



Ethernet communication module
ETHM-1 Plus



Firmware version 2.00

ethm1_plus_en 07/14

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

WARNINGS

The module should 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.

FreeRTOS is used in this device (www.freertos.org).

The SATEL's goal is to continually upgrade the quality of its products, which may result in alterations of their technical specifications and firmware. The current information on the introduced modifications is available on our website.

Please visit us:
<http://www.satel.eu>

The declaration of conformity may be consulted at www.satel.eu/ce

The following symbols may be used in this manual:



- note;



- caution.

CONTENTS

1	General.....	2
2	Field of application.....	2
3	Electronics Board.....	3
4	Setting address.....	3
4.1	Module connected to INTEGRA / INTEGRA Plus control panel	4
4.2	Module connected to VERSA control panel.....	4
5	Installation	4
6	Configuring	6
6.1	Module parameters and options	6
6.1.1	Module connected to INTEGRA / INTEGRA Plus control panel	6
6.1.2	Module connected to VERSA control panel	9
6.2	Virtual keypad.....	11
6.2.1	Module connected to INTEGRA / INTEGRA Plus control panel	11
6.2.2	Module connected to VERSA control panel	12
6.3	User functions [INTEGRA / INTEGRA Plus].....	12
6.4	Macro commands [INTEGRA / INTEGRA Plus]	12
6.4.1	Groups	13
6.4.2	Definitions.....	14
6.4.3	Defining macro commands.....	16
6.4.4	Exporting macro file.....	20
7	Remote programming / operating of control panel via Ethernet.....	21
7.1	GuardX program.....	21
7.1.1	Configuring ETHM-1 Plus module	21
7.1.2	Configuring GUARDX program	21
7.1.3	Initiating connection from GUARDX program	22
7.1.4	Initiating connection from keypad (through control panel)	22
7.2	Web browser	22
7.2.1	Configuring ETHM-1 Plus module	22
7.2.2	Configuring computer	22
7.2.3	Establishing communication	22
7.3	Mobile phone	24
7.3.1	Configuring ETHM-1 Plus module	24
7.3.2	Configuring mobile phone	24
7.3.3	Establishing communication – MOBILEKPD	24
7.3.4	Establishing communication – MOBILEKPD-2 / MOBILEKPD-2 PRO	24
8	Specifications	25

1 General

The ETHM-1 Plus module enables the INTEGRA Plus, INTEGRA and VERSA alarm control panels to communicate via the Ethernet network. The data transmission is encrypted by means of an advanced algorithm based on 192-bit key.

The module firmware can be updated using the application available on www.satel.eu

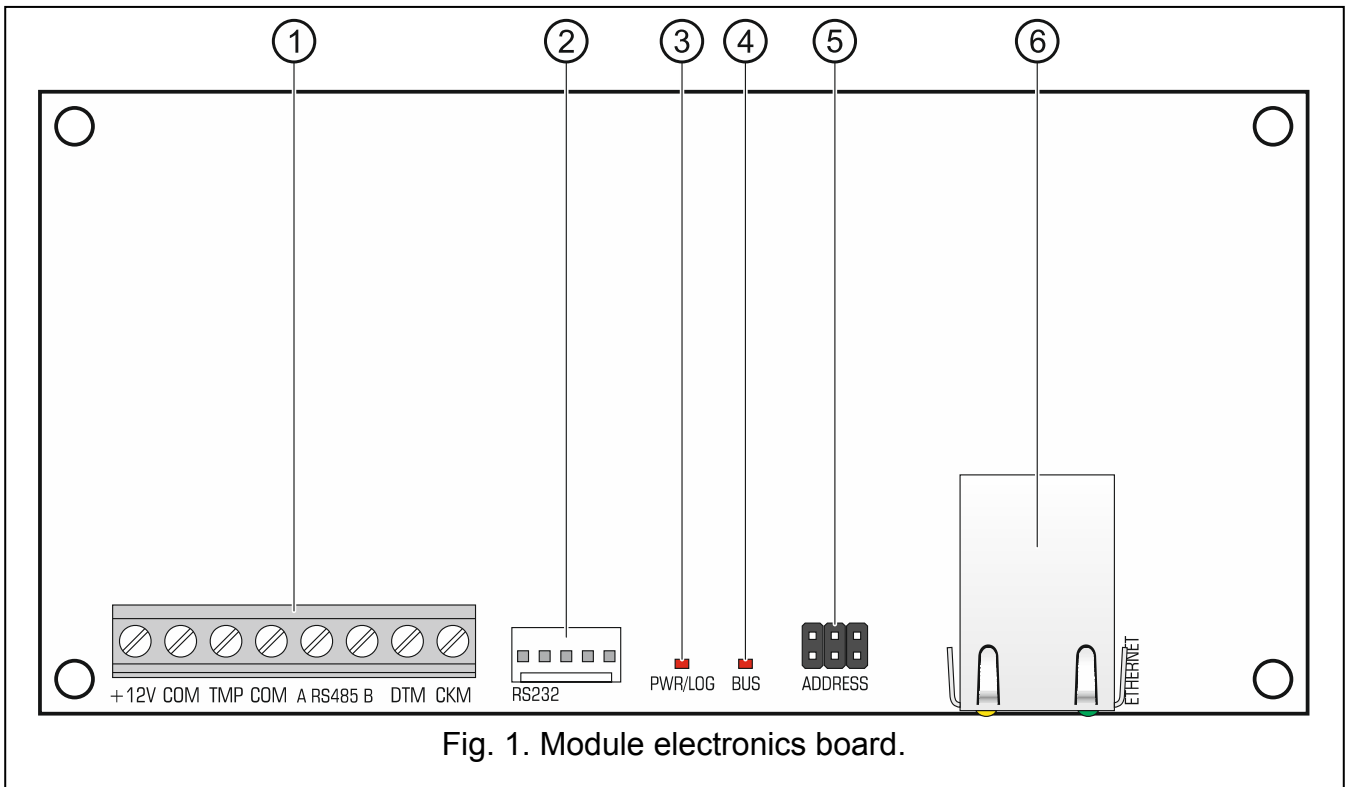
2 Field of application

- Control panel configuration using the DLOADX program from a computer with Internet access.
The feature is available for the INTEGRA Plus, INTEGRA (firmware version 1.03 or newer) and VERSA (firmware version 1.01 or newer) control panels.
- Management of the alarm system using the GUARDX program from a computer with Internet access.
The feature is available for the INTEGRA Plus and INTEGRA (firmware version 1.03 or newer) control panels.
- Operation and configuration of the control panel using a web browser which supports JAVA applications.
The feature is available for the INTEGRA Plus and INTEGRA (firmware version 1.03 or newer) control panels.
- Operation and configuration of the control panel using the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application from a mobile phone with Internet access. The mobile phone acts as an additional keypad for the alarm system.
The feature is available for the INTEGRA Plus and INTEGRA (firmware version 1.03 or newer) control panels.
- Reporting events from the control panel to the monitoring station via the Ethernet network. This contributes considerably to reducing the costs of reporting.
The feature is available for the INTEGRA Plus, INTEGRA (firmware version 1.04 or newer) and for the VERSA (firmware version 1.01 or newer) control panels.
- Notification of events in the alarm system using e-mail messages. The message body is generated automatically and corresponds to the description in the event log.
The feature is available for INTEGRA Plus (firmware version 1.13 or newer) control panels.
- Integration of the control panel with other systems, due to the open protocol for communication over Ethernet. It is a dedicated solution for companies engaged in integration of the object-oriented systems, which requires development of own software.
The feature is available for the INTEGRA Plus and INTEGRA (firmware version 1.06 or newer) control panels.



For additional information on the open communication protocol, please visit www.satel.eu

3 Electronics Board



① terminals:

- +12V** - +12 V DC power input.
- COM** - common ground.
- TMP** - tamper input (NC) – if not used, it should be shorted to common ground.
- A RS485 B** - terminals provided for future applications (RS-485).
- DTM** - data (communication bus).
- CKM** - clock (communication bus).

② RS-232 port.

③ PWR/LOG LED:

- OK – power OK,
- blinking – control panel being programmed or operated by means of the module.

④ BUS LED – blinking LED indicates that data exchange with the control panel is in progress.

⑤ pins for setting the module address (see "Setting address").

⑥ RJ-45 connector for Ethernet network. It is provided with two LEDs:

- green – indicates connection to the network and data transmission,
- yellow – indicates negotiated transmission rate (ON: 100 Mb; OFF: 10 Mb).

4 Setting address

To set an address, you must place jumpers across the ADDRESS pins. Table 1 shows how to use jumpers in order to set a specific address (■ - jumper on; □ - jumper off).

Address	0	1	2	3	4	5	6	7
Pins status								

Table 1.

4.1 Module connected to INTEGRA / INTEGRA Plus control panel

Set an address in the module within the range:

- from 0 to 3, if it is connected to INTEGRA 24 or INTEGRA 32 control panel,
- from 0 to 7, if it is connected to another INTEGRA or INTEGRA Plus control panel.

The address set must be different from that in the other devices connected to the keypad bus of the control panel (the control panel does not support devices with the same address).

4.2 Module connected to VERSA control panel

Set address 4 in the module. No keypad with the address 4 may be connected to the control panel.

5 Installation



Disconnect power before making any electrical connections.

The device is designed to be used only in the local area networks (LAN). It must not be connected directly to the public computer network (MAN, WAN). For establishing connection with public networks, use a router or xDSL modem.

The device is designed for installation indoors, in spaces with normal air humidity.

1. Secure the module electronics board in the enclosure. The module should be installed in the same enclosure as the control panel. This will facilitate connecting the RS-232 ports of control panel and module, which is required, if the control panel is to be configured via Ethernet using the DLOADX program.
2. Set the module address (see "Setting address").
3. Connect the +12V, COM, DTM and CKM module terminals to the control panel terminals (Fig. 2). It is recommended that an unshielded non-twisted cable be used for making the connection. If you use the twisted-pair type of cable, remember that CKM (clock) and DTM (data) signals must not be sent through one twisted-pair cable. The wires must be run in one cable.

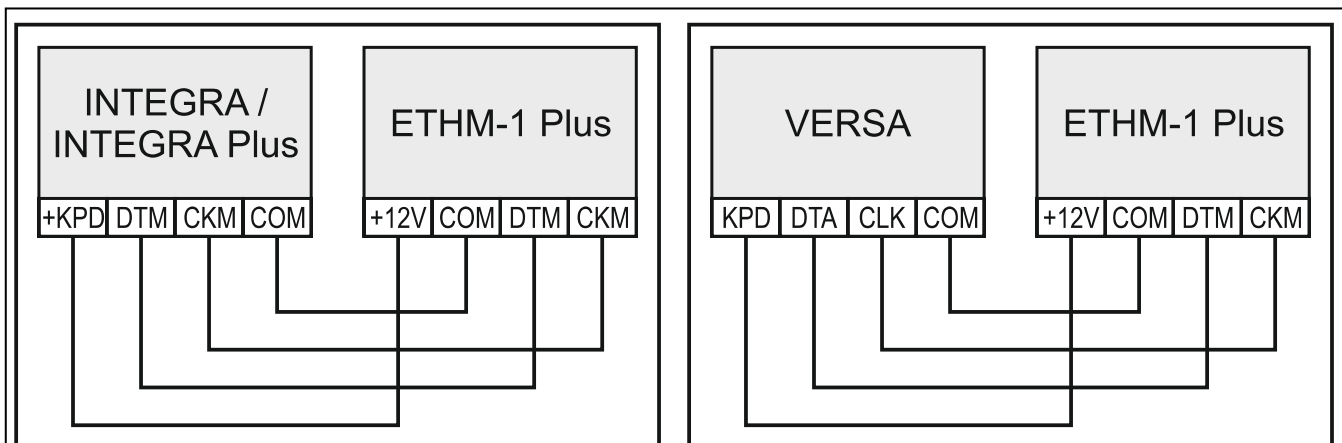


Fig. 2. Connecting the module to the control panel.

4. If the module is to supervise the enclosure tamper switch, connect the tamper switch wires to the TMP and COM terminals. Otherwise, connect the TMP terminal to the module COM terminal.
5. Connect the module to the Ethernet network. Use a cable compliant with the 100Base-TX standard (identical as for connecting the computer to the network).
6. Power on the alarm system.
7. Start the identification function in the control panel (see the control panel installer manual). The module will be identified as "ETHM-1".
8. Configure the module (see "Configuring").
9. If the control panel is to be configured via the module using the DLOADX program, connect the module RS-232 port to the control panel RS-232 port. Depending on the control panel, use the following cable to make the connection:

INTEGRA with connector socket of PIN5 type: **PIN5/PIN5** (Fig. 3)

INTEGRA with connector socket of RJ / INTEGRA Plus type: **RJ/PIN5** (Fig. 4)

VERSA: **PIN5/RJ-TTL**

The above mentioned cables are available in SATEL's product offering.

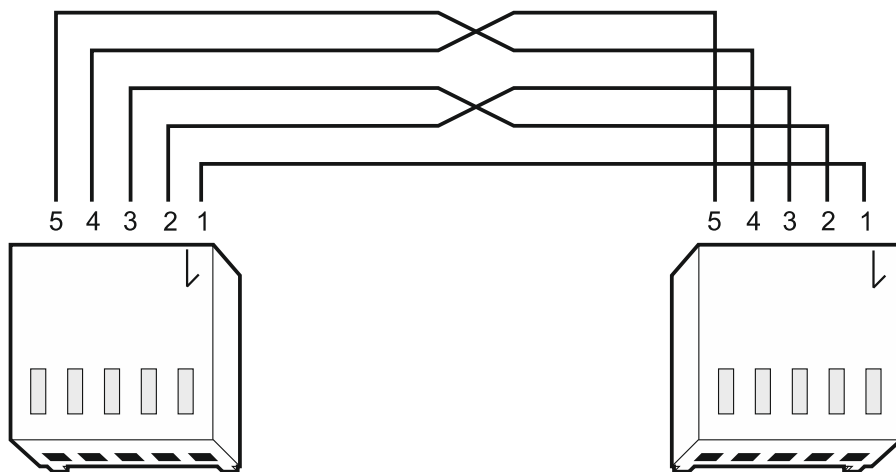


Fig. 3. Wiring diagram of the cable connecting RS-232 ports of ETHM-1 Plus module and INTEGRA control panel with PIN5 connector socket.

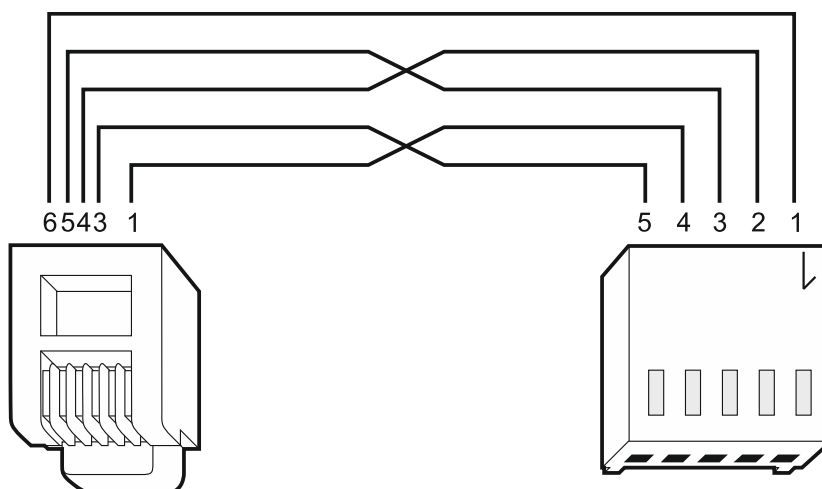


Fig. 4. Wiring diagram of the cable connecting RS-232 ports of ETHM-1 Plus module and INTEGRA / INTEGRA Plus control panel with RJ type connector socket.

6 Configuring

The module can be configured via the control panel, using a keypad or a computer with DLOADX program installed on it.

6.1 Module parameters and options

6.1.1 Module connected to INTEGRA / INTEGRA Plus control panel

You can configure parameters and options of the module using:

- LCD keypad: ►SERVICE MODE ►STRUCTURE ►HARDWARE ►LCD KEYPADS ►SETTINGS ►[*module name*],
- DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" branch →[*module name*] → "ETHM-1" tab (Fig. 5).

Shown in square brackets are the names of parameters and options as they are presented on the LCD keypad display.

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

Tamper signaled in part. [Tamper in part.] – partition where alarm will be triggered in the event of module tamper.

Obtain IP address automatically (DHCP) [DHCP] – if this option is enabled, the module will automatically download data on IP address, subnet mask and gateway from the DHCP server (in such a case, you do not have to program these parameters).



The IP address assigned to the module can be read:

- *in the keypad: using the **IP/MAC ETHM-1** user function available in the TESTS submenu. For a detailed description of the function please refer to the user manual for the control panel.*
- *in the DLOADX program: below the module parameters and options (Fig. 5).*

IP address – module IP address.

Subnet mask [Netmask] – the mask of the subnet in which the module is working.

Gateway – IP address of the network device through which the other devices in the local network can communicate with devices in other networks.

Obtain DNS server address automatically [DHCP-DNS] – if this option is enabled, the DNS server IP address is downloaded automatically from the DHCP server. The option is available, when the OBTAIN IP ADDRESS AUTOMATICALLY (DHCP) option is enabled.

DNS server – IP address of the DNS server which is to be used by the module. It can be programmed, if the OBTAIN DNS SERVER ADDRESS AUTOMATICALLY option is disabled.

DloadX

DloadX->ETHM-1 connection [Connect DloadX] – if this option is enabled, it is possible to initiate connection with the control panel via Ethernet from the DLOADX program.

Port [Port (DloadX)] – number of the TCP port used for communication with the DLOADX program. You can enter values from 1 to 65535. The value must be different from that entered for the other ports. Default value: 7090.

DloadX key [Key (DloadX)] – a string of up to 12 alphanumeric characters (digits, letters and special characters) defining the key for data encryption during communication with the DLOADX program.

DLOADX server [DloadX IP] – address of the computer running the DLOADX program. If the computer is not in the same local network, it must be a public address. You can enter either the IP address or the domain name.



In the LCD keypad, the function for programming address of the computer with DLOADX program is available in the user menu, CHANGE OPTIONS submenu (available to service and administrators).

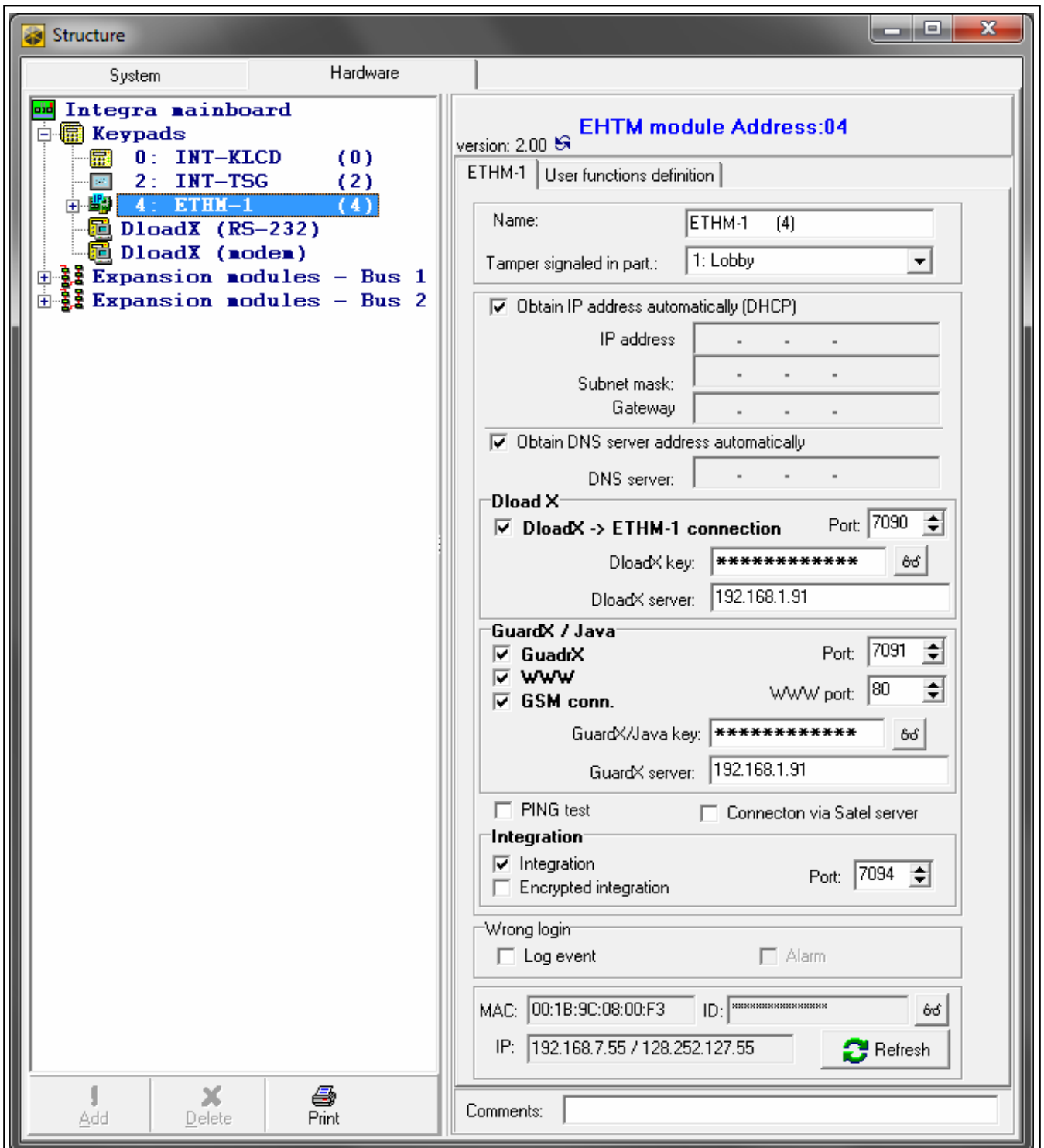


Fig. 5. DLOADX program: parameters and options of ETHM-1 Plus module connected to INTEGRA / INTEGRA Plus control panel.

GuardX / Java

GuardX [Connect GuardX] – if this option is enabled, it is possible to initiate connection with the control panel via Ethernet from the GUARDX program.

WWW [Connect Intern.] – if this option is enabled, it is possible to initiate connection with the control panel via Ethernet from the web browser.

GSM [Connect GSM] – if this option is enabled, connection with the control panel via Ethernet can be initiated from the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application.

Port [Port (others)] – number of the TCP port used for communication with:

- GUARDX program,
- JAVA application in the web browser,
- MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO in the mobile telephone.

You can enter values from 1 to 65535. The value must be different from that entered for the other ports. Default value: 7091.

WWW port – number of the TCP port used for communication with the web browser. You can enter values from 1 to 65535. The value must be different from that entered for the other ports. Default value: 80.

GuardX/Java key [Key (others)] – a string of up to 12 alphanumeric characters (digits, letters and special characters) defining the key for data encryption during communication with:

- GUARDX program,
- JAVA application in the web browser,
- MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO in the mobile telephone.

GuardX server [GuardX IP] – address of the computer running the GUARDX program. If the computer is not used in the same local network, it must be a public address. You can enter either the IP address or the domain name.



In the keypad, the function for programming address of the computer with GUARDX program installed is available in the user menu, CHANGE OPTION submenu (available to service and administrators).

PING test

PING test – if this option is enabled, the module can perform a communication test using the ping command sent to the indicated network device. Parameters related to the communication test should be programmed in the control panel:

LCD keypad: ►SERVICE MODE ►OPTIONS ►PING TEST,

DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" branch.

SATEL server

Connection via Satel server [SATEL server] – if this option is enabled, communication with the module can be effected via the SATEL server. For communication via the SATEL server, you do not need to additionally configure the network device through which the module connects to the public network.

Integration

Integration [Integrate] – if this option is enabled, the module can be used for integration of the alarm control panel with other systems.

Encrypted integration [Coded integr.] – if this option is enabled, communication with other systems is encrypted. The integration encryption key should be programmed in the control panel:

LCD keypad: ►SERVICE MODE ►OPTIONS ►INTEGRATE KEY,

DLOADX program: →"Options" window →"Service" tab.

Port [Port (integr.)] – number of the TCP port used for integration. You can enter values from 1 to 65535. The value must be different from that entered for the other ports. Default value: 7094.

Wrong login

Log event [Fail. – event] – if this option is enabled, all unauthorized attempts to connect to the module are written to the event log.

Alarm [Fail. – alarm] – if this option is enabled, any unauthorized attempt to connect to the module will trigger the tamper alarm. The option is available, if the LOG EVENT option is enabled.

Information

MAC – module hardware address.

ID – identifier assigned to the module for the purposes of communication via the SATEL server.

IP – local address / public address of the module.

6.1.2 Module connected to VERSA control panel

Parameters and options of the module can be configured using:

- LCD keypad: ►SERVICE MODE ►2. HARDWARE ►1. KPDS. & EXPS. ►2. SETTINGS ►[*module name*],
- DLOADX program: →"Versa – Structure" window →"Hardware" tab →"Expansion modules" branch →[*module name*] (Fig. 6).

Shown in square brackets are the names of parameters and options as they are presented on the LCD keypad display.

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

Tamper signaled in part. [Tamper in p.] – partition where alarm will be triggered in the event of module tamper.

Obtain IP address automatically (DHCP) [DHCP] – if this option is enabled, the module will automatically download data on IP address, subnet mask and gateway from the DHCP server (in such a case, you do not have to program these parameters).



*The IP address assigned to the module can be read in the LCD keypad using the **MODULE VER.** user function available in the TESTS submenu. For a detailed description of the function please refer to the user manual for the control panel.*

IP address – module IP address.

Subnet mask [Netmask] – the mask of the subnet in which the module is working.

Gateway – IP address of the network device through which the other devices in the local network can communicate with devices in other networks.

Obtain DNS server address automatically [DHCP-DNS] – if this option is enabled, the DNS server IP address is downloaded automatically from the DHCP server. The option is available, when the OBTAIN IP ADDRESS AUTOMATICALLY (DHCP) option is enabled.

DNS server – IP address of the DNS server which is to be used by the module. It can be programmed, if the OBTAIN DNS SERVER ADDRESS AUTOMATICALLY option is disabled.

DloadX

DloadX->ETHM-1 connection [DloadX→ETHM-1] – if this option is enabled, it is possible to initiate connection with the control panel via Ethernet from the DLOADX program.

Port [DloadX port] – number of the TCP port used for communication with the DLOADX program. You can enter values from 1 to 65535. The value must be different from that entered for the other ports. Default value: 7090.

DLOADX server [DloadX] – address of the computer running the DLOADX program. If the computer is not in the same local network, it must be a public address. You can enter either the IP address or the domain name.

DloadX key [DloadX key] – a string of up to 12 alphanumeric characters (digits, letters and special characters) defining the key for data encryption during communication with the DLOADX program.

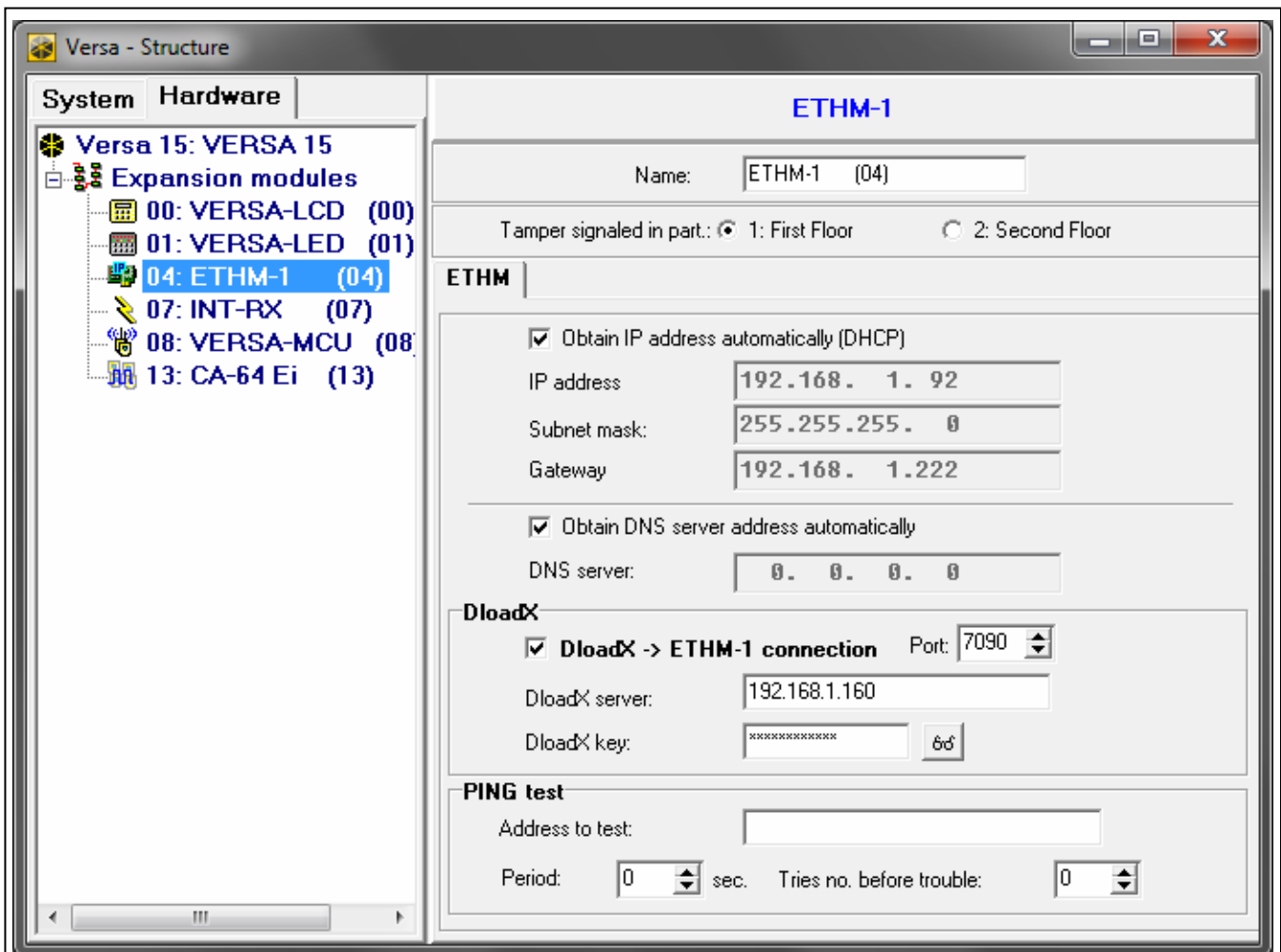


Fig. 6. DLOADX program: parameters and options of the ETHM-1 Plus module connected to VERSA control panel.

PING test

Address to test [PING] – address of the device to which a ping command to test communication is to be sent by the module. You can enter IP address or domain name.

Period [PING period] – the time interval between successive communication tests using the ping command. If value 0 is programmed, the communication test is disabled.

Tries no. before trouble [PING tries] – the number of failed communication tests (the module received no answer to the ping command sent), after which the trouble will be reported. If value 0 is programmed, the communication test is disabled.

6.2 Virtual keypad

The virtual keypad allows you to operate and program the alarm system in much the same way as using a physical keypad.

6.2.1 Module connected to INTEGRA / INTEGRA Plus control panel

You can use the virtual keypad in the DLOADX and GUARDX programs, web browser and in the mobile phone (after installation of the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application).

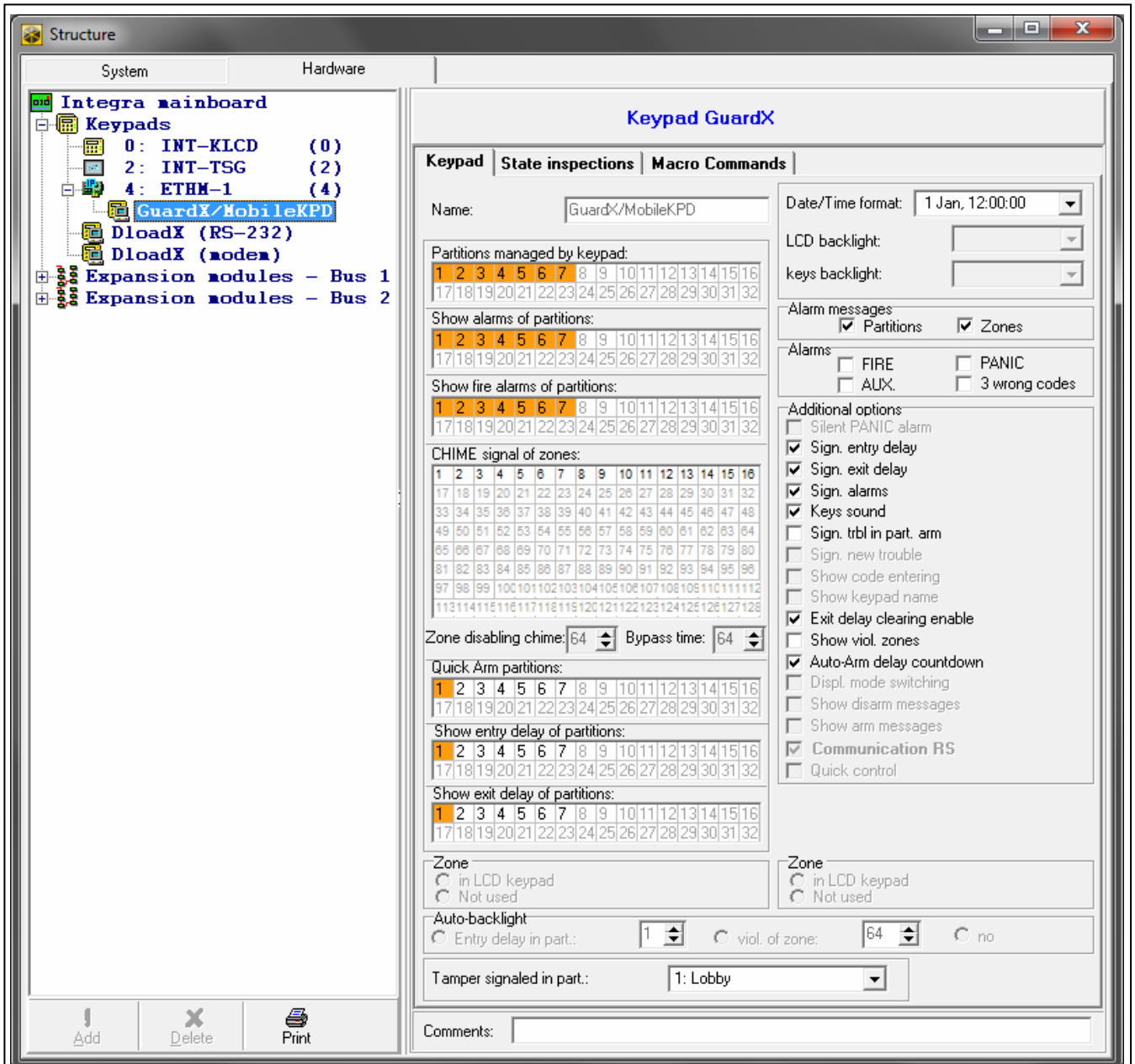


Fig. 7. DLOADX program: parameters and options of the virtual keypad available in GUARDX program, web browser or mobile phone.

Parameters and options of the virtual keypad available in the DLOADX program can be programmed using:

- LCD keypad: ►SERVICE MODE ►STRUCTURE ►HARDWARE ►LCD KEYPADS ►SETTINGS ►DLOADX RS,

- DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" branch →"DloadX (RS-232)" item.

Settings of the virtual keypad available in the GUARDX program, web browser or mobile phone can be programmed using:

- LCD keypad: ►SERVICE MODE ►STRUCTURE ►HARDWARE ►LCD KEYPADS ►SETTINGS ►GUARDX ADDR. n [n = module address],
- DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" branch →[*module name*] branch →"GuardX/MobileKPD" item (Fig. 7).

For description of the keypad parameters and options, please refer to the programming manual for INTEGRA / INTEGRA Plus control panel (only some of these parameters and options are available for the virtual keypad).

6.2.2 Module connected to VERSA control panel

You can use the virtual keypad in the DLOADX program. Parameters and options of the virtual keypad cannot be configured.

6.3 User functions [INTEGRA / INTEGRA Plus]

If the MOBILEKPD-2 / MOBILEKPD-2 PRO application is used in the mobile phone, the virtual keypad allows you to quickly start user functions after entering the code and pressing an arrow key. The functions can be assigned to individual keys using:

- LCD keypad: ►SERVICE MODE ►STRUCTURE ►HARDWARE ►LCD KEYPADS ►SETTINGS ►[*module name*] ►CODE+ARROWS,
- DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" branch →[*module name*] →"User functions definition" tab (Fig. 8).

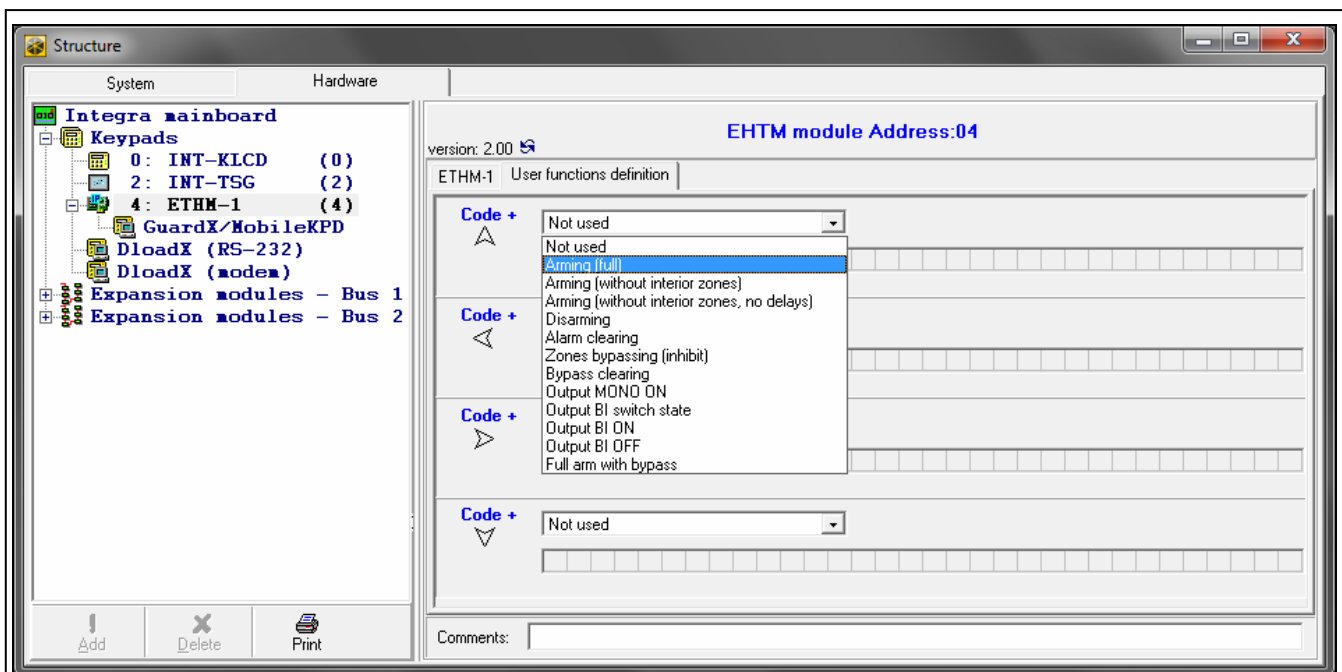


Fig. 8. Program DLOADX: "User functions definition" tab.


6.4 Macro commands [INTEGRA / INTEGRA Plus]

The MOBILEKPD-2 PRO application allows to control the alarm system by means of macro commands, thus making it possible to quickly and easily run a number of different functions by touching just a few keys. The macro commands can be defined in the DLOADX program

(→"Structure" window →"Hardware" tab →"Keypads" branch →[module name] branch →"GuardX/MobileKPD" item →"Macro Commands" tab).

Defined macro commands will be automatically downloaded by the MOBILEKPD-2 PRO application after establishing connection with the ETHM-1 Plus module.

Macro commands can be loaded into the application without establishing connection with the module. The file containing macro commands can be exported, and then saved to the telephone memory (to transfer the file, you can use a memory card or other solutions available for the given phone). This method allows you to use macro commands defined for the INT-KSG keypad in the MOBILEKPD-2 PRO application. Instead of a file with macro commands defined for the ETHM-1 Plus module, you can load a file with macro commands defined for the LCD keypad.

i *The data related to macro commands are stored in the module memory. Before you start defining the macro commands, click on the "Read" button in the "Macro commands" tab to read the data from the module. Having defined the macro commands, click on the "Write" button in the "Macro commands" tab to write the data to the module. The macro command related data are not read / written when you click on the  button in the main menu of DLOADX program.*

6.4.1 Groups

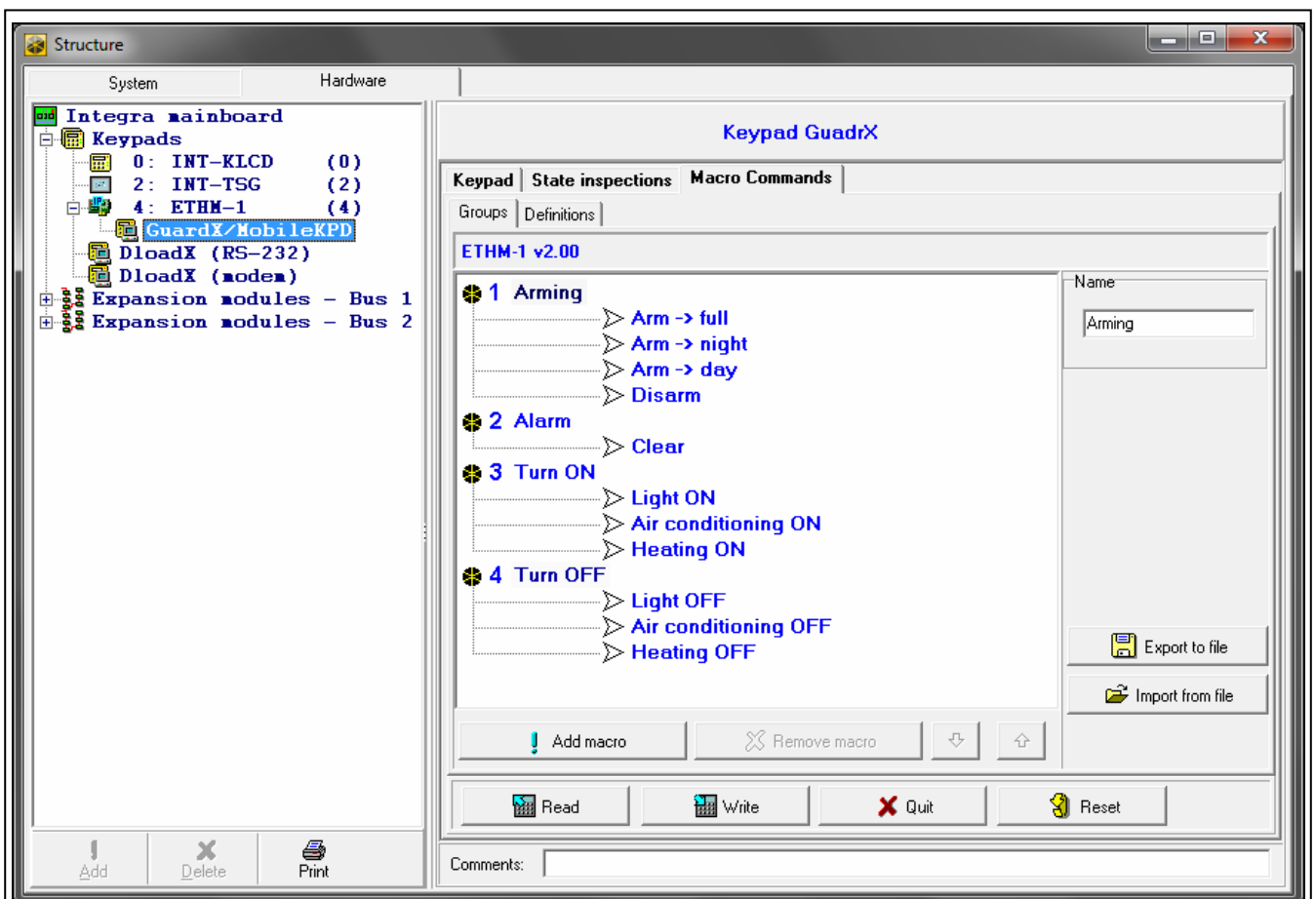


Fig. 9. DLOADX program: "Groups" tab.

The macro commands which are to be available to the keypad users must be assigned to one of the four groups. You can assign up to 16 macro commands to the groups. The DLOADX program presents the macro command groups and the macro commands assigned to them in the tree form.

Name – name of the macro command group (up to 8 characters). It is presented on the macro key.

Add macro – button available after you click on a macro command group. Clicking on the button will display a list of defined macro commands. Click on the name to add the macro command to the group.

Remove macro – click on the button to delete the selected macro command from the group.



– click on the button to move the highlighted macro command down within the group.



– click on the button to move the highlighted macro command up within the group.

Read – click on the button to read the macro command related data from the module.

Write – click on the button to write the macro command related data to the module.

Quit – click on the button to cancel reading or writing the macro command related data.

Reset – click on the button to delete all the defined macro commands (and restore factory default settings).

Export to file – click on the button to export defined macro commands to a file. The file with macro commands can be loaded into the MOBILEKPD-2 PRO application or imported to another ETHM-1 Plus module or to a INT-KSG keypad (i.e. macro commands can be copied between the devices).

Import from file – click on the button to import macro commands from a file.

6.4.2 Definitions

Macro commands can be created and configured in the "Definitions" tab. The macro command is a sequence of actions, composed of single commands, which are to be done by the control panel when running the macro command.

New macro – click on the button to create a new macro command.

Remove macro – click on the button to remove the selected macro command.

Name – individual macro command name (up to 32 characters).

Code – the code which is to be used for authorization when executing commands contained in the macro command. The code must have an appropriate authority level for execution of such commands to be possible. The code is presented as a string of asterisks.



If the code turns out to be incorrect when running macro commands (e.g. it was changed in the meantime), the user will be able to enter the correct code. It will be automatically saved to the phone memory (to replace the invalid code).

Authorization required – if this option is enabled, the macro command will only be run after user authorization by means of code. The code entered in the "Code" field will be ignored.

Disabl. if armed – if this option is enabled, the macro command will not be available, if any of the partitions managed by the virtual keypad is armed.

Autoexecute – if this option is enabled and there is only one macro command in the group, the macro command will be run immediately on tapping the macro key (if the AUTHORIZATION REQUIRED option is enabled, user authorization by means of code will be required).

Commands list – commands assigned to the currently highlighted macro command. The



buttons allow you to change the order of commands (moving the highlighted command up and down).

Add – click on the button to add to the list a new command, selected in the "Command" field.

Change – click on the button to save the changes to the command parameters which were made after adding the command to the list (otherwise, the changes made will not be saved).

Delete – click on the button to remove the highlighted command from the list.

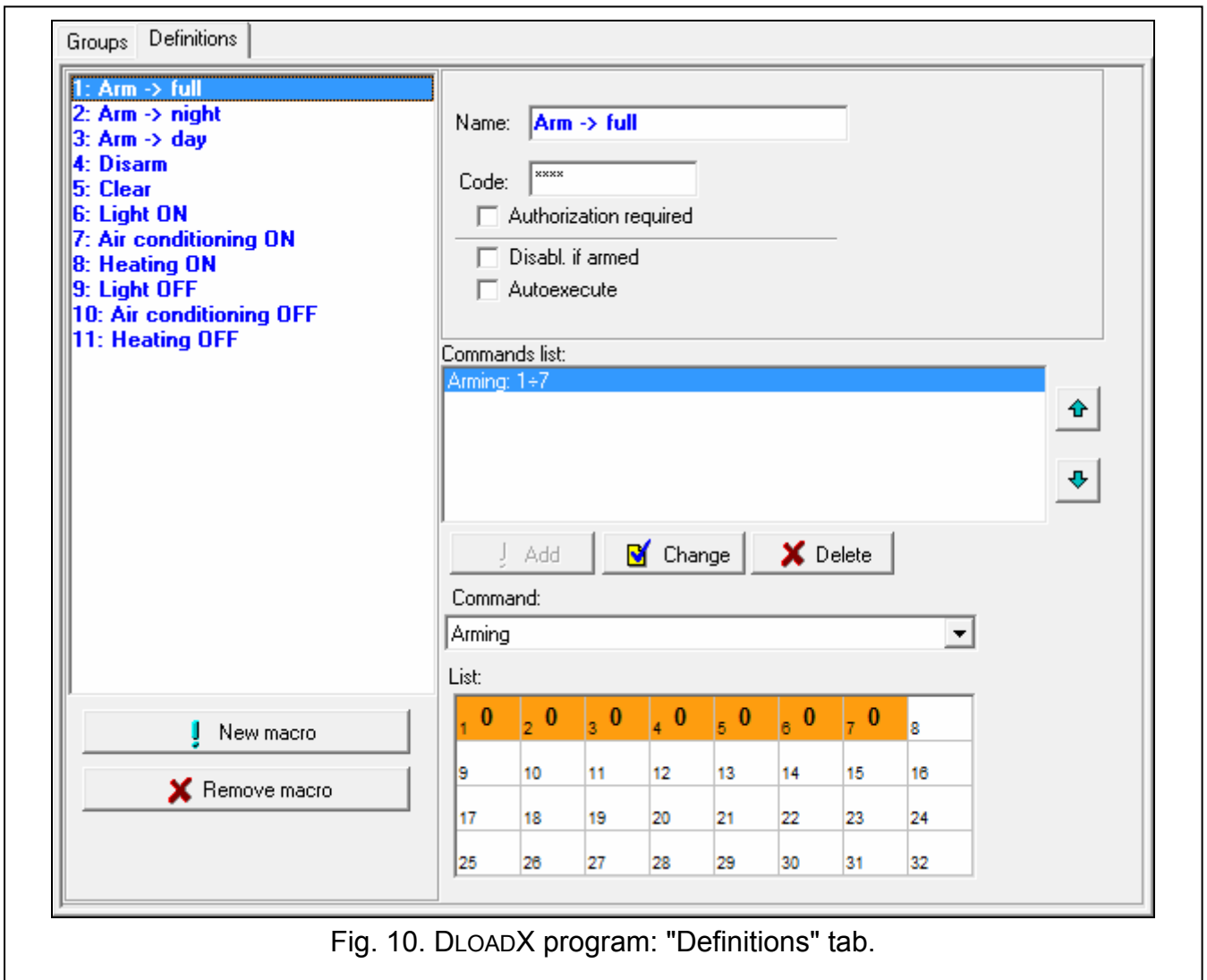



Fig. 10. DLOADX program: "Definitions" tab.

Command – function executed by the control panel, which can be assigned to the macro command. To display the list of all available functions, click on the  button. Depending on which function you have selected:

Arming – highlight the partitions which are to be armed (double-click on the field designated by the partition number) and define the arming mode (next clicks on the field designated by the partition number; the digit inside the field has the following meaning: 0 - fully armed; 1 – fully armed+bypasses; 2 – armed without interior; 3 - armed without interior and without entry delay).

Disarming – highlight the partitions which are to be disarmed (double-click on the field designated by the partition number).

Alarm clearing – highlight the partitions in which alarm is to be cleared (double-click on the field designated by the partition number).

Bypass zones – highlight the zones which are to be inhibited (double-click on the field designated by the zone number).

Unbypass zones – highlight the zones which are to be unbypassed (double-click on the field designated by the zone number).

Outputs ON – highlight the outputs which are to be activated (double-click on the field designated by the output number).

Outputs OFF – highlight the outputs which are to be deactivated (double-click on the field designated by the output number).

Change outputs state – highlight the outputs whose status is to be changed (double-click on the field designated by the output number).

KNX telegram – program the following parameters of KNX telegram:

INT-KNX module – INT-KNX module which is to send the telegram.

Group address – the group address which will be inserted in the telegram.

Type – the telegram type.

Value – the value that will be inserted in the telegram (parameter available for some types of the telegram).

Priority – telegram priority (if two elements of the bus start transmitting simultaneously, the telegram with higher priority will be sent first).

Exit delay clearing (no additional parameters to configure).

Quick arm – select the arming mode which is to be activated.



The partitions must be controlled by user code.

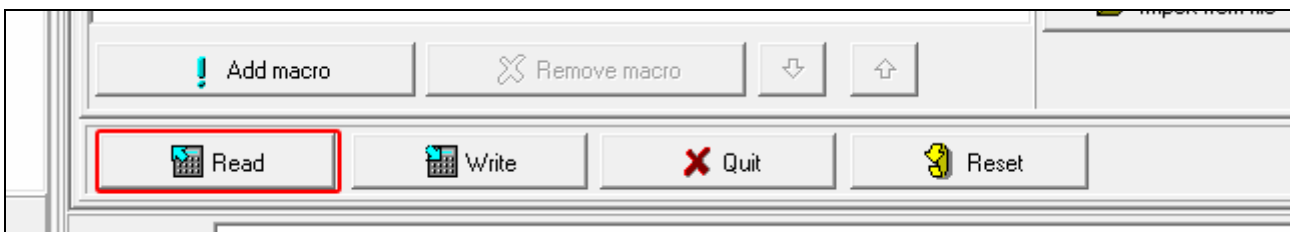
The zones must not have the BYPASS DISABLED option enabled.

The outputs must be the 24. MONO SWITCH, 25. BI SWITCH, 105. SHUTTER UP, 106. SHUTTER DOWN or REMOTE SWITCH type (they need not be assigned to any group of outputs).

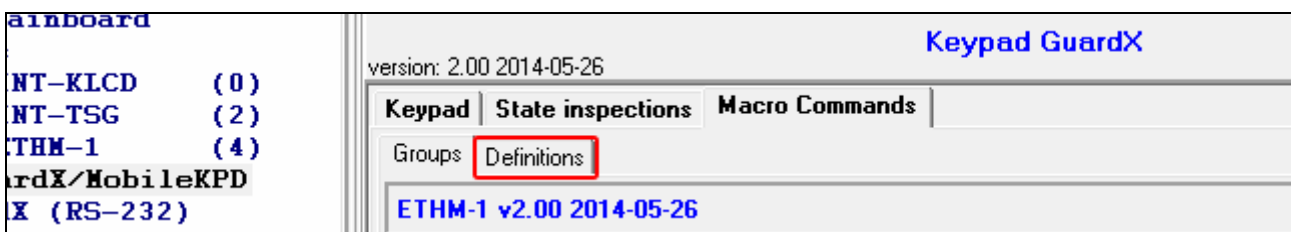
Using the MOBILEKPD-2 PRO application, you can control the KNX system, if the INT-KNX module is connected to the control panel.

6.4.3 Defining macro commands

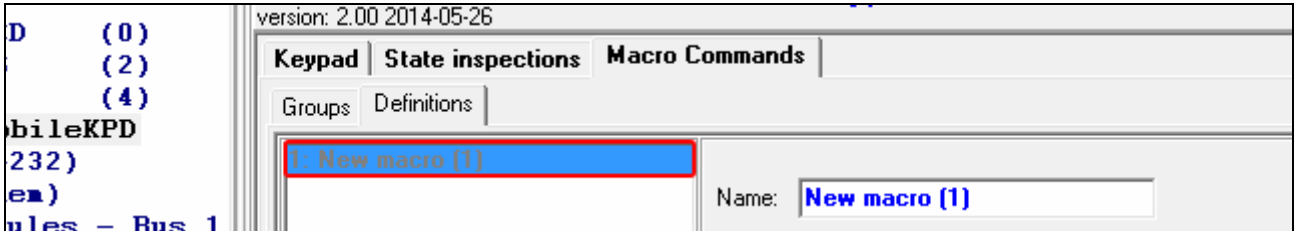
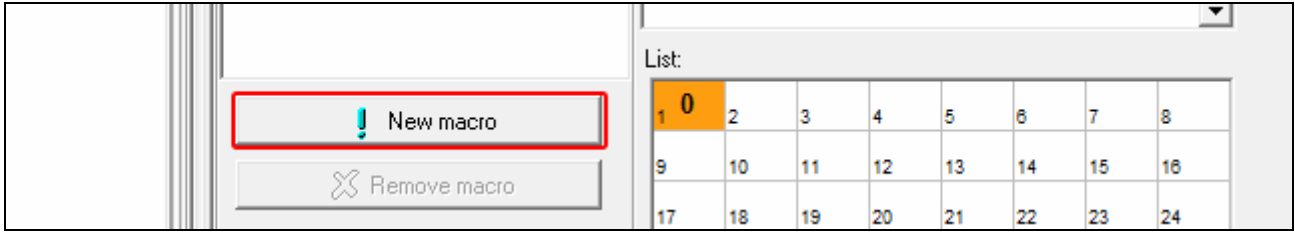
1. Click on the "Read" button to read the macro command related data from the module.



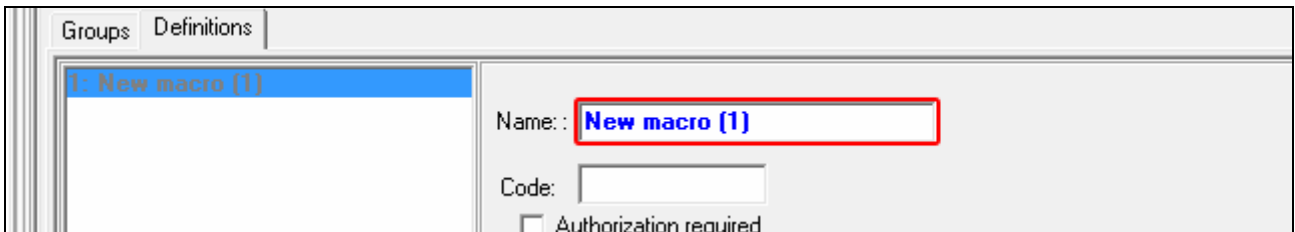
2. Click on the "Definitions" tab.



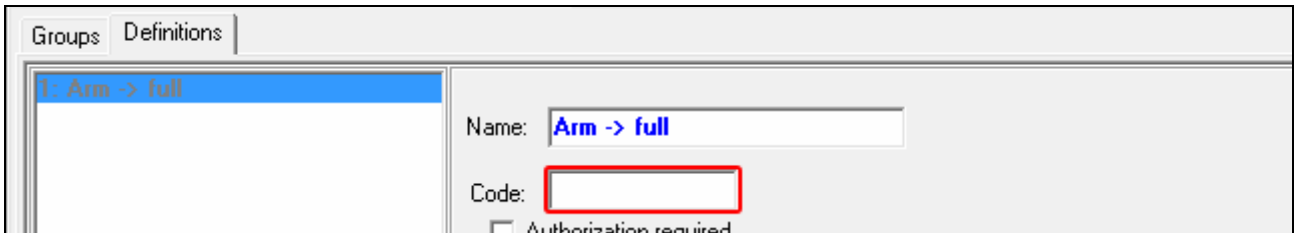
3. Click on the "New macro" button. A new macro command will appear on the list.



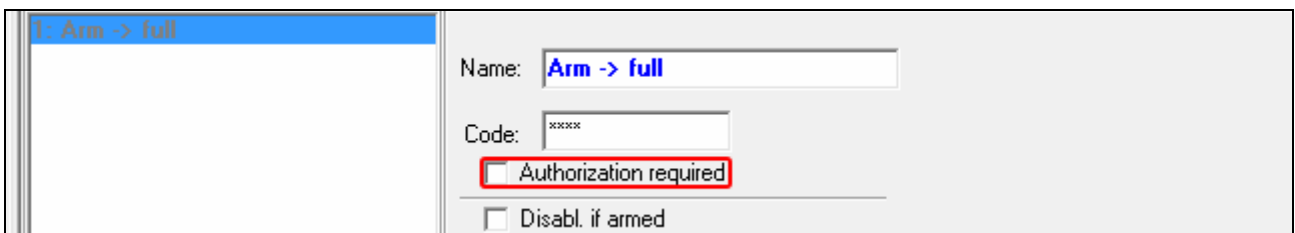
4. Enter a name for the new macro command.



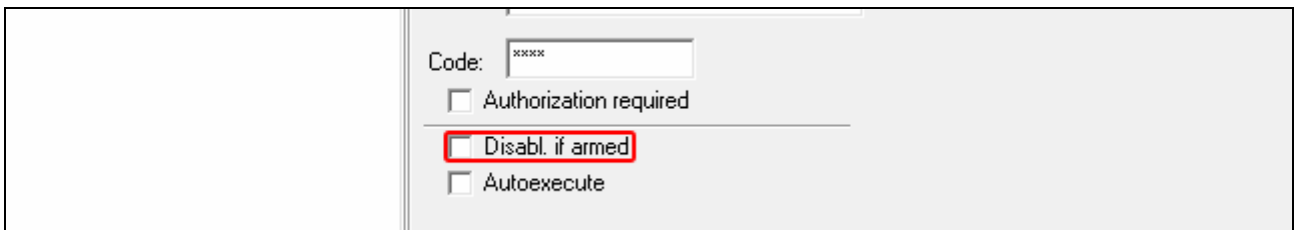
5. If the macro command is to be run without entering the code by the user, enter a code having appropriate authority level.



6. If running a macro command is to be each time preceded by user authorization, enable the AUTHORIZATION REQUIRED option.



7. If the macro command is to be unavailable when any of the partitions managed by the keypad is armed, enable the DISABL. IF ARMED option.



- 8. If the macro command is to be run immediately on tapping the macro key, enable the AUTOEXECUTE option (in such a case, only this one macro command is to be assigned to the group).

Code:

Authorization required

Disabl. if armed

Autoexecute

- 9. Click on the  button and select the function the new macro command is to execute.

! Add Change Delete

Command: Arming

List: 0

! Add Change Delete

Command: Arming

- Arming
- Disarming
- Alarm clearing
- Bypass zones
- Unbypass zones
- Outputs ON
- Outputs OFF
- Change outputs state
- KNX telegram
- Exit delay clearing
- Quick arming

! New macro

Remove macro

- 10. Configure the command parameters.

Command: Arming

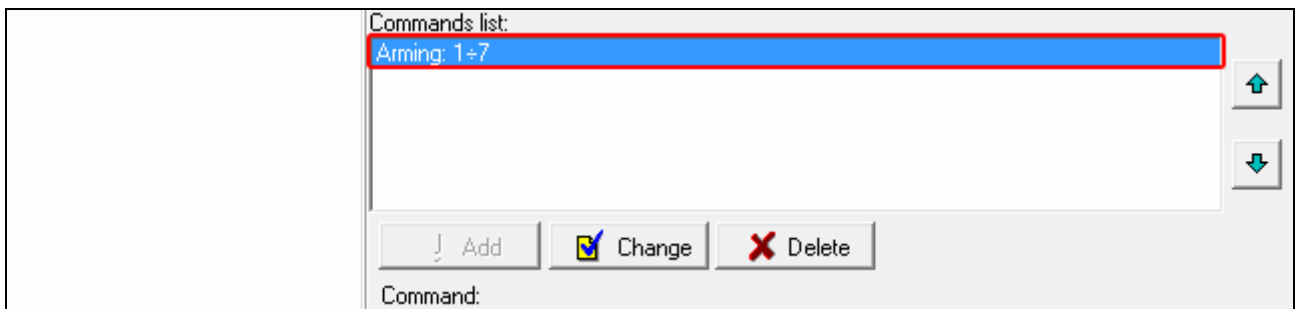
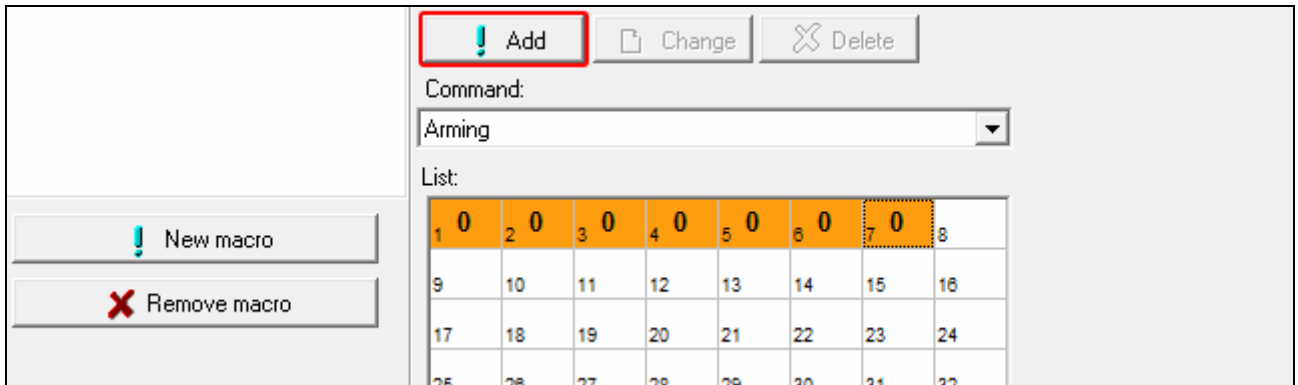
List:

1	0	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	17
17	18	19	20	21	22	23	24	25
25	26	27	28	29	30	31	32	

! New macro

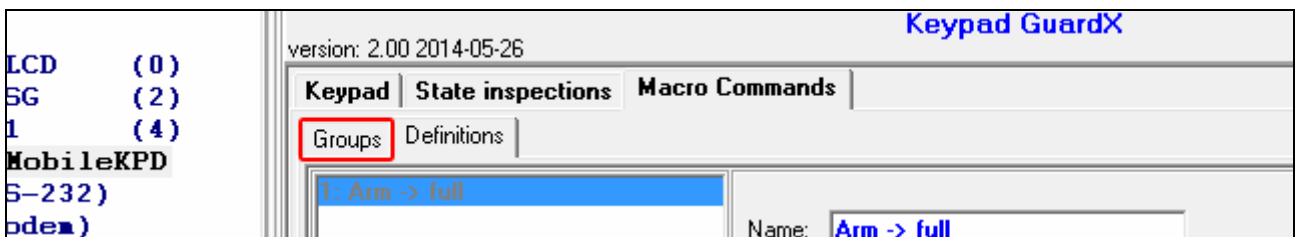
Remove macro

11. Click on the "Add" button. A new command will appear on the list of commands assigned to the macro command. You can still modify parameters of the command after clicking on it (having made the changes, click on the "Change" button).

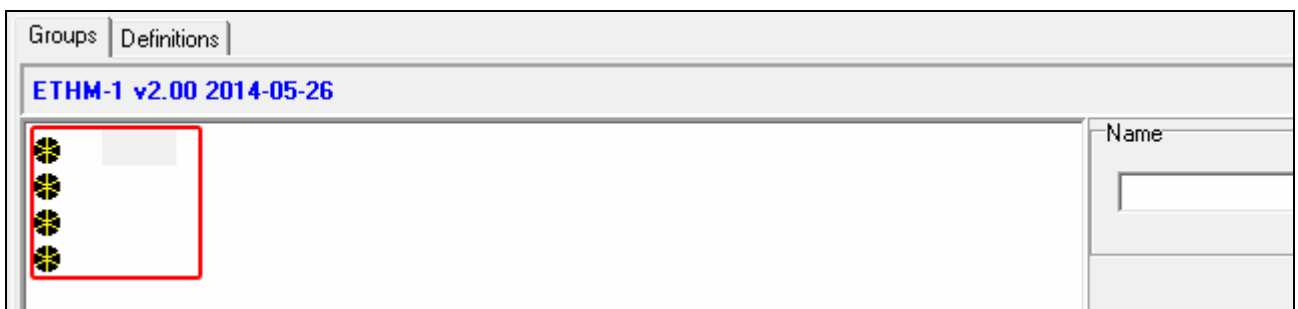


12. Repeat the steps 9-11, if you want to add next commands.

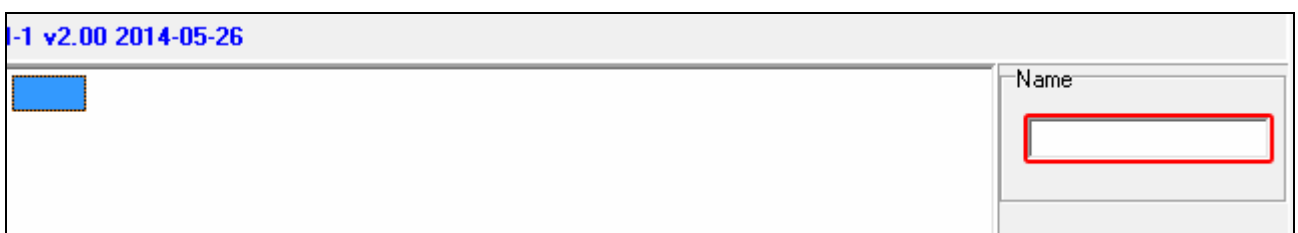
13. Click on the "Groups" tab.



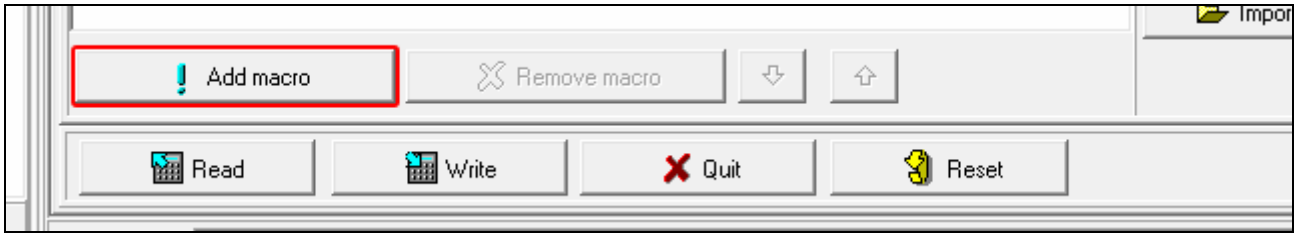
14. Click on the group you want to edit.



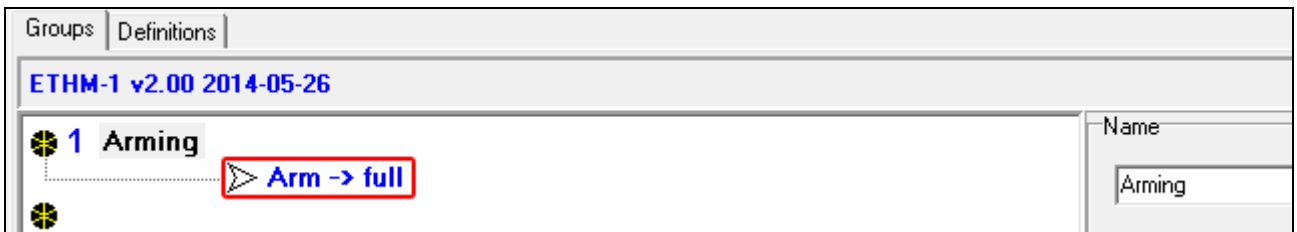
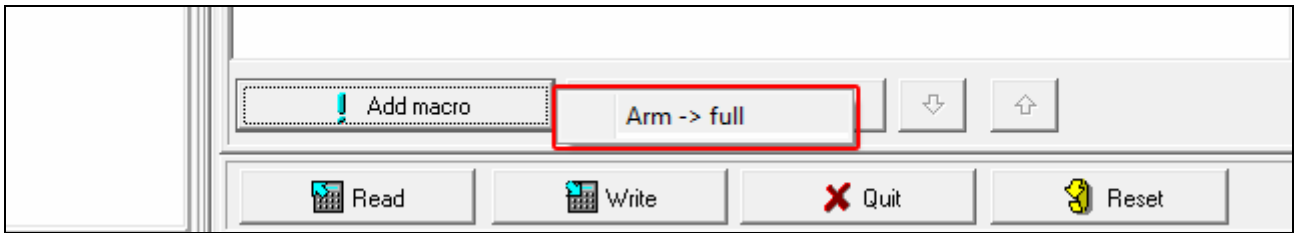
15. Enter the group name.



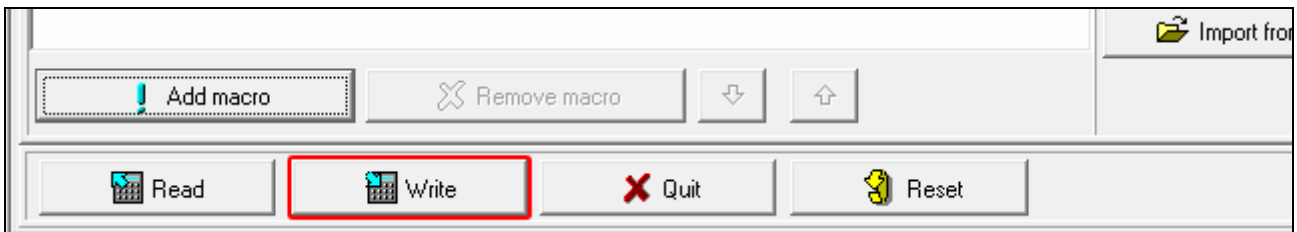
16. Click on the "Add macro" button. A list of all defined macro commands will be displayed.



17. Click on a macro command to add it to the group. The macro command will be put in the tree under the group.



18. Click on the "Write" button to write the macro command related data to the module.



6.4.4 Exporting macro file

i If the MOBILEKPD-2 PRO application is to run macro commands which have been defined for the INT-KSG keypad, the following operations must be carried out in the "Macro Commands" tab for the INT-KSG keypad.

1. Click on the "Groups" tab.
2. Click on the "Export to file" button.
3. In the window that will be displayed, enter the file name and then click on the "Save" button. Before you click on the "Save" button, you can indicate a location other than the default one, to which the file is to be saved.
4. In the window that will be displayed, enter the file encryption code (up to 24 alphanumeric characters), and then click "OK". The file encryption code will be required during loading of macro commands by the MOBILEKPD-2 PRO application.
5. A window will be displayed to inform you that the file has been saved.

7 Remote programming / operating of control panel via Ethernet



To enable communication with the control panel to be established from outside of the local network, the module must have a permanent public address.

After three consecutive attempts to establish communication with the module using an incorrect key, the module will stop responding for approx. 20 minutes to any attempts to establish communication from the given IP address.

For information related to configuring the control panel by means of the DLOADX program via the Ethernet network, please refer to the control panel programming manuals.

7.1 GuardX program

Communication between the GUARDX program and the control panel through the ETHM-1 Plus module can be established in two ways:

1. Initiating the connection from the GUARDX program. This method enables connection with the control panel to be established from any address.
2. Initiating the connection from the keypad (through the control panel). The alarm system can be managed remotely only with the knowledge of the control panel user, from the address programmed in the control panel.



Communication between the control panel and the GUARDX program can be established, if the communication identifiers in the program and in the control panel are identical (INTEGRA IDENTIFIER and GUARDX IDENTIFIER).

7.1.1 Configuring ETHM-1 Plus module

- Program the key for data encryption during communication with the GUARDX program (GUARDX/JAVA KEY).
- Enable the GUARDX option, if the connection is to be initiated from the GUARDX program.
- Enter the address of computer running GUARDX (GUARDX SERVER) program, if the connection is to be initiated from the keypad (through the control panel).
- Enter the number of TCP port which will be used for communication with the GUARDX program, if it is to be different from 7091.

7.1.2 Configuring GUARDX program

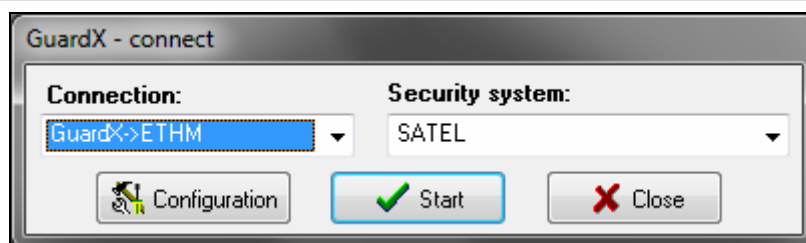


Fig. 11. GUARDX program: startup window.

In the startup window of GUARDX program (Fig. 11), click on the "Configuration" button. A window will be displayed, in which, in "TCP/IP" tab (Fig. 12), you should program:

- ETHM-1 Plus module address, if communication is to be initiated from GUARDX program,
- TCP port number (identical to that programmed in the module for communication with GUARDX program – except where communication occurs through a network device on which redirection to another port takes place),

- data encryption key (GUARDX/JAVA KEY).

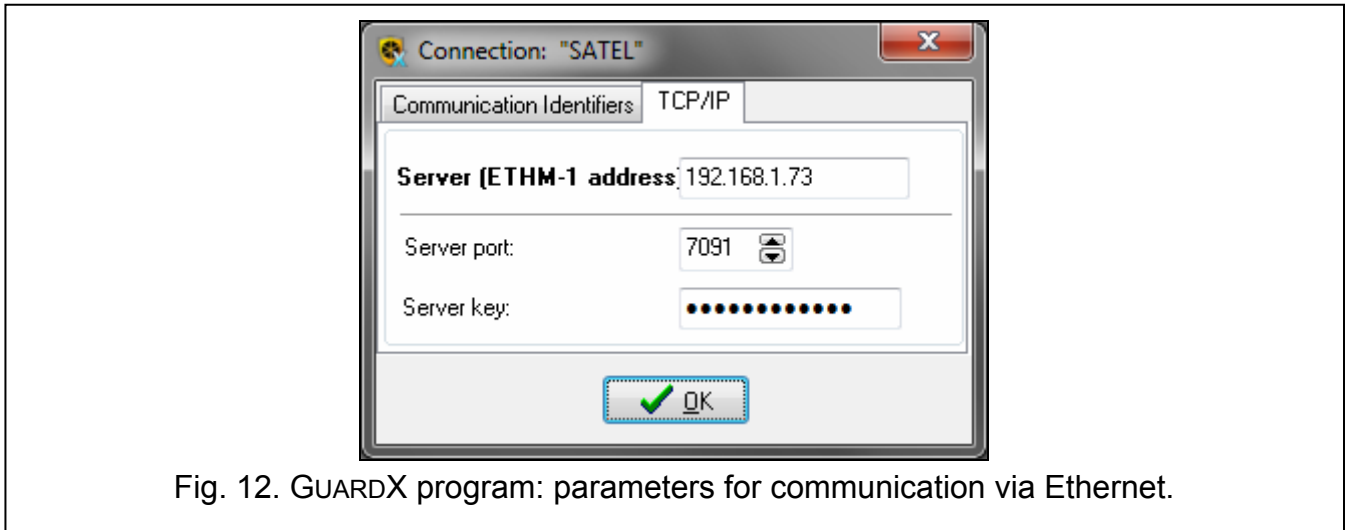


Fig. 12. GUARDX program: parameters for communication via Ethernet.

7.1.3 Initiating connection from GUARDX program

1. In the startup window, "Connection" field, select "GuardX -> ETHM" (Fig. 11), and then click on the "Start" button.
2. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

7.1.4 Initiating connection from keypad (through control panel)

1. In the startup window, "Connection" field, select "GuardX <- ETHM", and then click on the "Start" button.
2. Start in the keypad the ETHM-1 – GUARDX function ([code]* ► DOWNLOADING ► ETHM-1 – GUARDX). The function is available to the service, administrator and user having the DOWNLOADING STARTING right.
3. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

7.2 Web browser

7.2.1 Configuring ETHM-1 Plus module

- Enable the WWW option.
- Program the key for data encryption during communication with the JAVA application in the web browser (GUARDX/JAVA KEY).
- Enter the number of TCP port which will be used for communication with the web browser, if it is to be different from 80 (WWW PORT).
- Enter the number of TCP port which will be used for communication with the JAVA application in the web browser, if it is to be different from 7091.

7.2.2 Configuring computer

The Java Virtual Machine must be installed on your computer. You can download it from www.java.com

7.2.3 Establishing communication

1. Start the web browser.

2. In the address field, enter the IP address of ETHM-1 Plus module, and then press ENTER.



If a port other than 80 is to be used for communication between the module and the web browser, the address entered must be followed by a colon and the port number.

3. When the login page displays (Fig. 13), enter in the corresponding fields:

- data encryption key (GUARDX/JAVA KEY),
- TCP port number (identical to that programmed in the module for communication with the JAVA application in the web browser – except where communication occurs through a network device on which redirection to another port takes place),

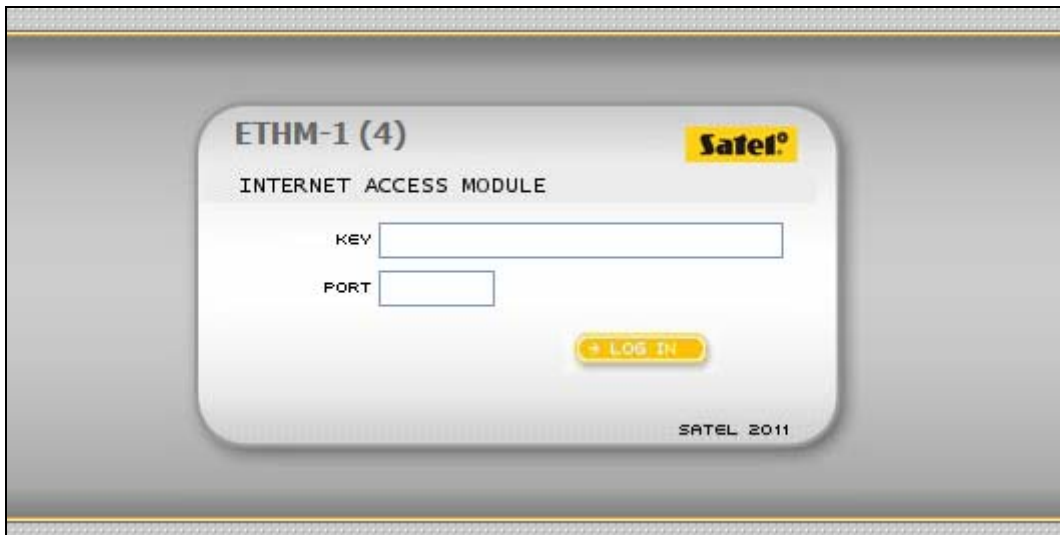


Fig. 13. Web browser: login page.

4. Click on the "Log in" button.

5. The virtual keypad will be displayed in the browser (Fig. 14).

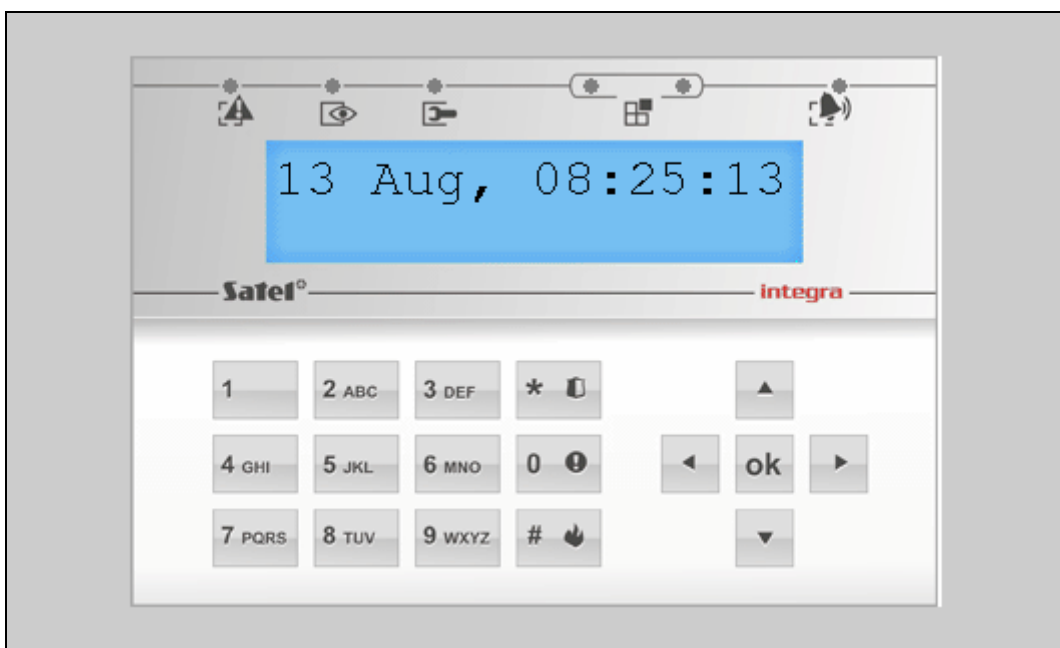


Fig. 14. Web browser: virtual keypad.

7.3 Mobile phone

7.3.1 Configuring ETHM-1 Plus module

- Enable the GSM option.
- Program the key for data encryption during communication with the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application in the mobile phone (GUARDX/JAVA KEY).
- Enter the number of TCP port which will be used for communication with the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application in the mobile phone, if it is to be different from 7091.

7.3.2 Configuring mobile phone

Install the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application on your phone. The application can be downloaded at www.satel.eu (select the application suitable for your mobile phone), from the internet stores "Google play" (Android system devices) or "App Store" (iOS system devices).

Having installed the application, enter:

- alarm system name,
- ETHM-1 Plus module address,
- TCP port number (identical to that programmed in the module for communication with the MOBILEKPD / MOBILEKPD-2 / MOBILEKPD-2 PRO application – except where communication occurs through a network device on which redirection to another port takes place),
- data encryption key (GUARDX/JAVA KEY).

After saving the above data to the phone memory, a list of alarm systems will be displayed.

Loading macro file – MOBILEKPD-2 PRO

In the case of MOBILEKPD-2 PRO application, macro commands can be loaded from file during configuration of parameters required for establishing communication with the alarm system. Having indicated the file containing macro commands, you must enter the file encryption code.

7.3.3 Establishing communication – MOBILEKPD

1. Using phone keys, select an alarm system from the list.
2. Select: →"Options" →"Start".
3. Elements of the virtual keypad will be shown on the display.

7.3.4 Establishing communication – MOBILEKPD-2 / MOBILEKPD-2 PRO

Touch the name of the alarm system. The virtual keypad will be displayed.



If parameters of only one alarm system are programmed, the screen with a list of systems will not be displayed after next application start, the virtual keypad will be displayed at once.

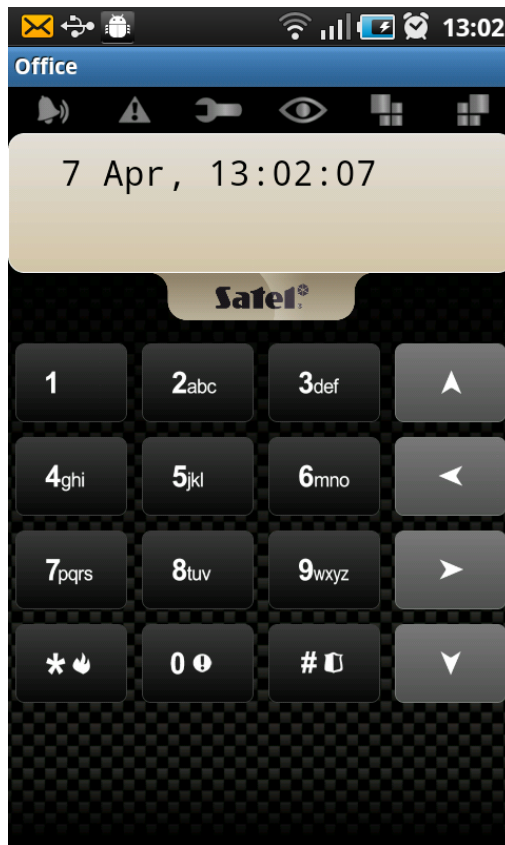


Fig. 15. MOBILEKPD-2 application (Android system phone): virtual keypad.

8 Specifications

Supply voltage	12 V DC ±15%
Standby current consumption	70 mA
Maximum current consumption	80 mA
Environmental class according to EN50130-5	II
Operating temperature range.....	-10...+55 °C
Maximum humidity	93±3%
Dimensions	68 x 140 mm
Weight.....	64 g