TCP/IP Communication Module

ETHM-1

Firmware version 1.05

ethm1_en 03/13

SATEL sp. z o.o.
ul. Schuberta 79
80-172 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.

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.

1 General

The ETHM-1 module enables the INTEGRA, INTEGRA Plus and VERSA alarm control panels to communicate via the Ethernet (TCP/IP) network. The data transmission is encrypted using an advanced algorithm based on 192-bit key.

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

2 Typical Applications

- Configuration of the control panel by 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 control panels (firmware version 1.01 or newer).

- Management of the security alarm system by using the GUARDX program from a computer with Internet access.

  The feature is available for the INTEGRA Plus and INTEGRA control panels (firmware version 1.03 or newer).

- Operation and configuration of the control panel by using a web browser which supports JAVA applications.

  The feature is available for the INTEGRA Plus and INTEGRA control panels (firmware version 1.03 or newer).

- Operation and configuration of the control panel by using the MOBILEKPD / MOBILEKPD2 application from a mobile phone with Internet access. The mobile phone can become an additional alarm system keypad.

  The feature is available for the INTEGRA Plus and INTEGRA control panels (firmware version 1.03 or newer).

i *The MOBILEKPD2 application can be installed on a variety of mobile devices running the Android, iOS or another operating system which supports Java applications.*

- Transfer of events from the control panel to the central monitoring station via the Ethernet (TCP/IP) network. This allows you to significantly reduce the cost of reporting.

  The feature is available for the INTEGRA Plus, INTEGRA (firmware version 1.04 or newer) and for the VERSA control panels (firmware version 1.01 or newer).

- Integration of the control panel with other systems over the Ethernet (TCP/IP) network, owing to the open-source communication protocol. This application is dedicated to the companies dealing with integration of the object-oriented systems and requires development of their own software.

  The feature is available for the INTEGRA Plus and INTEGRA control panels (firmware version 1.06 or newer).

i *Further information on the open-source communication protocol can be found at the www.satel.eu site.*

3 Electronics Board

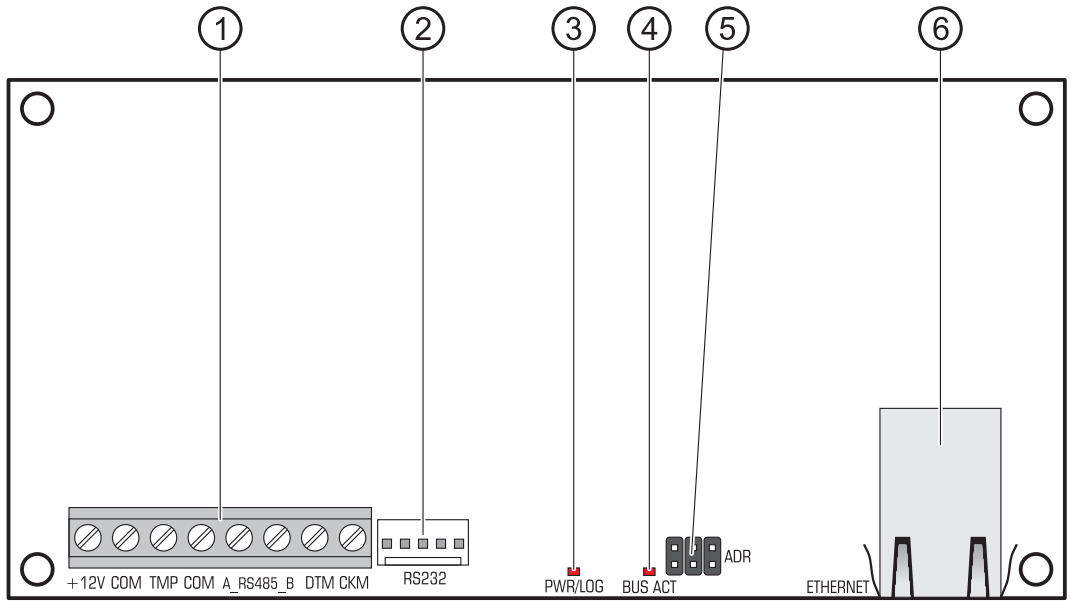

Fig. 1. Module electronics board.

① terminals:

+12V - power input (+12 V DC).

COM - common ground.

TMP - tamper input (NC). If not used, it should be connected to the common ground.

A_RS485_B - unused terminals.

DTM - data (communication bus).

CKM - clock (communication bus).

② RS-232 port.

③ PWR/LOG LED:

– lit – power supply present;

– blinking – control panel is being programmed or operated by means of the module.

④ BUS ACT LED blinking when data exchange with the control panel is going on.

⑤ ADR pins for setting the module address (see SETTING THE ADDRESS).

⑥ socket for connecting the module to Ethernet (TCP/IP) network. The socket has two built-in LEDs. The green one indicates network connection and data transfer, and the yellow one – the negotiated transmission rate (ON: 100 Mb; OFF: 10 Mb).

4 Installation and Start-up

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).

Connection to the public network may only be done through a router or xDSL modem.

The module should be installed indoors, in spaces with normal humidity of air.

1. Set the module address (see SETTING THE ADDRESS).
2. Install the module in the enclosure. If the control panel is to be configured via the Ethernet (TCP/IP) network using the DLOADX program, the module must be installed in the same enclosure with the control panel.
3. Connect the module terminals to the control panel terminals as shown in Table 1 (you can also use another control panel power output to supply the module). To make a connection, it is recommended that an unshielded straight-through cable be used. When using the twisted pair type of cable, keep in mind that CKM (clock) and DTM (data) signals must not be sent through one pair of twisted wires.

ETHM-1	INTEGRA	VERSA
+12V	+KPD	KPD
COM	COM	COM
DTM	DTM	DTA
CKM	CKM	CLK

Table 1.

4. Connect the enclosure tamper switch to the TMP and COM terminals (or connect the TMP terminal to the COM terminal).
5. Connect the module to the Ethernet network. Use a cable compatible with the 100Base-TX standard (identical to that used when connecting computer to the network).
6. If the control panel is to be configured via the Ethernet (TCP/IP) network using the DLOADX program, connect the module RS-232 port to the control panel RS-232 port. Depending on the control panel, the connection must be made with one of the following cables (these cables are available from SATEL):

   INTEGRA with PIN5 type socket: **PIN5/PIN5** (see Fig. 2)

   INTEGRA / INTEGRA Plus with RJ type socket: **RJ/PIN5** (see Fig. 3)

   VERSA: **PIN5/RJ-TTL**

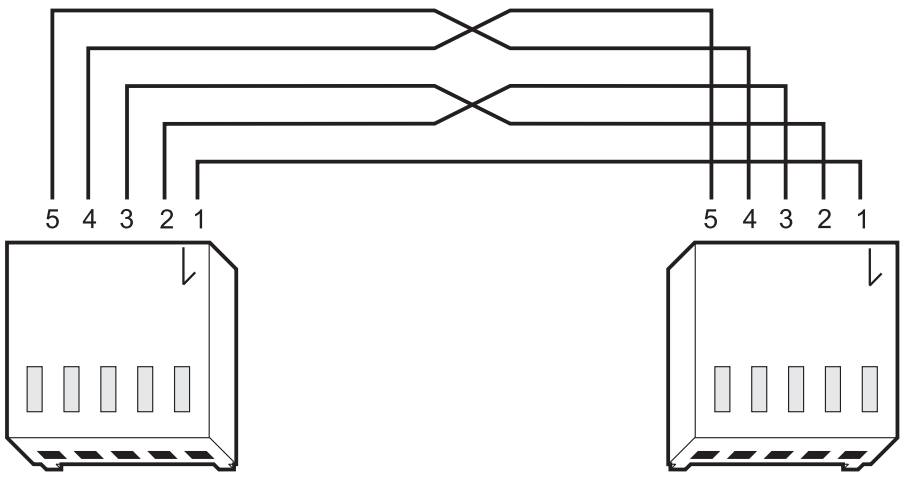

Fig. 2. Schematic of the cable used to connect the RS-232 ports of ETHM-1 module and INTEGRA control panel with PIN5 socket.

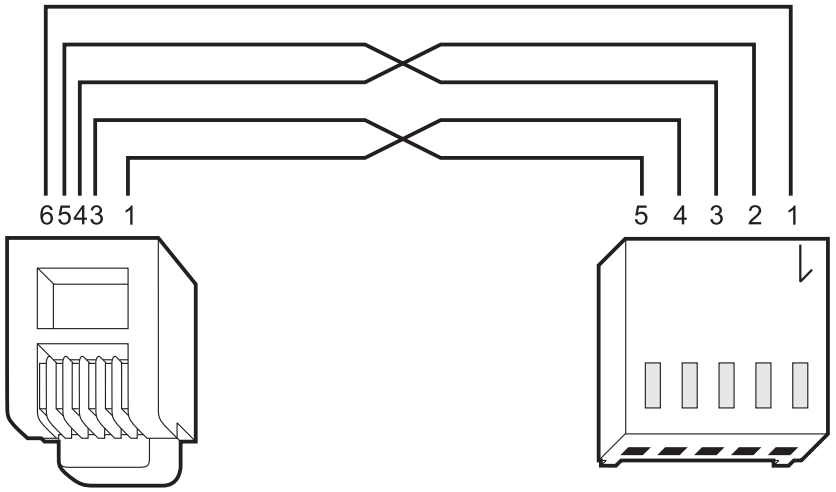

Fig. 3. Schematic of the cable used to connect the RS-232 ports of ETHM-1 module and INTEGRA / INTEGRA Plus control panel with RJ type socket.

7. Power-up the alarm system.
8. Start the device identification function in the control panel (see the installer manual for the respective control panel).

4.1 Setting the address

The address is set by means of jumpers placed across the ADR pins. Table 2 shows how to place the jumpers to set a specific address (- jumper on; - jumper off).

Address	0	1	2	3	4	5	6	7
Pins status								

Table 2.

4.1.1 Interfacing with INTEGRA / INTEGRA Plus control panel

Set the address in the 0 to 3 range (for INTEGRA 24 / INTEGRA 32) or in the 0 to 7 range (INTEGRA 64 / INTEGRA 128 / INTEGRA 64 Plus / INTEGRA 128 Plus). 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).

4.1.2 Interfacing with VERSA control panel

Address 4 must be set in the module. No keypad with the address 4 may be connected to the control panel.

5 Programming

Programming is done by means of the control panel, using the keypad or the computer running the DLOADX program.

5.1 Module settings

The module settings can be configured as follows:

- module connected to the INTEGRA / INTEGRA Plus control panel:
  - keypad: ▶SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶LCD KEYPADS ▶SETTINGS ▶[select a module from the list of devices];
  - DLOADX program: →"Structure" window →"Hardware" tab →"Keypads" item →[click on the module in the list of devices] (see Fig. 4).
- module connected to the VERSA control panel:
  - keypad: ▶SERVICE MODE ▶2. HARDWARE ▶1. KPDS. & EXPS. ▶2. SETTINGS ▶[select a module from the list of devices];
  - DLOADX program: →"Versa – Structure" window →"Hardware" tab →[click on the module in the list of devices] (see Fig. 5).

5.1.1 Parameters and options

The names of parameters and options which are available only when the module is connected to the INTEGRA or INTEGRA Plus control panel are highlighted by white text on a black background.

Shown in the square brackets are the names of parameters and options presented on the display of the INTEGRA / INTEGRA Plus alarm system keypad.

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

Tamper signaled in partition – the partition in which the 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 with the user function available in the TESTS submenu:

INTEGRA / INTEGRA Plus: ***IP/MAC ETHM-1****;*

VERSA: ***EXPANDER VER.*** *(for a detailed description of the function please refer to the user manual for the control panel).*

If the module is connected to the INTEGRA / INTEGRA Plus control panel, the IP address can be read in the DLOADX program (it is shown below the module settings – see Fig. 4).

The module must have a permanent public address if it is to be possible to establish communication with the control panel from outside the local network.

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.

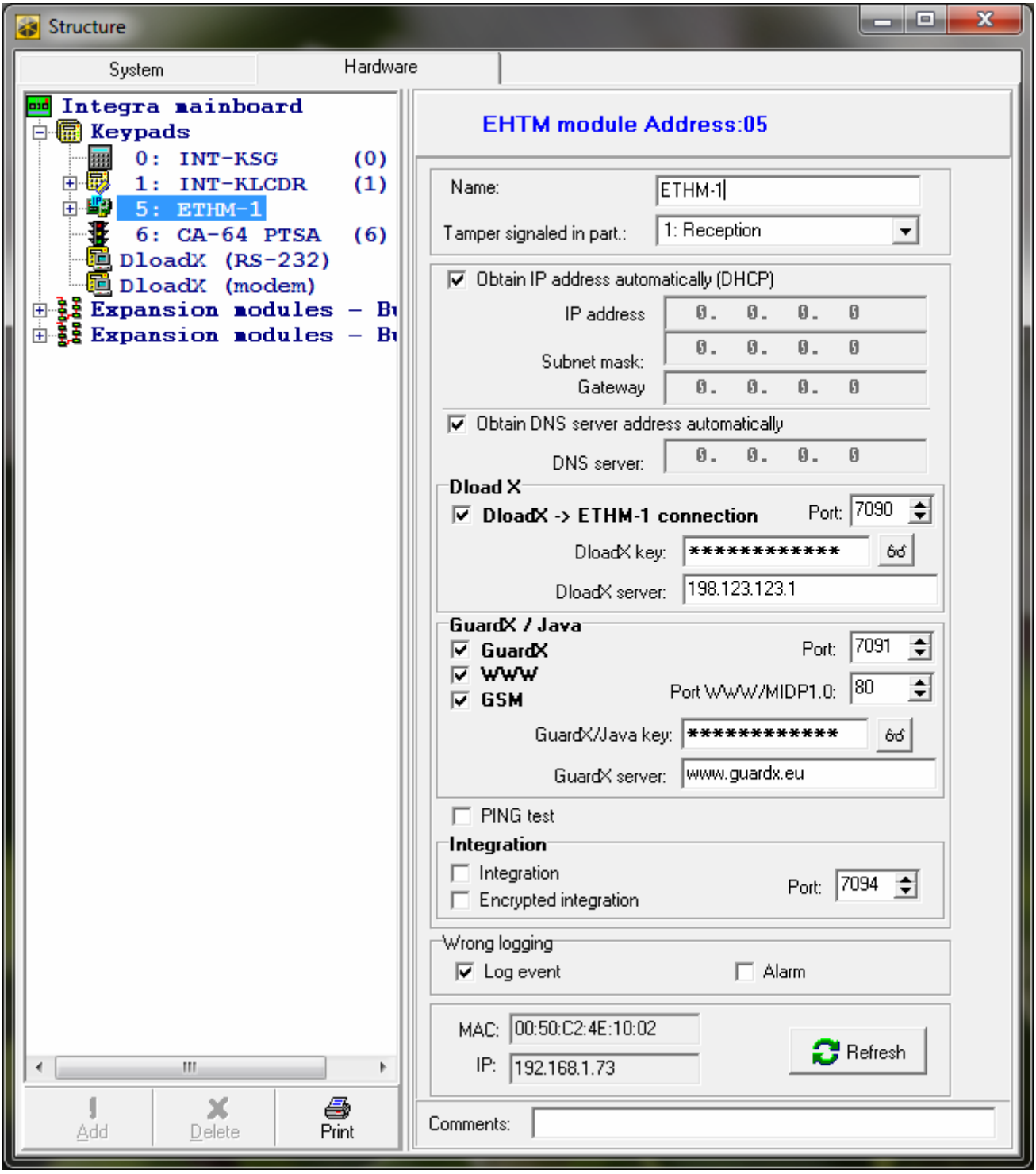

Fig. 4. DLOADX program: settings of the ETHM-1 module connected to INTEGRA control panel.

DloadX

DloadX->ETHM connection [Connect DloadX] – if this option is enabled, connection with the control panel can be initiated via the TCP/IP network from the DLOADX program.

Port [Port (DloadX)] – number of the TCP port used for communication with the DLOADX program. Values from 1 to 65535 can be entered. The value must be different from that entered for the other ports. By default: 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. It must be a public address, unless the computer is included in the same local network. The IP address or the domain name can be entered.

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

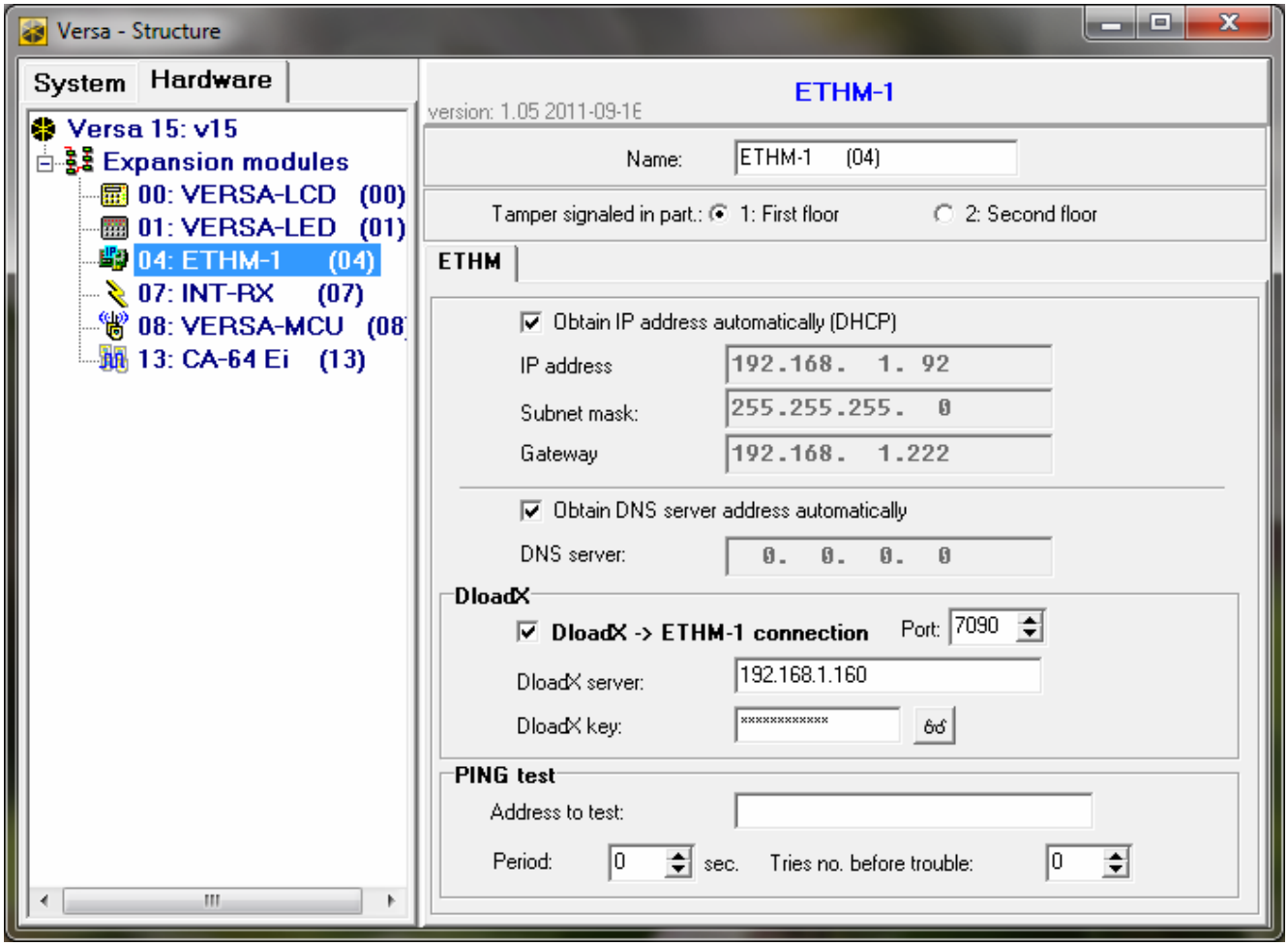

Fig. 5. DLOADX program: settings of the ETHM-1 module connected to VERSA control panel.

GuardX / Java

GuardX [Connect GuardX] – if this option is enabled, connection with the control panel via the TCP/IP network can be initiated from the GUARDX program.

WWW [Connect Intern.] – if this option is enabled, connection with the control panel via the TCP/IP network can be initiated from the web browser.

GSM conn. [Connect GSM] – if this option is enabled, connection with the control panel via the TCP/IP network can be initiated from the MOBILEKPD / MOBILEKPD2 application.

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

- GUARDX program;
- JAVA application in the web browser;
- MOBILEKPD application in the mobile telephone supporting the MIDP2.0 standard;

– MOBILEKPD2 application.

Values from 1 to 65535 can be entered. The value must be different from that entered for the other ports. By default: 7091.

Port WWW/MIDP1.0 [Port (WWW)] – number of the TCP port used for communication with:

– web browser;

– MOBILEKPD application in the mobile phone supporting the MIDP1.0 standard.

Values from 1 to 65535 can be entered. The value must be different from that entered for the other ports. By default: 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 / MOBILEKPD2 application in the mobile phone.

GuardX server [GuardX IP] – address of the computer running the GUARDX program. It must be a public address, unless the computer is included in the same local network. The IP address or the domain name can be entered.

In the keypad, the function for programming the address of computer with GUARDX program is included in the user menu in the CHANGE OPTIONS submenu (available to the 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.

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. Programming the value 0 disables the communication test.

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. Programming the value 0 disables the communication test feature.

If the module is connected to the VERSA control panel, the ping command test will be performed after the address for testing is entered, test interval is determined (the value must be different from 0) and the trouble reporting rules are defined (the value must be different from 0).

If the module is connected to the INTEGRA / INTEGRA Plus control panel, only the PING TEST option is available in the module settings. The other parameters are global (they apply to all the ETHM-1 modules connected to the control panel) and can be programmed:

– *keypad: by means of functions available in the PING TEST submenu (▶SERVICE MODE ▶OPTIONS ▶PING TEST);*

– *DLOADX program: by clicking on the keypad bus (→"Structure" window →"Hardware" tab →"Keypads" item).*

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 can be programmed:

- *keypad: using the INTEGRATE KEY function (▶SERVICE MODE ▶OPTIONS ▶INTEGRATE KEY);*
- *DLOADX program: in the "Service" tab (→"Options" window →"Service" tab).*

Port [Port (integr.)] – number of the TCP port used for integration. Values from 1 to 65535 can be entered. The value must be different from that entered for the other ports. By default: 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.

5.2 Virtual keypad settings

During communication with the control panel through the ETHM-1 module, you can use a virtual keypad to operate and program the alarm system. For the INTEGRA / INTEGRA Plus control panel, settings of the virtual keypad are configurable. Parameters and options of the virtual keypad available in the DLOADX program can be programmed as follows:

- keypad: by using the functions available in the DLOADX RS submenu (▶SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶LCD KEYPADS ▶SETTINGS ▶DLOADX RS);
- DLOADX program: by clicking on the "DloadX (RS-232)" item (→"Structure" window →"Hardware" tab →"Keypads" item →"DloadX (RS-232)" item).

Settings of the virtual keypad available in the GUARDX program, web browser or mobile phone are programmable:

- keypad: by using the functions available in the GUARDX ADDR. submenu (▶SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶LCD KEYPADS ▶SETTINGS ▶GUARDX ADDR. N (n = module address)];
- DLOADX program: by clicking on the "GuardX/MobileKPD" item (→"Structure" window →"Hardware" tab → "Keypads" item →"GuardX/MobileKPD" item – see Fig. 6).

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

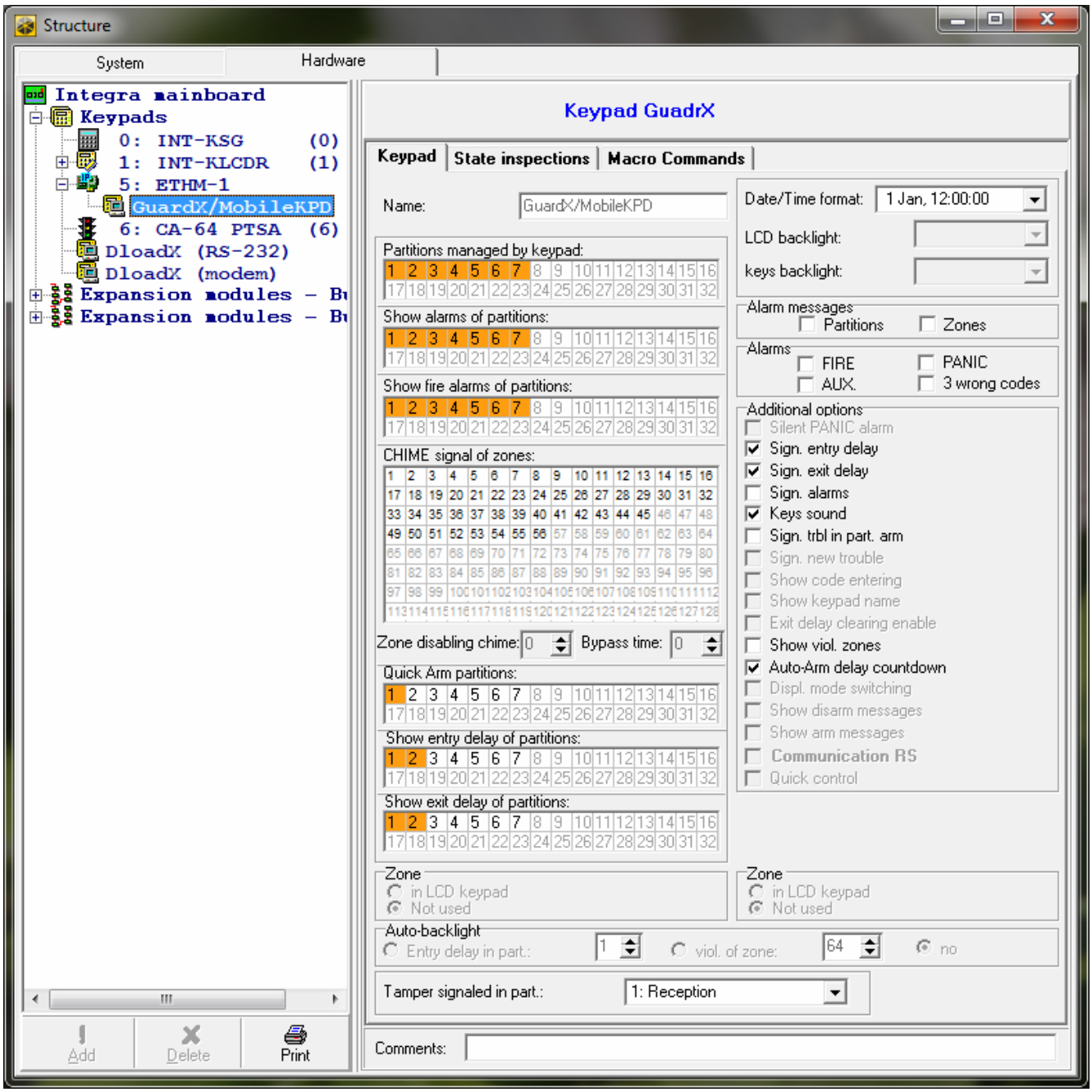

Fig. 6. DLOADX program: settings of the virtual keypad available in the GUARDX program, web browser or mobile phone.

5.3 Macro commands

The MOBILEKPD2 PRO application allows control of the INTEGRA / INTEGRA Plus alarm system by means of macro commands, thus enabling a number of different functions to be executed quickly and easily by touching just a few keys. The macro commands can be defined in the DLOADX program (→"Structure" window →"Hardware" tab →keypad bus →"GuardX/MobileKPD" item →"Macro commands" tab), and then saved to the mobile phone memory.

The MOBILEKPD2 PRO application can be used to run the same macro commands which have been defined for the INT-KSG keypad. In such a case, you do not have to program any separate macro commands.

5.3.1 Parameters and options

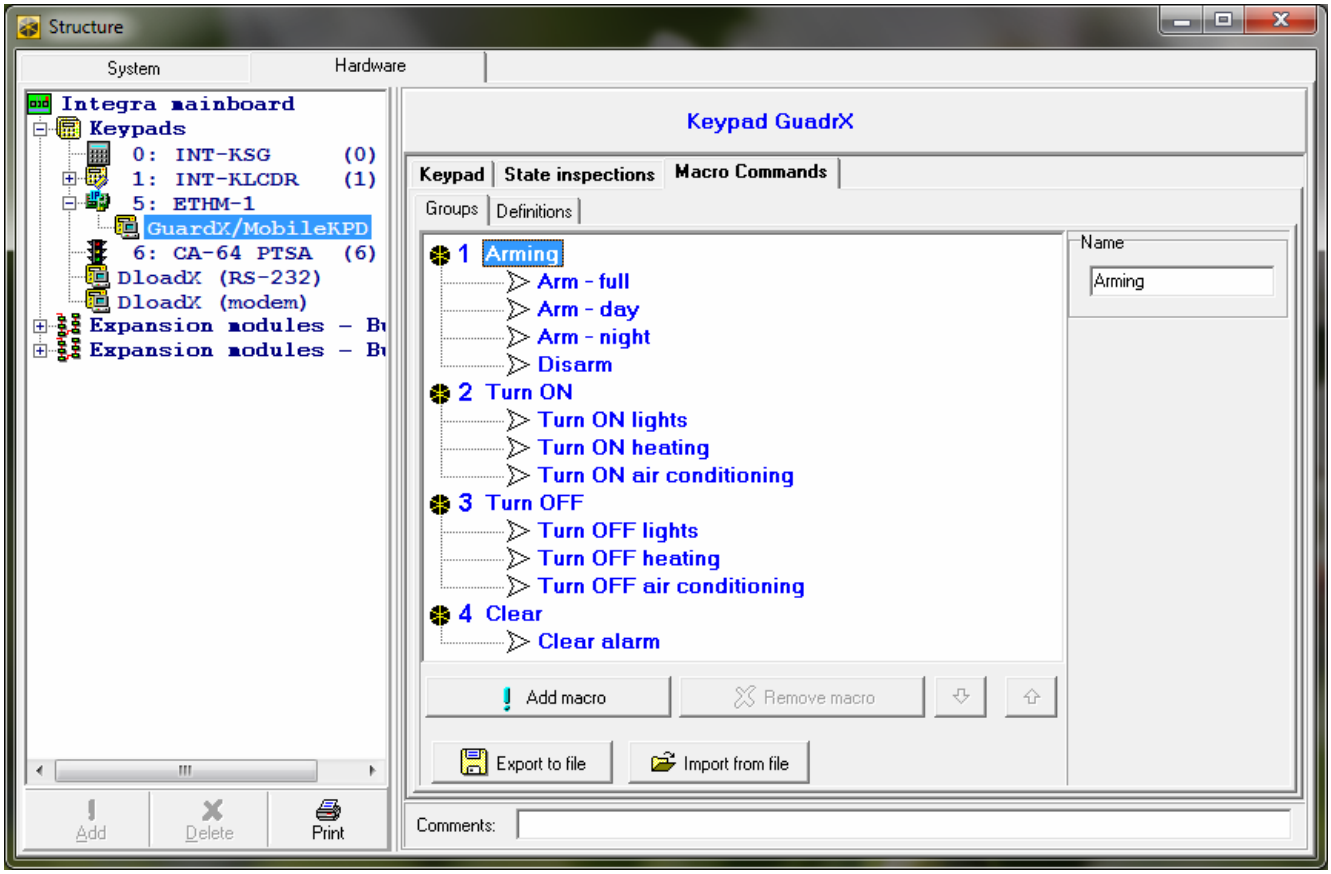

Fig. 7. DLOADX program: macro command groups programmed for the MOBILEKPD2 PRO application.

Macro command group – the list of macro commands which will be displayed on touching the macro key. You can define 4 macro command groups.

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

Macro command – a sequence of actions, composed of single commands, to be executed by the control panel on running the macro command.

Macro command name – an individual name of macro command (up to 32 characters).

Code – a code which is to be used for authorization when executing the commands contained in macro command. For execution of these commands to be possible, an adequate authority level has to be assigned to the code.

If, when running a macro command, it will turn out that the code is invalid (e.g. it has been changed in the meantime), the user will be able to enter the correct one. It will be automatically saved to the phone memory (and replace the invalid code).

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

Disabled if armed – if this option is enabled, the macro command will not be available, when any of the partitions operated by the keypad is armed.

Autoexecute – if this option is enabled and there is just one macro command in the group, touching the macro key will not display the list of macro commands, but will run the macro

command at once (if the AUTHORIZATION REQUIRED option is enabled, authorization by means of a code will be necessary).

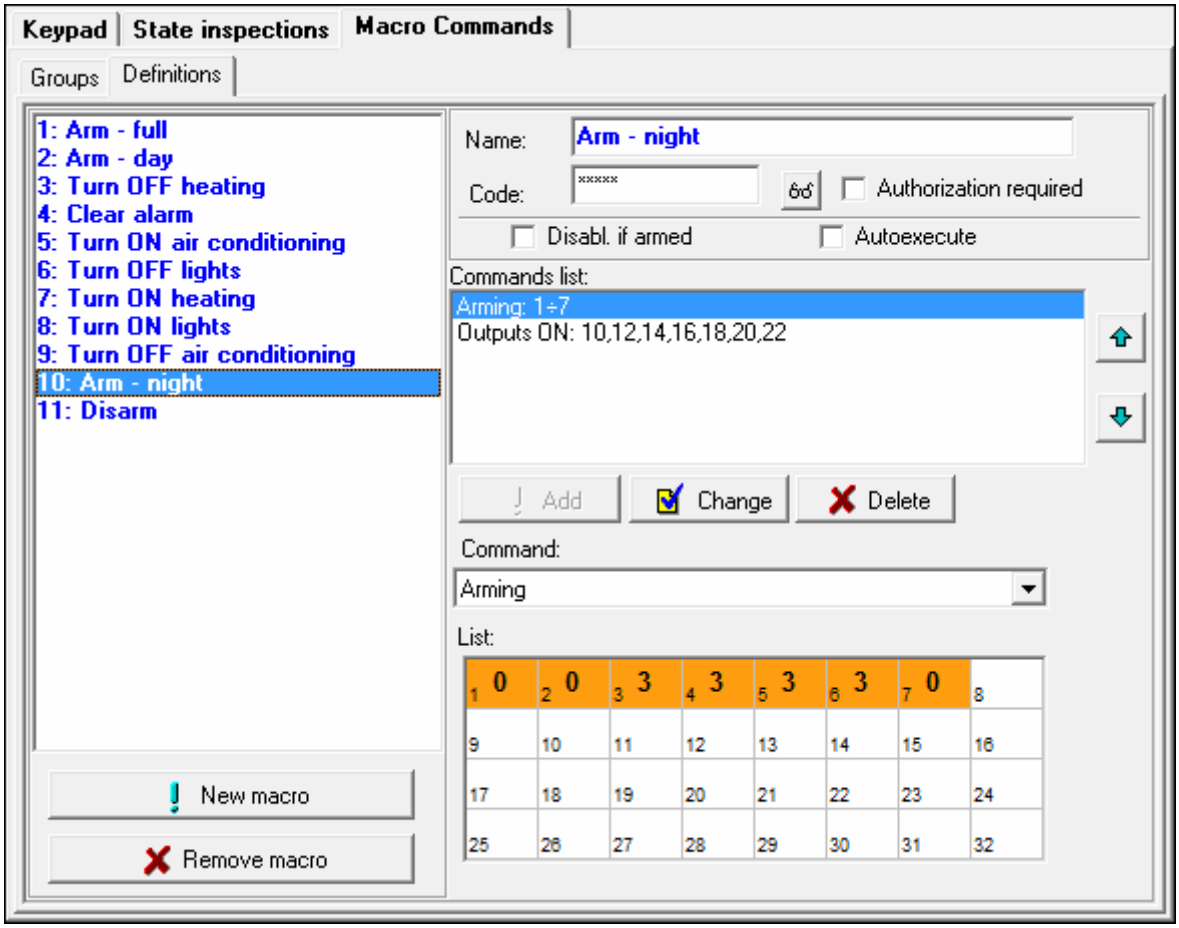

Fig. 8. DLOADX program: macro commands programmed for MOBILEKPD2 PRO application.

Command – control panel executed function which can be assigned to a macro command. It can be:

- arming selected partitions in a specified mode;
- disarming selected partitions;
- clearing alarm in selected partitions;
- inhibiting selected zones;
- unbypassing selected zones;
- activating selected outputs;
- deactivating selected outputs;
- changing status of selected outputs;
- sending KNX telegram;
- sending key sequences.

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 MOBILEKPD2 PRO application you can control the KNX system, provided that the INT-KNX module is connected to the control panel.

5.3.2 Defining the macro commands

1. Click on the "Definition" tab.
2. Click on the "New macro" button. A new macro command will appear in the list.
3. Enter a name for the new macro command.
4. If the macro command is to be run without entering the code by the user, enter the code with a suitable authority level.
5. If running the macro command is to be each time preceded by user authorization, enable the AUTHORIZATION REQUIRED option.
6. If the macro command is not to be available, when any of the partitions operated by the keypad is armed, enable the DISABLED IF ARMED option.
7. If the macro command is to be run instantly on touching the macro key, enable the AUTOEXECUTE option (in such a case, only this one macro command is to be assigned to the group).
8. Select from the list one of the commands to be executed by the new macro command.
9. Select the partitions (arming / disarming, alarm clearing), zones (inhibiting / unbypassing) or outputs (activating / deactivating) controlled by the command. Click twice to select/deselect the required field.
10. Click on the "Add" button. A new command will appear in the list of commands assigned to the macro command. After clicking on the command you can still make a correction to the list of partitions / zones / outputs controlled by the command. After making the changes, click on the "Change" button.
11. If necessary, repeat the steps 8-10 to add next commands.
12. Click on the "Groups" tab.
13. Click on the group to be edited.
14. Enter the group name.
15. Click on the "Add macro" button. Select in the pop-up menu the macro command which is to be added.

5.3.3 Preparing the macro command file for MOBILEKPD2 PRO application

If the MOBILEKPD2 PRO application is to run the same macro commands which have been defined for the INT-KSG ma keypad, the steps described below can be done 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 name of file, and then click on the "Save" button. If the file is to be saved in another location than the default one, indicate the suitable folder before you click on the "Save" button.
4. A window will open, where you should enter the file encryption code (up to 24 alphanumeric characters), and then click on the "OK" button. The file encryption code will be required when loading the macro commands by the MOBILEKPD2 PRO application.
5. A window will open with information that the file has been saved.

6 Remote Programming and Operation of the Control Panel via Ethernet Network

After three consecutive attempts to establish communication with the module using an incorrect key, the module will not respond for about 20 minutes to any attempts to establish communication from the given IP address.

For information regarding configuration of the control panel by means of the DLOADX program via the Ethernet (TCP/IP) network, please refer to the control panel programming manuals.

6.1 GuardX program

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

1. Initiating connection from the GUARDX program. This method enables establishing a connection with the control panel from any location.
2. Initiating connection from the keypad (by the control panel). The alarm system can be managed remotely from the specified location only, with the control panel user's knowledge.

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

6.1.1 Configuring the ETHM-1 module

In the ETHM-1 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;
- program the address of the computer running the GUARDX program (GUARDX SERVER), if the connection is to be initiated from the keypad (by the control panel);
- program the number of TCP port which will be used for communication with the GUARDX program, if it is to be different than 7091.

6.1.2 Configuring the GUARDX program

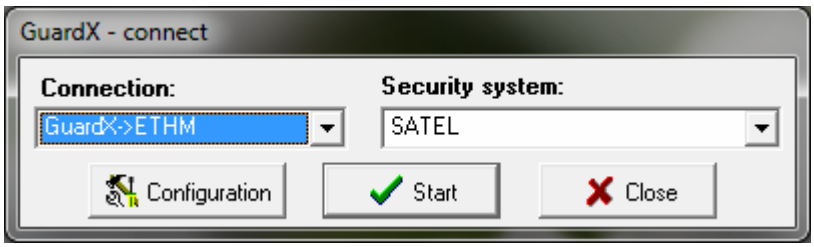

Fig. 9. GUARDX program: startup window.

In the GUARDX program startup window (see Fig. 9), click on the "Configuration" button. A window will open, in which, in the "TCP/IP" tab (see Fig. 10), you can program the following:

- TCP port number (identical to that programmed in the module for communication with the GUARDX program, except for the situation when communication is effected through a network device at which redirection to another port takes place);

- key for data encryption (identical to that programmed in the module for communication with the GUARDX program);
- address of the ETHM-1 module, if communication is to be initiated from the GUARDX program.

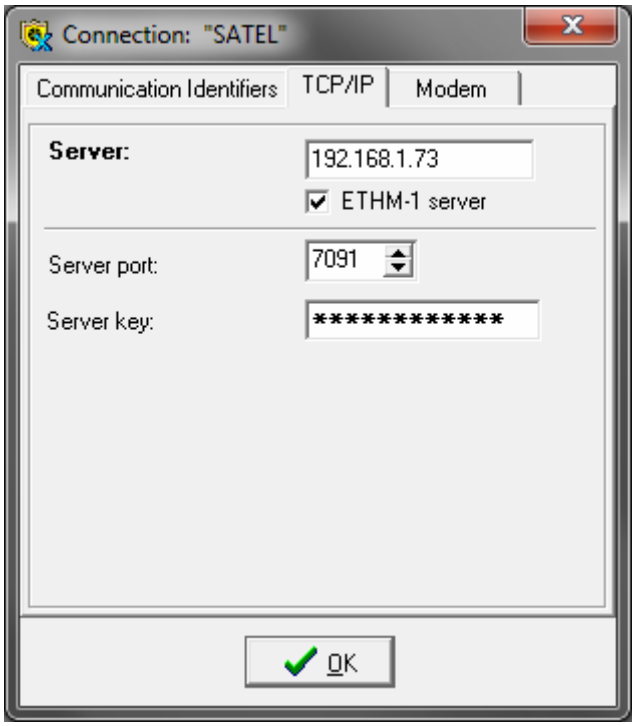

Fig. 10. GUARDX program: settings for communication via Ethernet (TCP/IP) network.

6.1.3 Initiating connection from the GUARDX program

1. In the startup window, "Connection" field, select "GuardX -> ETHM" (see Fig. 9), and then click on the "Start" button.
2. After establishing connection, a window will open, where you must enter the code of control panel administrator / user.

6.1.4 Initiating connection from the keypad (by the control panel)

1. In the startup window, "Connection" field, select "GuardX <- ETHM", and then click on the "Start" button.
2. In the keypad, start 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. After establishing connection, a window will open, where you must enter the access code of control panel administrator / user.

6.2 Web browser

6.2.1 Configuring the ETHM-1 module

In the module ETHM-1:

- enable the WWW option;
- program the key for data encryption during communication with the JAVA application in web browser (GUARDX/JAVA KEY);

- program the number of TCP port which will be used for communication with the web browser, if it is to be different than 80 (PORT WWW/MIDP1.0);
- program 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 than 7091.

6.2.2 Configuring the computer

Java Virtual Machine must be installed on the computer.

6.2.3 Establishing communication

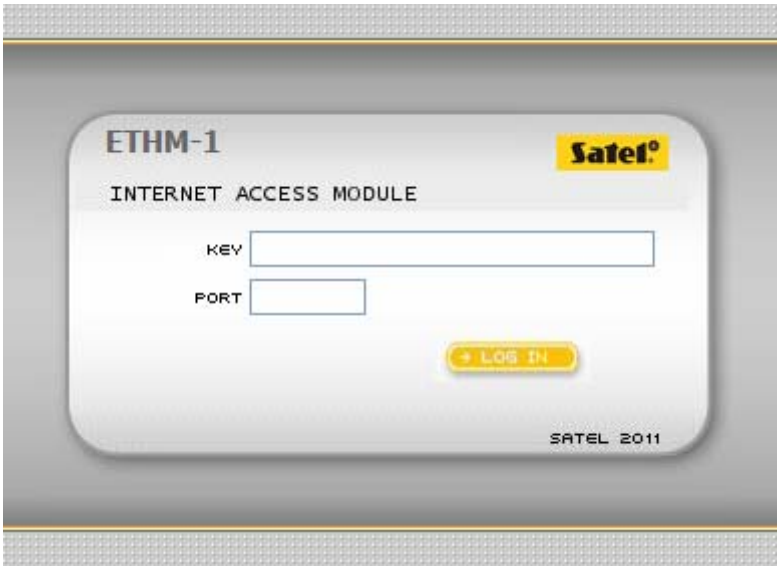

Fig. 11. Login screen displayed in the web browser.

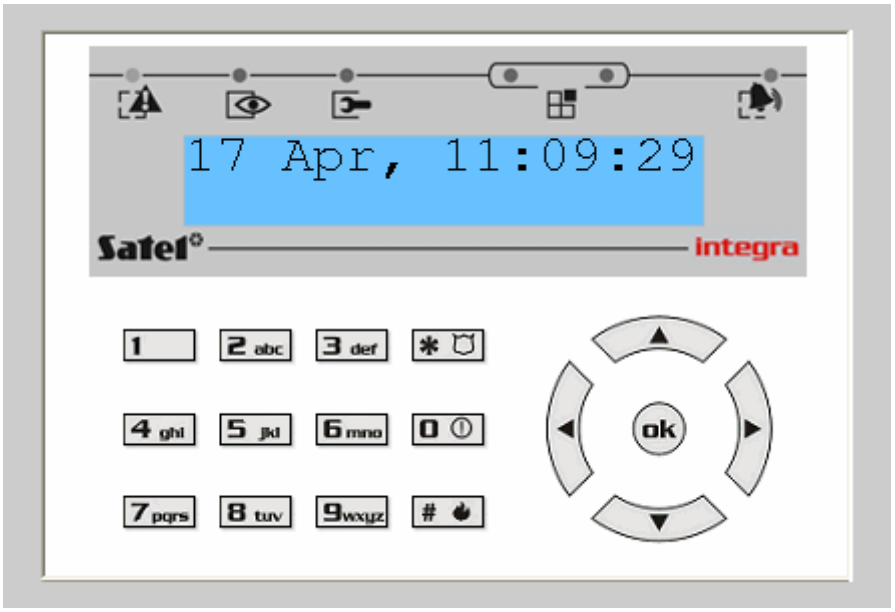

Fig. 12. Virtual keypad available in the web browser.

1. Start the web browser.
2. In the address field, enter the ETHM-1 module IP address, and then press ENTER.

If a port different than 80 has been programmed in the module settings for communication with the web browser, indicate the port number after entering the address followed by a colon.

3. When the login screen is displayed, enter in the appropriate fields:
   - the key for data encryption (identical to that programmed in the module for communication with the JAVA application in the web browser);
   - the TCP port number (identical to that programmed in the module for communication with the JAVA application in the web browser, except for the situation when communication is effected through a network device at which redirection to another port takes place).
4. Click on the "Log in" button.
5. A virtual keypad will be displayed in the browser, which will allow you to operate and program the alarm system.

6.3 Mobile phone

6.3.1 Configuring the ETHM-1 module

In the ETHM-1 module:

- enable the GSM option;
- program the key for data encryption during communication with the MOBILEKPD / MOBILEKPD2 application in the mobile phone (GUARDX/JAVA KEY);
- program the number of TCP port which will be used for communication with the MOBILEKPD / MOBILEKPD2 application in the mobile phone, if it is to be different than that in the factory settings.

6.3.2 Configuring the mobile phone

Install the MOBILEKPD / MOBILEKPD2 application in your cell phone. The application is available for downloading at the www.satel.eu site (select the application suitable for your mobile phone), from the "Google play" internet store (Android system devices) or from the "App Store" (iOS system devices).

Having installed the application, enter the:

- name of the alarm system;
- address of the ETHM-1 module;
- TCP port number (identical to that programmed in the module for communication with the MOBILEKPD / MOBILEKPD2 application, except for the situation when communication is effected through a network device at which redirection to another port takes place);
- key for data encryption (identical to that programmed in the module for communication with the MOBILEKPD / MOBILEKPD2 application).

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

Loading the macro command file – MOBILE KPD2 PRO

For the MOBILEKPD2 PRO application, you can load the macro commands when configuring parameters required to establish communication with the alarm system. The macro command file must be preliminarily saved to the phone memory. Having indicated the file which contains macro commands, you must enter the file encryption code.

6.3.3 Establishing communication – MOBILEKPD

1. Using the phone keys, select the alarm system from the list.
2. Select: →"Options" →"Start".
3. Virtual keypad elements will appear on the display. Using the cell phone, you can program and operate the alarm system.

6.3.4 Establishing communication – MOBILEKPD2

Touch the name of alarm system. The virtual keypad will be displayed, which can be used for operating and programming the alarm system.

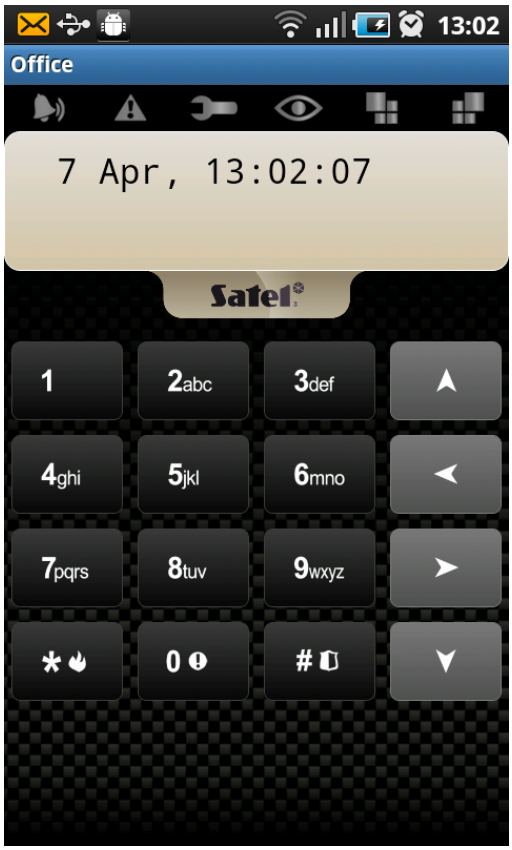

Fig. 13. Virtual keypad available in the MOBILEKPD2 application (phone with Android operating system).

If parameters of only one alarm system are programmed, the screen with the list of systems will not appear after the application is started next time – the virtual keypad will be displayed at once.

7 Specifications

Supply voltage ..... 12 V DC ±15%
Standby current consumption ..... 120 mA
Maximum current consumption ..... 120 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