

Ethernet communication module

ETHM-1 Plus

Firmware version 3.11

EN

CE

ethm1_plus_en 11/24

Satel® 

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

IMPORTANT

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).

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.

Please visit us at:
<https://support.satel.pl>

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

Signs in this manual



Caution – information on the safety of users, devices, etc.



Note – suggestion or additional information.

CONTENTS

1	General.....	2
2	Features	2
3	Electronics board.....	3
4	Address setting.....	4
4.1	Module connected to INTEGRA / INTEGRA Plus control panel	4
4.2	Module connected to PERFECTA 64 M control panel	4
4.3	Module connected to VERSA control panel.....	4
5	Installation	5
6	Programming the settings.....	6
6.1	Module connected to INTEGRA / INTEGRA Plus control panel	7
6.1.1	Programming in the DLOADX program.....	7
6.1.2	Programming from the keypad.....	7
6.1.3	Module settings.....	7
	ETHM-1.....	7
	INT-GSM functions.....	12
	IP filter.....	12
	Remote firmware update.....	14
	IP zone.....	15
	User functions	17
	Virtual keypad	17
	Macro commands.....	18
6.2	Module connected to PERFECTA 64 M control panel.....	28
6.2.1	Programming in the PERFECTA Soft program	28
6.2.2	Programming from the keypad.....	28
6.2.3	Module settings.....	28
6.3	Module connected to VERSA control panel.....	29
6.3.1	Programming in the DLOADX program.....	29
6.3.2	Programming from the keypad.....	29
6.3.3	Module settings.....	30
	LAN.....	32
	Messaging.....	32
7	Programming and operating the alarm system via Ethernet.....	34
7.1	INTEGRA Plus / INTEGRA system.....	34
7.1.1	GUARDX program	34
	Programming the GUARDX program settings.....	35
	Initiating connection from GUARDX program.....	36
	Initiating connection from keypad (through control panel).....	37
	Initiating connection by SMS message	37
	Establishing connection via the SATEL server.....	37
7.1.2	Web browser.....	38
7.1.3	INTEGRA CONTROL application.....	39
	Programming the settings in INTEGRA CONTROL application (Android)	39
	Programming the settings in INTEGRA CONTROL application (iOS).....	41
	Establishing the communication.....	43
7.2	PERFECTA 64 M system	43
7.3	VERSA system	43
8	Specifications	44

1 General

The ETHM-1 Plus module enables the INTEGRA Plus, INTEGRA, PERFECTA 64 M 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.



If the ETHM-1 Plus module is connected to the INTEGRA Plus / INTEGRA control panel, you can connect the INT-GSM / INT-GSM LTE module to the module. This will allow the cellular data network to be used as a backup communication path and enable dual path reporting.

If the ETHM-1 Plus module is connected to the PERFECTA 64 M control panel, Ethernet is the primary communication path and the cellular data network is used as a backup communication path.

2 Features

- Programming of the alarm system from a computer with internet access:
INTEGRA Plus / INTEGRA: firmware version 1.03 or newer – DLOADX program,
PERFECTA 64 M: firmware version 2.03 or newer – PERFECTA Soft program,
VERSA: firmware version 1.01 or newer – DLOADX program.
- Administration of the alarm system from a computer with internet access:
INTEGRA Plus / INTEGRA: firmware version 1.03 or newer – GUARDX program.
- Operation and programming of the alarm system from a web browser supporting JAVA applications:
INTEGRA Plus / INTEGRA: firmware version 1.03 or newer.
- Operation of the alarm system from a mobile device:
INTEGRA Plus / INTEGRA: firmware version 1.03 or newer – INTEGRA CONTROL app,
PERFECTA 64 M: firmware version 2.03 or newer – PERFECTA CONTROL app,
VERSA: firmware version 1.04 or newer – VERSA CONTROL app.
- Reporting events to the monitoring stations via Ethernet:
INTEGRA Plus / INTEGRA: firmware version 1.04 or newer,
PERFECTA 64 M: firmware version 2.02 or newer,
VERSA: firmware version 1.01 or newer.
- Event notification using e-mail messages:
INTEGRA Plus: firmware version 1.13 or newer – content of the message corresponds to the description in the control panel event log,
VERSA: firmware version 1.04 or newer – content of the message is generated automatically by the control panel.
- Receiving notifications sent by IP cameras (IP zones):
INTEGRA Plus / INTEGRA: firmware version 1.22 or newer.
- Administration of the alarm system from the INTEGRUM application:
INTEGRA Plus / INTEGRA: firmware version 1.13 or newer.

- Integration of the alarm system with other systems, due to the open protocol for communication over Ethernet:

INTEGRA Plus / INTEGRA: firmware version 1.06 or newer.



This function is designed for businesses specializing in the integration of object-oriented systems and requires development of own software. For more information on the open communication protocol, please go to www.satel.pl.

- Capability to connect the INT-GSM / INT-GSM LTE module (cellular data network as a backup communication path):
INTEGRA Plus / INTEGRA: firmware version 1.19 or newer.
- Module firmware updated locally from a computer connected to the module's RS-232 port.
- Module firmware updated remotely via Ethernet using the UpServ update server [only INTEGRA Plus / INTEGRA].
- Powered with 12 V DC.

3 Electronics board

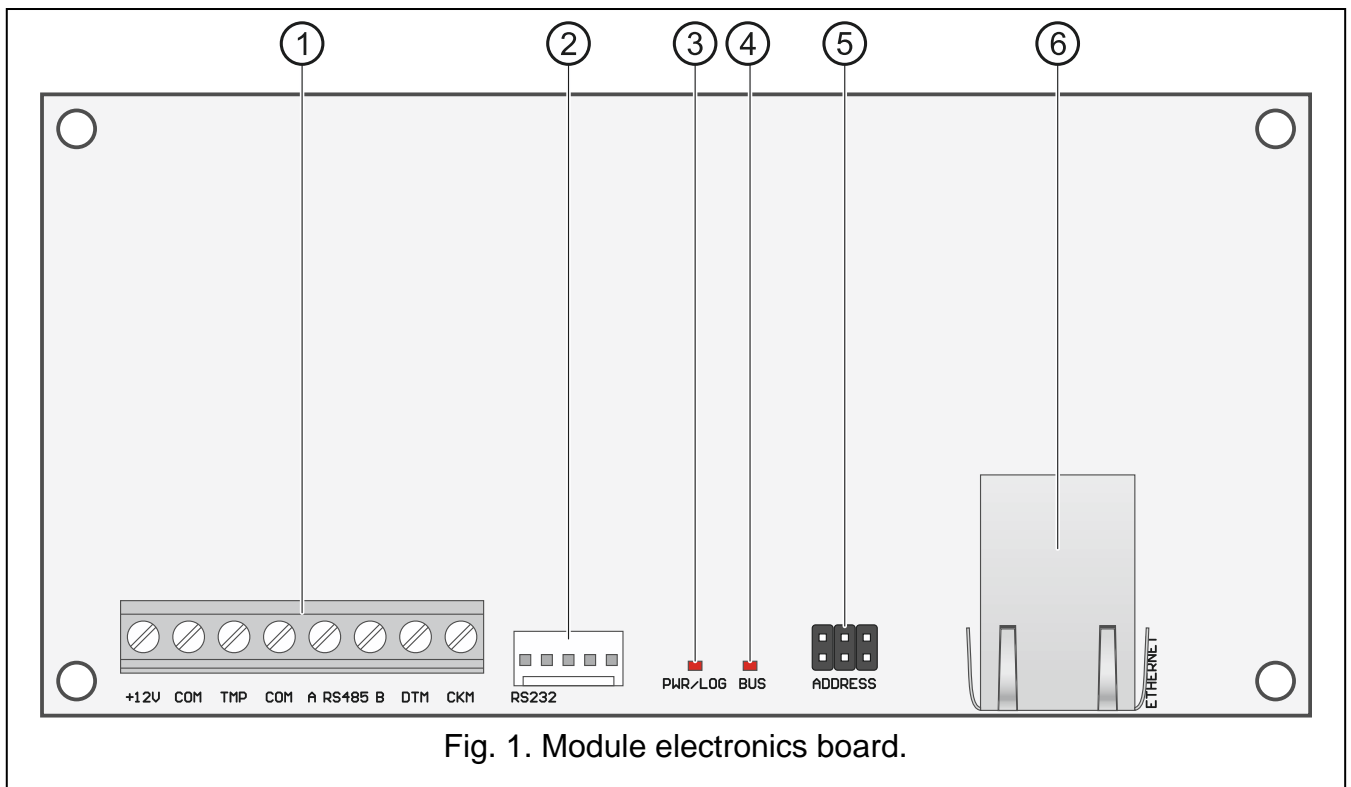


Fig. 1. Module electronics board.

① terminals:

+12V - +12 VDC power input.

COM - common ground.

TMP - tamper input (NC) – if not used, it should be shorted to common ground.

A RS485 B - RS-485 port for connecting INT-GSM / INT-GSM LTE module if the ETHM-1 Plus module is connected to the INTEGRA Plus / INTEGRA (required control panel firmware version: 1.19 or newer).

DTM - data (communication bus).

CKM - clock (communication bus).

② RS-232 port. It enables:

- connecting a computer for the purpose of updating the module firmware.
- connecting to the control panel RS-232 port. Depending on the alarm system in which the module is installed:

INTEGRA Plus / INTEGRA: required for programming the system in the DLOADX program via Ethernet; recommended for system administration in the GUARDX program via Ethernet.

PERFECTA 64 M: required for programming the system in the PERFECTA Soft program via Ethernet or operating the system in the PERFECTA CONTROL app via Ethernet.

VERSA: required for programming the system in the DLOADX program via Ethernet.

③ PWR/LOG LED:

OK – power OK,
flashing – communication via the module in progress.

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

⑤ pins for setting the module address (see “Address setting”).

⑥ RJ-45 connector for Ethernet network. It is provided with two LEDs: green – ON when the module is connected to the network, yellow – flashes during data transmission.

4 Address setting

To set an address, place jumpers across the ADDRESS pins. Table 1 shows how to place the 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 PERFECTA 64 M control panel

Set address 6 in the module.

4.3 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

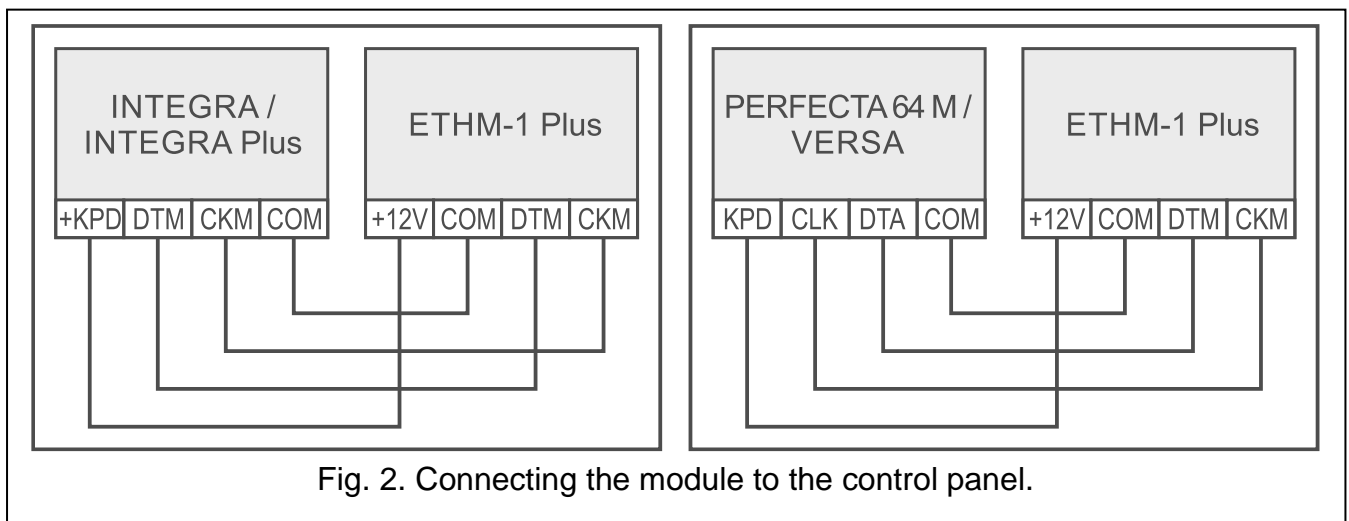


Disconnect power before making any electrical connections.

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, if it is required.
2. Set the module address (see “Address setting”).
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.
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).



If the module is connected to the INTEGRA Plus / INTEGRA control panel and the INT-GSM / INT-GSM LTE module is connected to the RS-485 port, the module will be identified as “ETHM+GSM”.

8. Configure the module (see “Programming the settings”).
9. If it is required, connect the module RS-232 port to the control panel RS-232 port. Depending on the control panel, use the following:
 INTEGRA with connector socket of PIN5 type: **PIN5/PIN5** cable (Fig. 3)
 INTEGRA with connector socket of RJ / INTEGRA Plus type: **RJ/PIN5** cable (Fig. 4)
 PERFECTA 64 M / VERSA: **RS232-RSTTL** converter

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



Connecting the RS-232 ports of the module and control panel is required if the alarm system is to be programmed via Ethernet.

In the INTEGRA Plus / INTEGRA system, connecting the RS-232 ports of the module and control panel is recommended if the alarm system is to be administered in the GUARDX program via Ethernet. This will speed up the communication.

In the PERFECTA 64 M system, connecting the RS-232 ports of the module and control panel is also required if the system is to be operated in the PERFECTA CONTROL app via Ethernet.

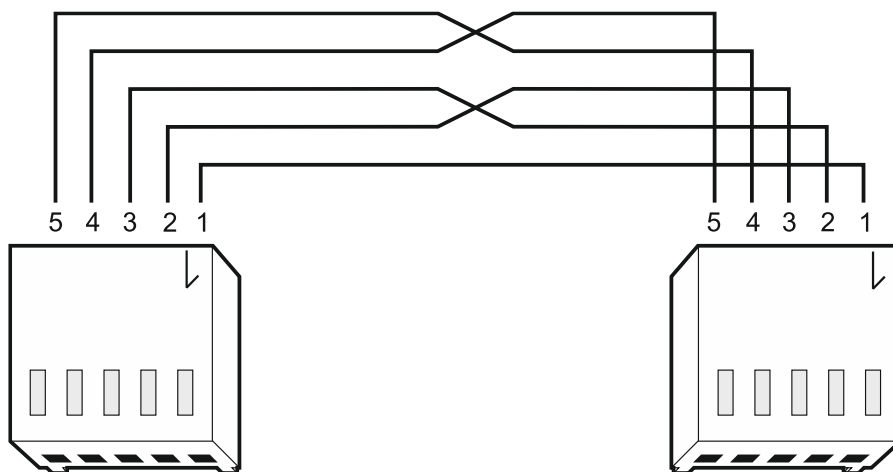


Fig. 3. Wiring diagram of the cable connecting RS-232 ports of ETHM-1 Plus module and INTEGRA control panel with PIN5 connector socket.

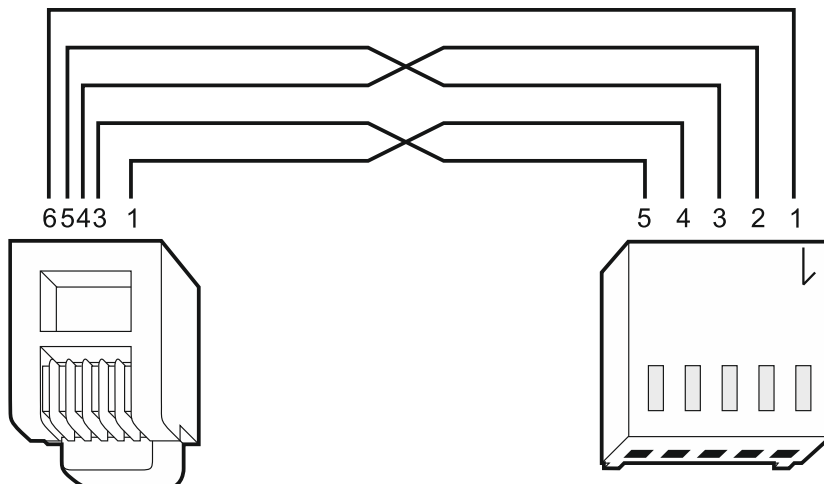


Fig. 4. Wiring diagram of the cable connecting RS-232 ports of ETHM-1 Plus module and INTEGRA / INTEGRA Plus control panel with RJ type connector socket.

6 Programming the settings

The module settings differ, depending on the control panel to which the module is connected.

6.1 Module connected to INTEGRA / INTEGRA Plus control panel

You can configure all of the module settings using a computer with the DLOADX program installed. From the keypad, you can configure only some of the settings.





If the module has been identified as “ETHM+GSM” (the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module), the INT-GSM / INT-GSM LTE module will take over tasks from the ETHM-1 Plus module if the Ethernet connection is lost. These tasks are performed via cellular data network. Therefore many options and parameters apply to both modules. This should be borne in mind when configuring the settings.






6.1.1 Programming in the DLOADX program

Required version of the DLOADX program: 1.22.000 (or newer).



1. Click  in the main menu. The “Structure” window will be displayed.
2. Click the “Hardware” tab.
3. Click the “Keypads” branch.
4. Click the name of the module whose settings you want to configure.
5. Configure the module settings.
6. Click  in the main menu to save changes to the control panel. For settings stored in the module (IP zones, macro commands), click the “Write” button.

6.1.2 Programming from the keypad

1. Enter the **service code** (by default: 12345) and press  . The user menu will be displayed.
2. Press . The service menu will be displayed.
3. Start the **SETTINGS** function (▶STRUCTURE ▶HARDWARE ▶LCD KEYPADS ▶SETTINGS).
4. Find the module whose settings you want to configure (use the up or down arrow key) and press  .
5. Program the module settings using the available functions.

6.1.3 Module settings

Names of parameters and options from the DLOADX program are used in this manual. When a parameter or an option is described, you will find in the square brackets their name displayed on the keypad.

ETHM-1

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.

Network settings

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 **IP/MAC/IMEI/ID** 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 and 6).

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.

The screenshot shows the DLOADX program interface for configuring the ETHM module. The left sidebar shows a tree view of the system hardware, with 'ETHM-1' selected under 'Keypads'. The main window is titled 'ETHM module Address:05' and contains the following settings:

- General:** Name: ETHM-1 (5), Tamper signaled in part: 1: Lobby
- IP Configuration:**
 - Obtain IP address automatically (DHCP)
 - IP address: 0. 0. 0. 0
 - Subnet mask: 0. 0. 0. 0
 - Gateway: 0. 0. 0. 0
 - Obtain DNS server address automatically
 - DNS server: 0. 0. 0. 0
- DLOADX:**
 - Communication with DLOADX
 - DLOADX key: *****
 - DLOADX server: 192.168.8.38
 - Port: 7090
- GUARDX/INTEGRA CONTROL:**
 - GUARDX
 - WWW
 - GSM conn.
 - INTEGRUM (client)
 - GUARDX key: *****
 - WWW port: 80
 - GUARDX server: 192.168.8.38
 - Port: 7091
- Integration:**
 - PING test
 - Connection via Satel server
 - Push notifications
 - Integration
 - Encrypted integration
 - Port: 7094
 - Wrong login
 - Log event
 - Alarm
- MAC/ID:**
 - MAC: 00:1B:9C:08:34:91
 - ID: *****
 - Buttons: QR-code, Refresh
- LAN uplink loss report delay:** 0 sec.
- Comments:** [Empty text field]

Fig. 5. DLOADX program: settings of the module connected to INTEGRA / INTEGRA Plus control panel (module is identified as “ETHM-1”).

INT-GSM options

Options applicable to the INT-GSM / INT-GSM LTE module are available if the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module (the module is identified as “ETHM+GSM”).

SIM 1 / SIM 2 [SIM1 / SIM2] – if this option is enabled, the given SIM card is supported by the INT-GSM / INT-GSM LTE module. Disable the option, if the given card is not to be used. Disabling the option will prevent unnecessary reporting of troubles related to that card.

SMS/CLIP messaging [SMS messaging] – if this option is enabled, the INT-GSM / INT-GSM LTE module can send notifications about alarm system events using SMS/CLIP.

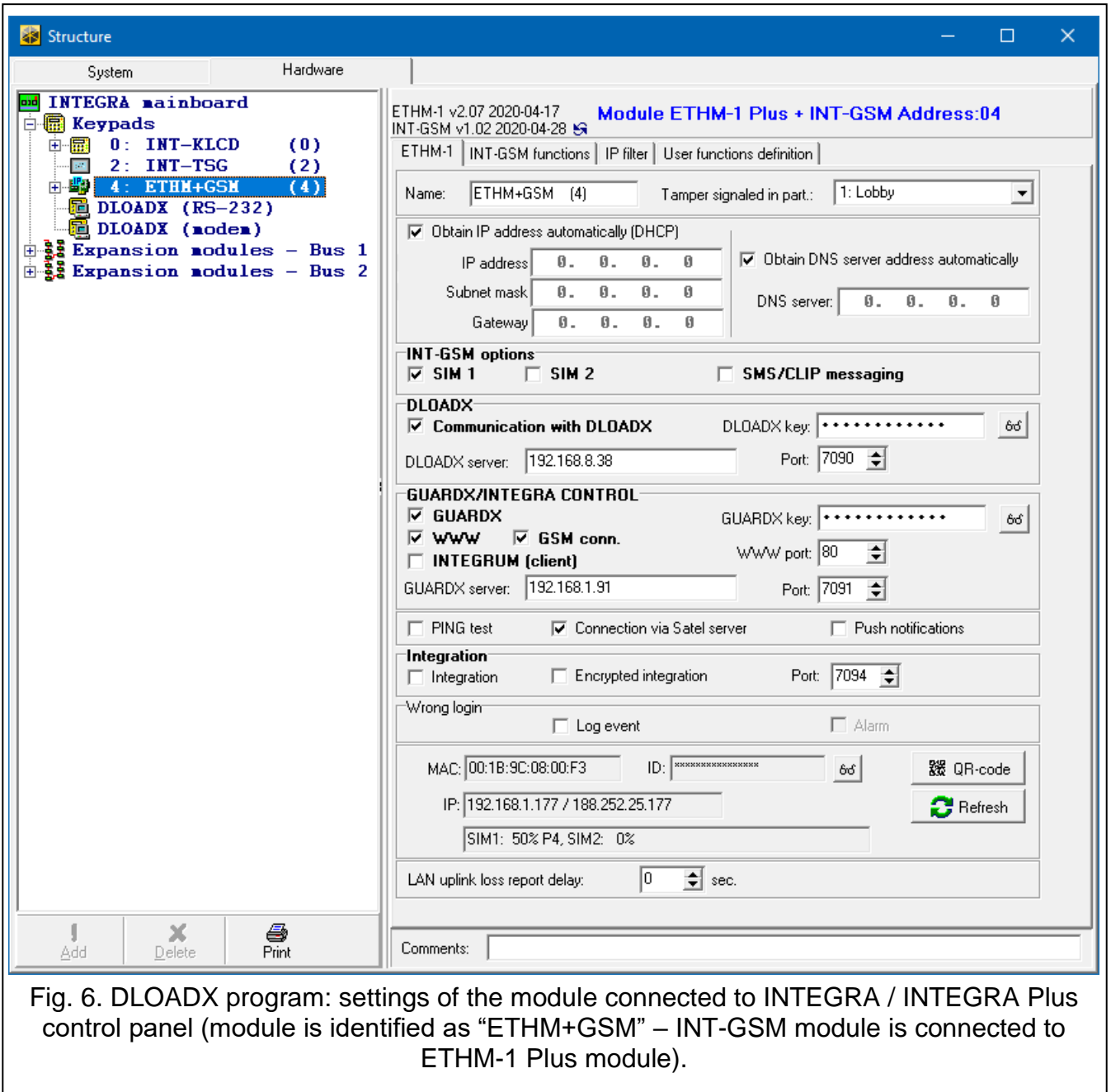


Fig. 6. DLOADX program: settings of the module connected to INTEGRA / INTEGRA Plus control panel (module is identified as “ETHM+GSM” – INT-GSM module is connected to ETHM-1 Plus module).

DLOADX

Communication with DLOADX [Connect DLOADX] – if this option is enabled, connection can be established between the DLOADX program and the alarm control panel via the module.

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

DLOADX server [DLOADX IP] – address of the computer running the DLOADX program. If the communication takes place in a wide area 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).

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.

GUARDX/INTEGRA CONTROL

GUARDX [Connect GUARDX] – if this option is enabled, connection can be established between the GUARDX program and the alarm control panel via the module. The option is not available when the *INTEGRUM (client)* option is enabled.

WWW [Connect Intern.] – if this option is enabled, connection can be established between the web browser and the alarm control panel via the module. The option is not available when the *INTEGRUM (client)* option is enabled.

GSM conn. [Connect GSM] – if this option is enabled, connection can be established between the INTEGRA CONTROL application / INTEGRUM server and the alarm control panel via the module. The option is not available when the *INTEGRUM (client)* option is enabled.

INTEGRUM (client) [INTEGRUM] – if this option is enabled, the module initiates connection to the INTEGRUM server to establish communication between the control panel and the INTEGRUM server. This method of establishing communication is supported by the INTEGRUM server with version 2.0 (or newer). In the *GUARDX server* field enter the INTEGRUM server address, and in the *Port* field enter the communication port number. When the option is enabled, the *GUARDX*, *WWW* and *GSM conn.* options are not available (the module does not support the GUARDX program / web browser / INTEGRA CONTROL app).

GUARDX server [GUARDX IP] – address of the computer running the GUARDX program or INTEGRUM server. If the communication takes place in a wide area 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 / INTEGRUM system server is available in the user menu, CHANGE OPTION submenu (available to service and administrators).

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

- GUARDX program,
- JAVA application in the web browser,
- INTEGRA CONTROL in the mobile device,
- INTEGRUM system.

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.

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

- GUARDX program,
- JAVA application in the web browser,
- INTEGRA CONTROL in the mobile device,
- INTEGRUM system.

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



The port cannot be used by several services at a time. The port can only be used by one service (e.g. when communication with the INTEGRUM server is ongoing, you will not be able to connect to the control panel in the GUARDX program, the web browser or the INTEGRA CONTROL application).

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 the option is enabled, the module connects to the SATEL server and the communication via the SATEL server with the control panel can be established (Connection Setup Service). This way of communication requires no additional configuring of the network device through which the module connects to the public network.



For establishing communication with the SATEL server, the DNS server must be used.

For communication via the SATEL server, the ports of 1024-65535 range are used as outgoing ports. These ports must not be blocked.

Push notifications – if this option is enabled, the INTEGRA CONTROL application can provide information about alarm system events by means of push notifications.

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. Program the encryption key (*Integration encryption key*) in:

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

DLOADX program: →“Structure” window →“Hardware” tab →“Keypads” branch.

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 – individual ID number assigned to the module by the SATEL server.



If the module is to be used in another alarm system, the hitherto used ID number must be deleted. You should do it after connecting the module to the new control panel and establishing connection with the SATEL server, using the CHANGE ID function available from the keypad (►SERVICE MODE ►STRUCTURE ►HARDWARE ►LCD KEYPADS

► *SETTINGS* ► *[module name]* ► *CHANGE ID*), if the control panel is connected to the SATEL server. Having deleted the old ID number, the control panel will receive a new one. The INTEGRA CONTROL applications using the old ID number will be unable to connect to the control panel.

IP – local address / public address of the module.

[Cellular network signal] – information about cellular signal strength and cellular network operator. The information is displayed when the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module (module is identified as “ETHM+GSM”).

QR-code – click the button to open the window in which the QR code is displayed. The QR code contains information required when configuring settings of communication through the SATEL server. You can read the QR code by using a mobile device or export to the file and transmit to the users. The QR code facilitates configuring the INTEGRA CONTROL application settings.

Refresh – click to refresh all information.

LAN uplink loss report delay – if the Ethernet network is not available for a preset period of time, the module will report a trouble. A delay in reporting the trouble prevents sending information about short-time loss of Ethernet connectivity.

INT-GSM functions

These settings apply to the INT-GSM / INT-GSM LTE module. They are available if the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module (the module is identified as “ETHM+GSM”). For description of the settings, refer to the INT-GSM / INT-GSM LTE module manual.

IP filter

The module connected to the INTEGRA / INTEGRA Plus control panel with firmware version 1.15 (or newer) offers IP filter. Using IP filtering allows you to enhance security level of the alarm system. Establishing connection with the Ethernet module (alarm control panel) will only be possible from defined IP addresses or subnets. IP filtering does not apply to communication via the SATEL server.

You can configure IP filtering for the incoming connections:

- from DLOADX program,
- from GUARDX program (applies also to web browser, mobile application and INTEGRUM system),
- as part of integration.

In each case you can define the filtering rules in one of the following configurations:

- up to 4 allowed IP addresses,
- 1 allowed subnet and up to 2 allowed IP addresses,
- up to 2 allowed subnets.



To activate the filtering feature, enter a value in one of the four fields available for the given type of incoming connections.

The screenshot shows the 'IP filter' configuration window for the DLOADX program. It has tabs for 'ETHM-1', 'IP filter', 'Remote firmware update', 'IP zone', and 'User functions definition'. The 'Allowed IP addresses' section is expanded, showing three sub-sections: 'DLOADX', 'GUARDX', and 'Integration'. Each sub-section contains two rows of input fields: 'IP address' and 'Subnet mask'. To the right of each 'IP address' field is a 'subnet' checkbox. In the 'DLOADX' and 'GUARDX' sections, the 'subnet' checkbox is checked. In the 'Integration' section, the 'subnet' checkbox is unchecked. The values for the 'IP address' fields are: DLOADX (192.168.2.0, 192.168.1.91, 0.0.0.0), GUARDX (192.168.2.0, 192.168.1.91, 192.168.7.110), and Integration (0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0). The 'Subnet mask' field in the DLOADX and GUARDX sections is set to 255.255.255.0.

Fig. 7. DLOADX program: "IP filter" tab.

IP Address – if the *subnet* option is disabled: the network address from which connection with the Ethernet module can be established. If the *subnet* option is enabled: the IP address used for defining the subnet from which connection with the Ethernet module can be established.

subnet – if the option is enabled, you can define the subnet from which incoming connections will be received by the module.

Subnet mask – mask used for separating the portion defining subnet from the IP address.

Filtering by IP address

In the *IP Address* field, enter the network address from which establishing connection with the module (control panel) is to be possible. The *subnet* option on the right-hand side of the field must not be selected.

The image shows two examples of IP address input fields. The first example shows an 'IP Address' field containing '0.0.0.0' with a red box around the field and an unchecked 'subnet' checkbox. The second example shows an 'IP Address' field containing '192.168.1.75' with a red box around the field and a checked 'subnet' checkbox.

Filtering by subnet

1. Select the *subnet* option. Description of one of the *IP Address* fields will change to *Subnet mask*. From now on, the *IP Address* and *Subnet mask* fields constitute a pair.

IP Address:	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/> subnet
IP Address:	<input type="text" value="0.0.0.0"/>	

IP Address:	<input type="text" value="0.0.0.0"/>	<input checked="" type="checkbox"/> subnet
Subnet mask:	<input type="text" value="0.0.0.0"/>	

2. Enter the address to be used to define the subnet.

IP Address:	<input type="text" value="0.0.0.0"/>	<input checked="" type="checkbox"/> subnet
Subnet mask:	<input type="text" value="0.0.0.0"/>	

3. Enter the mask to be used to separate the portion defining subnet in the IP address.

IP Address:	<input type="text" value="192.168.2.0"/>	<input checked="" type="checkbox"/> subnet
Subnet mask:	<input type="text" value="0.0.0.0"/>	

IP Address:	<input type="text" value="192.168.2.0"/>	<input checked="" type="checkbox"/> subnet
Subnet mask:	<input type="text" value="255.255.255.0"/>	

Remote firmware update



The following is relevant if the INT-GSM / INT-GSM LTE module is not connected to the ETHM-1 Plus module. If INT-GSM / INT-GSM LTE is connected to ETHM-1 Plus, please refer to the INT-GSM / INT-GSM LTE module manual for description of remote update settings.

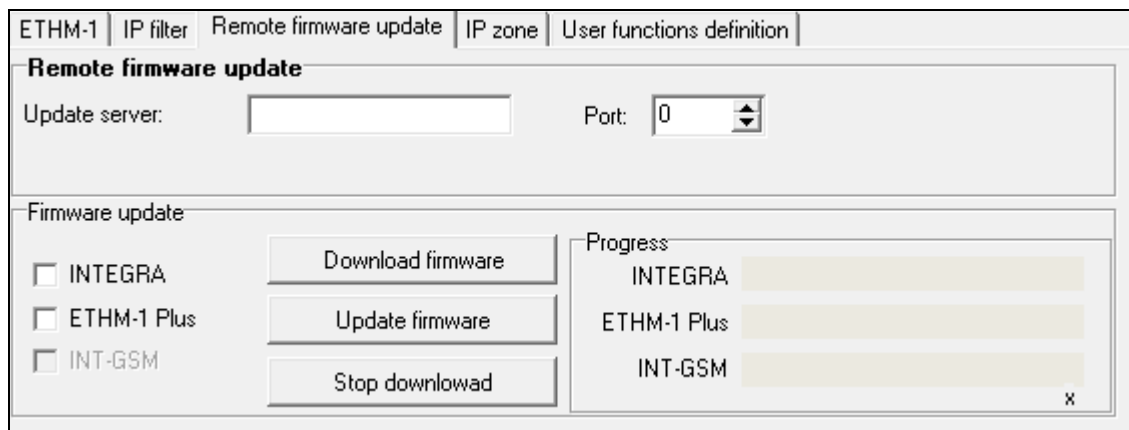


Fig. 8. DLOADX program: "Remote firmware update" tab.

The module firmware can be updated remotely using the UpServ update server, which is included in the SATEL product portfolio. You can start the update process in the DLOADX program. You can update the firmware for:

- INTEGRA Plus / INTEGRA control panel – only if the DLOADX program and the control panel are connected via the ETHM-1 Plus module (the RS-232 ports of control panel and module are connected),
- ETHM-1 Plus module.

Update server – address of the UpServ update server. You can enter the IP address or domain name.

Port – number of the TCP port used for communication with the UpServ update server. You can enter values from 0 to 65535 (0=disabled).

Firmware update



The module does not perform its normal functions during firmware update.

Before updating the module firmware, enter the SERVICE MODE in the alarm control panel. Otherwise, starting the update process will trigger tamper alarm (module not present).

INTEGRA – if this option is enabled, the INTEGRA Plus / INTEGRA control panel firmware will be updated.

ETHM-1 Plus – if this option is enabled, the ETHM-1 Plus module firmware will be updated.

Download firmware – click to download new version of firmware.

Update firmware – click to update the device(s) to the latest firmware version. If you have not downloaded the firmware, it will be downloaded automatically now. The update will begin after the download is complete.

Stop download – click to stop the process of updating the firmware.

Progress – progress bars show the process of downloading the firmware.

IP zone



IP zones are supported by INTEGRA / INTEGRA Plus control panels with firmware version 1.22 (or newer).

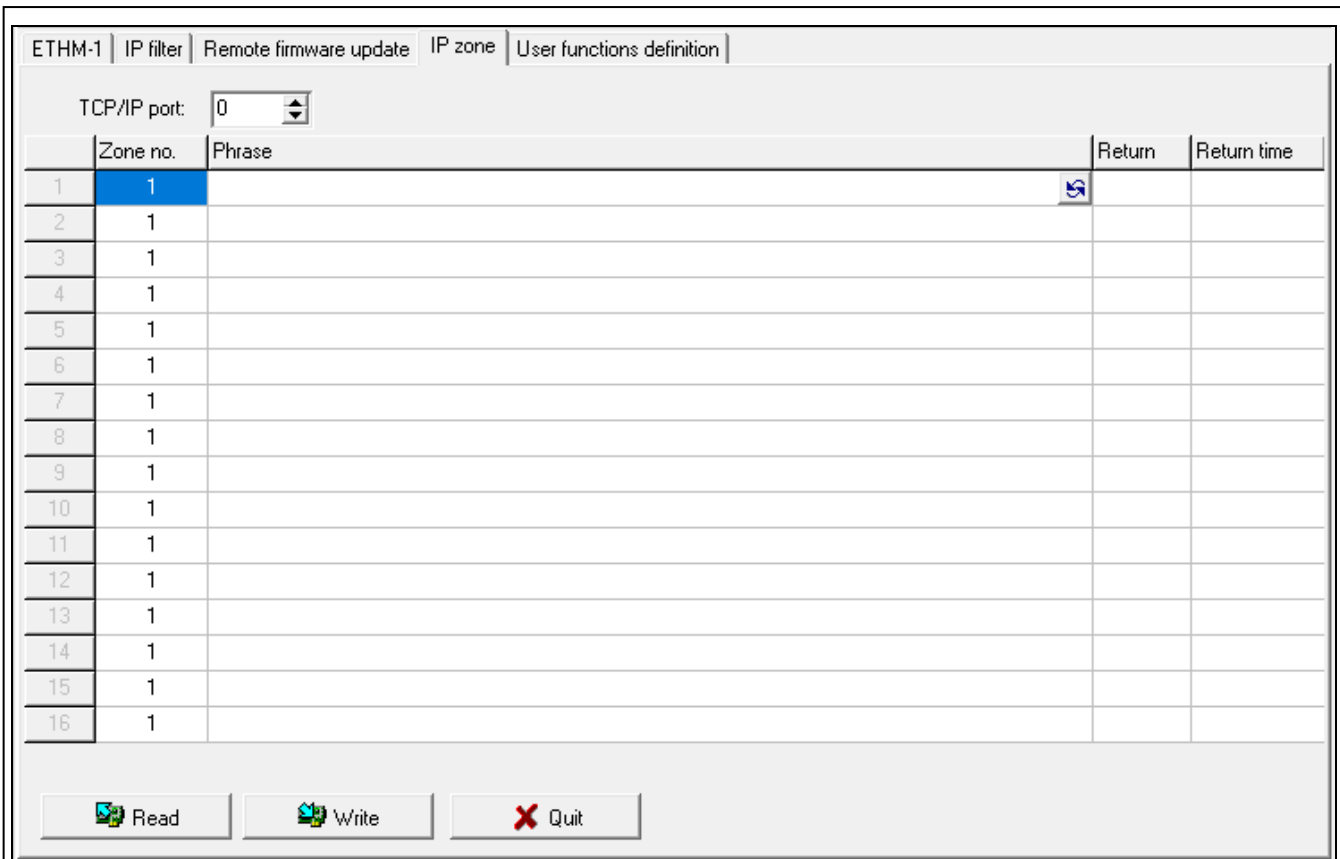


Fig. 9. DLOADX program: "IP zone" tab.

The module can be used as the HTTP notification server and it can receive notifications sent by IP cameras in case of different events (e.g. motion detection). In the "IP zone" tab, the settings of HTTP notification support are available. The notifications can control the alarm system zones. The cameras must operate in the same local network as the ETHM-1 Plus module.

The IP zones settings are stored in the ETHM-1 Plus module memory.



Before you make any changes, click the "Read" button. After you have made the changes – click "Write". The settings stored in the module are not read / written after you click / in the main menu.

TCP/IP port – number of the port used for receiving HTTP notifications. You can enter values from 1 to 65535. The value must be different from that entered for the other ports.

Zone no. – number of the zone in the system that will be violated after an HTTP notification is received. The wiring type programmed for the zone must be other than *no detector* or *Follow output*.

Phrase – string of characters that must be included in the received HTTP notification for the zone to be violated. You can enter up to 128 characters. You can generate a random string of characters by clicking . Enter the same string of characters in the camera settings.

Return – if this option is enabled, when the module receives an HTTP notification that includes the defined string of characters and the "Action": "Stop" message, the zone will return to normal state (zone restore).

Return time – time after which the zone will return to normal state (zone restore). The countdown is reset after each violation.

Read – click to read the IP zones settings from the module.

Write – click to write the IP zones settings to the module.

Quit – click to cancel reading / writing the settings.

User functions

If the INTEGRA CONTROL application is used in the mobile device, the virtual keypad allows you to quickly start user functions after entering the code and pressing an arrow key.

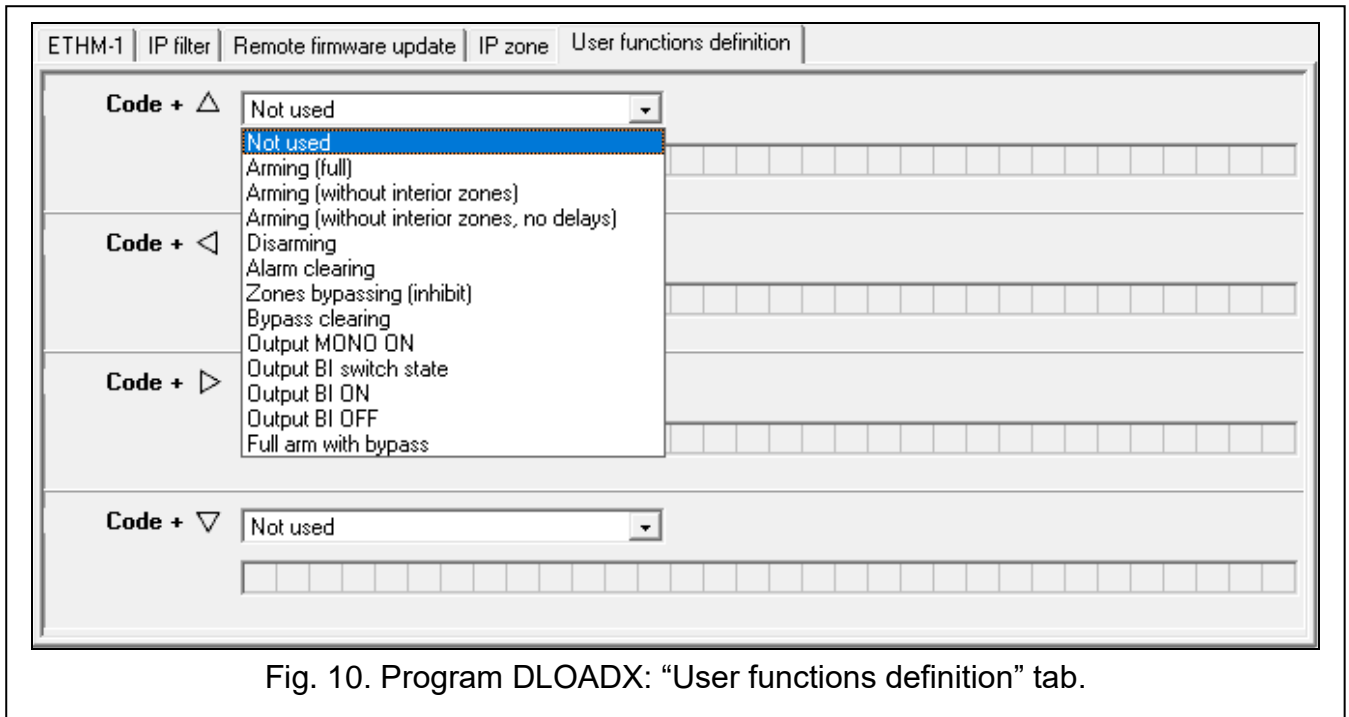


Fig. 10. Program DLOADX: “User functions definition” tab.

Virtual keypad

The virtual keypad allows you to operate and program the alarm system in much the same way as using a physical keypad. You can use the virtual keypad in the DLOADX and GUARDX programs, web browser and in the mobile device (after installation of the INTEGRA CONTROL application).

The virtual keypad settings 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 device 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/INTEGRA CONTROL” item (Fig. 11).

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

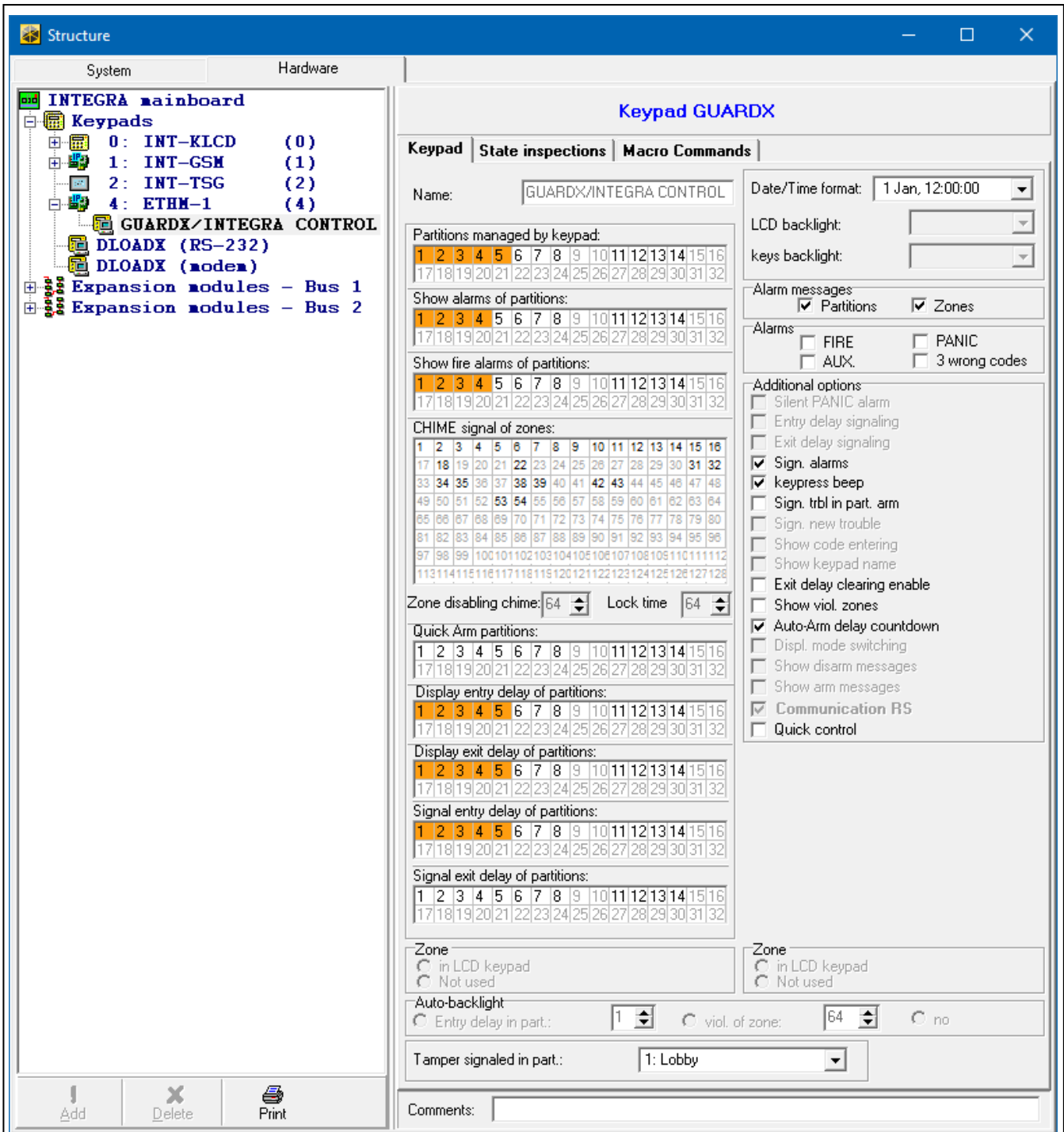


Fig. 11. DLOADX program: parameters and options of the virtual keypad available in GUARDX program, web browser or mobile device.

Macro commands

In the DLOADX program you can prepare macro commands that will be used in the INTEGRA CONTROL app: →“Structure” window →“Hardware” tab →“Keypads” branch →[*module name*] branch →“GUARDX/INTEGRA CONTROL” item →“Macro Commands” tab. The macro command is a sequence of actions to be performed by the control panel. The macro commands help the user to operate the alarm system. Instead of performing several operations (e.g. in order to arm the selected partitions), the user can run a macro command and the control panel will execute the functions assigned to it.

The macro commands settings are stored in the ETHM-1 Plus module memory. The INTEGRA CONTROL app can download the macro commands from the module after establishing connection. Prepared macro commands can also be exported to a file. After the file is copied to a mobile device, the macro commands can be imported to the app. This method allows you to import macro commands prepared e.g. for the INT-TSG keypad.

The buttons related to the macro command settings are displayed on the bottom of the tab:

Read – click to read the macro command settings from the module.

Write – click to write the macro command settings to the module.

Quit – click to cancel reading / writing the macro command settings.

Reset – click to delete the macro command settings (and restore factory settings).



Before you make any changes, click the “Read” button. After you have made the changes – click “Write”. The settings stored in the module are not read / written after

you click  /  in the main menu.


Groups

In the “Groups” tab you can configure the settings of macro command groups. The macro commands must be assigned to groups. There are 4 groups available. You can assign up to 16 macro commands to each group. The macro commands not assigned to any group will not be available in the app. The groups and the macro commands assigned to them are presented as a tree structure.



In the INTEGRA CONTROL app, each group is displayed on a separate screen.

Name – name of the macro command group (up to 16 characters in two lines, up to 8 characters in the line). Do not enter the name if it is not to be displayed.

Icon – the macro command group icon. Click  to display the list of icons, then click the icon that is to be used.



The macro command group icon is not used in the INTEGRA CONTROL app.

Add macro – click to display the list of defined macro commands, then click the macro command name to add it to the group.

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



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



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

Export to file – click to export defined macro commands to a file. The file with macro commands can be loaded into the INTEGRA CONTROL application or imported to another device that support macro commands.

Import from file – click to import macro commands from a file.

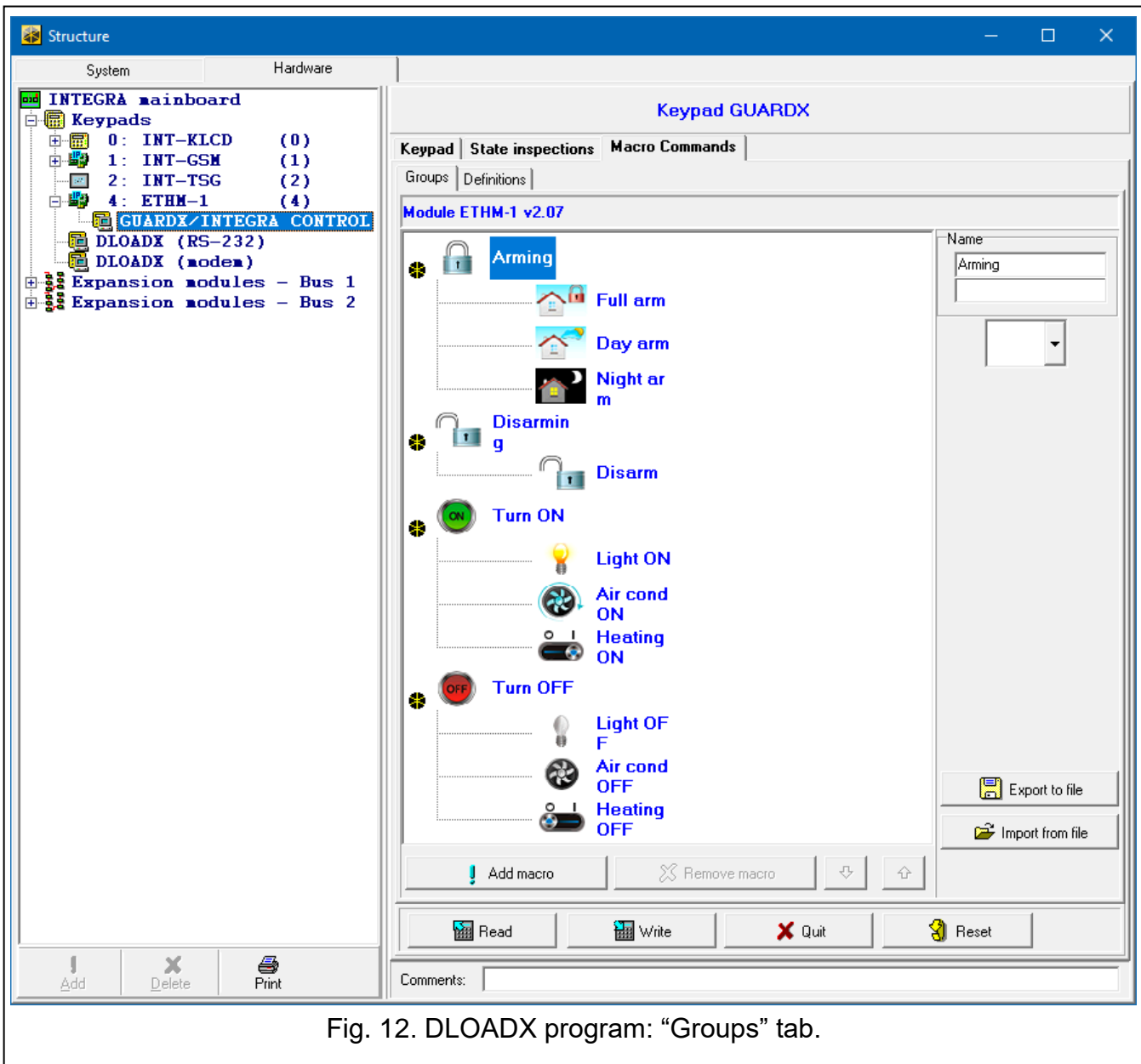


Fig. 12. DLOADX program: "Groups" tab.

Definitions

In the "Definitions" tab you can configure the macro command settings.

New macro – click to create a new macro command.

Remove macro – click to remove the selected macro command.

Name – individual macro command name (up to 16 characters in two lines, up to 8 characters in the line).

Code – this parameter does not apply to the INTEGRA CONTROL app.

Authorization required – if this option is enabled, the macro command will only be run after user additional authorization.

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, there is no need to enter the group to run the macro command. In the INTEGRA CONTROL app, the macro commands with the *Autoexecute* option enabled are presented on a separate screen. It is displayed before the screen that shows the macro commands in the group.

No confirmation messages – this option does not apply to the INTEGRA CONTROL app.

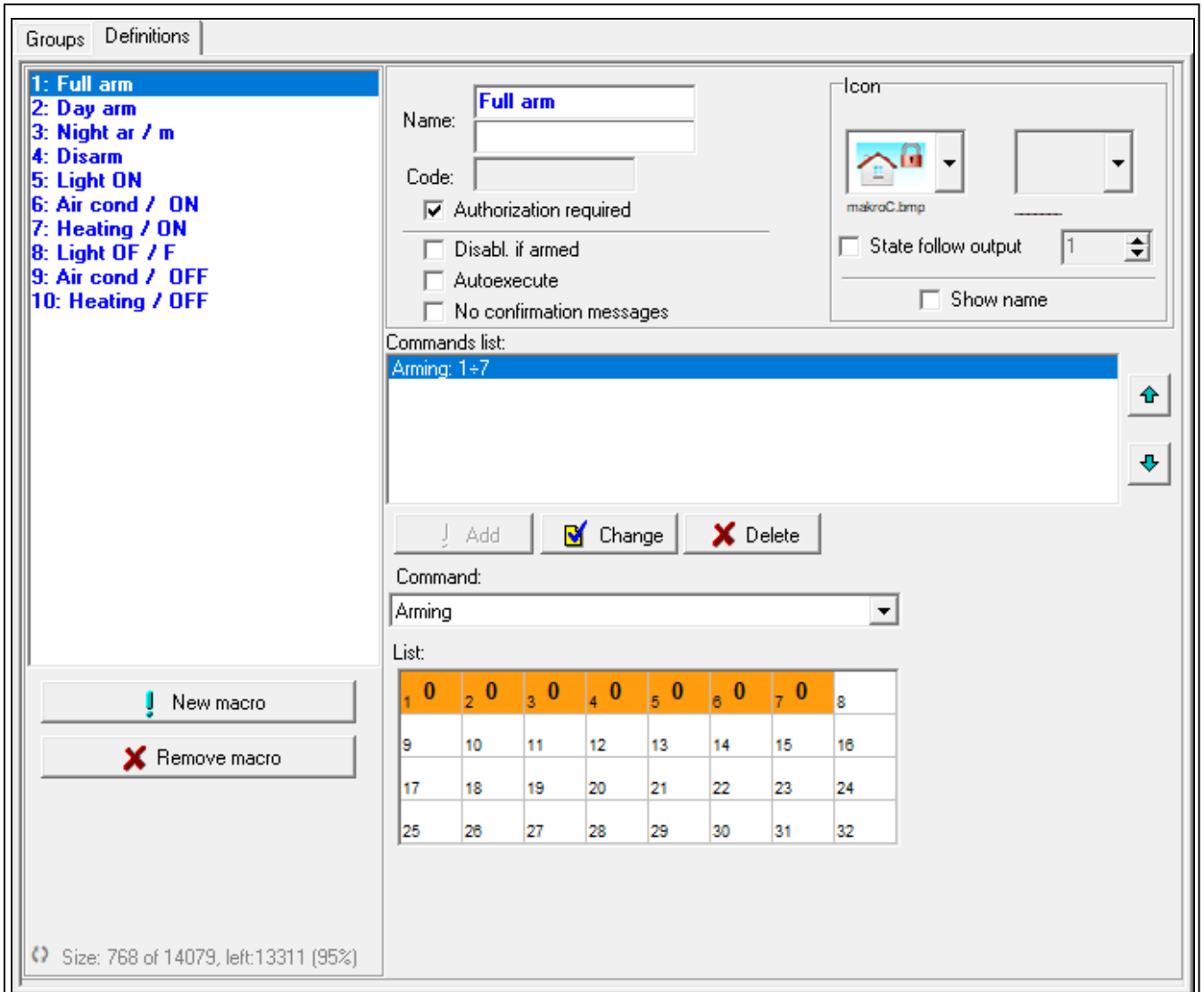




Fig. 13. DLOADX program: "Definitions" tab.

Icon

Icon – the macro command icon. Click  to display the list of icons, then click the icon that is to be used. If the *State follow output* option is enabled, select 2 icons for the macro commands. One icon will be displayed when the output is inactive, and the other – when the output is active.



 *The macro command icon used in the INTEGRA CONTROL app is different from the icon presented in the DLOADX program.*

State follow output – if this option is enabled, the icon of macro command will change depending on the status of output whose number should be selected in the field on the right side. Select an output, the status of which depends on the actions taken by the control panel after running the macro command. Thus it will be possible to inform the user by means of macro command icons about, for example, the status of outputs controlled by macro commands or the status of partitions which are armed by a macro command.

Show name – if this option is enabled, the macro command name will be displayed.

Commands


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

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

Add – click to add to the list a new command, selected in the “Command” field.

Change – click 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 to remove the highlighted command from the list.

Command – function that you can assign to the macro command. Click  to drop down the list of available functions, then click the function that you want to assign to the macro command.

List – table displayed for most functions. Its fields represent the system elements (partitions / zones / outputs) that can be controlled by the function. The numbers of the fields in the table correspond to the numbers of the elements in the system. The color of the field indicates:

orange – function controls this system element,

white – function does not control this system element.

Double-click the field to change its color.

Depending on the selected function:

Arming – select the partitions to be armed and define the arming mode (keep clicking the field). The digit inside the field indicates:

0 – fully armed,

1 – fully armed + bypasses,

2 – armed without interior,

3 – armed without interior and without entry delay.

Disarming – select the partitions to be disarmed.

Alarm clearing – select the partitions in which alarm is to be cleared.

Bypass zones – select the zones which are to be inhibited.

Unbypass zones – select the zones which are to be unbypassed.

Outputs ON – select the outputs to be turned on.

Outputs OFF – select the outputs to be turned off.

Change outputs state – select the outputs whose state is to be changed.



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).

KNX telegram – the following settings are available for the function:

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).

KNX telegram (v2) – the following settings are available for the function:

Module INT-KNX – INT-KNX-2 module in which the value is to be set.

Macro Command – name of the “Virtual (macro)” type object, defined in INT-KNX-2 module.

Data type – size and meaning of the communication object data defined in INT-KNX-2 module for selected object.

Value – value to be set (if the type of data provides for sending a sequence of characters, you can enter up to 13 characters).

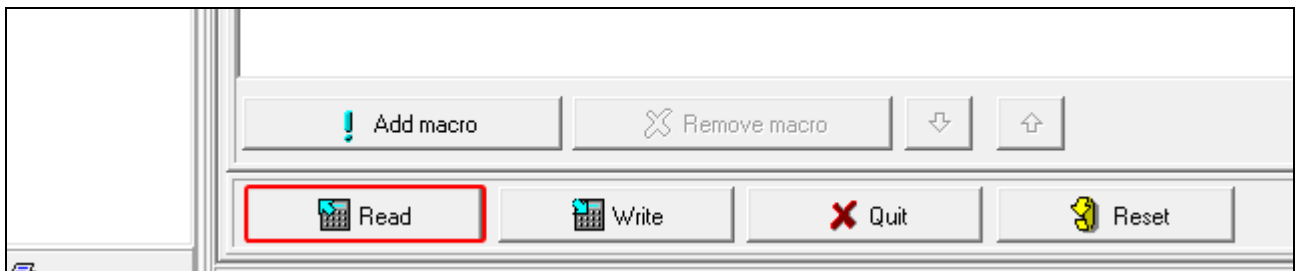
i | *The Telegram KNX and Telegram KNX (v2) functions allow you to control the KNX system if the INT-KNX or the INT-KNX-2 module is connected to the control panel.*

Exit delay clearing – no settings available for the function.

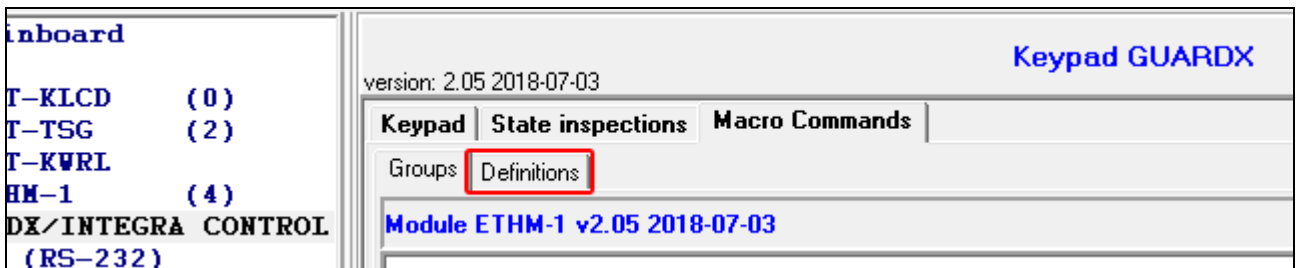
Quick arm – for the function you must select the arming mode to be activated.

Preparing macro commands

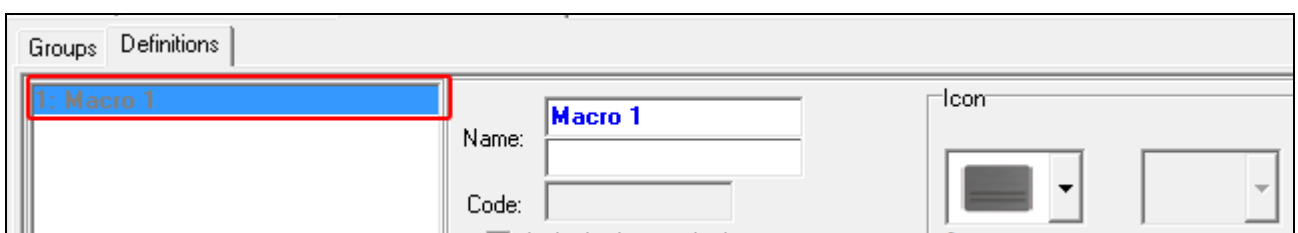
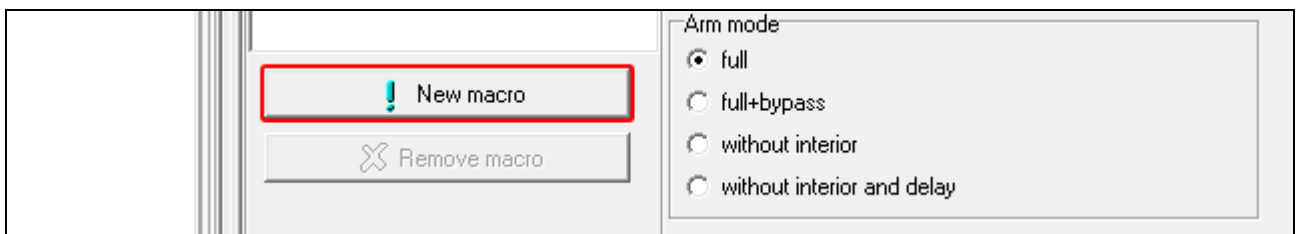
1. Click the “Read” button to read the macro command related data from the module.



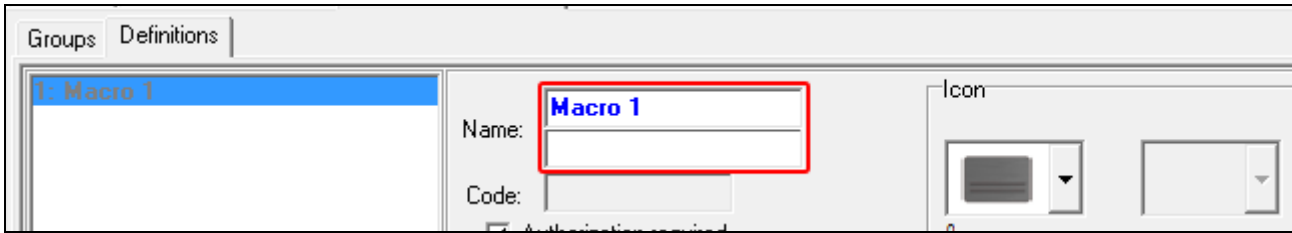
2. Click the “Definitions” tab.



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



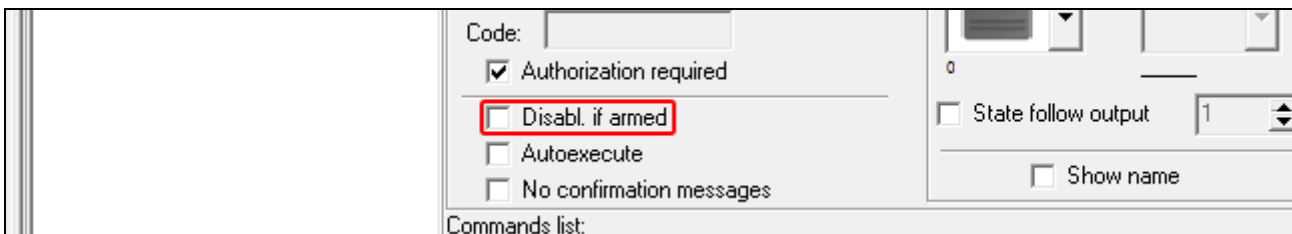
4. Enter a name for the new macro command.



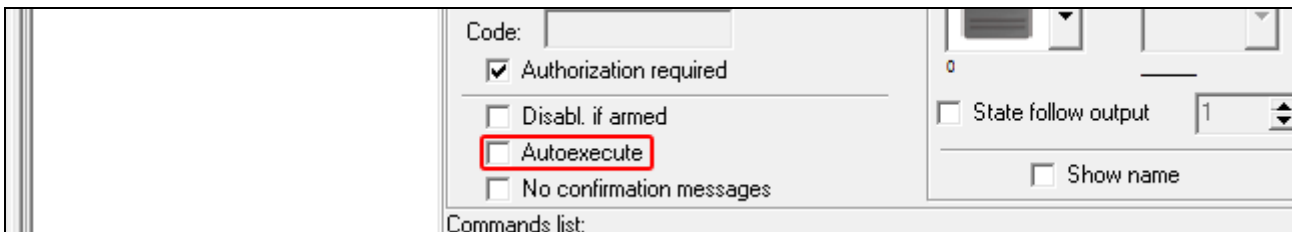
5. If running a macro command is to be each time preceded by user authorization, enable the *Authorization required* option.




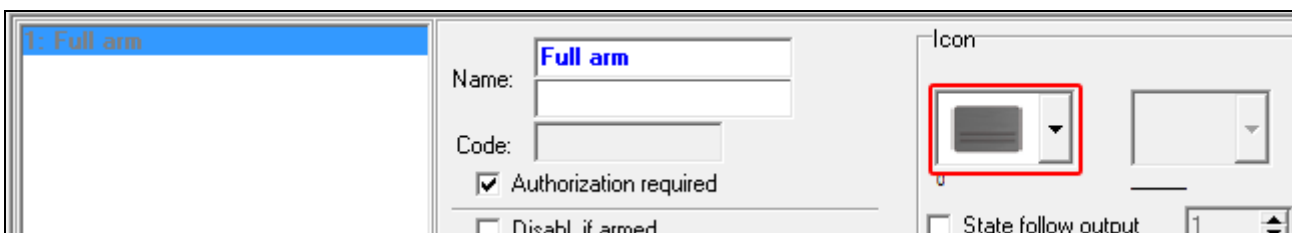
6. If the macro command is to be unavailable when any of the partitions managed by the keypad is armed, enable the *Disabl. if armed* option.



7. If the macro command is to be available without entering the group (displayed in the INTEGRA CONTROL app on a separate screen), enable the *Autoexecute* option.

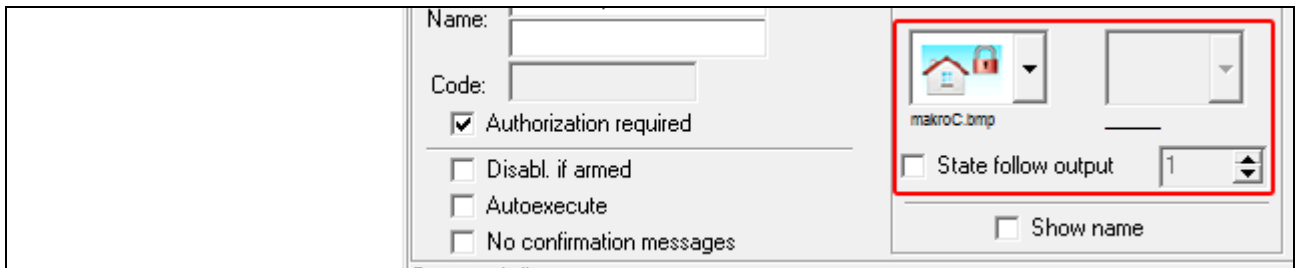


8. Click  and select the icon for the macro command.

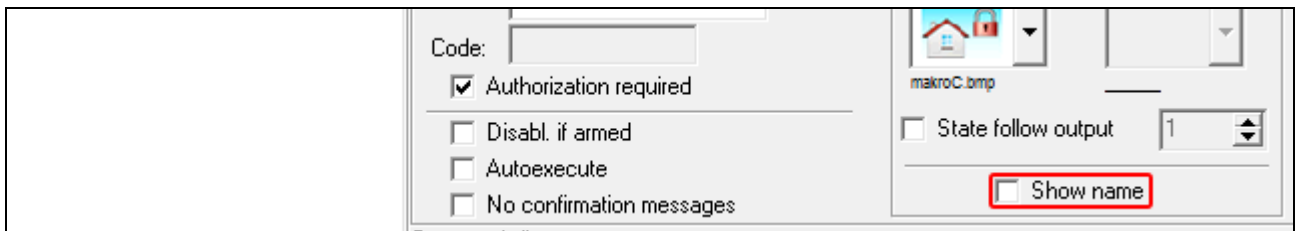



9. If the icon is to change depending on the selected output state:

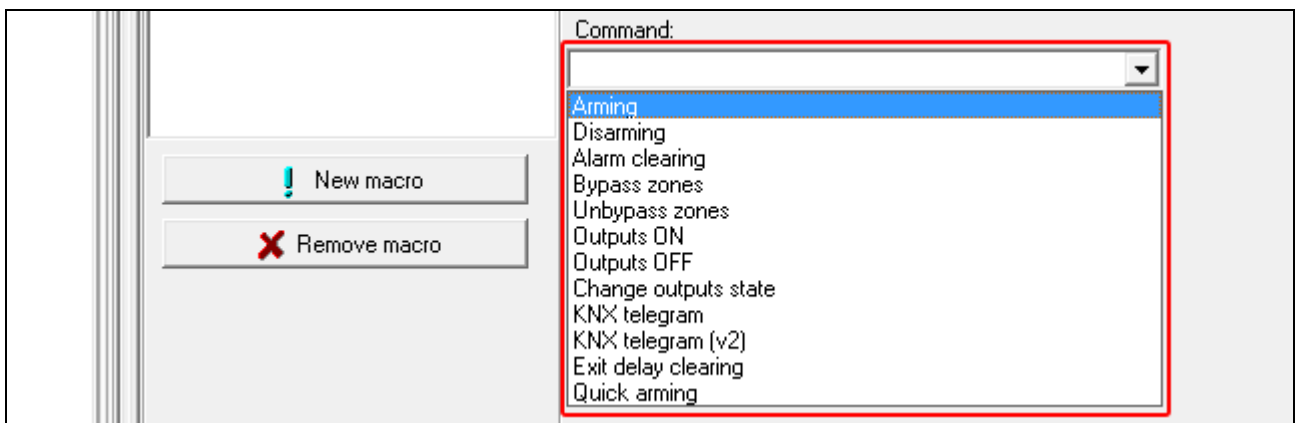
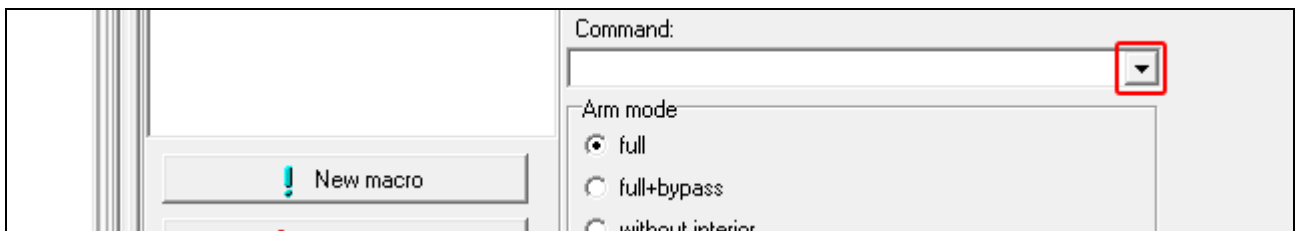
- enable the *State follow output* option;
- indicate the output number;
- select the icons.



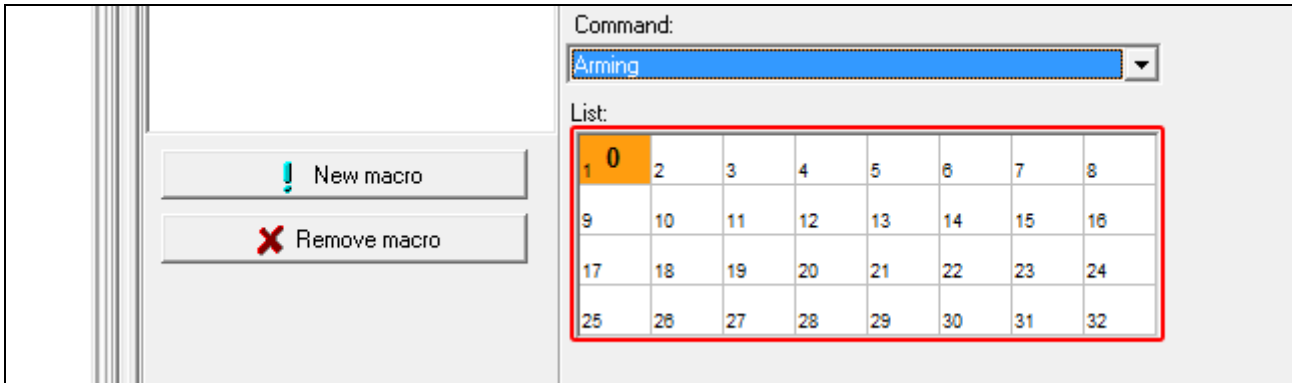
10. If the macro command name is to be displayed, enable the *Show name* option.



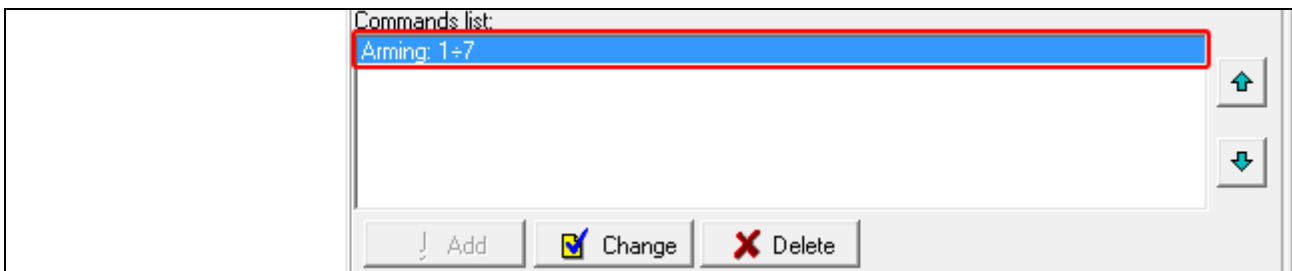
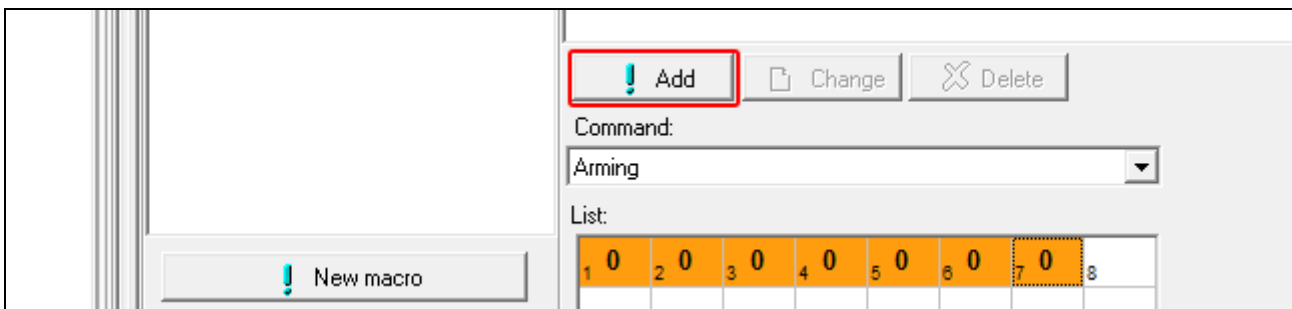
11. Click  in the *Command* field and select the function the new macro command is to execute.



12. Configure the command parameters.

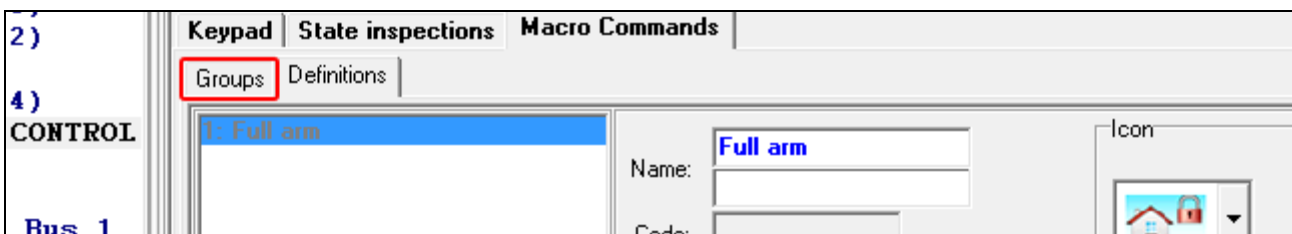


13. Click the “Add” button. A new command will appear on the list of commands assigned to the macro command. You can still modify parameters of the command after clicking on it (having made the changes, click the “Change” button).

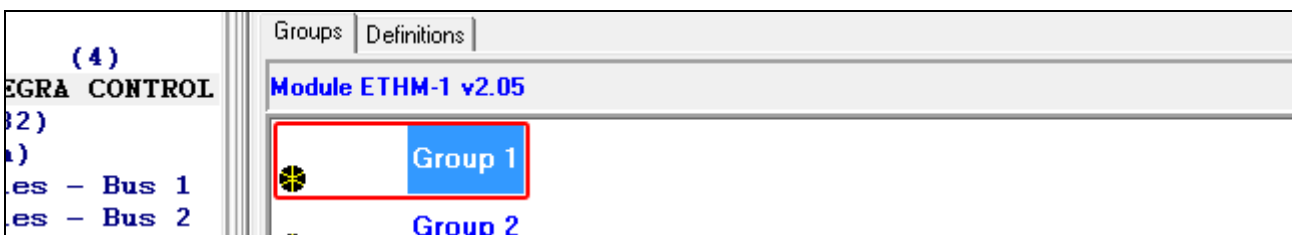


14. Repeat the steps 12-14, if you want to add next commands.

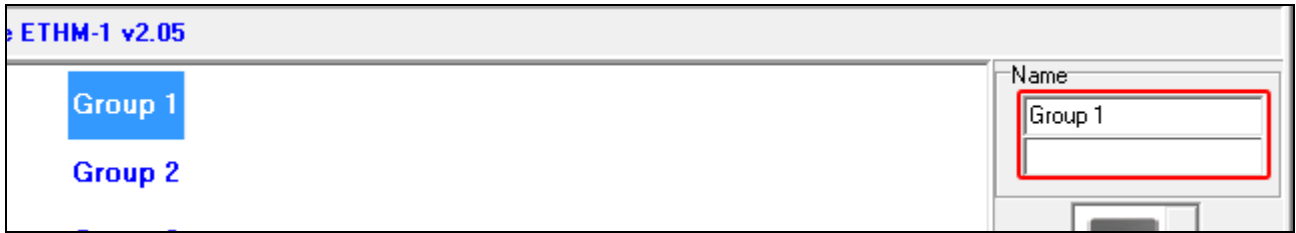
15. Click the “Groups” tab.




16. Click the group you want to edit.



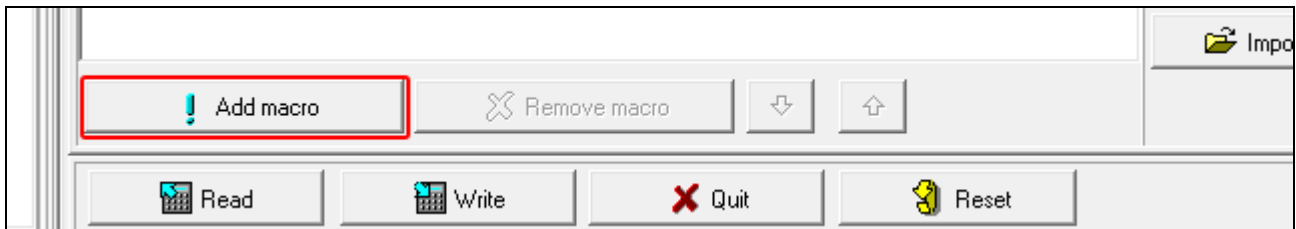
17. Enter the group name, if it is to be displayed.



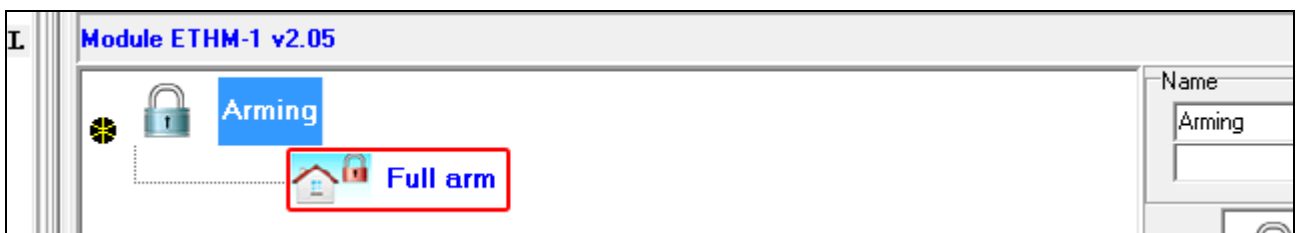
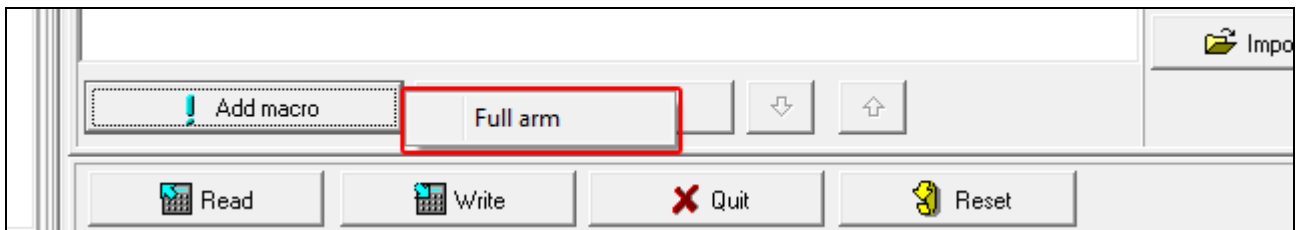
18. Click  and select the icon for the macro command group.



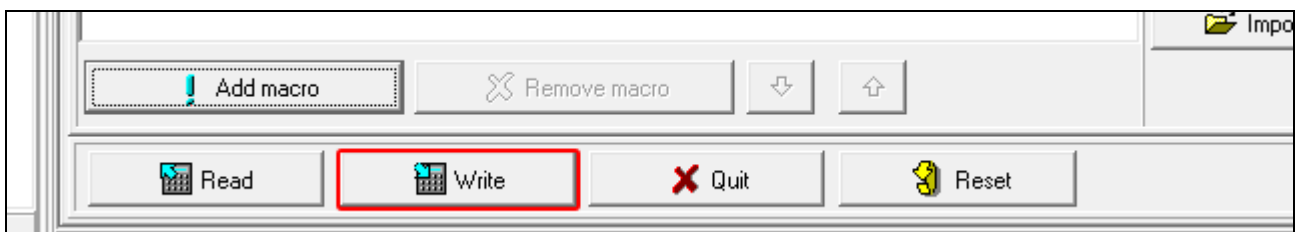
19. Click the “Add macro” button. A list of all defined macro commands will be displayed.



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



21. Click the “Write” button to write the macro command related data to the module.




6.2 Module connected to PERFECTA 64 M control panel











You can configure the module settings using a computer with the PERFECTA Soft program installed or using the keypad.

6.2.1 Programming in the PERFECTA Soft program

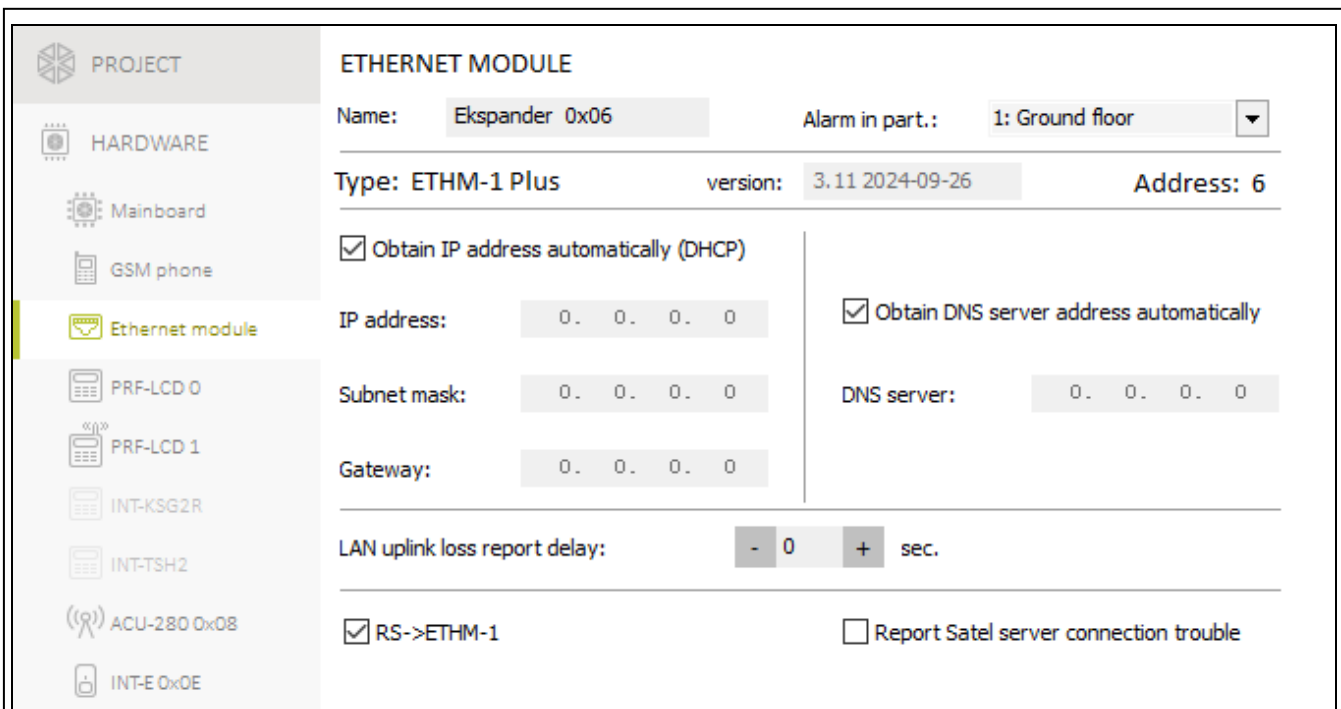
Required version of the PERFECTA Soft program: 2.01 (or newer).

1. Click the "Hardware" tab.
2. Click the Ethernet module.
3. Configure the module settings.
4. Click  to save changes to the control panel.

6.2.2 Programming from the keypad

1. Enter the **service code** (by default: 12345) and press  . The user menu will be displayed.
2. Press  .
3. When the  cursor indicates the SERVICE MODE function, press  . The service menu will be displayed.
4. Press   . The functions available in the 2.EXPANDERS submenu will be displayed.
5. Program the module settings using the available functions.

6.2.3 Module settings



The screenshot shows the 'ETHERNET MODULE' configuration screen in the PERFECTA Soft program. On the left is a sidebar with a tree view of hardware components, with 'Ethernet module' selected. The main panel displays the following settings:

- Name:** Ekspander 0x06
- Alarm in part.:** 1: Ground floor
- Type:** ETHM-1 Plus
- version:** 3.11 2024-09-26
- Address:** 6
- Obtain IP address automatically (DHCP)
- Obtain DNS server address automatically
- IP address:** 0. 0. 0. 0
- Subnet mask:** 0. 0. 0. 0
- DNS server:** 0. 0. 0. 0
- Gateway:** 0. 0. 0. 0
- LAN uplink loss report delay:** - 0 + sec.
- RS->ETHM-1
- Report Satel server connection trouble

Fig. 14. PERFECTA Soft program: settings of the module connected to PERFECTA 64 M control panel.

Names of parameters and options from the PERFECTA Soft program are used in this manual. When a parameter or an option is described, in square brackets you will find one of the following information:

- name of the function used to configure a parameter or option in the keypad,
- name of a parameter or option from the keypad.

Name [286.Ex. 06 name] – individual name of the module (up to 16 characters).

Alarm in part. [226.Ex. 06 part] – the partition in which alarm will be generated in the event of module tamper.

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

IP address [2191.Address] – module IP address. This field is available if the *Obtain IP address automatically (DHCP)* option is disabled.

Subnet mask [2192.Netmask] – the mask of the subnet in which the module is working. This field is available if the *Obtain IP address automatically (DHCP)* option is disabled.

Gateway [2193.Gateway] – IP address of the network device through which the other devices in the local network can communicate with devices in other networks. The field is available if the *Obtain IP address automatically (DHCP)* option is disabled.

Obtain DNS server address automatically [DNS-DHCP] – 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 [DNS] – IP address of the DNS server which is to be used by the module. The field is available if the *Obtain DNS server address automatically* option is disabled.

LAN uplink loss report delay [2195.LANtrb.del] – time after which the loss of LAN cable connection is reported.

RS->ETHM [RS->ETHM-1] – if this option is enabled, the module RS-232 port can be used for communication with the control panel (the RS232-RSTTL converter is required to connect the module and control panel ports). The option must be enabled if the alarm system is to be programmed / operated via Ethernet.



Report Satel server connection trouble [ETHM-1 SRV TRBL] – if this option is enabled, the module will report a trouble in case of communication problems with the SATEL server.

6.3 Module connected to VERSA control panel









You can configure all of the module settings using a computer with the DLOADX program installed. From the keypad, you can configure only some of the settings.




6.3.1 Programming in the DLOADX program

Required version of the DLOADX program: 1.22.000 (or newer).

1. Click  in the main menu. The “Structure” window will be displayed.
2. Click the “Hardware” tab.
3. Click the “Expansion modules” branch.
4. Click the name of the module whose settings you want to configure.
5. Configure the module settings.
6. Click  in the main menu to save changes to the control panel. For settings stored in the module (e-mail messaging), click the “Write” button.

6.3.2 Programming from the keypad

1. Enter the **service code** (by default: 12345) and press . The user menu will be displayed.
2. Press   . The service menu will be displayed.
3. Press     to start the 2.SETTINGS function.

4. Find the module whose settings you want to configure (use the  or  key) and press .
5. Program the module settings step by step.

6.3.3 Module settings

Names of parameters and options from the DLOADX program are used in this manual. When a parameter or an option is described, you will find in the square brackets their name displayed on the keypad.

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.

DLOADX->ETHM-1 connection [DLOADX→ETHM-1] – if this option is enabled, connection can be established between the DLOADX program and the alarm control panel via the module.

DLOADX

DLOADX server [DLOADX] – address of the computer running the DLOADX program. If the communication takes place in a wide area network, it must be a public address. You can enter either the IP address or the domain name.

Port [DLOADX port] – number of the TCP port used during communication between control panel and a computer with DLOADX program via Ethernet. 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 – a string of up to 12 alphanumeric characters (digits, letters and special characters) which is used for data encryption during communication with the DLOADX program via module.

SATEL service

LAN [SATEL server LAN] – if the option is enabled, the module connects to the SATEL server and the communication via the SATEL server with the control panel can be established (Connection Setup Service). This way of communication requires no additional configuring of the network device through which the module connects to the public network.



For establishing communication with the SATEL server, the DNS server must be used.

For communication via the SATEL server, the ports of 1024-65535 range are used as outgoing ports. These ports must not be blocked.

Do not report SATEL server connection trouble [No SATEL trbl.] – if this option is enabled, loss of communication with the SATEL server will not be reported.

Communication with mobile application [Mobile app.] – if this option is enabled, connection can be established between the VERSA CONTROL application and the alarm control panel via the module. The option is available if the *LAN* option is enabled.

Alarm 3 incorrect codes (mobile application) [Al.3 wrong codes] – if this option is enabled, entering an invalid code three times from the VERSA CONTROL application will trigger an alarm.

Push notifications – if this option is enabled, the VERSA CONTROL application can provide information about alarm system events by means of push notifications.

Information

MAC – module hardware address.

ID – individual ID number assigned to the module by the SATEL server.

i | *If the module is to be used in another alarm system, the hitherto used ID number must be deleted. You should do it after connecting the module to the new control panel and establishing connection with the SATEL server, from the keypad, when programming the Ethernet module, in the last step. Having deleted the old ID number, the module will receive a new one. The VERSA CONTROL applications using the old ID number will be unable to connect to the control panel.*

IP – local address / public address of the module.

QR-code – click the button to open the window in which the QR code is displayed. The QR code contains information required when configuring settings of communication through the SATEL server. You can read the QR code by using a mobile device or export to the file and transmit to the users. The QR code facilitates configuring the VERSA CONTROL application settings.

Refresh – click to refresh all information.

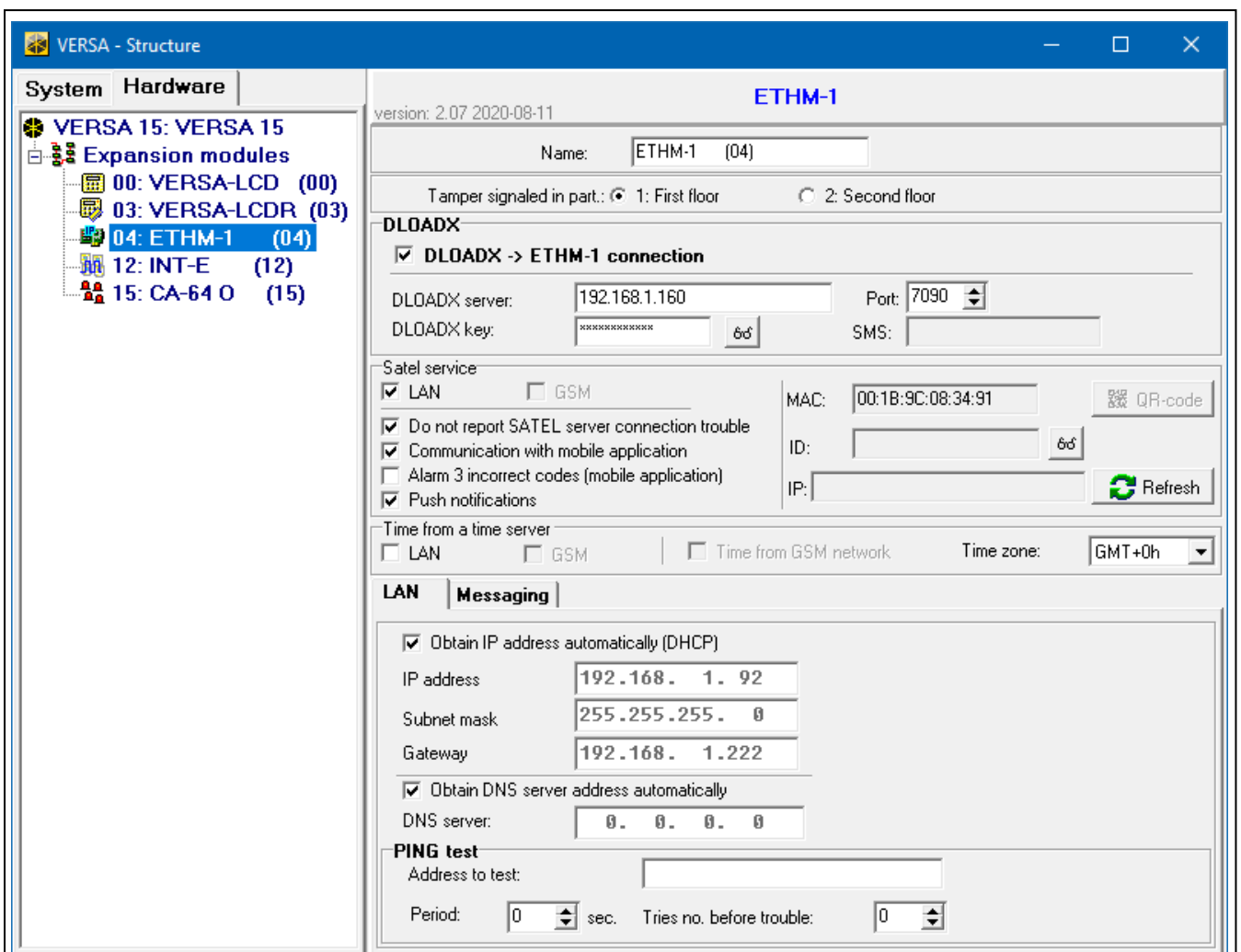


Fig. 15. DLOADX program: settings of the module connected to VERSA control panel.

Time from a time server

LAN [Time from srvLAN] – if the option is enabled, the control panel clock will be synchronized with the time server once a day.

i | *For communication with the time server, the DNS server must be used.*

Time zone – difference between the universal time (GMT) and the zone time. The parameter is required, if the control panel clock is to be synchronized with the time server.

LAN

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.

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.

Messaging

E-MAIL

The e-mail messaging settings stored in the ETHM-1 Plus module memory.



Before you make any changes, click the “Read” button. After you have made the changes – click “Write”. The settings stored in the keypad are not read / written after

you click  /  in the main menu.

LAN – if the option is enabled, the control panel can notify of occurrence of specified events by means of e-mail messages.

Email address – e-mail address to which messages are to be sent for notification of events.



Because the message is sent to many recipients, the addressees are hidden. If you want the addressee to be shown, place @ before the email address (e.g. @j.smith@example.com).

ON – with this option enabled, it will be possible to send messages to the given e-mail address for notification of events.

Events type – define of which events the given e-mail address is to be notified.

Part. – define the partitions, about the events from which the given e-mail address is to be notified.

- SMTP account** – click to open “SMTP account” window.
- Read** – click to read the data related to e-mail messaging.
- Write** – click to write the data related to e-mail messaging.

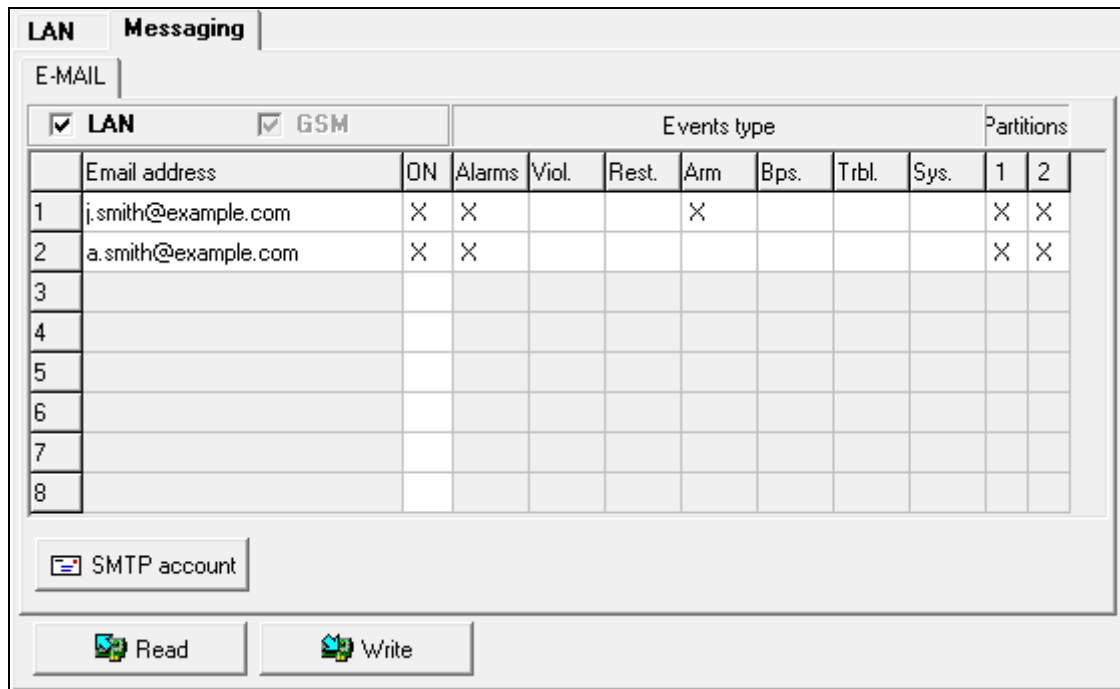


Fig. 16. DLOADX program: configuring the e-mail messaging.

SMTP account

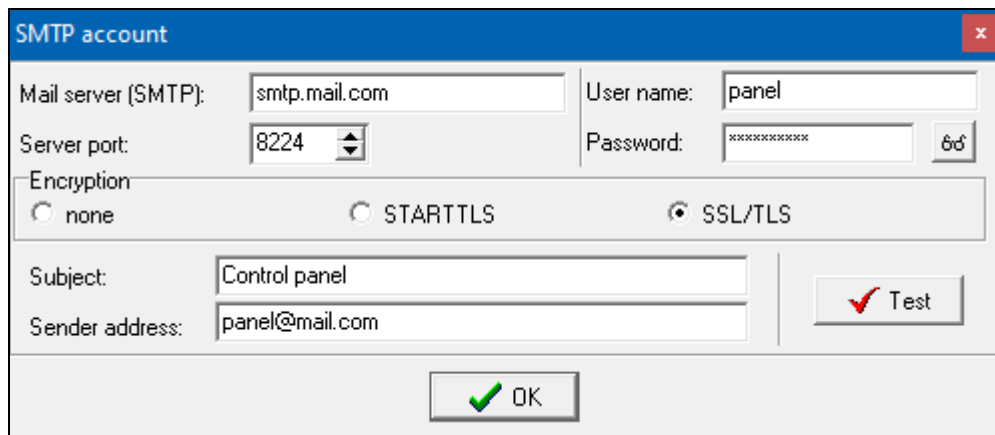


Fig. 17. DLOADX program: “SMTP account” window. The presented settings are just an example.

i | It is required to have an e-mail account so as to enter its parameters in the DLOADX program for the purpose of e-mail messaging.

- Mail server (SMTP)** – address of outgoing mail server.
- Server port** – number of outgoing mail port.
- User name** – name of the e-mail account used for authorization by the SMTP server (login to e-mail account).
- Password** – the password used for authorization by the SMTP server.

Encryption – you can define if and how the outgoing mail is encrypted:

none – outgoing mail is not encrypted.

STARTTLS – outgoing mail will be encrypted using the STARTTLS protocol.

SSL/TLS – outgoing mail will be encrypted using the SSL/TLS protocol.

Subject – subject of the e-mail message. It will be inserted in each e-mail message to be sent.

Sender address – e-mail address which will be inserted in the outgoing e-mail message as the sender address. If this field is blank, the name of e-mail account will be treated as the sender address.

7 Programming and operating the alarm system via Ethernet

An alarm system in which the ETHM-1 Plus module is installed can be programmed and operated remotely via Ethernet. Details vary depending on the alarm system.

7.1 INTEGRA Plus / INTEGRA system

The Ethernet communication can be used to:

- program the alarm system in the DLOADX program,
- administer the alarm system in the GUARDX program,
- operate and program the alarm system in the INTEGRA CONTROL mobile app,
- operate and program the alarm system in a web browser that supports JAVA applications.

For information on how to program the alarm system via Ethernet using the DLOADX program, please refer to the control panel programming manual.



If the INT-GSM / INT-GSM LTE module is connected to the ETHM-1 Plus module, the cellular data network is used as a backup communication path.

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.

The GUARDX program, the web browser, the INTEGRA CONTROL application and the INTEGRUM system cannot simultaneously connect to the INTEGRA / INTEGRA Plus control panel (e.g. when communication with the INTEGRUM server is ongoing, you will not be able to connect to the control panel in the GUARDX program, a web browser or the INTEGRA CONTROL application).

7.1.1 GUARDX program

Connection between the GUARDX program and the control panel via the ETHM-1 Plus module can be established using one of the following ways:

1. Connection initialized from the GUARDX program. If communication takes place in a wide area network, the Ethernet module must have a public IP 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. If communication takes place in a wide area network, the computer with GUARDX program module must have a public IP address.
3. Initiating connection by SMS message. The computer with GUARDX program must have a public IP address. The INT-GSM / INT-GSM LTE module must be connected to the ETHM-1 Plus module.

- Establishing connection via the SATEL server (Connection Setup Service). The control panel can be operated from any location. No public IP address is required for the control panel or the computer with GUARDX program.

Required settings of the module for all methods of establishing connection:

- enabled *GUARDX* option,
- programmed data encryption key (*GUARDX* key).

Programming the GUARDX program settings



Fig. 18. GUARDX program: startup window.

- Select the communication method in the GUARDX program startup window, “Connection” field: “TCP/IP: GUARDX->ETHM”, “TCP/IP: GUARDX<-ETHM/INT-GSM” or “TCP/IP: SATEL server” (Fig. 18).
- Click the “Configuration” button. The “System name” window will be displayed.
- Enter the system name and click the “OK” button. The “Connection” window will be displayed.

“Communication Identifiers” tab

Panel’s identifier – identifier of the alarm control panel. It must consist of 10 characters (digits or letters from A to F).

PC identifier – identifier of the computer with GUARDX program. It must consist of 10 characters (digits or letters from A to F).



You must enter the same identifiers in the GUARDX program and in the control panel.

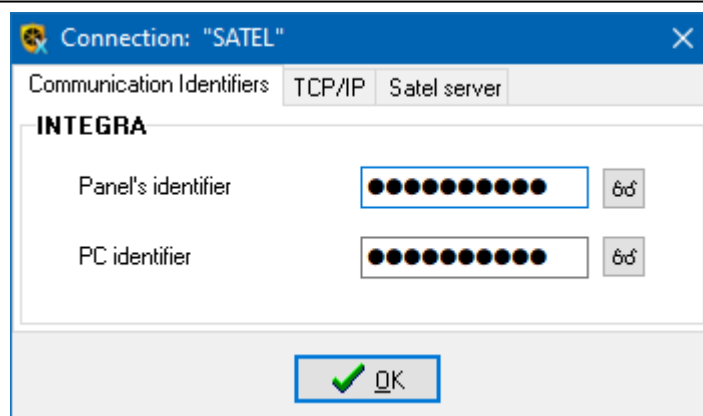


Fig. 19. GUARDX program: “Communication Identifiers” tab in “Connection” window.

“TCP/IP” tab

The settings below apply to direct communication with the module.

Server (ETHM-1 address) – address of the Ethernet module. If the Ethernet module is not in the same local network as the computer with GUARDX program, it must be a public address. You can enter either the IP address or the domain name.

Server port – the number of TCP port used during communication between the control panel and computer with GUARDX program.

Server key – a string of up to 12 alphanumeric characters (digits, letters and special characters) used for data encryption during communication between the control panel and the computer with GUARDX.

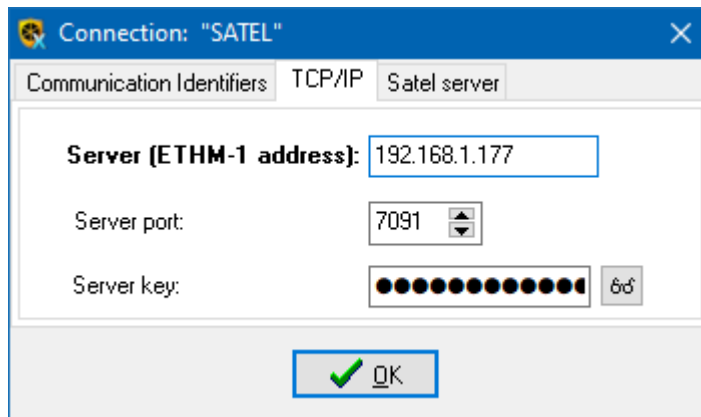


Fig. 20. GUARDX program: "TCP/IP" tab in "Connection" window.

"Satel sever" tab

The settings below apply to communication via the SATEL server.

Select the "ETHM-1 MAC" variant.

ETHM-1 MAC – hardware address of Ethernet module.

ETHM-1 ID – individual ID number assigned to the module by the SATEL server.

Server key – a string of up to 12 alphanumeric characters (digits, letters and special characters) used for data encryption during communication between the control panel and the computer with GUARDX.

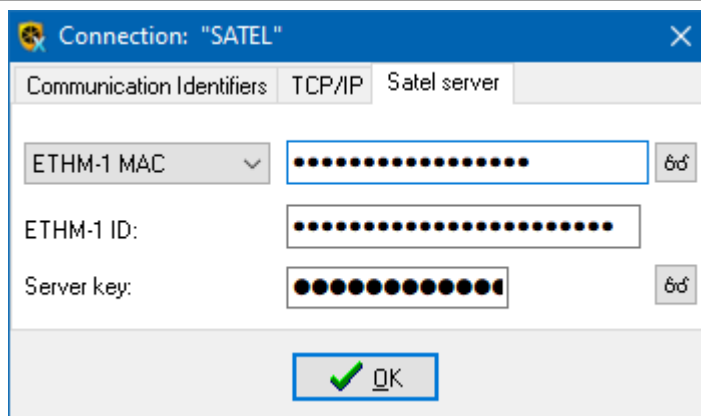


Fig. 21. GUARDX program: "Satel sever" tab in "Connection" window.

Initiating connection from GUARDX program

Required settings of the module:

- programmed number of TCP port used for communication.

Required settings of the GUARDX program for direct communication with the module:

- programmed: ETHM-1 Plus module address (*Server (ETHM-1 address)*), number of TCP port used for communication and data encryption key (*GUARDX key*).

1. In the startup window (Fig. 18), "Connection" field, select "TCP/IP: GUARDX->ETHM", and then click the "Start" button.
2. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

Initiating connection from keypad (through control panel)

Required settings of the module:

- programmed: address of computer with GUARDX program (*GUARDX server*) and number of TCP port used for communication.

Required settings of the GUARDX program for direct communication with the module:

- programmed: number of TCP port used for communication and data encryption key (*GUARDX key*).
1. In the startup window (Fig. 18), "Connection" field, select "TCP/IP: GUARDX<-ETHM/INT-GSM", and then click the "Start" button.
 2. Ask the user to 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. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

Initiating connection by SMS message

Required settings of the module:

- programmed: address of computer with GUARDX program (*GUARDX server*) and number of TCP port used for communication,
- programmed control command which, if sent in the SMS message, will initiate connection with the GUARDX program (*SMS initiating GUARDX connection*).

Required settings of the GUARDX program for direct communication with the module:

- programmed: number of TCP port used for communication and data encryption key (*GUARDX key*).
1. In the startup window (Fig. 18), "Connection" field, select "TCP/IP: GUARDX<-ETHM/INT-GSM", and then click the "Start" button.
 2. Send to the INT-GSM / INT-GSM LTE module the following SMS message:
xxxx= ("xxxx" – the control command to initiate establishment of communication with GUARDX program) – the module is to connect to the computer address programmed in the module,
xxxx=aaaa:p= ("xxxx" – the control command to initiate establishment of communication with GUARDX program; "aaaa" – address of the computer with GUARDX program (IP address or domain name); "p" – TCP port) – the module is to connect to the computer whose address has been given in the SMS message and use for communication the TCP port given in the SMS message.
 3. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

Establishing connection via the SATEL server

Required settings of the module:

- enabled *Connection via Satel server* option.

Required settings of the GUARDX program for communication via the SATEL server:

- programmed: ID number assigned to the module by the SATEL server (*ETHM-1 ID*), MAC address of the module (*ETHM-1 MAC*) and data encryption key (*Server key*).

1. In the startup window (Fig. 18), “Connection” field, select “TCP/IP: SATEL server”, and then click the “Start” button.
2. In the window that will be displayed after establishing communication, enter the code of administrator / user of the control panel.

7.1.2 Web browser

Required settings of the module:

- enabled WWW option,
- programmed data encryption key (*GUARDX key*),
- programmed the number of TCP port which will be used for communication with the web browser (*WWW port*),
- programmed the number of TCP port which will be used for communication with the JAVA application in the web browser (*Port*).

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



It is recommended that the 32-bit version of Java Virtual Machine be installed.

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. 22), enter in the corresponding fields:
 - data encryption key (*GUARDX 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),

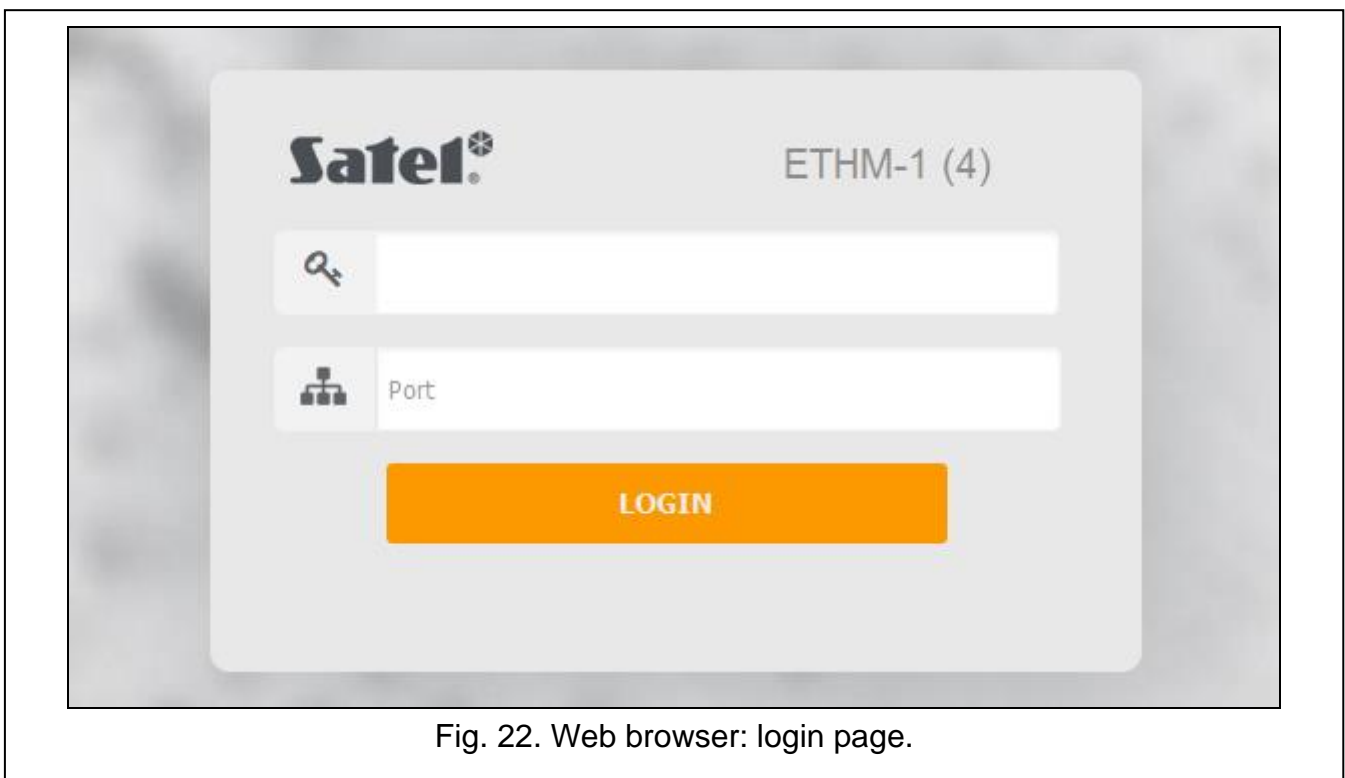


Fig. 22. Web browser: login page.

4. Click "LOGIN".
5. The virtual keypad will be displayed in the browser (Fig. 23).



Fig. 23. Web browser: virtual keypad.

7.1.3 INTEGRA CONTROL application

The INTEGRA / INTEGRA Plus alarm system can be operated and configured from a mobile device, if the INTEGRA CONTROL application is installed. If the IP cameras are installed in the protected premises, in the application you can watch video from these cameras.

The application can be downloaded from the internet store "Google play" (Android system devices) or "App Store" (iOS system devices). On the www.satel.eu website, you will find links to the locations from which the applications can be downloaded.

The INTEGRA CONTROL app can connect directly to the ETHM-1 Plus module (the module must have a public IP address) or establish connection via the SATEL server (Connection Setup Service – the module requires no public IP address).


Required module settings for both ways of establishing connection:

- enabled *INTEGRA CONTROL* option,
- programmed data encryption key (*GUARDX* key),
- enabled *Connection via Satel server* option, if connection is to be established via the SATEL server,
- programmed the number of TCP port which will be used for communication, if connection is to be established directly with the module.

To configure settings for communication via SATEL server in the INTEGRA CONTROL app, you can use the QR code (see p. 12). If the communication settings are configured in one mobile device, you can easily copy them to another mobile device. You just need to display the QR code on the device in which the settings for communication with the given module are already configured and read it on another device.

Programming the settings in INTEGRA CONTROL application (Android)

When you launch the application for the first time, the screen for adding a control panel will be displayed. It allows you to configure the settings required for establishing connection to the control panel.

1. Configure the communication settings. You can enter the settings manually (see “Adding communication settings manually”) or import them by using a QR code (see “Importing communication settings by using a QR code”).
2. Enter the name for alarm system. The name helps to identify the system when the application is in use (you can define settings for multiple alarm systems).
3. If you want to watch video from IP cameras in the application, enter the addresses of cameras. If you do not want to use the application to watch video from IP cameras, skip this step. You can add new IP cameras or change the settings for cameras already added at any time while using the application.
4. Define the language of the alarm control panel.
5. Define how the macro commands should be handled. Default settings provide for importing macro commands from the module (they will be downloaded during the first connection). If the macro commands are not to be imported or are to be imported from file, touch the screen in the “Macros” area and change the settings. If you select import from file, you will have to indicate location of the file containing macro commands.
6. Tap  to save settings.

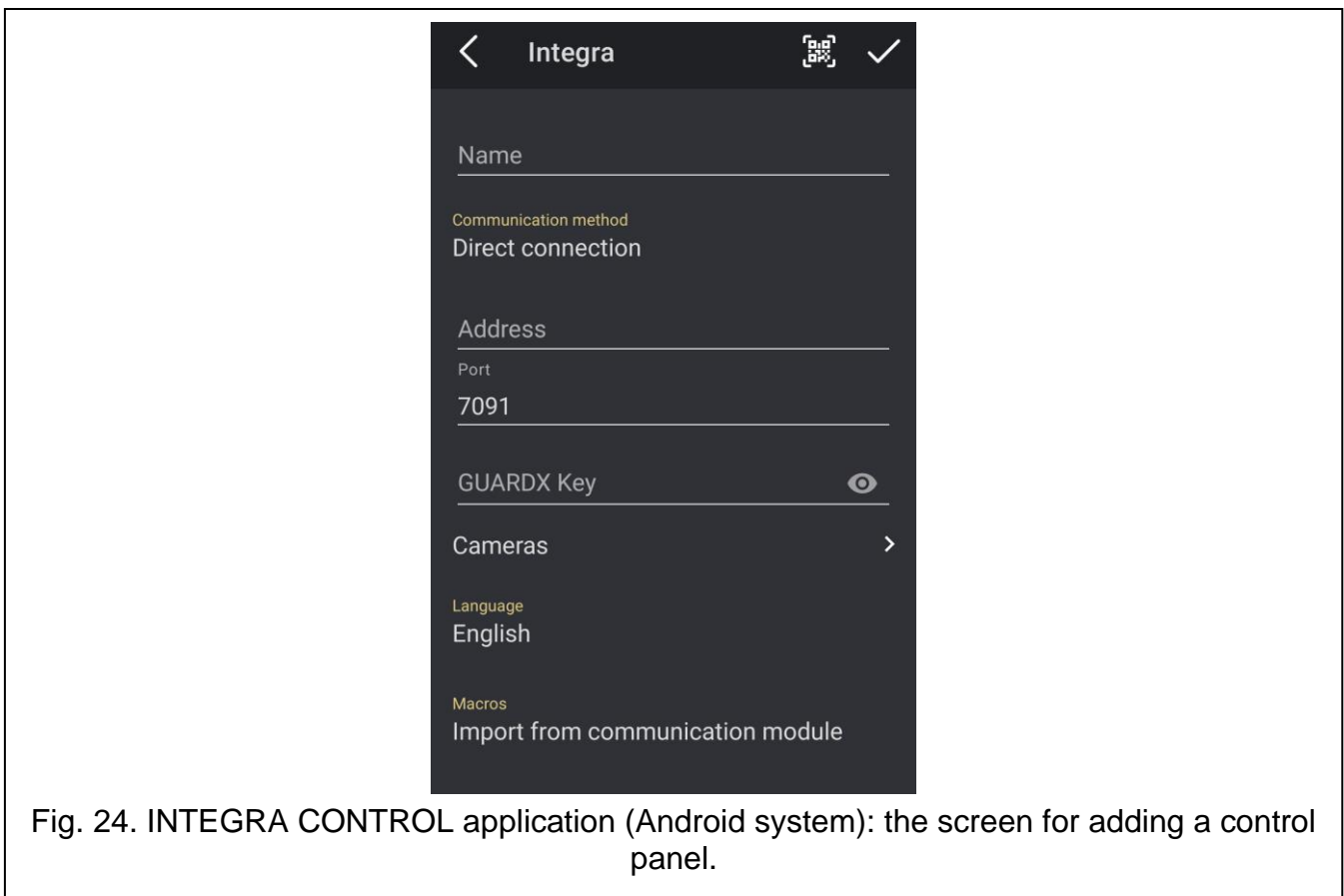


Fig. 24. INTEGRA CONTROL application (Android system): the screen for adding a control panel.

Adding communication settings manually



The alarm system user can use the LCD keypad to find the data required to configure communication settings (IP/MAC/IMEI/ID user function available in the TESTS submenu – see the control panel user manual).

Direct communication with the module

1. Select the “Direct connection” communication method.
2. Enter the module’s network address.
3. Enter the number of TCP port.


4. Enter the data encryption key – the same as in the module (*GUARDX* key).

Communication via the SATEL server


1. Select the “Connection via SATEL server using MAC address” communication method.
2. Enter the module’s MAC address.
3. Enter the module’s ID number (identifier assigned to the module by the SATEL server).
4. Enter the data encryption key – the same as in the module (*GUARDX* key).

Importing communication settings by using a QR code

Scanning the QR code with a camera

1. Tap .
2. Tap “Scan QR code”.
3. Allow the application to access the camera.
4. Scan the QR code.
5. Enter the password for the QR code and tap “OK”.

Importing the QR code from a file

1. Tap .
2. Tap “Select an image”.
3. Allow the application to access files on the mobile device.
4. Select the image with QR code.
5. Enter the password for the QR code and tap “OK”.

Programming the settings in INTEGRA CONTROL application (iOS)

When you launch the application for the first time, the “Objects” screen will be displayed.

1. Tap “New”. The screen for adding a control panel will be displayed.
2. Configure the communication settings. You can enter the settings manually (see “Adding communication settings manually”) or import them by using a QR code (see “Importing communication settings by using a QR code”).
3. Enter the name for alarm system. The name helps to identify the system when the application is in use (you can define settings for multiple alarm systems).
4. Define the language of the alarm control panel.
5. Define how the macro commands should be handled. Default settings provide for importing macro commands from the module (they will be downloaded during the first connection). If the macro commands are not to be imported or are to be imported from file, touch the screen in the “Import macros” area and change the settings.
6. If you want to watch video from IP cameras in the application, enter the addresses of cameras. If you do not want to use the application to watch video from IP cameras, skip this step. You can add new IP cameras or change the settings for cameras already added at any time while using the application.
7. Tap “Save” to save the settings.

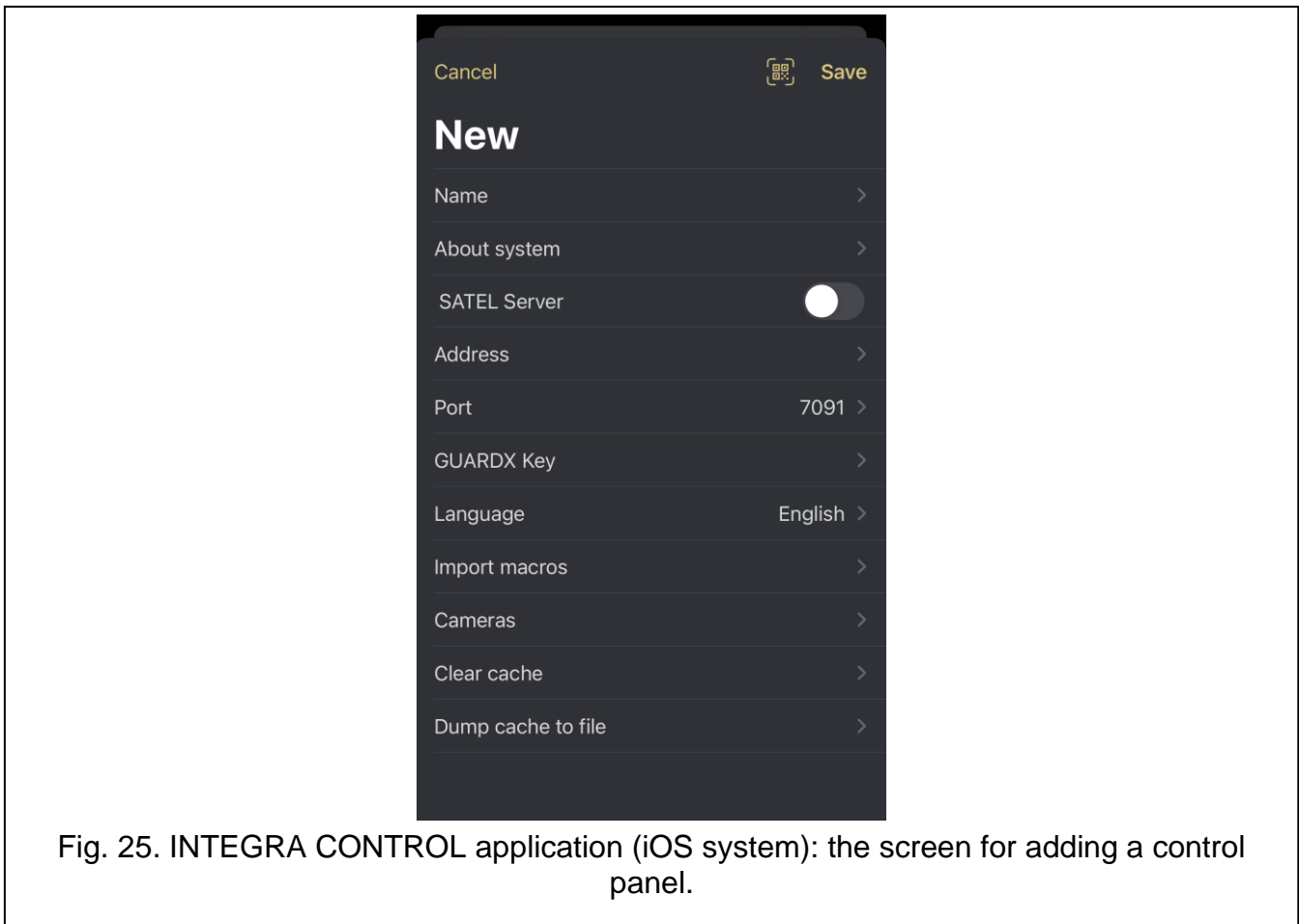


Fig. 25. INTEGRA CONTROL application (iOS system): the screen for adding a control panel.

Adding communication settings manually



The alarm system user can use the LCD keypad to find the data required to configure communication settings (IP/MAC/IMEI/ID user function available in the TESTS submenu – see the control panel user manual).


Direct communication with the module

1. Enter the module's network address.
2. Enter the number of TCP port.
3. Enter the data encryption key – the same as in the module (*GUARDX key*).

Communication via the SATEL server

1. Enable the "Server Satel" option.
2. Enter the module's MAC address.
3. Enter the module's ID number (identifier assigned to the module by the SATEL server).
4. Enter the data encryption key – the same as in the module (*GUARDX key*).

Importing communication settings by using a QR code

1. Tap .
2. Allow the application to access the camera.
3. Scan the QR code.
4. Enter the password for the QR code and tap "OK".

Establishing the communication

Tap the name of the alarm system. After communication with the control panel is established, the application will ask you to enter the user code. After you enter the code, the “Macros” screen will be displayed (in the iOS system you can define, which screen will be displayed as the first one after the next communication is established).

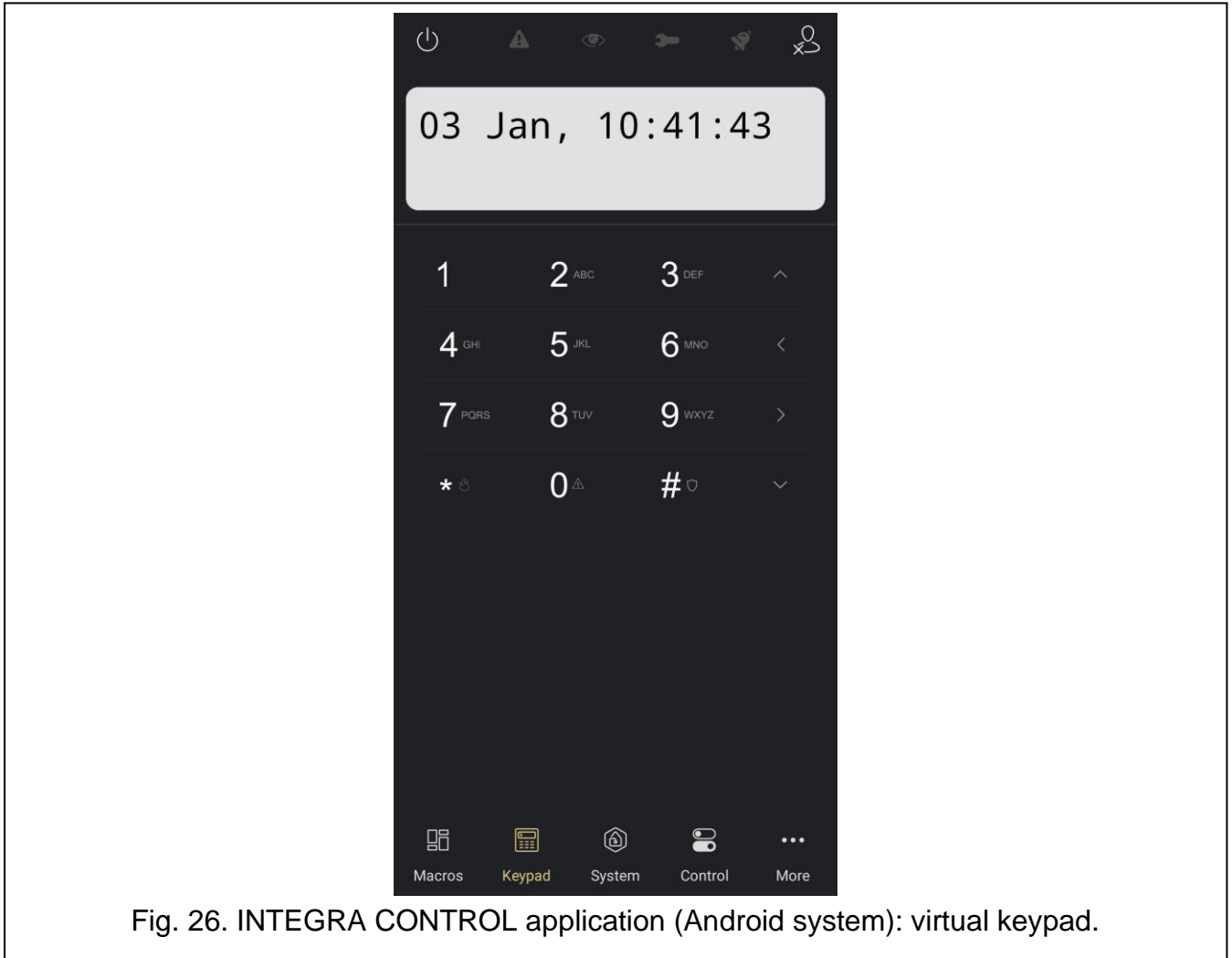


Fig. 26. INTEGRA CONTROL application (Android system): virtual keypad.

7.2 PERFECTA 64 M system

The Ethernet communication can be used to:

- program the alarm system in the PERFECTA Soft program,
- operate the alarm system in the PERFECTA CONTROL mobile app.

For information on how to program the alarm system remotely using the PERFECTA Soft program, please refer to the control panel programming manual.

For information on the PERFECTA CONTROL app, please refer to the control panel user manual.



Ethernet is the primary communication path. The cellular data network is used as a backup communication path.

7.3 VERSA system

The Ethernet communication can be used to:

- program the alarm system in the DLOADX program,

- operate the alarm system in the VERSA CONTROL mobile app.

For information on how to program the alarm system via Ethernet using the DLOADX program, please refer to the control panel programming manual.

For information on the VERSA CONTROL app, please refer to the control panel user manual.

8 Specifications

Supply voltage	12 VDC \pm 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 \pm 3%
Dimensions	68 x 140 mm
Weight.....	64 g