuit to which the transformer is connected. The module will start operating.

The above mentioned power-up sequence (battery first, 230 V AC mains after) will permit proper operation of the power supply unit and electronic protection circuits, thus preventing defects which might be caused by possible installation errors. Should a situation occur when the power supply has to be entirely disconnected, disconnect first the AC voltage and then the battery.

7. Connect the computer to the module RS-232 (TTL) port (see: section "Local programming through RS-232 (TTL) port").
8. Turn on the module power supply.
9. Using the GPRS-SOFT program, define PIN code for the SIM card (if the card requires entering the PIN code) to be installed in the module.
10. Turn off the module power supply.
11. Insert the nano-SIM card into the socket (see: Fig. 7).

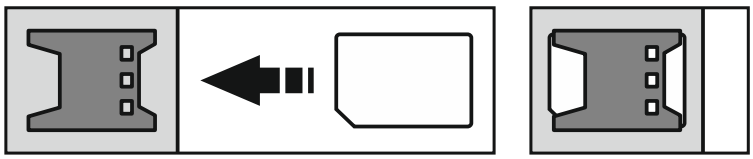


Fig. 7. Installing the SIM card.

12. Turn on the module power supply. Logging the telephone into the GSM network may take a few minutes.

If the SIM card PIN code is inconsistent with that defined in module settings, the inconsistency will be indicated by the electronics board LEDs (see: Fig. 2 Example F). The second attempt of using the PIN code will be made after 30 seconds. After the third attempt to use the invalid PIN code, the SIM card will be blocked. In order to enter the PUK code and unblock the SIM card, remove it and insert into the mobile phone.

3.8 WIRELESS DEVICES INSTALLATION

Installation of the wireless devices may only begin after starting the module, when it is possible to check the quality of communication between the wireless devices and the module. If transmissions from the intended place of installation fail to reach the module, you should choose a different installation location. Sometimes, you just need to move the device from ten to twenty centimeters for the transmissions to be correctly received by the module. Only then you can install the device permanently.

The MICRA module supports:

1. wireless detectors:
   – MSD-300 smoke and heat detector,
   – MPD-300 passive infrared detector,
   – MMD-300 magnetic contact,
   – MMD-302 magnetic contact with input for roller shutter detector,

– MFD-300 water flood detector,
– MGD-300 glass-break detector.

2. wireless keypad MKP-300.

The wireless devices should be registered using the GPRS-SOFT program.

3.8.1 ADDING NEW WIRELESS DEVICES

Wireless detectors

You can add the wireless devices in the "Options, zones, outputs" tab, "Wireless zones" table:

1. Click your mouse pointer on one of the fields at the detector you want to add.
2. Click on the "New detector" button. The "New detector Zn" window will open, where n means the zone number (Z6 – Z13).
3. According to the command displayed in the window, close and open the tamper contact of the detector.
4. A message will be displayed in the window to confirm that the detector type and serial number have been read. Click "OK". The window will close, and the data read will be displayed in the corresponding fields.

Make sure that the serial number read by the module corresponds to the number of detector to be added.

5. Enter the detector name in the "Name" field.
6. Save the data to the module.

Wireless keypad

You can add the MKP-300 wireless keypad in the "MKP-300 keypad" tab:

1. Click on the "Register" button.
2. The "MKP-300 keypad" window will open, where the command to open the keypad tamper contact will be displayed. When this action is completed, click "OK".
3. After receiving the transmission by the module, the keypad will be registered in the system.
4. Save the data to the module.

3.8.2 REMOVING WIRELESS DEVICES

Wireless detectors

1. Select in the "Options, zones, outputs" tab, "Wireless zones" table, any field corresponding to the required detector, and then click on the "Remove detector" button.
2. Save the changes made to the module.

Wireless keypad

1. Select the keypad serial number in the "MKP-300 keypad" tab, "Serial number" field, and then delete it.
2. Save the changes made to the module.

4. PROGRAMMING AND CONFIGURING THE MODULE

For programming and configuring the module, the GPRS-SOFT program version 1.06.000 is required. The program is delivered free of charge with the device. Communication between the program and the module can be effected locally or remotely. The module with factory default settings can only be programmed locally.

You can also program some module functions by means of SMS messages.

4.1 LOCAL PROGRAMMING THROUGH RS-232 (TTL) PORT

Connect the module RS-232 (TTL) port with the USB port on a computer. To make the connection, use the USB-RS converter offered by SATEL. Indicate in the GPRS-SOFT program the computer COM port to be used for communication with the module. To do so, click on the "Configuration" button (see: Fig. 8 and explanations for the figure) and, in the window that will open, select the proper COM port. After activation of the selected COM port, the program will establish communication with the module.

4.2 REMOTE PROGRAMMING USING GPRS TECHNOLOGY

During the remote programming of the module, all functions that require the use of GSM telephone will be disabled.

Remote programming is possible when the "Remote programming" option is enabled in the module and the following items have been programmed:

- PIN code (if the card requires entering PIN code);
- Access Point Name (APN) for Internet GPRS connection;
- user name for Internet GPRS connection;
- password for Internet GPRS connection;
- DNS server IP address which is to be used by the module (the DNS server address requires no programming, if the computer address is entered in the form of IP address, not a name);
- initialization code for computer connection.

APN, user name, password and DNS server address can be obtained from the GSM network operator.

The computer on which the GPRS-SOFT program will be running must have its address visible in the Internet (so-called public address). Otherwise, the network server port must be redirected to that computer, so as to make connection with the computer possible.

In order to establish communication between the module and the computer, do the following:

1. Start the GPRS-SOFT program.
2. Click on the "Configuration" button (see: Fig.8 and explanations for the figure) and, in the window that will open, enter the number of TCP port selected for communication with the module. The number will have to be included in the body of SMS message which will be sent to the module GSM telephone number to initialize communication.
3. Click on the button (see Fig. 8). In the menu that will open, select "TCP/IP" to activate the server.
4. Send SMS message to the module GSM telephone number. The SMS message should have the following form: **xxxx=aaaa:p=** ("xxxx" is the module defined code to initialize communication with GPRS-SOFT program – "Initiating SMS"; "aaaa" is the address of the computer with which the module is to establish communication, shown in the IP address form or as a name; "p" stands for the number of network port through which communication with the GPRS-SOFT program is to be effected). The module will connect to the computer whose address was given in the SMS message.

4.3 DESCRIPTION OF THE PROGRAM

4.3.1 MAIN MENU

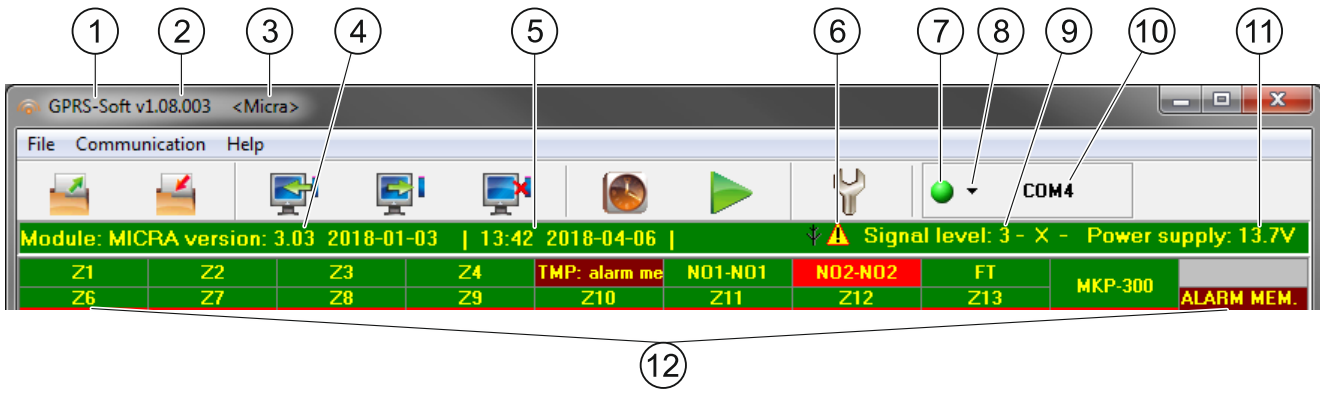


Fig. 8. Main menu of GPRS-SOFT program.

Explanations for Figure 8:

(1) program name.

(2) version of program.

(3) name of data file.

(4) version of module firmware (version number and build date).

(5) time and data by the module clock. When logging into a network, the module will update these data automatically, if such a feature is offered by the GSM network operator.

Time and date in the module will be synchronized automatically after each restart, according to the data sent by the operator (for example, if periodic module restart has been preprogrammed – see: "Autorestart every" function).

(6) icon to indicate trouble. Hover your cursor over the icon to display additional information about the type of trouble.

(7) **Connection** – depending on the mode of communication with module, selected using the button, click on the button to:

- enable/disable the computer COM port (local programming through RS-232 port);
- activate/deactivate the server (remote programming with the use of GPRS technology and TCP/IP protocol) – a click on the button will simultaneously open a window indicating the server status.

The button color indicates the current communication status:

- – green – computer COM port enabled / server active;
- – yellow – data transfer in progress;
- – gray – computer COM port disabled / server inactive.

(8) button for selecting the mode of communication with the module: local programming through the RS-232 port or remote programming with the use of GPRS technology and TCP/IP protocol.

(9) level of signal received by the GSM antenna and the name of service provider used by the module.

(10) information on the mode of communicating with the module:
- COMn (n = COM port number) – communication through the RS-232 port;
- TCP/IP – communication with the use of GPRS technology.

(11) present voltage at the output of built-in power supply (in the event of AC power loss this is the voltage supplied from battery).

(12) status information about:
- Z1...Z4 and TMP – hardwired zones. Depending on the operating mode, the colors convey the following information:

  communication device:
  - green – zone in normal state;
  - blue – zone bypassed (blocked);
  - red – digital zone violated / voltage has exceeded the value preset for threshold H of analog zone,
  - orange – voltage has dropped below the value preset for threshold L of analog zone,
  - gray – zone not used.

  alarm device:
  - green – zone in normal state;
  - blue – zone bypassed (blocked);
  - light-green – zone violated;
  - red – alarm;
  - burgundy – alarm memory;
  - gray – zone not used.
- Z6...Z13 – wireless zones. Depending on the operating mode, the colors convey the following information:

  communication device:
  - green – zone in normal state;
  - blue – zone bypassed (blocked);
  - red – zone violated;
  - orange – zone tamper;
  - gray – zone not used.

  alarm device:
  - green – zone in normal state;
  - blue – zone bypassed (blocked);
  - light-green – zone violated;
  - orange – zone tamper;
  - red – alarm;
  - burgundy – alarm memory;
  - gray – zone not used.

  A bar indicating the level of communication between detector and module appears under each wireless zone. The bar color provides the following information:
  - red – no transmission from the detector for 30 minutes.

  - green – quality of communication between detector and module. The bar length illustrates the number shown in parentheses in the particular zone field, “Presence check” column, “Options, zones, outputs” tab. The shorter the bar and the lower the number in parentheses, the lower the communication quality.
- NO1-NO1 and NO2-NO2 – relay outputs:

  green – output inactive;

  red – output active.
- FT – FT output (colors have the same meaning as for the relay outputs);;
- MKP-300 – wireless keypad:

  green – keypad registered;

  orange – keypad tamper;

  gray – keypad not registered.

  Under the field corresponding to the wireless keypad, a bar is displayed to illustrate the level of communication between keypad and module. The bar color provides the following information:
  - red – no transmission from the keypad for 30 minutes.
  - green – quality of communication between keypad and module. The bar length illustrates how many packets were received during the last transmission.
- module operating in alarm device mode (e.g. about armed mode, exit delay, entry delay, alarm).

Buttons:

Read from file – button enables loading configuration data from file.

Write to file – button enables saving configuration data to file.

Read – button enables reading data from the module.

Write – button enables saving data to the module.

Abort – button enables terminating the data reading/writing.

Set RTC – button enables writing computer time to the module.

Start test transmission – button starts sending the test transmission (in case of remote programming, the test transmission will only be sent after completion of the communication with the module).

Configuration – button enables opening the “Connection” window. The window enables configuration of parameters relating to the mode of communication between program and module:

- select the computer COM port through which local programming is to be effected;
- enter the number of TCP port to be used for remote programming of the module. Values from 1 to 65535 can be entered.

4.3.2 "OPTIONS, ZONES, OUTPUTS" TAB

Operation mode

Selection of the operating mode will change the module functionality.

Select the mode in which the module is to work:

Communication device – the main task of the device is to provide information about the state of equipment connected to the module, as well as of the module itself, by means of reporting or messaging.

Alarm device – the main task of the device is to be protection of the premises and signaling a burglary, if any (default setting).

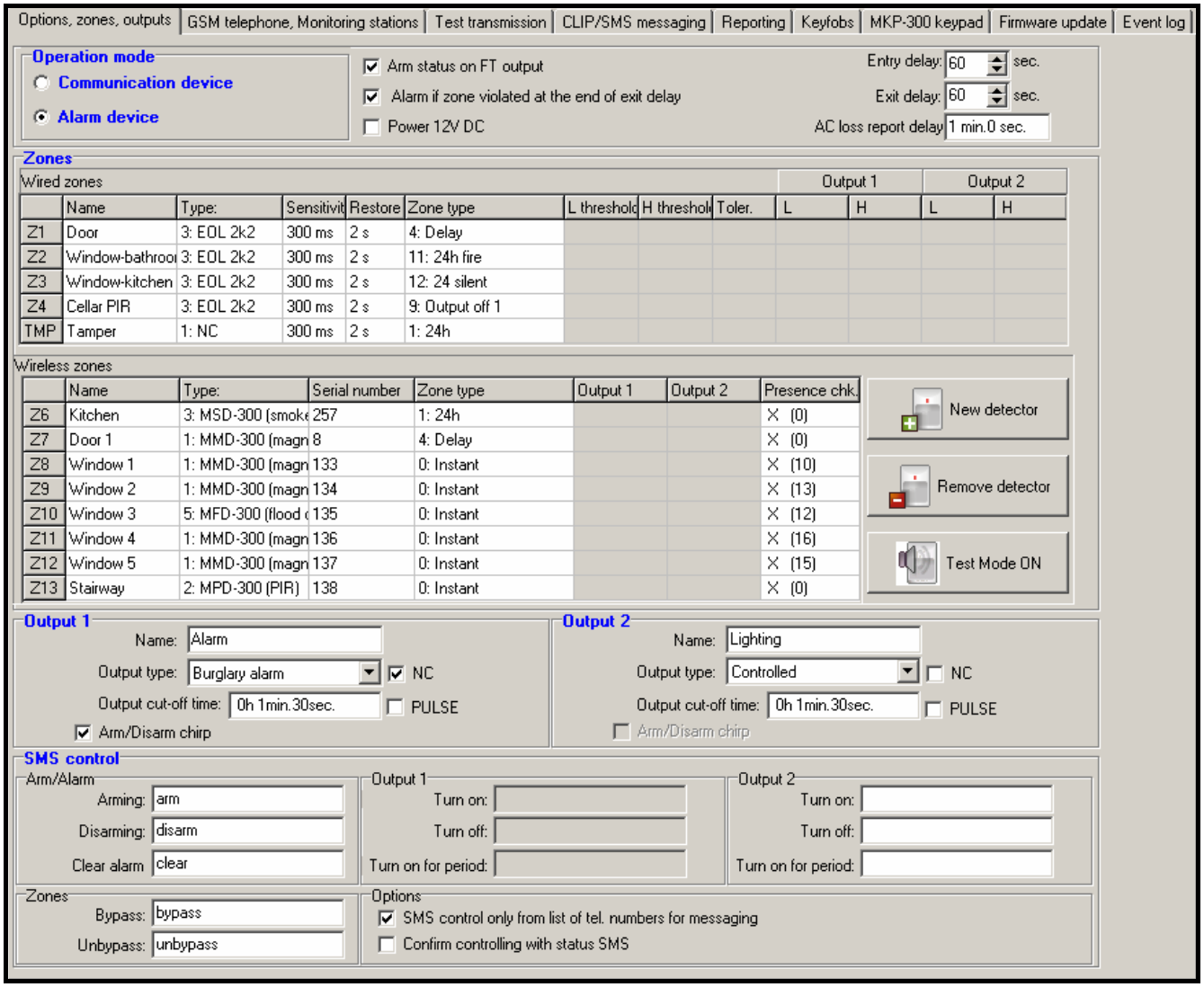


Fig. 9. "Options, zones, outputs" tab, when alarm device mode has been selected.

Parameters and options

Arm status on FT output – option available for the alarm device mode. If it is enabled, the FT output will work as an armed status indicator (it is active, when the module is armed). If the option is disabled, the output will work exactly in the same way as in the communication module mode, i.e. as an indicator of problems with logging into GSM network.

Alarm if zone violated at the end of exit delay – if this option is enabled, the alarm will be triggered if any zone (0. INSTANT, 1. 24H or 4. DELAYED type) is violated at the end of exit delay countdown. If the option is disabled, the alarm will only be triggered when the zone status changes from normal to violated during armed mode.

Power 12V DC – enabling this option will result in switching off the built-in power supply, its control system, and in disconnecting the battery. In order to connect and external power source to the device, connect the common ground to the COM terminal on the module electronics board, and 12 V DC voltage to the AUX terminal.

If the "Power 12V DC" option is enabled, do not connect battery to the module.

Entry delay – parameter available in the alarm device mode, denoting the time by which the alarm will be delayed when an armed zone of the 4. DELAY type is violated. It enables the zone to be disarmed before an alarm is triggered. You can program up to 255 seconds. If value 0 is programmed, violation of the armed 4. DELAY zone type will trigger an instant alarm.

Exit delay – parameter available in the alarm device mode, denoting the time counted from the moment of arming. Violation of a 0. INSTANT or 4. DELAY zone type during the exit delay countdown will trigger no alarm, which allows you to leave the protected area without setting off alarm. You can program up to 255 seconds. If value 0 is programmed, all zones will be instantly armed.

AC loss report delay – the time during which the module AC power must be lost for a trouble to be reported. The trouble report delay prevents momentary outages, which do not affect the normal operation of the module, from being reported. You can program up to 99 minutes and 99 seconds.

Zones

Working parameters for hardwired and wireless zones are programmed in separate tables.

Wired zones

Name – individual name of zone (up to 16 characters).

Type – you can program the following wiring types (you can make your selection in the right-click drop-down menu, or by entering a digit corresponding to the wiring type):

0. disabled – select this type, if no device is connected to the zone;

1. NC – select this type, if a device with normally closed contacts is connected to the zone;

2. NO – select this type, if a device with normally open contacts is connected to the zone;

3. – depending on the operating mode:

- communication device: **3. analog** – select this type, if the zone is to supervised analog signals;
- alarm device: **3. EOL 2k2** – select this type, if a 2.2 kΩ EOL resistor is used.

Sensitivity – time during which:

- the NC type zone must be disconnected from the ground so that the module can register the zone violation,
- the NO type zone must be shorted to ground so that the module can register the zone violation,
- the EOL type zone must be shorted to ground or disconnected from the ground so that the module can register the zone violation,
- voltage on the analog zone must drop below threshold L (minus tolerance) or rise above threshold H (plus tolerance) so that the module can register exceeding the preset value (see Fig. 10).

Values from the 0 to 5100 ms range can be programmed (every 20 ms).

Restore – time during which:

- the NC type digital zone must be again shorted to ground so that the module can register zone restore,

– the NO type digital zone must be again disconnected from the ground so that the module can register zone restore,
– resistance will reappear on the EOL type zone, so that the module can register zone restore,
– voltage on the analog zone must rise above threshold L (plus tolerance) or drop below threshold H (minus tolerance) so that the module can register zone restore (see Fig. 10).

The defined time makes it possible to reduce the number of sent transmissions. Values from the 0 to 255 seconds range can be programmed.

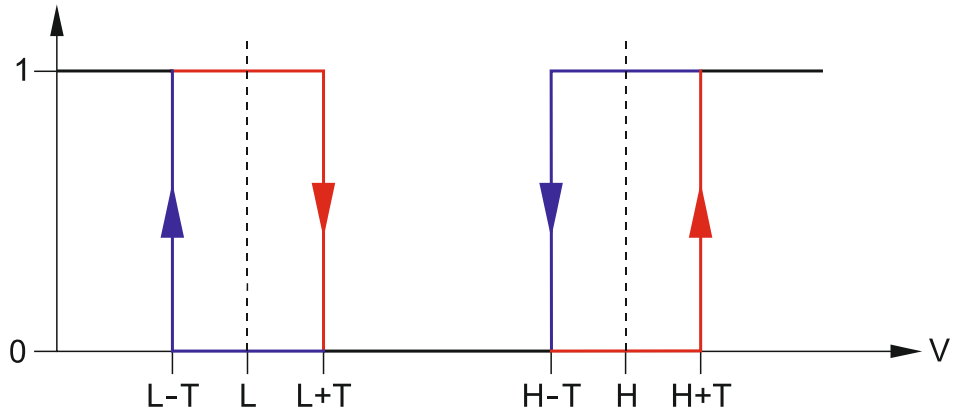


Fig. 10. Operation manner of analog zone. 0 – no violation. 1 – violation. L-T – voltage level L minus tolerance. L – lower voltage level. L+T – voltage level L plus tolerance. H-T – voltage level H minus tolerance. H – upper voltage level. H+T – voltage level H plus tolerance.

Blocking – option available for the communication device mode. If enabled, the zone will function as a blocking zone, i.e. its violation will result in blocking other zones of the module. Only one module zone from among the wired and wireless ones can perform the function of blocking zone.

Blocked – option available for the communication device mode. If enabled, the zone will be blocked upon violation of a blocking zone or after receiving by the module of a suitable control command in SMS message (content of the command being defined in the "Bypass" field).

Zone type – parameter available in the alarm device mode. You can select one of the following zone types (you can make your selection in the right-click drop-down menu, or by entering a digit corresponding to the zone type):

0. INSTANT – instant alarm zone.

1. 24H – always armed alarm zone.

2. ARM/DISARM (SWITCH) – zone violation activates and end of violation deactivates the armed mode.

3. ARM/DISARM (BUTTON) – zone violation activates or deactivates the armed mode, depending on its current status.

4. DELAY – delayed alarm zone. If armed, its violation will start the entry delay countdown. Unless disarmed, the zone will trigger alarm when the entry delay time expires.

5. OUTPUT ON 1 – violation of the zone will activate the output 1, if the output is of the CONTROLLED type.

6. OUTPUT ON 2 – violation of the zone will activate the output 2, if the output is of the CONTROLLED type.

7. **OUT 1 ON (TIME)** – violation of the zone will activate the output 1 for a preset cut-off time, if the output is of the CONTROLLED type.
8. **OUT 2 ON (TIME)** – violation of the zone will activate the output 2 for a preset cut-off time, if the output is of the CONTROLLED type.
9. **OUTPUT OFF 1** – violation of the zone will deactivate the output 1, if the output is of the CONTROLLED type.
10. **OUTPUT OFF 2** – violation of the zone will deactivate the output 2, if the output is of the CONTROLLED type.
11. **24H FIRE** – permanently armed zone, dedicated to handling the fire detectors.
12. **24H SILENT** – permanently armed zone, but the alarm from the zone will not trigger the loud signaling. Intended to handle e.g. the flood detector.

L threshold – the lower voltage threshold for analog zone. If the voltage drops below the defined value (minus tolerance), the module will register zone violation. Entering value 0 means that the voltage threshold is not controlled.

H threshold – the upper voltage threshold for analog zone. If the voltage rises above the defined value (plus tolerance), the module will register zone violation. Entering value 0 means that the voltage threshold is not controlled. The maximum value that can be programmed is 16.56 V.

Tolerance – the voltage value to be subtracted from the defined value at threshold L when the voltage drops below threshold L or added to the defined value at threshold H when the voltage rises above threshold H so that the module can register **exceeding the programmed value** / the voltage value to be added to the defined value at threshold L when the voltage rises above threshold L or subtracted from the defined value at threshold H when the voltage drops below threshold H so that the module can register **zone restore**. The field is available to analog zones.

Output 1 / 2 – fields available for the communication device mode. They allow you to define, if and how the zone will control the output. Click on the field twice to display successively:
- **blank field** – zone does not control the output,
- **ON** – violation of the zone or exceeding the voltage value at threshold L or H, as defined for the zone, will activate the output,
- **ON for a time** – violation of the zone or exceeding the voltage value at threshold L or H, as defined for the zone, will activate the output for a defined time (cut-off time must be defined for the output),
- **OFF** – violation of the zone or exceeding the voltage value at threshold L or H will deactivate the output.

Wireless zones

Name – individual name of a wireless zone (up to 16 characters).

Type – information on the type of wireless device:
- **0: no**;
- **1: MMD-300 (magnetic contact)**;
- **2: MPD-300 (PIR)**;
- **3: MSD-300 (smoke and heat detector)**;
- **5: MFD-300 (flood detector)**;
- **6: MMD-302 (roller)**;
- **7: MGD-300 (glass-break detector)**.

Serial number – displayed in the field is the detector serial number.

After the detector is added to the system and its serial number is displayed in the corresponding field, it is advisable to check it with the detector serial number.

Blocking – option available for the communication device mode. If enabled, the zone will function as a blocking zone, i.e. its violation will result in blocking other zones of the module. Only one module zone from among the wired and wireless ones can perform the function of blocking zone.

Blocked – option available for the communication device mode. If enabled, the zone will be blocked upon violation of a blocking zone or after receiving by the module of a suitable control command in SMS message (content of the command being defined in the "Bypass" field).

Zone type – parameter available for the alarm device mode. One of the zone types described in section “Wired zones” can be selected. You can make your selection in the dropdown menu which will be displayed after a right-click of your mouse, or by entering the digit corresponding to the zone type.

Output 1 / 2 – fields available for the communication device mode. They allow you to define, if and how the zone will control the output. Click on the field twice to display successively:
- **blank field** – zone does not control the output,
- **ON** – violation of the zone will activate the output,
- **ON for a time** – violation of the zone will activate the output for a defined time (cut-off time must be defined for the output),
- **OFF** – violation of the zone will deactivate the output.

Presence check – select the field (the field is selected, when the “x” symbol is shown in it), if the module is to control presence of the detectors. The module will then analyze the transmissions sent periodically by the detectors. In the field, the number of packets received during the last transmission will be shown in parentheses (up to 18). In the main menu, under the fields corresponding to the particular wireless zones, bars will appear to illustrate the quality of communication. The shorter the bar and the lower the number in parentheses, the lower the communication quality. If the field is selected and the module receives no transmission from a detector for one hour, a trouble will be reported by the module – the suitable message will be displayed in the GPRS-SOFT program (default: the option is disabled).

New detector – the button allows you to add a wireless detector (see: Adding new wireless devices). If a detector has already been added in the given position, a window will open with a prompt, whether the detector should be replaced with a new one. If the answer is affirmative, click “OK” to bring up the new detector adding window. The type and serial number will be replaced, but the name and the zone type assigned to the old detector will be retained.

Remove detector – the button allows you to remove a wireless detector (see: Removing wireless devices).

Test Mode ON / OFF – the button allows you to start / end the test mode in the module. The test mode enables the wireless and hardwired detectors to be checked for correct functioning. Detector violation will result in setting the module relay outputs to 300 ms (it applies to all output types, except for the “no” type). If a signaling device is connected to the output, each violation of the detector will be suitably signaled. On starting the test mode, the bars indicating the quality of communication in the main menu for the wireless detectors will change their color to red, and number 0 will be displayed in the "Presence check" fields. Only after receiving transmission from a wireless detector will the information on communication quality be displayed. The test mode will automatically be ended after 30 minutes. Arming will end the test mode.

Starting the test mode will block signaling the alarm triggered from the TMP zone programmed as type 1. 24h as well as the tamper alarms triggered by the wireless detectors and the wireless keypad.

Output 1 / Output 2

Name – the individual name of relay output.

Output type – parameter available in the alarm device mode. You can select one of the following types:

Not used – the output is not used.

Burglary alarm – signals:

- alarms from the zones of 0. INSTANT, 1. 24H and 4. DELAYED types;
- tamper alarms triggered by the wireless detectors and the wireless keypad;
- panic alarms triggered from the keyfob (the "10: panic alarm" is assigned to the button);
- alarms triggered from the wireless keypad (auxiliary, panic and three wrong codes).

The output is active throughout the preset cut-off time.

Burglary alarm latched – signals the same alarms as the BURGLARY ALARM output type, but remains active until the alarm is cleared.

Arm status – active when armed mode is on.

Controlled – controlled by means of zones, keyfobs or SMS messages.

Fire alarm – signals:

- alarms from the 11. 24H FIRE zone type;
- fire alarm triggered from the wireless keypad.

Fire alarm latched – signals the same alarms as the FIRE ALARM output type, but the output remains active until the alarm is cleared.

NC – if the option is enabled, the output will operate as the NC (normally closed) output. When the option is disabled, the output will operate as the NO (normally open) output.

Output cut-off time – the time during which the output is to be active. The parameter is valid when the output is activated for a period of time. If the output cut-off time is not programmed, activating the output for a period of time will be impossible.

PULSE – the option defines whether the output is to be signaling in the continuous or pulsating mode (1 / 1 sec.).

Arm/Disarm chirp – option available in the alarm device mode for the BURGLARY ALARM and BURGLARY ALARM LATCHED zone types. The output signals the following states by means of approx. 0.3 second pulses:

- arming – 1 pulse;
- disarming – 2 pulses;
- disarming, if there was an alarm during the armed mode – 4 pulses.

SMS control

Arm / Alarm

The following fields are available for the alarm device mode.

Arm – content of the control command which will be used to arm the module by means of SMS messages.

Disarm – content of the control command which will be used to disarm the module by means of SMS messages.

Clear alarm – content of the control command which will be used to clear alarms by means of SMS messages.

Output 1 / 2

Control of the outputs by means of commands sent in SMS messages is possible in the communication device mode and, for the **CONTROLLED** type outputs, in the alarm device mode.

Turn on – content of the control command which will be used to activate the relay output.

Turn off – content of the control command which will be used to deactivate the relay output.

Turn on for period – content of the control command which will be used to activate the relay output for a period of time (the cut-off time must be defined for the output).

Zones

Bypass – content of the control command that must be included in the SMS message being sent to the module for the zones to be bypassed (blocked). Depending on the module operating mode:

communications device – all zones with the “Blocked” option enabled will be blocked.

alarm device – the zones specified in the received SMS message will be bypassed. The SMS message should have the following form: **xxxx=n=** (where “xxxx” is the command, defined in the “Bypass” field, starting the zone bypassing function in the module; “n” is the number of zone to be bypassed – where two or more zones are to be bypassed, they must be separated by commas and then the command should have, for example, the following form: bypass=1,2,3=). The zone will remain bypassed until it is unbypassed by using the control command received in the SMS message.

Unbypass – content of the control command that must be included in the SMS message being sent to the module for the zones to be unbypassed (unblocked). Depending on the module operating mode:

communications device – all blocked zones will be unblocked.

alarm device – zones specified in the received SMS message will be unbypassed. The SMS message should have the following form: **yyyy=n=** (where “yyyy” is the command, defined in the "Unbypass" field, starting the zone unbypassing function in the module; “n” is the number of zone to be unbypassed – where two or more zones are to be unbypassed, they must be separated by commas and then the command should have, for example, the following form: unbypass=1,2,3=).

The armed zones cannot be bypassed / unbypassed (alarm device mode).

Options

The module can be controlled by using SMS messages. The control commands should be defined in consecutive tabs. The SMS message to be sent to the module may only contain one control command. The control command can be composed of up to 24 characters.

SMS control only from list of telephone numbers for messaging – if the option is enabled, only the SMS messages sent from authorized telephone numbers will allow:

– control (arming/disarming, alarm clearing, bypassing/unbypassing zones, activating/deactivating outputs),

– changing the content of text messages used for SMS notifications.

The telephone numbers must be included in the “Telephone numbers for messaging and test transmissions” list.

Confirm controlling with status SMS – if this option is enabled, starting the control function (arming/disarming, alarm clearing, bypassing/unbypassing zones, activating/deactivating outputs) will result in sending by the module of an SMS message

containing information on the module status to the telephone number from which the control message was sent (see: “Send SMS with module status to CLIP” option).

4.3.3 “GSM TELEPHONE, MONITORING STATIONS” TAB

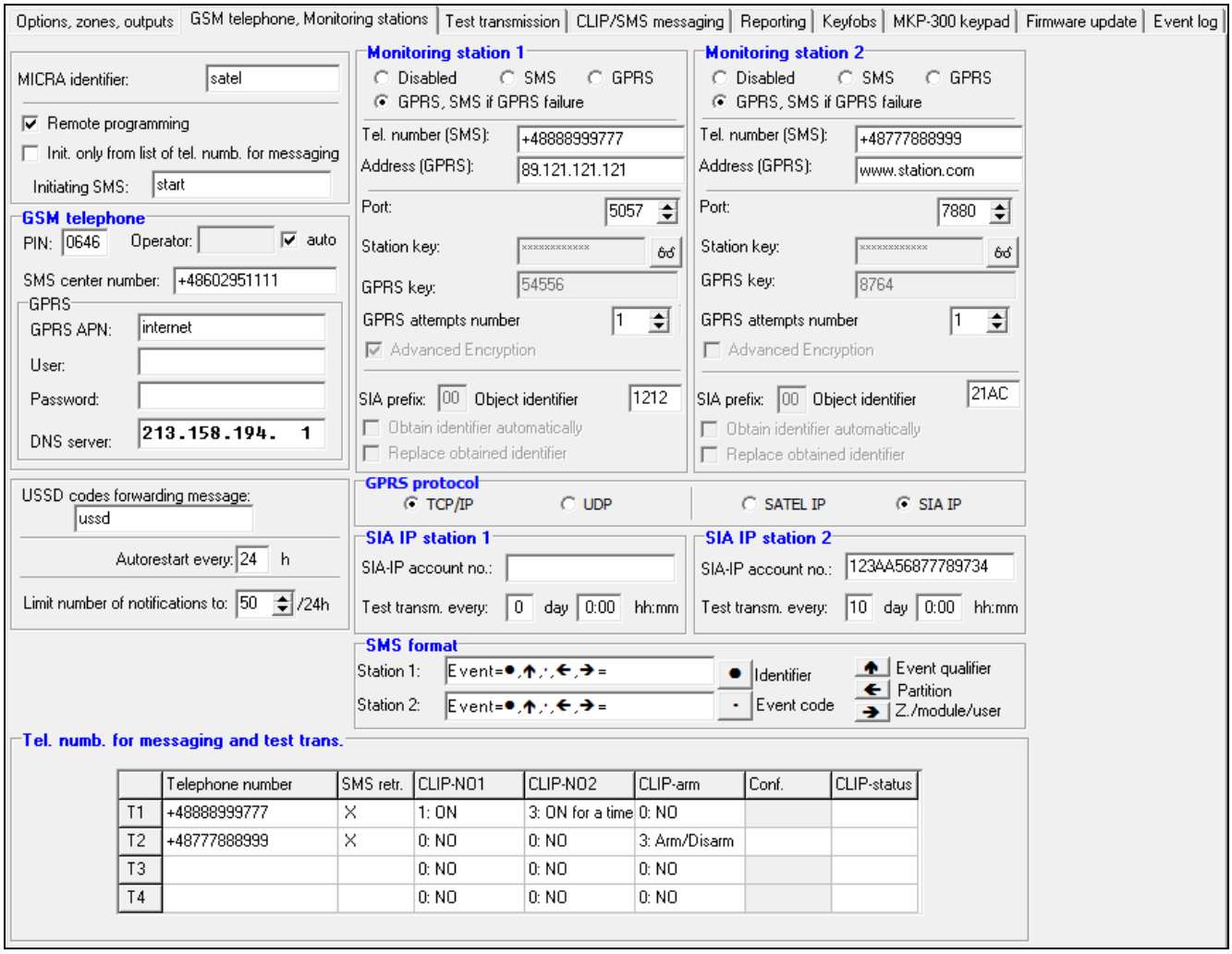


Fig. 11. “GSM telephone, Monitoring stations” tab.

Programming

MICRA identifier – a sequence of 1 to 8 alphanumeric characters to identify the module. Communication between the program and the module is only possible when the identifier entered in this field is consistent with that stored in the module. No identifier is preprogrammed in the module with factory default settings. Communication with such a module can be established without entering any identifier in the program, but as soon as the connection is established, the program will automatically generate a random identifier. It can be saved into the module or enter another one and save it.

Remote programming – enable this option if remote programming of the module with the use of GPRS technology is to be available.

Initiating number only from list of telephone numbers for messaging – if this option is enabled, the SMS message initiating the remote programming must be sent from a telephone whose number is stored in the module memory in the list of telephone numbers for messaging.

Initiating SMS – a code which must be included in the SMS message sent to the module GSM telephone number, so that the module can make an attempt to connect to the computer whose IP address and communication port are indicated in the SMS message.

GSM telephone

PIN – SIM card PIN code (if the card requires entering the PIN code).

Entering invalid PIN code may result in blocking the SIM card.

Operator – codes of the operator of the GSM network to which the module is to log in. Enter in turn:

– MCC (Mobile Country Code) – country code,

– MNC (Mobile Network Code) – operator code.

If you enter no code, the module will log into the network of SIM card operator. Keep in mind that entering incorrect data may render logging into the GSM network impossible.

auto – if this option is enabled, the module will log into the SIM card operator network.

SMS center number – telephone number of the Short Message Service Center, which delivers SMS messages. If the number has been saved by the operator to the memory of SIM card installed in the device, it need not to be entered into the field. In such a situation, it will be downloaded automatically. Otherwise, entering the number is necessary if the module is to send SMS messages. It should be remembered that the number stored in the module must be suitable for the network in which the GSM telephone is working (depending on the SIM card installed in the module).

GPRS APN – Access Point Name for Internet GPRS connection.

User – user name for Internet GPRS connection.

Password – password for Internet GPRS connection.

APN, user name and password must be defined, if GPRS data transmission (event codes, programming) is to be available.

DNS server – DNS server IP address which is to be used by the module. The DNS server address is necessary when GPRS technology is used for sending data, if the address of the device to which the module is to connect (monitoring station, computer with GPRS-SOFT program) has been entered as a name. If all addresses are given in the IP address form (4 decimal numbers separated by dots), programming the DNS server address is not required.

Module status

USSD codes forwarding message – content of the control command that must precede the USSD code in SMS message being sent to the module. The USSD codes make it possible e.g. to check the account status of SIM card installed in the module. The form of SMS message must be: **xxxx=yyyy=**, where “xxxx” is the control command, and “yyyy” – the USSD code served by the operator of GSM network in which the telephone is used (it depends on the SIM card installed in the module). Having received such an SMS message, the module will execute the USSD code contained therein. The answer received from the operator is sent in the form of SMS message to the telephone number from which the control command was sent.

Using the advanced functions available due to the USSD service (when menu is presented in reply to the code entered) is not recommended.

Autorestart every – if the restart of module settings is to be periodically repeated, you must define every how many hours it is to happen. The first restart of module settings will occur after the programmed time has elapsed since the settings were written to the module. If 0 is entered, the function will be disabled.

Limit number of notifications to – the field allows you to define the maximum number of transmissions (GPRS, SMS messages, CLIP services) to be sent by the module during a 24 hour period. The test transmissions and SMS messages containing information on

module status are not included in the number of transmissions and are not limited. You can enter any value from 0 to 255. Entering 0 means no transmission limit (default: 0).

Monitoring station 1 / Monitoring station 2

Using GPRS technology, event codes can be sent to the STAM-2 monitoring station or to the SMET-256 converter.

*Communication with the subscriber sending event codes with the use of GPRS technology should be tested by the monitoring station **as rarely as possible** (if a value lower than 1 minute is entered in the "Test period" field of the monitoring station, the time will be rounded up by the module to 1 minute). It is recommended that the maximum value be set, i.e. 255 seconds.*

Disabled – if this option is selected, event codes will not be sent to the monitoring station.

SMS – if this option is selected, event codes will be sent to the monitoring station in the form of SMS messages.

GPRS – if this option is selected, event codes will be sent to the monitoring station with the use of GPRS technology.

GPRS, SMS if GPRS failure – if this option is selected, event codes will be sent to the monitoring station with the use of GPRS technology, but after a specified number of failed attempts to send events (lack of receipt acknowledgement from the monitoring station), the event code will be sent in the form of SMS message.

Tel. number (SMS) – GSM telephone number used by the monitoring station for receiving SMS messages. Must be preceded by the country code.

Address (GPRS) – address of the monitoring station. It can be entered in the IP address form (4 decimal numbers separated by dots) or as a name.

Port – number of TCP port through which communication with the monitoring station will be effected. **The port number must be the same as that programmed in the monitoring station.**

Station key – enter in this field a string of 1 to 12 alphanumeric characters (digits, letters and special characters) which define the encryption key for the data to be sent to the monitoring station. **It must be consistent with that defined in the monitoring station for managing subscribers in the simple mode.** The parameter applies to SATEL IP format.

GPRS key – a string of 1 do 5 alphanumeric characters identifying the module. It must be consistent with that defined in the monitoring station ("ETHM/GPRS key"). The parameter applies to SATEL IP format.

GPRS attempts number – the number of failed attempts to send the event code to the monitoring station using the GPRS technology, after which the module will made an attempt to send the event code in the form of SMS message. The field is available if the "GPRS, SMS if GPRS failure" field is selected. You can enter values from 1 to 16 (default: 1).

Advanced encryption – enabling this option will increase the security level of data transmitted to the monitoring station. This option requires a SMET-256 converter with firmware version 1.06 or higher, or STAM-1 PE and STAM-1 RE cards, version 3.03 or higher. The parameter applies to SATEL IP format.

Object identifier – enter in this field 4 characters (digits or letters from A to F) which will serve as an identifier during the test transmissions sent by the module. Do not enter value 0000 (the module will not be sending test transmissions to the monitoring station). Using digit 0 in the identifier is not recommended.

GPRS protocol

TCP / IP – if this field is selected, the module will send event codes to the monitoring station using the TCP protocol.

UDP – if this field is selected, the event codes will be sent to the monitoring station by the module using the UDP protocol.

SATEL IP – if this field is selected, the module will send event codes to the monitoring station using the SATEL IP format.

SIA IP – if this field is selected, the event codes will be sent to the monitoring station by the module using the SIA-IP format (SIA DC-09 standard).

SIA IP station 1 / SIA IP station 2

If the events are to be sent in the SIA-IP format, you are required to program additional parameters for each monitoring station:

SIA-IP account no. – a sequence of up to 16 hexadecimal characters (digits or letters from A to F), used for identification of the device for the needs of reporting in SIA-IP format. If the account number is not defined, characters entered in the "Object identifier" field will be used for identification of the device.

Test transm. every – days, hour and minutes – an additional test transmission can be sent at specified time intervals to check connectivity with the monitoring station. You can program the number of days, hours, minutes and seconds between subsequent transmissions. Up to 45 days, 12 hours and 15 minutes can be programmed. Entering zeros alone will result in sending no additional transmission.

SMS format

The format of SMS messages for SMS reporting must be defined according to the monitoring station requirements. The default SMS messages format programmed in the module corresponds to the factory default settings of the STAM-2 monitoring station (program version 1.2.0 or later). If events are to be sent in the form of two characters, enter the ← partition symbol only.

Telephone numbers for messaging and test transmissions

Telephone number – it is possible to program 4 telephone numbers to which the module will be able to send SMS messages and test transmissions, and from which will be also possible to control the output and armed mode using the CLIP service. The telephone number must be preceded by the country dialing code.

SMS retransmission – select the field (the field is selected when the "x" symbol is displayed in it), if the SMS messages received by the module and sent from the telephone numbers which are not in the list (e.g. information received from the operator of GSM network in which the module is operating) are to be forwarded to the given telephone number.

CLIP-NO1 / NO2 – you can define in the field, whether and how the CLIP service effected from the selected telephone number (T1 – T4) is to control the output. There are the following options to choose from:

- 0: NO – CLIP service does not control the output,
- 1: ON – CLIP service will activate the output,
- 2: OFF – CLIP service will deactivate the output,
- 3: ON for a time – CLIP service will activate the output for a defined time (define the time in the "Output cut-off time" field, "Options, zones, outputs" tab).

CLIP-arm – you can determine in this field whether and how the CLIP service effected from the selected telephone number (T1 – T4) is to control the armed mode. There are the following options to choose from:

- 0: NO – CLIP service does not control the armed mode,

- 1: Arm – CLIP service will arm,
- 2: Disarm – CLIP service will disarm,
- 3: Arm / Disarm – depending on the current system status, the CLIP service will arm or disarm the system.

Confirmation – select this field, if the module is to use the CLIP service or SMS messages to notify about arming / disarming with the use of CLIP service. To choose the form of messaging and define the content of SMS message, go over to the "MKP-300 keypad" tab ("Messaging / reporting" table).

The CLIP service and SMS message settings are to be programmed in the "MKP-300 keypad" tab, whether or not the MKP-300 keypad is registered in the MICRA system.

CLIP-status – select this field, if an SMS message containing module status information is to be sent in reply to the CLIP from the given telephone number (see: "Send SMS with module status to CLIP" option, "Test transmission" tab). The field is available, if the "Send SMS with module status to CLIP" option is disabled.

4.3.4 "TEST TRANSMISSION" TAB

Test transmission

The module test transmissions may be sent periodically at defined time intervals, and also can be generated after identification of the telephone number of the calling party (CLIP service) or after receiving a command from the GPRS-SOFT program. The test transmission can have a form of SMS message sent to the selected telephone numbers, can be realized with the use of CLIP service to the selected telephone numbers or can be sent in the form of event code to the monitoring station.

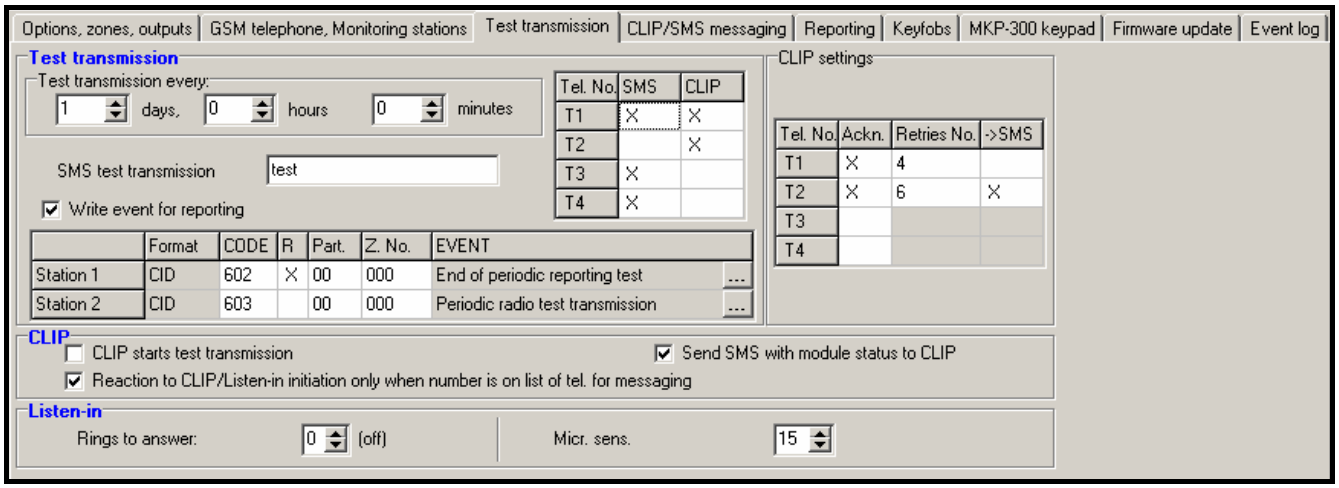


Fig. 12. "Test transmission" tab.

Test transmission every – if the module test transmission is to be of periodical nature, you have to program every how many days, hours and minutes it should be sent. The first test transmission will be sent after the preset time since saving the settings in the module has elapsed.

If an extra test transmission (using the CLIP service or the GPRS-SOFT program command) is generated, the time before sending the periodical test transmission will be counted from the beginning.

SMS test transmission – enter in this field the SMS message body which will be sent as the module test transmission to the selected telephone numbers.

If you have defined the time period after which the test transmission is to be sent, and the "SMS test transmission" field remains blank, SMS messages containing

information on the module status will be sent – as test transmissions – to the selected telephone numbers (see: "Send SMS with module status to CLIP" option).

Write event for reporting – if this option is enabled, each test transmission will be written to the event log. After enabling the option, you can send test transmissions to the monitoring stations. The method of sending the event code (SMS, GPRS) depends on the rules defined for each monitoring station in the "GSM telephone, Monitoring stations" tab. It is necessary to define the event code to be sent.

Event codes for module test transmission

The table makes it possible to define the Contact ID codes which will be sent to the monitoring stations for the module test transmission (the code will also be written to the event log).

Format – the field displays information that the code is sent in the Contact ID format.

CODE – program 3 digits of the event code in this field. You can also make use of the code editor. To open the code editor window, click on the button ... available in the "EVENT" field.

R – select this field, if the event code is to denote new restore/arming (click on the field twice to select/deselect it).

Part. – enter in this field the partition number which will be included in the event message sent to the monitoring station.

Z. No. – enter in this field the zone number which will be included in the event message sent to the monitoring station.

EVENT – the field displays description of the event whose code is entered in the "CODE" field. A button ..., which opens the editor of Contact ID codes, is also available in the "EVENT" field.

The test transmission will be sent as an event, if the following parameters and options are programmed for the monitoring station:

- *GPRS reporting (see section "Starting GPRS reporting") or SMS reporting (see section "Starting SMS reporting") is activated,*
- *object identifier different from "0000" is programmed,*
- *reporting format is programmed,*
- *event code different from "000" is programmed.*

Test transmissions to be sent to telephone numbers

The table allows you to define the form in which the test transmissions will be sent to the telephone numbers programmed in the "GSM telephone, Monitoring stations" tab. Click twice on the chosen field to select/deselect it (the field is selected if the "x" symbol is displayed in it).

SMS – select this field, if the module test transmission is to be sent to the selected telephone number in the form of SMS message.

CLIP – select this field, if the module test transmission for the selected telephone number is to be realized with the use of CLIP service (the module will dial the programmed number and then will be trying for 30 seconds to get through – the module telephone number will be displayed in the telephone).

Do not answer any call from the module, if the CLIP test transmission is to be effected without incurring any costs.

CLIP settings

The table makes it possible to determine in detail how the CLIP test transmissions are to be sent to the four telephone numbers programmed in the “GSM telephone, Monitoring stations” tab. Click twice on the chosen field to select/deselect it (the field is selected, if “x” symbol is displayed in it).

Acknowledgement – select this field if the module is to wait for the acknowledgement of receipt of test transmission using the CLIP service. In order to acknowledge receiving the CLIP test transmission, reject the call coming from the module.

Retries number – if the “Acknowledgement” field is selected, the test transmission with the use of CLIP service can be conducted a specified number of times. Values from 1 to 15 can be programmed. Acknowledgement of the CLIP test transmission receipt will make the module stop repeating such a transmission (e.g. if the test transmission is programmed to be repeated 5 times, but it is already received at the first attempt, the module will not send the other 4 transmissions).

-> SMS – if the “Acknowledgement” field is selected and receiving the CLIP test transmission is not acknowledged, the module may send a “CLIP failed” SMS message to the selected telephone number.

CLIP

CLIP starts test transmission – if this option is enabled, it is possible to send a test transmission with the use of CLIP service. Call the module telephone number and after hearing the dialing tone, hang up – the module will identify the telephone number of the calling party and send a test transmission according to the preprogrammed settings.

Send SMS with module status to CLIP – if this option is enabled, it is possible to obtain information about the module status with the use of CLIP service. Call the module telephone number and after hearing the dialing tone, hang up – the module will identify the telephone number of the calling party and send to that number an SMS message containing the following information:

– module name;
– version of module software (version number and date of build);
– S0 ÷ S4 – current level of signal received by the antenna;
– P – current supply voltage value.
– Z1 ÷ Z4 – information on the status of Z1 ÷ Z4 zones:
  i – digital / analog zone normal status,
  I – digital zone violated,
  L – voltage at analog zone has dropped below threshold L; information on voltage value,
  H – voltage at analog zone has exceeded threshold H; information on voltage value,
  b – digital / analog zone blocked,
  A – alarm,
  a – alarm memory.
– TMP – information on status of TMP zone:
  i – zone normal status,
  I – zone violated,
  b – zone blocked,
  A – alarm,
  a – alarm memory.
– Z6 ÷ Z13 – information on the status of Z6 ÷ Z13 zones:
  i – zone normal status,
  I – zone violated,

b – zone blocked,
A – alarm,
a – alarm memory,
T – zone tamper,
B – low battery in the wireless detector,
C – no communication with the wireless detector.

– information on the status of module working in the alarm device mode:
  ARM – armed,
  DISARM – disarmed.
– AC – information on the module voltage status:
  i – AC voltage OK,
  I – AC voltage loss.
– AK – information on the battery status:
  i – battery OK,
  I – low battery.
– OUT 1 ÷ OUT2 – information on relay outputs status OUT 1 ÷ OUT2:
  o – output inactive,
  O – output active.
– EVb – the maximum number of transmissions has been reached (see: "Limit number of notifications to" parameter, "GSM telephone, Monitoring stations" tab).

Reaction to CLIP / Listen-in initiation only when number is on list of telephones for messaging – if this option is enabled, the module will only send test transmission or SMS message with status information, or will initiate listen-in, when the telephone number, identified owing to the CLIP service, is one of the numbers programmed in the "GSM telephone, Monitoring stations" tab on the "Telephone numbers for messaging and test transmissions" list.

If the "Reaction to CLIP / Listen-in initiation only when number is on list of telephones for messaging" option is not enabled, the test transmissions and SMS messages with information on device status:

- *for the numbers in the list, they will be sent by the module immediately,*
- *for the numbers not in the list, they can be sent by the module every 10 minutes at the most.*

Listen-in

Rings to answer – enter in this field the number of rings after which the module will answer the call and turn on the microphone. You can program values from 0 to 9. If value 0 is programmed, the listen-in feature is disabled.

Micr. Sens. – microphone sensitivity can be programmed within the range from 0 to 15.

4.3.5 "CLIP / SMS MESSAGING" TAB

Notification can be effected by means of SMS messages or by using the CLIP service (when the CLIP service is used, the module does not inform about zone restore / end of trouble).

For the analog inputs, the messaging parameters are to be defined separately for each of the defined thresholds.

CLIP T1 – T4 – select the fields of telephones (see: numbers in the list "Telephone numbers for messaging and test transmissions", programmed in the "GSM telephone, Monitoring stations" tab), which will be informed about a change in the given zone status or occurrence of the particular trouble by using the CLIP service.

SMS T1 – T4 – select the fields of telephones (see: numbers in the list “Telephone numbers for messaging and test transmissions”, preprogrammed in the “GSM telephone, Monitoring stations” tab), to which an SMS message is to be sent to notify about a change in the given zone status or occurrence of the particular trouble.

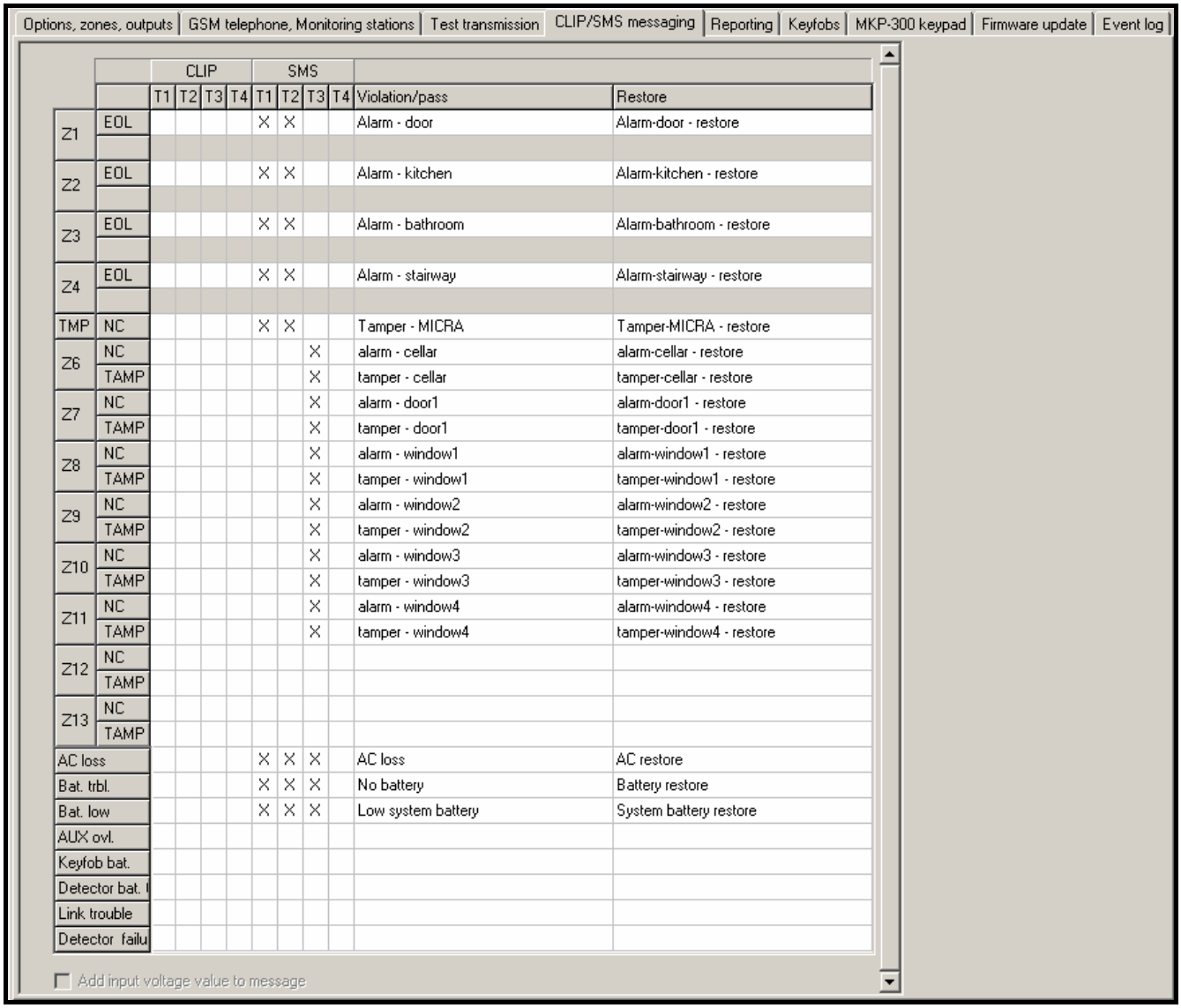


Fig. 13. “CLIP/SMS messaging” tab for the alarm device mode.

Violation/pass – content of the SMS message that will be sent on the zone violation / exceeding the preprogrammed zone voltage value (rise above the defined value at threshold H or drop below the defined value at threshold L) / occurrence of trouble. The message may consist of up to 24 characters. Its content must not contain any diacritical characters. If the field is left blank, the message will not be sent.

Restore – content of the SMS message that will be sent on the zone restore / end of trouble. The message may consist of up to 24 characters. Its content must not contain any diacritical characters. If the field is left blank, the message will not be sent.

Add input voltage value to message – option available for the communication device mode. If the option is enabled, information on the current voltage value at the zone input will be added to the SMS message about the analog zone status.

4.3.6 "REPORTING" TAB

Set CID codes automatically – option available for the alarm device mode. If the option is enabled, the program will automatically select Contact ID codes for:

– events from the zones of 0. INSTANT, 1. 24H, 2. ARM/DISARM (SWITCH), 3. ARM/DISARM (BUTTON) and 4. DELAY type;

– troubles, module related events (settings restart, clock programming) and SMS control;

– arming/disarming, alarm clearing and panic alarm triggering by using a keyfob (the codes of these events can be programmed in the "Keyfobs" tab).

With the "Set CID codes automatically" option enabled, entering the event codes manually will be unavailable.

Reporting parameters

Options, zones, outputs | GSM telephone, Monitoring stations | Test transmission | CLIP/SMS messaging | Reporting | Keyfobs | MKP-300 keypad | Firmware update | Event log

☑ Set CID codes automatically

				Violation/pass				Restore			
		S1	S2	CODE	Part.	Z. No.	EVENT	CODE	Part.	Z. No.	EVENT
Z1	EOL	X		1-134	01	001	Burglary-entry/exit	3-134	01	001	Burglary-entry/exit restore
Z2	EOL	X		1-110	01	002	Fire alarm	3-110	01	002	Fire alarm restore
Z3	EOL	X		1-110	01	003	Fire alarm	3-110	01	003	Fire alarm restore
Z4	EOL	X		1-130	01	004	Burglary	3-130	01	004	Burglary restore
TMP	NC	X		1-137	01	005	Tamper	3-137	01	005	Tamper restore
Z6	NC	X		1-133	01	006	Burglary/24 hour	3-133	01	006	Burglary/24 hour restore
	TAMP	X		1-144	01	006	Detector tamper	3-144	01	006	Detector tamper restore
Z7	NC	X		1-130	01	007	Burglary	3-130	01	007	Burglary restore
	TAMP	X		1-144	01	007	Detector tamper	3-144	01	007	Detector tamper restore
Z8	NC	X		1-130	01	008	Burglary	3-130	01	008	Burglary restore
	TAMP	X		1-144	01	008	Detector tamper	3-144	01	008	Detector tamper restore
Z9	NC	X		1-130	01	009	Burglary	3-130	01	009	Burglary restore
	TAMP	X		1-144	01	009	Detector tamper	3-144	01	009	Detector tamper restore
Z10	NC	X		1-130	01	010	Burglary	3-130	01	010	Burglary restore
	TAMP	X		1-144	01	010	Detector tamper	3-144	01	010	Detector tamper restore
Z11	NC	X		1-130	01	011	Burglary	3-130	01	011	Burglary restore
	TAMP	X		1-144	01	011	Detector tamper	3-144	01	011	Detector tamper restore
Z12	NC	X		1-130	01	012	Burglary	3-130	01	012	Burglary restore
	TAMP	X		1-144	01	012	Detector tamper	3-144	01	012	Detector tamper restore
Z13	NC	X		1-130	01	013	Burglary	3-130	01	013	Burglary restore
	TAMP	X		1-144	01	013	Detector tamper	3-144	01	013	Detector tamper restore
AC loss		X		1-301	01	000	AC loss	3-301	01	000	AC restore
Bat. trbl.		X		1-311	01	000	Battery missing	3-311	01	000	Battery restore
Bat. low		X		1-302	01	000	Low system battery	3-302	01	000	System battery restore
AUX ovl.				1-321	01	000	Bell 1/output trouble	3-321	01	000	Bell 1/output restore
Keyfob bat.		X		1-384	01	000	RF transmitter low battery	3-384	01	000	RF transmitter battery restore
Restart				1-305	01	000	System restart				
Progr. RTC				1-625	01	000	Time/date programming				
GSM trbl				1-357	01	000	Long range radio transmitter VSWR fault	3-357	01	000	Long range radio transmitter VSWR restore
GPRS trbl				1-357	01	000	Long range radio transmitter VSWR fault	3-357	01	000	Long range radio transmitter VSWR restore
Disarm (SMS)				3-407	01	000	Remote arm	1-407	01	000	Remote disarm
Alm clear (SMS				1-406	01	000	Alarm cancelling				
Link trouble				1-381	01	000	Loss of RF supervision	3-381	01	000	RF supervision restore
Detector bat. trl				1-384	01	000	RF transmitter low battery	3-384	01	000	RF transmitter battery restore
Detector failure				1-380	01	000	Detector trouble - global	3-380	01	000	Detector trouble restore - global

Fig. 14. "Reporting" tab for the alarm device mode.

For the analog inputs, the reporting related parameters are to be determined separately for each of the defined thresholds.

S1 – select this field if the event code is to be sent to the monitoring station 1.

S2 – select this field if the event code is to be sent to the monitoring station 2.

Violation/pass / Restore

CODE – the event code in the Contact ID format that will be sent to the monitoring station. For each event to be monitored, 4 digits should be programmed in the Q-XYZ form, where:

– **Q** – digit 1 or 3 (1 – new event/disarming, 3 – new restore/arming),
– **XYZ** – 3-digit event code.

Code entering is facilitated by the Contact ID code editor, which you can start by clicking the ... button, available in the "EVENT" field.

Part. – partition number which will be sent in the event code. You can enter numbers and letters from A to F.

If events are to be sent in the form of two characters (partition number only), you should not use the code editor.

Z. No. – zone / module / user number which will be sent in the event code.

EVENT – event description corresponding to the Contact ID code entered in the "CODE" field. Available in the "EVENT" field is also the ... button, which enables opening of the code editor.

4.3.7 "KEYFOBS" TAB

Keyfobs

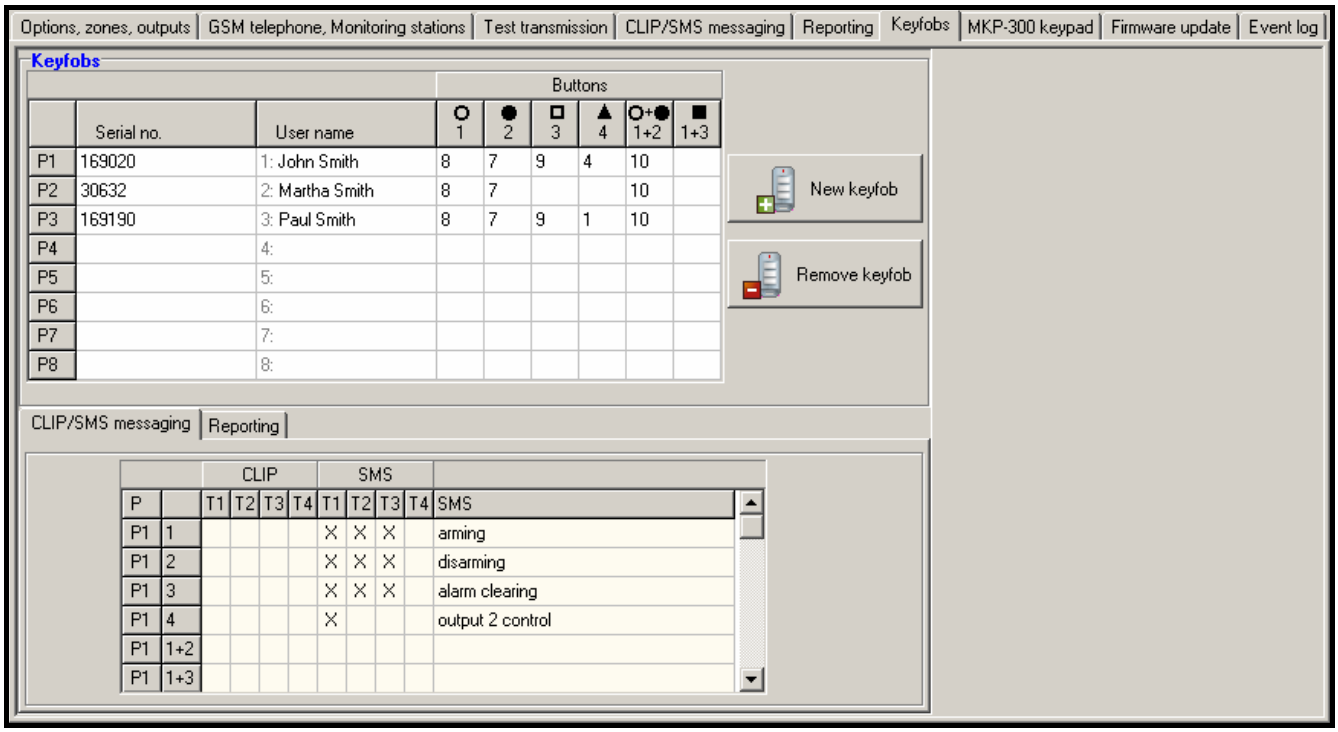


Fig. 15. "Keyfobs" tab.

Serial no. – keyfob serial number is displayed in the field.

User name – you can enter in this field the name of user to whom the keyfob is assigned. The name can have up to 16 characters. After entering the name, a digit (1 – 8), corresponding to the code number in the MKP-300 keypad, will appear automatically next to the name.

Buttons – you can assign one of the functions below to each of the keyfob buttons and to the 1 & 2 / ○+● plus 1 & 3 / ■ combinations of buttons (you can make your selection in the right-click drop-down menu, or by entering a digit corresponding to the selected function):
0: no function

1: out 1 ON
2: out 2 ON
3: out 1 ON (time)
4: out 2 ON (time)
5: out 1 OFF
6: out 2 OFF
7: bypass zones [communications device] / 7: disarming [alarm device]
8: unbypass zones [communications device] / 8: arming [alarm device]
9: clear alarm [alarm device]
10: panic alarm [alarm device]

The button numbers and their combinations refer to the P-2, P-4, T-1, T-2, T-4 keyfobs, while the icons and their combinations refer to the MPT-300 and MPT-350 keyfobs.

Even if pressing a button starts no function in the module ("0: no function" is selected), it may result in sending an event code which has been assigned to that button below, in the "Reporting" tab. Thus you can trigger e.g. the silent panic alarm – the event code will be sent to the monitoring station, but the alarm will be in no way signaled by the module.

New keyfob – the button allows you to add a keyfob (if a keyfob has already been added in the given position, it will be replaced with a new one, but the name and functions assigned to the keyfob buttons will be retained).

Remove keyfob – the button allows you to remove a keyfob (the name and functions assigned to keyfob buttons will also be deleted).

Adding keyfobs – serial number entered manually

1. In the "Serial no." field, enter the serial number of the keyfob to be added.
2. In the "User name" field, enter the name of user.
3. Write the data to the module.

Adding keyfobs – serial number read out during transmission

1. Click on one of the fields at the keyfob you want to be added.
2. Click the "New keyfob" button to open the "New keyfob no. n" window (n – keyfob number).
3. Following the instruction displayed in the window, press any keyfob button.
4. After the keyfob serial number is displayed in the window, click "OK". The window will close and the keyfob serial number read out during the transmission will be displayed in the appropriated field.
5. Enter a name for the user in the "User name" field.
6. Write the data to the module.

Assigning functions to keyfob buttons

1. Click at the selected keyfob on the column corresponding to the button (combination of buttons) to which you want a function to be assigned.
2. Click the right mouse button to open a drop-down menu in which you can select the required function. You can also enter the function number using the keyboard (the numbers of all available functions are given above, in the "Buttons" field description) and confirm with "Enter".
3. Write the data to the module.

"CLIP / SMS messaging" tab

Similarly to notification about other events, the information about the use of a keyfob button can be conveyed by means of SMS messages or by using the CLIP service.

CLIP T1 – T4 – select the fields of telephones (see: numbers in the list "Telephone numbers for messaging and test transmissions", programmed in the "GSM telephone, Monitoring stations" tab), which will be informed about using a button of the given keyfob by means of the CLIP service.

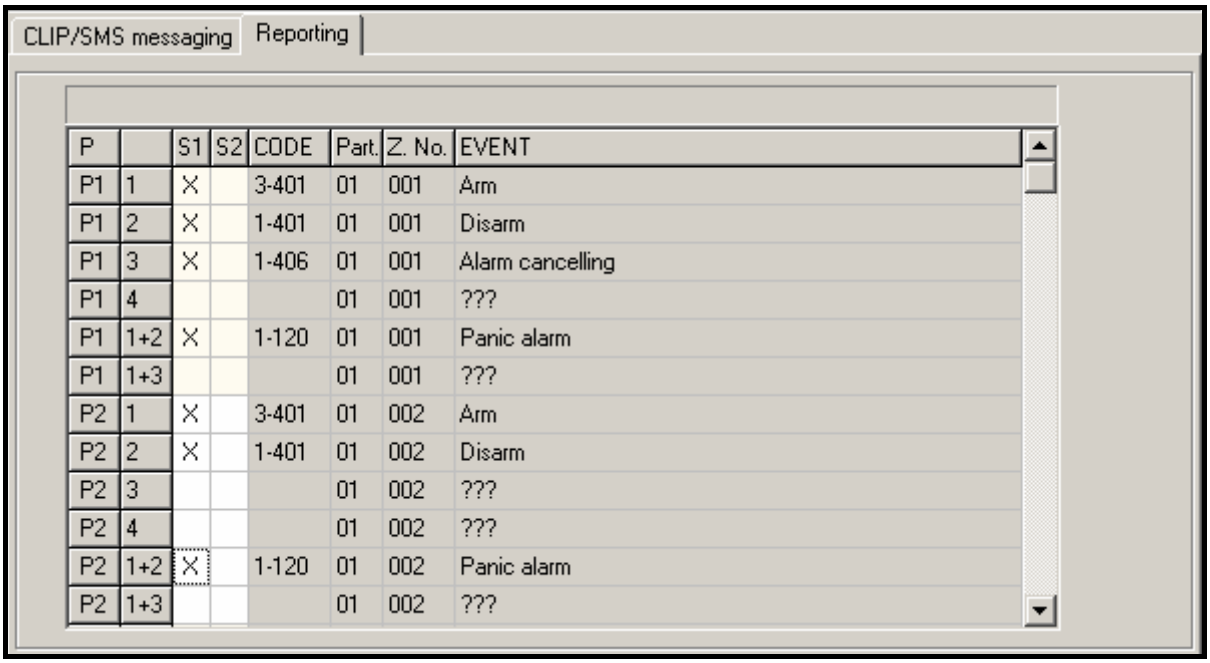
SMS T1 – T4 – select the fields of telephones (see: numbers in the list "Telephone numbers for messaging and test transmissions", preprogrammed in the "GSM telephone, Monitoring stations" tab), to which an SMS message is to be sent to notify about using a button of the given keyfob.

SMS – content of the SMS message that will be sent on using a button of the given keyfob. The message may consist of up to 24 characters. Its content must not contain any diacritical characters.

"Reporting" tab

If the "Set CID codes automatically" option is enabled (see p. 32), entering the event codes manually will be unavailable.

The rules of programming are the same as described in section "Reporting parameters" (p. 32).



P		S1	S2	CODE	Part.	Z. No.	EVENT
P1	1	X		3-401	01	001	Arm
P1	2	X		1-401	01	001	Disarm
P1	3	X		1-406	01	001	Alarm cancelling
P1	4				01	001	???
P1	1+2	X		1-120	01	001	Panic alarm
P1	1+3				01	001	???
P2	1	X		3-401	01	002	Arm
P2	2	X		1-401	01	002	Disarm
P2	3				01	002	???
P2	4				01	002	???
P2	1+2	X		1-120	01	002	Panic alarm
P2	1+3				01	002	???

Fig. 16. "Reporting" tab in "Keyfobs" tab.

4.3.8 "MKP-300 KEYPAD" TAB

MKP-300

Serial number – shown in this field is the keypad serial number.

Register – the button allows you to register the keypad in the system.

Keypad presence control – enable this option, if the module is to check the keypad presence. The module will then analyze the transmissions sent periodically by the keypad. In the main menu, a bar illustrating the communication quality will appear under the field corresponding to the keypad. The shorter the bar, the lower the communication quality. If the field is selected and the module receives no transmission for an hour, it will generate a trouble event – the suitable message will be displayed in the GPRS-SOFT program.

Alarm 3 incorrect codes – if this option is enabled, an alarm will be triggered by entering three times an invalid code from the keypad.

Fire alarm – if this option is enabled, the module will signal the fire alarm triggered from the keypad (after you press and hold down the [*] key for about 3 seconds).

Aux. alarm – if this option is enabled, the module will signal the medical alarm triggered from the keypad (after you press and hold down the [0] key for about 3 seconds).

Panic alarm – if this option is enabled, the module will signal the panic alarm triggered from the keypad (after you press and hold down the [#] key for about 3 seconds).

Silent panic alarm – if this option is enabled, the panic alarm from the keypad will be treated as the silent panic alarm (without being signaled on the alarm outputs). The field gets active after selecting the “Panic alarm” option.

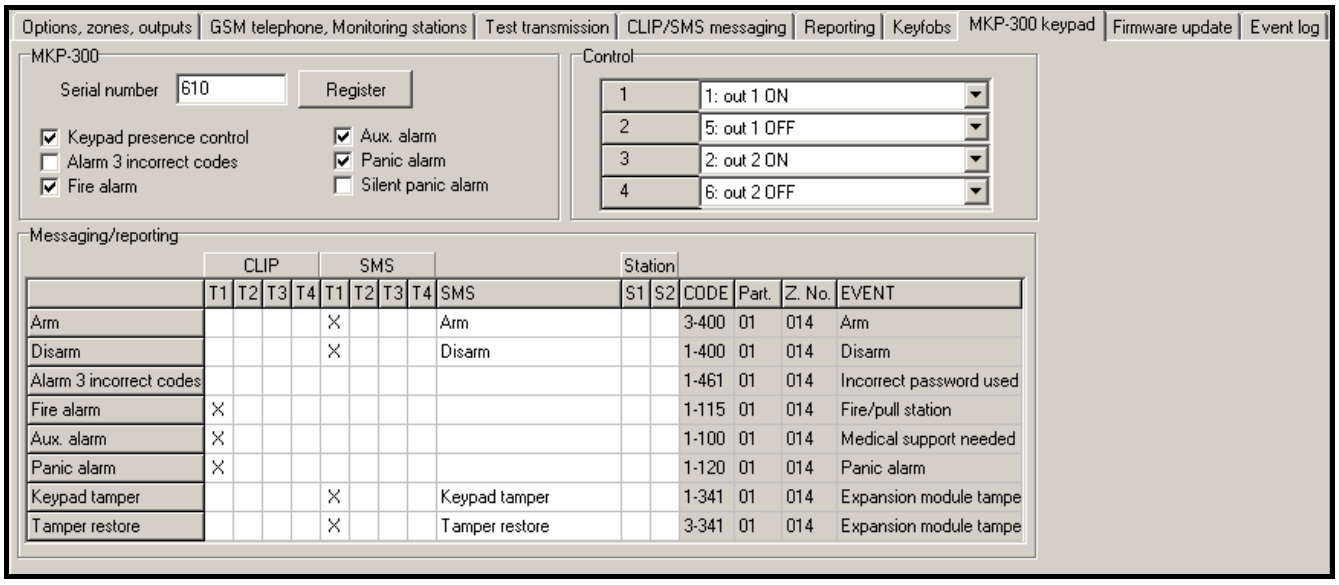


Fig. 17. “MKP-300 keypad” tab.

Control

The output control functions can be assigned to keys 1 – 4. To each of them you can assign one of the functions below (you can make your choice in the drop-down menu that will be brought up with a click on the ▼ button, or by entering the digit which corresponds to the selected function):

0: NO,
1: out 1 ON,
2: out 2 ON,
3: out 1 ON (time),
4: out 2 ON (time),
5: out 1 OFF,
6: out 2 OFF.

Messaging / reporting

Notifications on using the keypad to arm / disarm the system, trigger an alarm, or on keypad tamper, can be delivered in form of an SMS message or with the use of CLIP. You can also specify in the table whether the code relating to any of these events is to be reported to the monitoring station.

CLIP T1 – T4 – select the fields of telephones (see: numbers programmed in the “GSM telephone, Monitoring stations” tab, “Telephone numbers for messaging and test transmissions” list) which will be informed by means of the CLIP service, if any of the above described events occurs.

SMS T1 – T4 – select the fields of telephones (see: numbers programmed in the "GSM telephone, Monitoring stations" tab, "Telephone numbers for messaging and test transmissions" list) to which an SMS message will be sent to notify about occurrence of any of the above described events.

SMS – SMS message content that will be sent, if any of the above described events occurs. The message can contain up to 24 characters. Its content must not contain any diacritical characters.

The rules of programming the reporting related parameters are the same, as described in section "Reporting parameters" (p. 32).

4.3.9 "FIRMWARE UPDATE" TAB

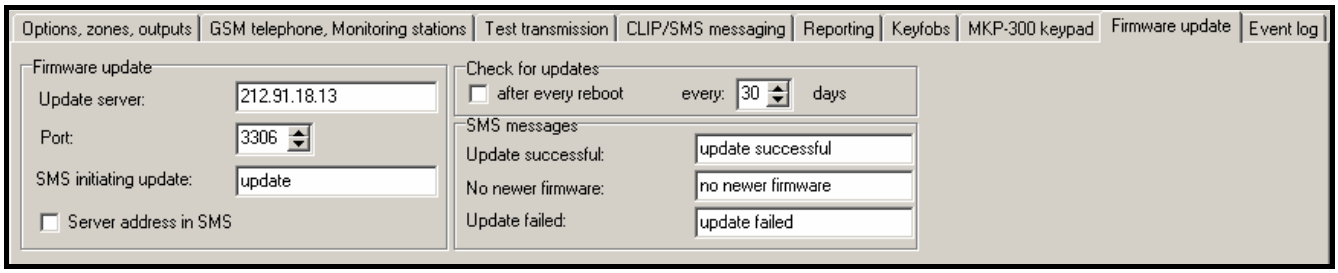


Fig. 18. "Firmware update" tab.

Remote update of the module firmware via GPRS is possible for the units with u-blox LEON-G100 industrial GSM telephone and firmware version 3.00.

Modules with firmware version older than 3.00 can only be updated to version 3.00 at Satel's service location.

*For information on the firmware update server please refer to the **www.satel.eu** website.*

Update server – address of the server to which the module is to connect in order to update the firmware. It can be entered as an IP address or as a name.

Port – number of the server port indicated in the decimal format.

SMS initiating update – content of the control command which must be included in the SMS message sent to the module telephone number to initiate the firmware update process.

Server address in SMS – if this option is enabled, you can enter the address of server to which the module is to connect, and the port number, in the content of SMS initiating the connection. If the address is not entered, the module will connect to the server whose address has been programmed in the module.

Check for updates

after every reboot – if this option is enabled, the module will connect to the firmware update server after each restart to check if a new firmware version is available.

every… days – if the module is to periodically check the server for updates, you should indicate every how many days it should be done. You can program up to 31 days. Value 0 means that the module will not periodically connect to the firmware update server.

SMS messages

Update successful – SMS message which will be sent after the process of module firmware update has been finished successfully.

No newer firmware – SMS message which will be sent after the module has checked that no newer firmware is available.

Update failed – SMS message which will be sent after an unsuccessful attempt to update the module firmware.

The SMS messages with information on results of the update may contain up to 32 characters.

4.3.10 "EVENT LOG" TAB

The tab presents a list of events. The events are downloaded on pressing the "Read" button and displayed sorted by date and time in descending order (the latest at the top, the oldest at the bottom). The following information is presented in individual columns:

Date – date of event occurrence.

Time – time of event occurrence.

Source – what generated the event (e.g. zone, trouble, keyfob button, SMS message command, etc.). The (R) symbol, which may be additionally put in the field, means restore (e.g. zone restore, end of trouble).

CODE – code in the Contact ID format and its description, which have been assigned to the given event (if no code has been assigned to the event in the "Reporting" tab, this field will remain blank).

S1 S2 – reporting status (S1 – monitoring station 1, S2 – monitoring station 2):

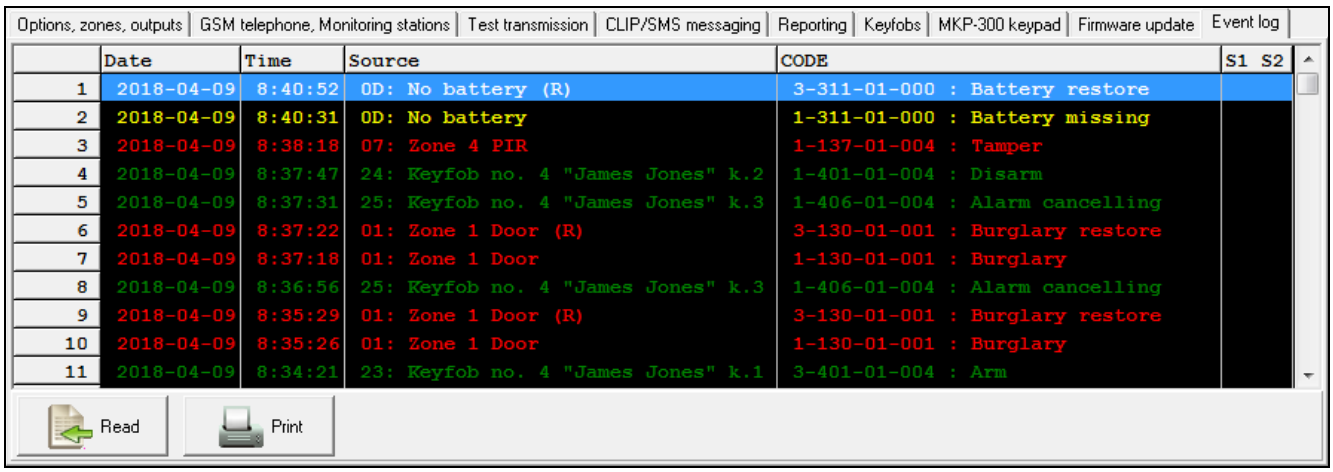
no symbol – the event is not reported.

+ – event successfully reported to the monitoring station.

. – event waiting to be reported to the monitoring station.

Read – button enables data reading from the module.

Print – button opening the "Print" window.



	Date	Time	Source	CODE	S1 S2
1	2018-04-09	8:40:52	0D: No battery (R)	3-311-01-000 : Battery restore	
2	2018-04-09	8:40:31	0D: No battery	1-311-01-000 : Battery missing	
3	2018-04-09	8:38:18	07: Zone 4 PIR	1-137-01-004 : Tamper	
4	2018-04-09	8:37:47	24: Keyfob no. 4 "James Jones" k.2	1-401-01-004 : Disarm	
5	2018-04-09	8:37:31	25: Keyfob no. 4 "James Jones" k.3	1-406-01-004 : Alarm cancelling	
6	2018-04-09	8:37:22	01: Zone 1 Door (R)	3-130-01-001 : Burglary restore	
7	2018-04-09	8:37:18	01: Zone 1 Door	1-130-01-001 : Burglary	
8	2018-04-09	8:36:56	25: Keyfob no. 4 "James Jones" k.3	1-406-01-004 : Alarm cancelling	
9	2018-04-09	8:35:29	01: Zone 1 Door (R)	3-130-01-001 : Burglary restore	
10	2018-04-09	8:35:26	01: Zone 1 Door	1-130-01-001 : Burglary	
11	2018-04-09	8:34:21	23: Keyfob no. 4 "James Jones" k.1	3-401-01-004 : Arm	

Fig. 19. "Event log" tab.

"Print" window

In the window, you can define parameters of the printout containing the event log.

Printer – information about the selected printer.

Print to text file – select this field if the event log is to be exported to text file (instead of being printed).

Range – you can define the printout range by selecting one of the options below:

All – all events will be printed / exported.

Pages – in the field to the right, define the number of pages of events to be printed / exported. The number of events making up the selected number of pages will be displayed in brackets.

Selection – the option is available when events in the event log are selected. Only the selected events will be printed / exported.

Buttons:

Properties – click to select a printer and set its parameters.

Print – click to print the event log or export it to file.

Cancel – click to close the window.

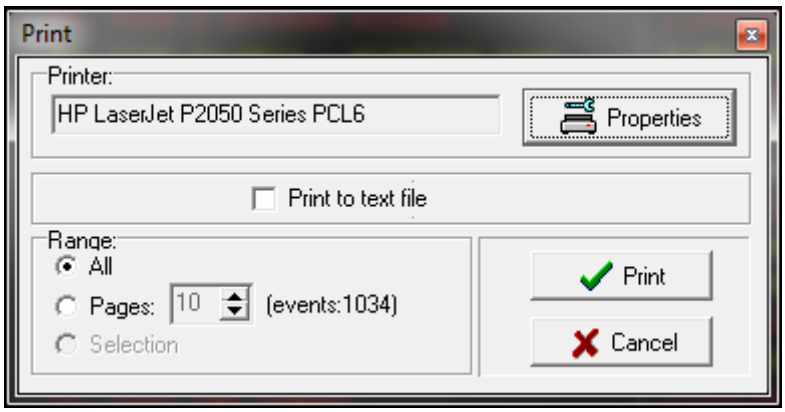


Fig. 20. “Print” window.

4.4 PROGRAMMING WITH THE USE OF SMS MESSAGES

The module can be programmed using SMS messages:

- at any moment from the telephone whose number is programmed in the “Telephone numbers for messaging and test transmissions” list, “GSM telephone, Monitoring stations” tab;
- for 15 minutes after starting (restarting) the module from any telephone. On receiving the SMS message intended for programming, the programming mode will be each time prolonged by 15 minutes, running from the moment the message is received.

Using the SMS message you can:

1. Add telephone numbers to the “Telephone numbers for messaging and test transmissions” list (“GSM telephone, Monitoring stations” tab, GPRS-Soft program), sending:
   “**SET1=+48XXXXXXXXX=**” – adds T1 telephone number,
   “**SET2=+48XXXXXXXXX=**” – adds T2 telephone number,
   “**SET3=+48XXXXXXXXX=**” – adds T3 telephone number,
   “**SET4=+48XXXXXXXXX=**” – adds T4 telephone number,
   where XXXXXXXXX denotes the digits of the telephone number being added.
2. Delete telephone numbers from the “Telephone numbers for messaging and test transmissions” list, sending:
   “**DEL1**” – deletes T1 telephone number,
   “**DEL2**” – deletes T2 telephone number,
   “**DEL3**” – deletes T3 telephone number,
   “**DEL4**” – deletes T4 telephone number.
3. Delete all telephone numbers from the “Telephone numbers for messaging and test transmissions” list, sending "**DELALL**".
4. Reset the number of transmissions sent by the module, sending "**RESET**" (see: “Limit number of notifications to” parameter, “GSM telephone, Monitoring stations” tab, GPRS-Soft program). Having received such a message, the module will start counting anew the transmissions sent.
5. Set time in the module from the telephone, sending “**TIME**”.
6. Start the test mode, sending “**TESTON**”.
7. End the test mode, sending “**TESTOFF**”.

The module is case-sensitive, hence the content of SMS messages for programming the module settings should be entered in upper-case letters.

4.5 CONFIGURING THE MODULE TO WORK IN ALARM DEVICE MODE

1. Click the “Options, zones, outputs” tab and then:
   – enable the “Alarm device” option;
   – define the wired zone parameters (wiring type, sensitivity, restore and zone type), register and configure the wireless detectors (zone type, presence check option);
   – if delayed zones are used, define the entry delay time;
   – if the exit delay countdown is to run, allowing you to leave the premises without triggering alarm, define the suitable parameter;
   – define the output parameters (output type, cut-off time);
   – if the module users are to be authorized to remotely control the system by means of SMS messages (arming/disarming, clearing alarms, bypassing/unbypassing zones, controlling outputs), define the suitable control commands.
2. If the module is to be operated by means of keyfobs, click on the “Keyfobs” tab and add the keyfobs (see: description of adding keyfobs, p. 34-34).
3. If the module is to be operated by means of the MKP-300 keypad, click on the “MKP-300 keypad” tab, register the device (see: Adding new wireless devices) and program it accordingly (see: “MKP-300 keypad” tab).
4. Click on the “Reporting” tab and then enable the “Set CID codes automatically” option. The codes will be automatically matched to corresponding events (see: description of the “Set CID codes automatically” option, p. 32). Enabling the option is recommended not only when event codes are to be sent to the monitoring station. The codes and their descriptions are written to the event log, thus facilitating diagnostics.
5. If the module is to execute the reporting or messaging functions, configure suitable parameters and options, as recommended in sections “Starting GPRS reporting”, “Starting SMS reporting” and “Starting CLIP / SMS messaging”.

4.6 STARTING GPRS REPORTING

1. Enter the GPRS communication parameters (“GSM telephone, Monitoring stations” tab):
   – Access Point Name (APN) for Internet GPRS connection;
   – user name for Internet GPRS connection;
   – password for Internet GPRS connection;
   – DNS server IP address which is to be used by the module (the DNS server address requires no programming, if the IP address is entered for the monitoring station).
2. Configure parameters of the monitoring station(s) (“GSM telephone, Monitoring stations” tab):
   – select the “GPRS” option;
   – enter the monitoring station address (“Address (GPRS)” field);
   – enter the number of TCP port through which communication with the monitoring station will be effected;
   – for the SATEL IP format, enter the encryption key for data to be sent to the monitoring station (“Station key”);
   – for the SATEL IP format, enter the GPRS key.
3. Define the protocol to be used by the module for sending event codes to the monitoring station (“TCP/IP” or “UDP”).
4. Define the format to be used by the module for sending event codes to the monitoring station (“SATEL IP” or “SIA-IP”).

5. When the SIA-IP format is selected:
   – define the account number to be used to identify the control panel for the reporting purposes (“SIA-IP account no.” field);
   – define the time interval at which an additional test transmission is to be sent (“Test transm. every” field).
6. Indicate the monitoring station to which the event code is to be sent (the event may be sent to both stations) and define the Contact ID codes for events to be reported. It should be done in the “Reporting” tab, the “Keyfobs” tab (“Reporting” tab) and in the “MKP-300 keypad” tab, “Messaging / reporting” table. In the alarm module mode, with the “Set CID codes automatically” option enabled, the codes are assigned automatically.

4.7 STARTING SMS REPORTING

1. Enter the telephone number of Short Message Service Center in “SMS center number” field in the “GSM telephone, Monitoring stations” tab”, unless it has been saved by the operator to the SIM card memory.
2. Configure parameters of the monitoring station(s) (“GSM telephone, Monitoring stations” tab):
   – select the “SMS” field;
   – enter the GSM telephone number through which the monitoring station receives SMS messages (“Tel. number (SMS)” field).
3. Define the SMS message format in which the received event codes will be sent to the monitoring station (“GSM telephone, Monitoring stations” tab).
4. Indicate the monitoring station to which the event code is to be sent (the event may be sent to both monitoring stations) and define the Contact ID codes or two-character codes for events to be reported. It should be done in the “Reporting” tab and the “Keyfobs” tab (“Reporting” tab) and in the “MKP-300 keypad” tab, “Messaging / reporting” table. In the alarm module mode, with the “Set CID codes automatically” option enabled, the codes are assigned automatically.

4.8 STARTING CLIP / SMS MESSAGING

The SMS or CLIP messaging is conducted irrespective of the monitoring.

1. Enter the telephone number of Short Message Service Center in “SMS center number” field in the “GSM telephone, Monitoring stations” tab”, unless it has been saved by the operator to the SIM card memory.
2. Enter the telephone numbers which are to be notified by the module, using the SMS messages or CLIP service (“Telephone numbers for messaging and test transmissions” table in the “GSM telephone, Monitoring stations” tab).
3. Define about which events and in what form (CLIP or SMS) the predefined telephone numbers are to be notified. In case of SMS messaging, it is necessary to define the content of SMS message. It should be done in the “CLIP / SMS messaging” tab and the “Keyfobs” tab (“CLIP / SMS messaging” tab) and in the “MKP-300 keypad” tab, “Messaging / reporting” table. For events related to the analog zones, you can additionally enable the “Add input voltage value to message” option.

4.9 CHANGING THE TEXT MESSAGES BY USING SMS

The content of SMS message defined:

– in the “Violation / pass” and “Restore” fields, “CLIP/SMS messaging” tab,
– in the “SMS” field, “Keyfobs” tab,
– in the “SMS” field, “MKP-300 keypad” tab,

can be changed by sending an SMS message in the “current message content=new message content” form.

It should be remembered that the current message content must be entered exactly in the same way as it was written in the program.

If the message is to be sent from the phone whose number is programmed in the “Telephone numbers for messaging and test transmissions” list, “GSM telephone, Monitoring stations” tab, select the “SMS control only from list of telephone numbers for messaging” option, “Options, zones, outputs” tab.

If the message is to be sent from any phone number, the “SMS control only from list of telephone numbers for messaging” option, “Options, zones, outputs” tab, must be disabled.

The message can be sent at any moment.

5. INITIATING THE MODULE FIRMWARE UPDATE BY MEANS OF SMS MESSAGES

Send an SMS message containing the control command to initiate the process of module firmware update (“SMS initiating update”, “Firmware update” tab) to the module telephone number. The module will connect to the firmware update server, whose address is programmed in the module.

If the “Server address in SMS” option is enabled in the module (“Firmware update” tab), you can send a message with the **xxxx=yyyy:zz=** content, where “xxxx” is the control command, programmed in the module, which starts the update process, “yyyy” is the address of server with current firmware for the module (IP address or name), and “zz” is the server port number. The module will connect to the computer whose address is given in the SMS message. If the control command in the SMS message is correct, and the other data are wrong, the address and port of the server to which the module is to connect will be downloaded from the settings programmed in the module.

After completion of the update, an SMS message with information on the result of update process and module firmware version will be sent to the telephone number from which the SMS message initiating the firmware update process was sent.

6. MICRA CONTROL APPLICATION

MICRA CONTROL is the software used for remote operation of the MICRA alarm modules (version 2.05 and later) by means of devices running the Android operating system (version 2.0 and later). The application allows you to arm/disarm the system, clear alarms, control outputs, as well as bypass/unbypass zones. It also enables the MICRA system status to be monitored. Communication between the MICRA CONTROL application and the MICRA module is effected by means of SMS messages. The application can be downloaded free of charge from the Google Play store.

When using the application, remember that all commands are transferred to the MICRA module in the form of SMS messages. In reply to each received command, the module sends an SMS message with information on the current status of the system. Therefore, remote operation of the system involves financial costs.

For the application to function properly, the “Confirm controlling with status SMS” option *(see p. 22) must be enabled in the module.*

If no answer is received within 1 minute of sending the SMS message to the module, the application will inform the user that there is no answer from the module.

If the "SMS control only from list of telephone numbers for messaging" option (see p. 22) is enabled in the module, the telephone number of the device with MICRA CONTROL application must be on the "Telephone numbers for messaging and test transmissions" list (see p. 26).

The appearance of the application and its way of operation depend on the version of Android operating system.

If the GPRS reporting is active, the module response to commands may be delayed.

If the given function is not available (e.g. bypassing zones is impossible, when the system is armed), the user will be informed about it by a suitable message.

6.1 FIRST LAUNCH OF THE APPLICATION

1. After launching the application, the system selection screen will be displayed. Bring up the menu, using the function button of the device with MICRA CONTROL installed, and then touch the "New" command.
2. In the menu that will be displayed, touch the "Name" command.
3. In the window that will open, enter the name of MICRA system to be operated by means of the application. Touch the "OK" button. The window will close.
4. Touch the "Telephone number" command in the menu.
5. In the window that will open, enter the telephone number of MICRA module. Touch the "OK" button. The window will close.
6. Touch the "Save" button. The programmed MICRA system will be displayed in the list.

If necessary, repeat the steps 1-6 to add next MICRA systems.

7. Touch one of the displayed MICRA systems. An SMS message will be sent to the MICRA module. In reply, the module will send back, in the form of several SMS messages, the configuration data required for remote control of the MICRA system using the application.
8. After the SMS messages with configuration data are received, the main screen for MICRA system control will be displayed.

The downloaded configuration data are written to the memory of the device running the MICRA CONTROL application.

9. Touch the  button to get information on the current status of the system. An SMS message will be sent to the MICRA module. In response, the module will send back information on the system status in the form of SMS message.
10. You can proceed to control of the MICRA system.

6.2 SYSTEM SELECTION SCREEN

The first screen, which is displayed after starting the application, allows you to program basic parameters of the MICRA system, which is to be operated by means of the application (see section "First launch of the application"). You can program parameters of a few different MICRA systems. After they have been programmed, a list of MICRA systems that can be controlled will be available.

Touch one of the displayed MICRA systems to go to the main control screen of that system (if this is the first touch, SMS messages will be exchanged to download the configuration data).

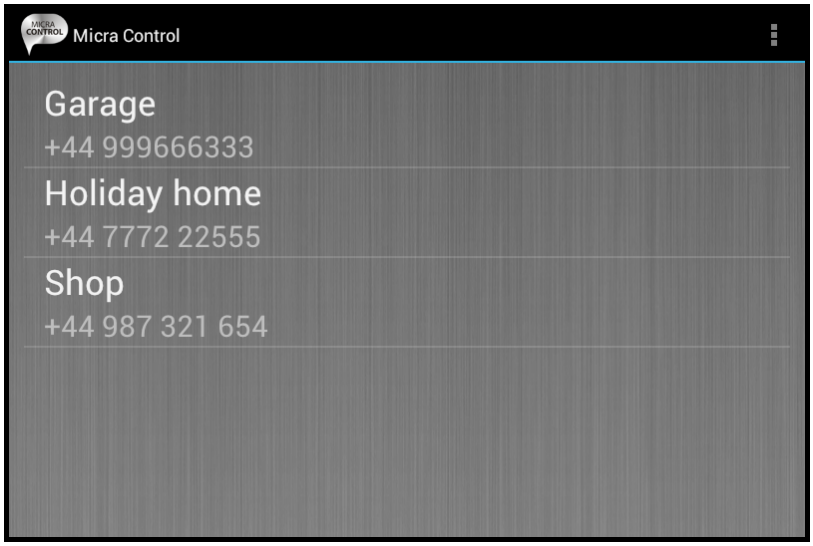


Fig. 21. Typical data on the system selection screen.

Touch and hold the selected MICRA system to display the menu with the following commands:

Select – takes you to the main control screen for the selected system.

Edit – takes you to editing the name and telephone number of the selected system.

Download configuration data – updates the configuration data of the selected system. The update is only required when the system configuration data have been changed (e.g. the content of control commands, names of zones or outputs, etc.).

Remove – deletes the selected system.

6.2.1 PROGRAM ACCESS PROTECTION

The system selection screen enables also access to the program to be protected using a code. To do so:

1. Use the function key of the device with MICRA CONTROL application installed to open the menu, and then touch the “Settings” command.
2. In the screen that will open, touch the “Protect with code” command.
3. Enter the code which will be required for authorization when starting up the application.
4. Enter the same code again in the field below.
5. Touch the “OK” key to confirm the changes made. When running the application next time, authorization by means of a code will be necessary.

6.3 BUTTONS FOR NAVIGATION BETWEEN SCREENS

touch the button to open the main screen for MICRA system control

touch the button to open the screen for output control

touch the button to open the zone screen

6.4 MAIN SCREEN FOR MICRA SYSTEM CONTROL

The screen allows you to arm/disarm and clear alarms in the system. It also contains information on the MICRA module version and system status. The on-screen icons are described below.


the level of signal received by the GSM module antenna (the presented icon corresponds to the maximum signal level – if the signal is weaker, the icon will change)


the current value of module supply voltage is shown next to the icon


the system is armed


module tamper


AC loss


battery trouble


the defined limit of transmissions sent by module per day exceeded (see: „Limit number of notifications to" parameter p. 24).

The following on-screen buttons are available:


press the button to refresh information on the system status


press the button to arm the MICRA system


press the button to disarm the MICRA system


press the button to clear alarm in the MICRA system

6.5 OUTPUT CONTROL SCREEN

The screen informs you about the status of relay outputs. Next to the output name, information on the output status is shown: OFF – inactive, ON – active. If the output is of the "Controllable" type, it can be controlled with the buttons:

touch the button to activate the output


touch the button to activate the output for time

touch the button to deactivate the output

If the output is not of the "Controllable" type, the buttons are grayed out.

6.6 ZONE SCREEN

The screen shows the status of zones and allows you to bypass/unbypass the zones. The icons illustrating the status of zones are described below.


normal zone status


zone bypassed


zone violated


alarm


alarm memory


tamper


tamper memory


low battery in the wireless detector assigned to the zone


loss of communication with the wireless detector assigned to the zone

Next to the zone name, on its left side, there is a field that can be selected by touching it if the zone is to be bypassed / unbypassed.

Using the function button of the device with the MICRA CONTROL application installed, you can open the menu in which the following commands are available:

Bypass – the selected zones will be bypassed.

Unbypass – the selected zones will be unbypassed.

Select all – all zones will be selected.

Deselect all – all zones will be deselected.

7. RESTORING FACTORY DEFAULT SETTINGS

7.1 USING THE GPRS-SOFT PROGRAM

1. Select the “Communication” command in the menu bar.
2. Select the “Factory default settings” function in the menu that will be displayed.
3. Confirm your intention to restore the converter factory defaults in the window that will open.

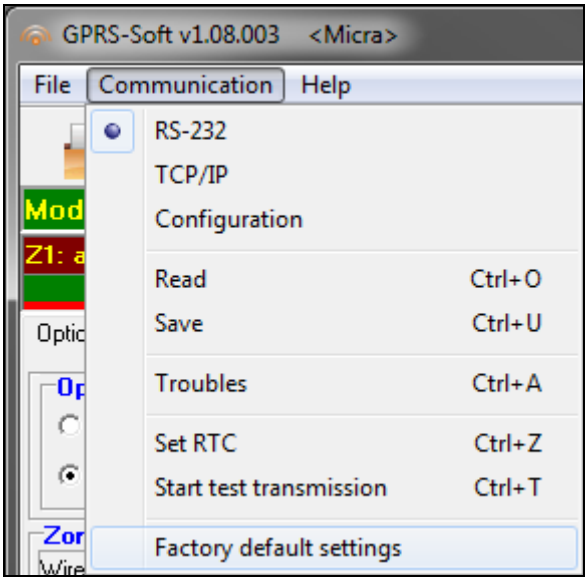


Fig. 22. ”Factory default settings" function in the “Communication” menu.

7.2 USING JUMPER PLACED ACROSS THE RS-232 TTL PORT PINS

1. Turn off the module power supply.
2. Place a jumper across the RS-232 TTL port pins on the module electronics board, as shown in Fig. 23.

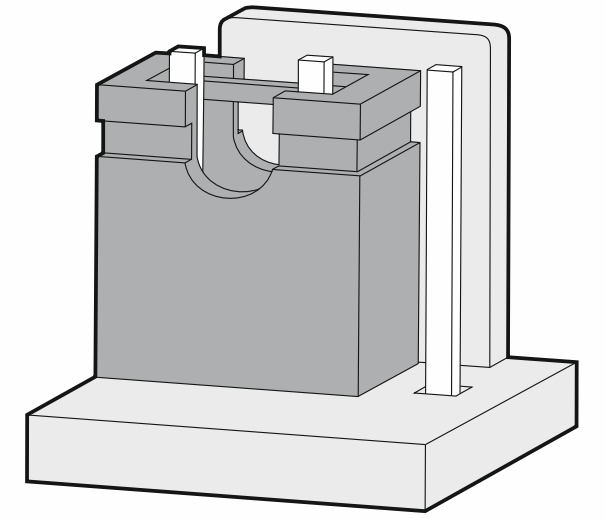


Fig. 23. The way of placing a jumper across the RS-232 TTL port pins.

3. Turn on the module power supply.
4. The on-board LED B will blink, and then all LEDs will be lit simultaneously for approx. 4 seconds.
5. Blinking of the LEDs A and B indicates that the factory default settings have been restored. Turn off the module power supply.
6. Remove the jumper.
7. Turn on the module power supply.

8. SPECIFICATIONS

Number of hardwired zones ..... 4+1
Number of outputs: relay 2
low-current, OC type 1
power 1
Supply voltage: ..... 18 V AC ±10%
Recommended transformer type ..... TR40VA (40VA / 18VAC)
Type of module power supply ..... A
Built-in power supply output current ..... 2 A
Current consumption from 230 V mains: standby ..... 50 mA
maximum ..... 150 mA
Current consumption from battery: standby ..... 120 mA
maximum ..... 420 mA
Battery failure voltage threshold ..... 11 V ±10%
Battery cut-off voltage ..... 10.5 V ±10%
Battery charging current ..... 250 mA ±20%
Power supply output voltage range ..... 10.5…13.8 V DC
AUX output ..... 500 mA / 12 V DC
FT output ..... 50 mA / 12 V DC
Relay output rating (resistive load) ..... 1000 mA / 24 V AC/DC
Number of supported keyfobs 8
Types of supported keyfobs P-2, P-4, T-1, T-2, T-4, MPT-300, MPT-350
Keyfob range (in open area)
P-2 / P-4 / T-1 / T-2 / T-4 / MPT-300 ..... up to 100 m
MPT-350 ..... up to 400 m
(any obstacles between transmitter and receiver will reduce operating range of the device)
Number of supported wireless detectors 8
Number of supported wireless keypads 1
Operating frequency range for wireless devices ..... 433.05 ÷ 434.79 MHz
Type of microphone socket ..... Jack 3.5 mm
Environmental class according to EN50130-5 II
Working temperature range ..... -10...+55 C
Maximum humidity ..... 93±3%
Electronics board dimensions ..... 120 x 68.5 mm
Dimensions of device with enclosure ..... 266 x 286 x 100 mm
Weight of device with enclosure (without transformer and battery) ..... 1072 g

9. MANUAL UPDATE HISTORY

DATE	FIRMWARE	CHANGES MADE
2012-04	2.03	• Information on MFD-300 wireless water flood detector has been added (p. 11 and 19). • Description of the "Alarm if zone violated at the end of exit delay" option has been supplemented (p. 16). • Description of the "Burglary alarm" output type has been supplemented (p. 21). • Description of the "Burglary alarm latched" output type has been modified (p. 21).
2012-07	2.04	• Information on the recommended microphone has been added (p. 5). • Description of the figure in section "Description of electronics board" has been modified (p. 5). • Description of the figure in section "Connecting detectors and other devices to zones" has been modified (p. 8). • Figure in section "Main menu" has been changed (p.13). • Content of section "<<Options, zones, outputs>> tab" has been updated (p.16). • Figure in section "<<Options, zones, outputs>> tab" has been changed (p. 16). • Information on new zone types has been added (p. 18). • Information on new output types has been added (p. 21). • Information on new option for outputs has been added (p. 21). • Description of the option "SMS control only from list of telephone numbers for messaging" has been changed (p. 22). • Description of the option "Confirm controlling with status SMS" has been changed (p. 22). • Content of section "<<GSM telephone, Monitoring station>> tab" has been updated (p. 23). • Figure in section "<<GSM telephone, Monitoring station>> tab" has been changed (p. 23). • Content of section "<<Test transmission>> tab" has been updated (p. 27). • Information on characters which may be included in the defined SMS messages (p. 31, 35 and 37). • A new section - "Changing the text messages by using SMS" - has been added (p. 41). • Content of section "Restoring factory default settings" has been modified (p. 46).
2012-11	2.05	• Information on the ability to remotely operate the module by means of MICRA CONTROL application has been added (p. 3). • Information on the necessity to check the serial number when adding wireless detectors has been added (p. 11). • Figure in section "<<Options, zones, outputs>> tab" has been changed (p. 16). • Information on new option for outputs has been added (p. 21). • A new section - " MICRA CONTROL application " - has been added (p. 42). • Numbering of figures in section "Restoring factory default settings" has been updated (p. 44 and 47).
2013-06	3.00	• Information on the ability to send event codes to the monitoring stations using the TCP and UDP protocols has been added (p. 3). • Information on the ability to remotely update the module firmware via GPRS has been added (p. 3). • Information on MMD-302 wireless magnetic contact with input for roller shutter detector has been added (p. 10 and p. 19). • Section "Main menu" has been modified (p. 13). • Description of "GPRS, SMS if GPRS failure" option has been updated (p. 25). • Information on "GPRS attempts number" new parameter has been added (p. 25). • Description of GPRS reporting new parameters has been added (p. 26). • New section “<<Firmware update>> tab" has been added (p. 37). • Section "Starting GPRS reporting" has been updated (p. 40). • New section "Initiating the module firmware update by means of SMS messages" has been added (p. 42). • Some figures and their numbering have been updated.
2013-12	3.00	• Information on MGD-300 wireless glass-break detector has been added (p. 11 and 19).

2017-05	3.03	• Information on the possibility of sending events to monitoring stations using SATEL IP or SIA-IP format has been added (p. 3). • Information on the possibility of defining the operator of the GSM network the module is to log into has been added (p. 3). • Figure in section “Main menu” has been changed (p. 13). • Figure in section “<<GSM telephone, Monitoring stations>> tab” has been changed (p. 23). • Descriptions of “Operator” and “auto” new functions have been added (p. 24). • Description of monitoring station parameters have been updated (p. 25). • Description of “GPRS protocol” function has been updated (p. 26). • Description of “SIA IP station 1 / SIA IP station 2” new function has been added (p. 26). • Figure in section “<<Event log>> tab” has been changed and section content has been modified (p. 38). • Content of section “Starting GPRS reporting” has been updated (p. 40). • Technical data have been updated (p. 48).
2018-03	3.03	• Figure in section “Description of electronics board” has been changed (p. 4). • Figure in section “The MICRA module installation” has been changed (p. 7). • Figure in section “Connecting power supply and starting the module” has been changed (p. 10). • Figure in section “Restoring factory default settings” has been changed (p. 23). • Technical data have been updated (p. 48).
2018-04	3.03	• Information about MPT-350 keyfob has been added (p. 34). • Technical data have been updated (p. 48).