MONITORING STATION
STAM-2

USER MANUAL

CE

STAM-2 BS

Program STAM-2
(licencja na 3 stanowiska),
sprzętowy klucz zabezpieczający

STAM-2 software
(3 workstations license),
protection dongle

STAM-2 BE

Zestaw: Karta STAM-1 PE,
Program STAM-2
(licencja na 3 stanowiska),
sprzętowy klucz zabezpieczający

Hardware bundle: STAM-1 PE
receiver card, STAM-2 software
(3 workstations license),
protection dongle

STAM-2 BT

Zestaw: Karta STAM-1 P,
Program STAM-2
(licencja na 3 stanowiska),
sprzętowy klucz zabezpieczający

Hardware bundle: STAM-1 P
receiver card, STAM-2 software
(3 workstations license),
protection dongle

The dongle number,
required to register this software with the Manufacturer:

Minimum hardware requirements for the monitoring station server:

- computer with installed Microsoft Windows 2000 or Microsoft Windows XP operating system
- Pentium II 400 MHz processor
- 128 MB RAM
- CD-ROM
- free PCI slot
- free serial COM port
- free USB port
- monitor with 1024 x 768 resolution support

Minimum hardware requirements for the monitoring station client:

- computer with installed Microsoft Windows 98 SE, Microsoft Windows Millennium Edition (ME), Microsoft Windows 2000 or Microsoft Windows XP operating system (Microsoft Windows 2000 or Microsoft Windows XP recommended)
- Pentium II 400 MHz processor
- 128 MB RAM
- CD-ROM
- monitor with 1024 x 768 resolution support

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

CONTENTS

The STAM-2 is an advanced solution offered to the companies engaged in the business of monitoring signals derived from security alarm systems. The STAM-2 monitoring station consists from cards installed in the computer, as well as software which enables management of the signals received by modules. It is possible to receive transmissions sent through telephone line, Ethernet (TCP/IP) or GSM (SMS and CLIP) networks. The STAM-2 program works in WINDOWS environment. It is a client-server type of application which enables incoming events to be handled by some operators on a number of workstations.

1. MONITORING STATION FEATURES

- easy-to-install cards
- optional expansion of the station by adding more cards
- receiving transmissions sent via telephone line, Ethernet (TCP/IP) network or GSM (SMS) network
- detecting telephone line defect (telephone receiver cards), no network cable or communication with Ethernet module (Ethernet receiver cards)
- compatible with:
    - GSM-4 and GSM LT-1 modules (manufactured by SATEL)
    - VISONIC RC-4000 radio station
- automatic recognition of one of the following transmission formats:
    - Silent Knight, Ademco slow
    - Sescoa, Franklin, DCI, Vertex
    - Silent Knight fast
    - Radionics 1400 Hz
    - Radionics 2300 Hz
    - Radionics with parity 1400 Hz
    - Radionics with parity 2300 Hz
    - Ademco Express
    - Silent Knight, Ademco slow - extended
    - Sescoa, Franklin, DCI, Vertex - extended
    - Silent Knight fast - extended
    - Radionics 1400 Hz - extended
    - Radionics 2300 Hz - extended
    - Contact ID (CID)
- user friendly STAM-2 software, working in WINDOWS environment
- client-server type of application which enables incoming events to be handled by several operators on a number of workstations
- smart distribution of events between workstations
- encrypted client-server communication
- monitoring station data stored in an encrypted database file
- defining the program user authority levels
- simplified work of the monitoring station program operator:
    - selection of intervention requiring events
    - list of program user required actions

- − storing program user reactions in memory
- − reminder of unhandled events
- saving major operations of the system users into event log
- reporting situations which require intervention:
  - − alarm
  - − trouble (including lack of test transmission or transmission at wrong time)
  - − check for site status correctness (armed, disarmed)
- status overviews of supervised sites:
  - − alarm reporting systems
  - − trouble reporting systems – possible verification of troubles occurring in the system
  - − armed systems – in case of bigger sites: a list of armed partitions
  - − status of communication with the systems
- unlimited number of subscribers
- detailed subscribers' data:
  - − up to a dozen or so identifiers of different types
  - − any number of information drawings (BMP, JPG, GIF or PNG files)
  - − decode tables (each code meaning and event description)
  - − priority differentiation – order of reporting events which require intervention when events are incoming simultaneously from many subscribers
  - − patterns of action in case of events which require intervention in partition – up to 5 items
- extended event filtering
- system of notes:
  - − information exchange between users
  - − defined validity period
  - − automatic display option
- printing documentation regarding subscribers, reports for subscribers, reports on program users and station system in PDF format

2. CARD DESCRIPTION

The card is a complete receiver of data sent by the control panels which enables a supervision center to be organized for monitoring the security system status. It can be installed on board of any PC computer (PCI slot), deriving only +12V power supply and RESET signal from the computer. It is capable of working without the computer, if power supply of approx. +12...15V is provided. The RESET signal is only necessary for operation with the use of computer.

SATEL offers the following cards:

STAM-1 P – base telephone receiver card (available in STAM-2 BT bundle);

STAM-1 R – expansion telephone receiver card;

STAM-1 K – expansion telephone termination receiver card for connecting mimic boards;

STAM-1 PE – base Ethernet receiver card (available in STAM-2 BE bundle);

STAM-1 RE – expansion Ethernet receiver card ;

Each telephone receiver card means that it is possible to connect the telephone line, i.e. assign 1 telephone number to the monitoring station. Also, connecting the GSM module to

the COM port of the computer denotes that 1 additional telephone number is assigned to the station. Each Ethernet receiver card means that it is possible to assign 1 IP address to the monitoring station.

The card selection depends on what method of data transmission is used. The cards can be connected with each other, which enables the monitoring station to support different transmission methods and increase the number of telephone lines / IP addresses. The STAM-2 monitoring station may comprise up to 16 interconnected cards (base receiver card + 15 expansion receiver cards of various types). Also, when GSM modules are connected to the computer COM ports, the total number of supported cards and GSM modules is 16.

The STAM-1 K card accepts the **STAM-1 PTSA** mimic boards which enable visualization of the status of monitored sites by means of LED indicators. One mimic board makes it possible to visualize the status of 64 objects. Additional mimic boards must be used for a greater number of objects. Altogether, 63 mimic boards can be used for 1 monitoring station, which means 4032 visualized objects.
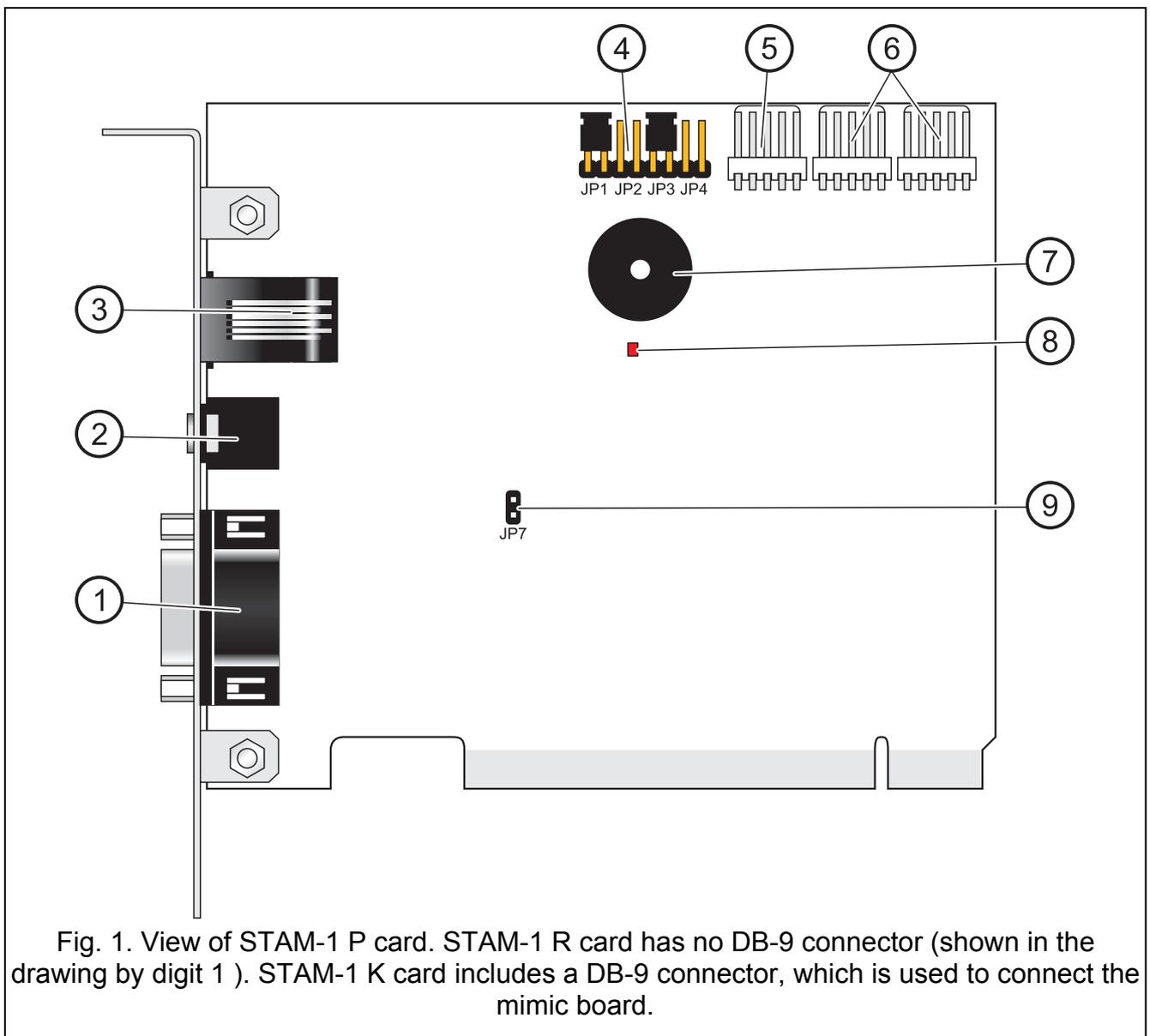

Fig. 1. View of STAM-1 P card. STAM-1 R card has no DB-9 connector (shown in the drawing by digit 1). STAM-1 K card includes a DB-9 connector, which is used to connect the mimic board.

Explanations for Fig. 1:

1 – DB-9 male connector (RS-232 port) which enables the card to be connected to the computer COM port.

2 – headset mini-jack socket to enable telephone line eavesdropping by means of high-resistance loudspeaker or headset.

3 – RJ-11 socket for connecting telephone line.

4 – card address setting pins (see: Addressing cards).

5 – connector for additional control signaling.

6 – connectors for expansion receiver cards (RS-232 and sound for telephone receiver cards).

7 – buzzer.

8 – LED indicator. Lit during connection.

9 – pins to enable/disable telephone line eavesdropping.
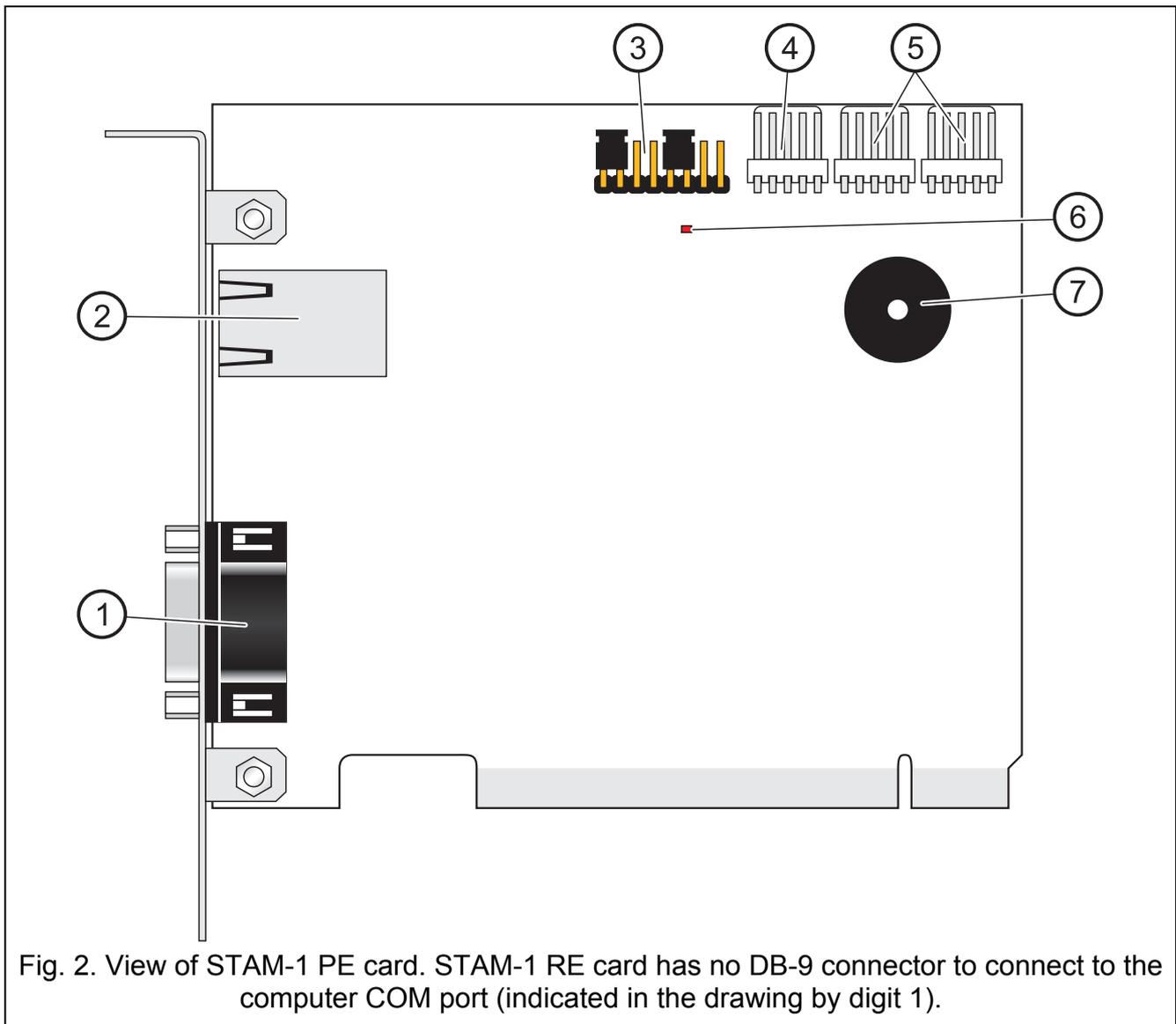
Fig. 2. View of STAM-1 PE card. STAM-1 RE card has no DB-9 connector to connect to the computer COM port (indicated in the drawing by digit 1).

Explanations for Fig. 2:

1 – DB-9 male connector (RS-232 port) which enables the card to be connected to the computer COM port.

2 – RJ-45 socket for connecting the Ethernet network. The socket incorporates two LEDs. The green one indicates network connection and transmission, and the yellow one - network transmission rate (OFF: 10Mb / ON: 100Mb).

3 – card address setting pins (see: ADDRESSING CARDS).

4 – connector for additional control signaling.
5 – connectors for expansion receiver cards (RS-232 and sound for telephone receiver cards).
6 – LED indicator.
7 – buzzer.

3. ADDRESSING CARDS

An individual address must be set for each installed card. The addresses may not be used repeatedly. To set an address, use the pins (see Figures 1 and 2). The pin pairs are designated JP1, JP2, JP3 and JP4. Addressing is carried out by means of jumpers placed on the pins. The pins allow setting addresses from 0 to 15 (in hexadecimal mode: from 0 to F). In order to determine the address of a card, add up the values set on consecutive pin pairs, according to Table 1.

Pin pair	JP1	JP2	JP3	JP4
Numerical value (after setting the jumper)	1	2	4	8

Table 1.

4. INSTALLING CARDS

⚠ **Prior to installation of a card in the computer, disconnect the computer from the source of power supply.**

In order to install the STAM-1 P or STAM-1 PE card in the computer:

1. Set the card address (see: ADDRESSING CARDS).
2. Open the computer case.
3. Install the card in PCI slot.
4. Close the computer case.
5. Using the cable included in the bundle, connect the card DB-9 connector to the computer serial COM port.
6. Connect the telephone line (STAM-1 P card) or network cable (STAM-1 PE card) to the card socket.

In order to install the STAM-1 R, STAM-1 K or STAM-1 RE extension card in the computer:

1. Set the card address (see: ADDRESSING CARDS).
2. Open the computer case.
3. Install the card in PCI slot.
4. Using the cable delivered with the expansion card, connect the card to the base receiver card or another expansion card.
5. Close the computer case.
6. Connect the telephone line (STAM-1 R and STAM-1 K cards) or network cable (STAM-1 RE card), or, optionally, the mimic board (STAM-1 K card) to the extension card.

If the card is to be installed outside the computer, proceed in the same way as described above, skipping the steps which refer to installation of the card in computer PCI slot.

5. PROTECTION DONGLE

Installation of the STAM-2 server program is impossible without the protection dongle (hardware key). Having installed the server program, leave the dongle in the USB port. If the dongle is removed for more than 30 minutes, it will be unregistered and functionality of the monitoring station will be limited. Such functions as editing subscribers and users accounts, creating reports and configuring the server will be unavailable. 2 weeks after unregistering the dongle, the monitoring station program will stop working.

> ⚠️ **If your dongle gets damaged, please contact the SATEL Company. Replacement is possible after you return the damaged dongle and pay a small handling charge.**
>
> **The SATEL Company shall not be held responsible for lost or stolen dongles. If you loose your dongle, you must be prepared for high costs connected with delivery of a new one.**

6. STAM-2 PROGRAM INSTALLATION

Insert the CD with installation program into the CD-ROM drive. The welcome screen should appear in a while. Click on the command of chosen program installation and follow the instructions.

If the splash screen fails to appear after the disk is inserted into the CD-ROM drive, the autostart function of your CD-ROM must have been disabled. If this is the case, click twice on the „My computer" icon and, after the resource window opens, on the CD-ROM icon. There is the **SetupStam2.exe** file on the installation disk. Open it, e.g. by clicking on it twice, to bring up the splash screen.
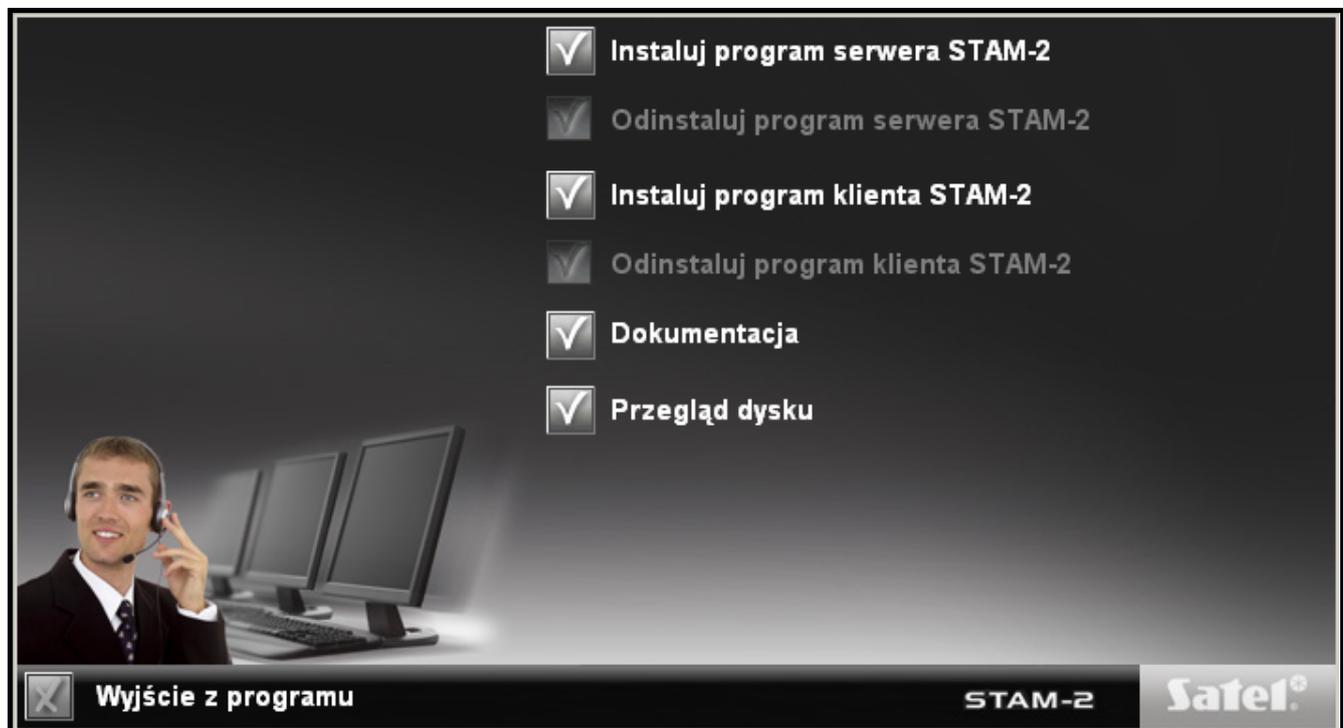

Fig. 3. Welcome screen of the installation package.

6.1 INSTALLATION OF STAM-2 SERVER PROGRAM

The server program should be installed on a computer to the serial COM port of which the STAM-1 P or STAM-1 PE card is connected. If the server program finds no STAM-1 P or STAM-1 PE card within a few minutes after being started, it will be terminated.

To begin installation, click on the „Install STAM-2 server program" command. During installation, the protection dongle must be inserted into the computer USB port.

At installation stage, the users of STAM-1 monitoring station can import data from the program. To do so, you must select the option „I have STAM-1 installed and want to import data from it" (see Fig. 4), and then indicate the folder where the STAM-1 program is installed.
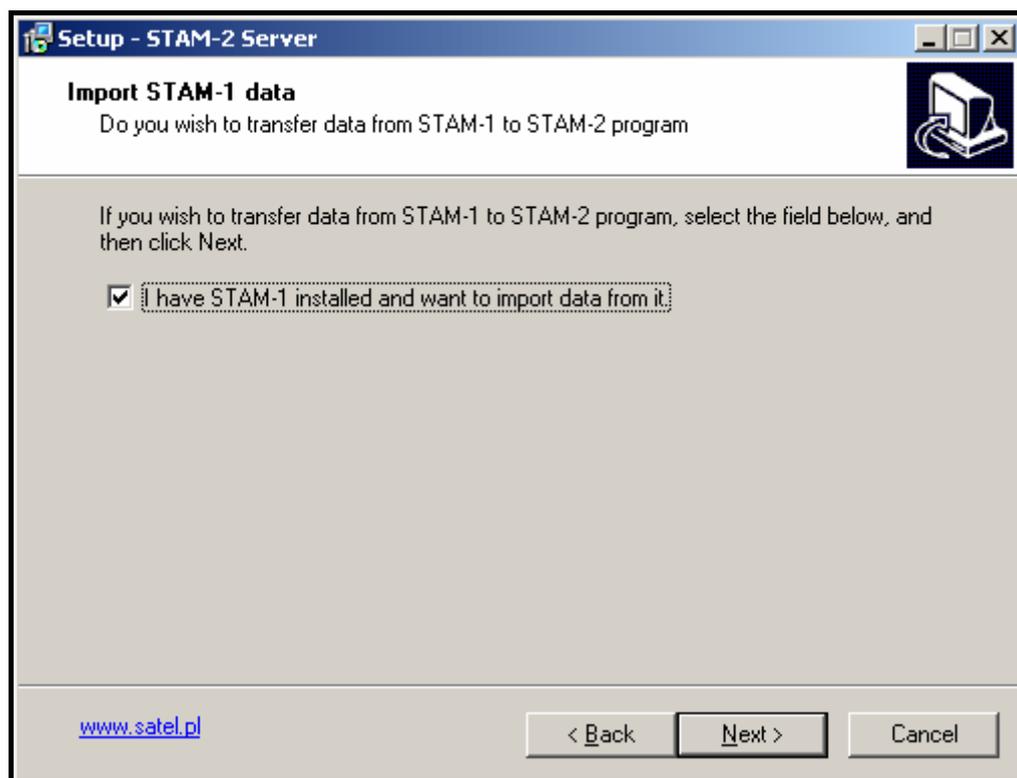
Fig. 4. Importing STAM-1 program data.

Notes:

- *The database of STAM-1 monitoring station can only be imported during installation.*
- *The database of STAM-2 monitoring station cannot be exported or imported.*

The STAM-2 monitoring station needs to be registered within 31 days of the server program installation. After expiry of this period, the server program will stop working. The server installer program offers optional registration at the end of installation procedure. Registration is also possible at a later date on the website www.stam2.satel.pl or by using the form included in the bundle. When filled in, the form should be sent by fax to the number 0-58 320 94 01. After registration, SATEL will send a license file to the e-mail address, or to the mailing address (in case of regular postal mail). Installation of the license file will enable the server program to be used without any time limitations.

6.2 INSTALLATION OF STAM-2 CLIENT PROGRAM

Installation of the client program is possible on the same computer on which the server program has been installed. In addition, it may be installed on any number of workstations, however the server program can support up to 3 or up to 10 clients, depending on the license held.

To begin installation, click on the „Install STAM-2 client program" command. The Java Virtual Machine is required for the client program to be operable, hence the option of its installation is enabled by default (see Fig. 5).
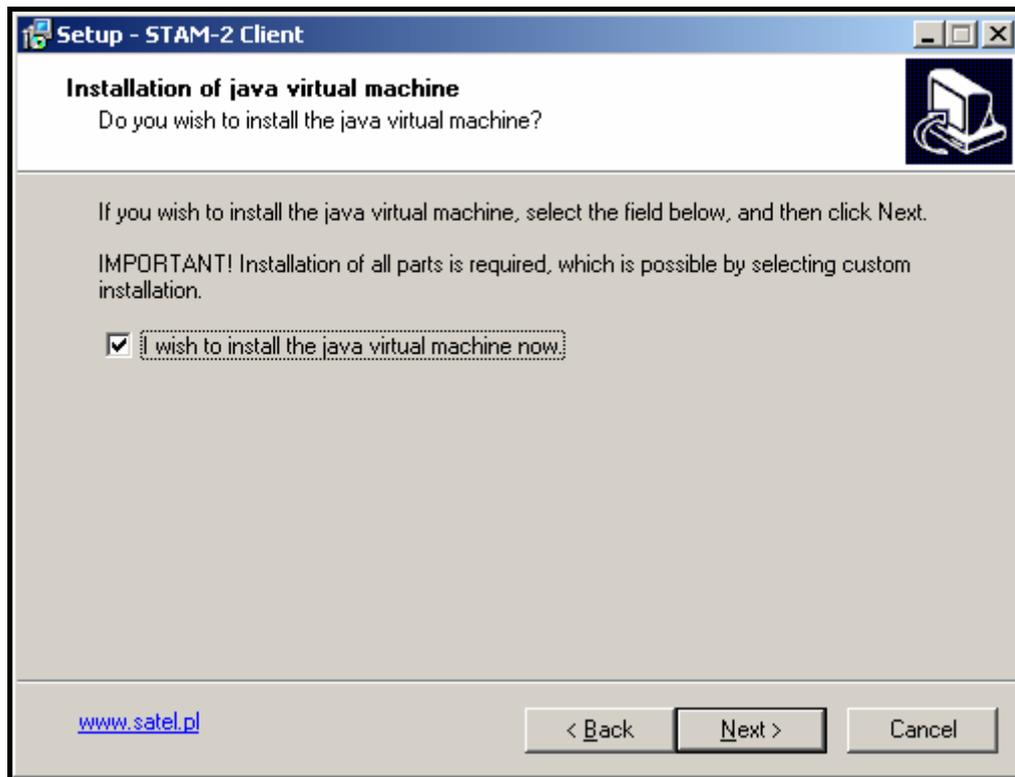
Fig. 5. Installation of Java Virtual Machine.

Installation of the Java Virtual Machine will begin after client program files have been installed. When choosing the installation type, select the „Custom setup" (see Fig. 6).
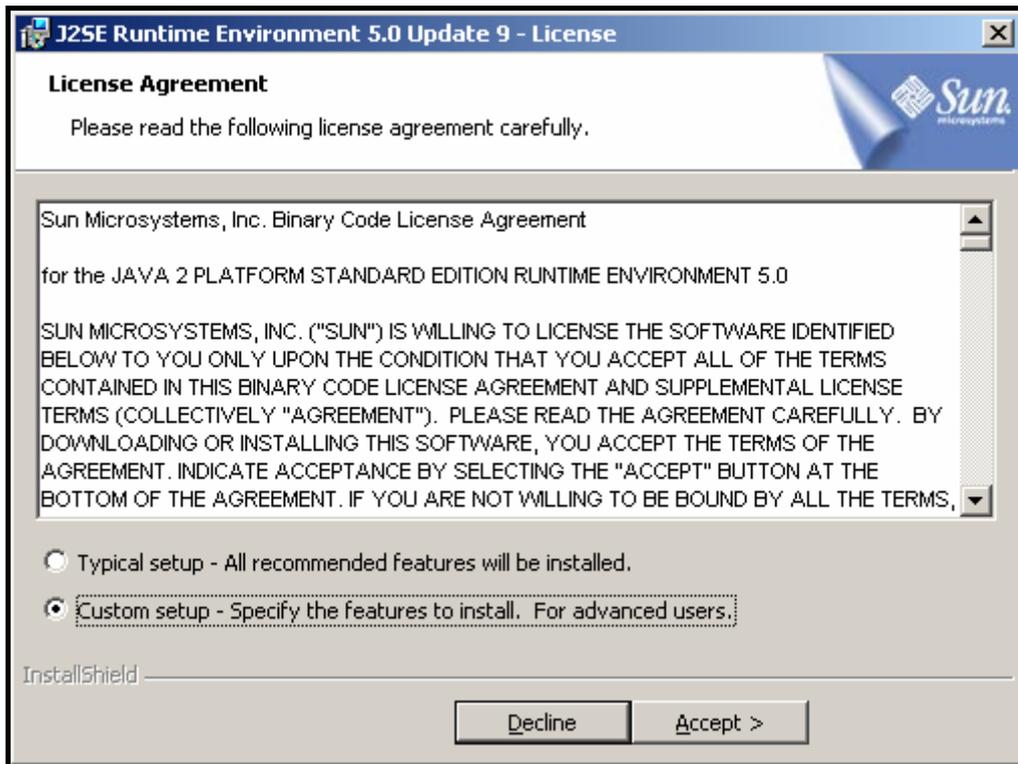
Fig. 6. Selecting installation type of Java Virtual Machine.

All available components of the Java Virtual Machine must be installed on the computer hard disk (see Fig. 7).
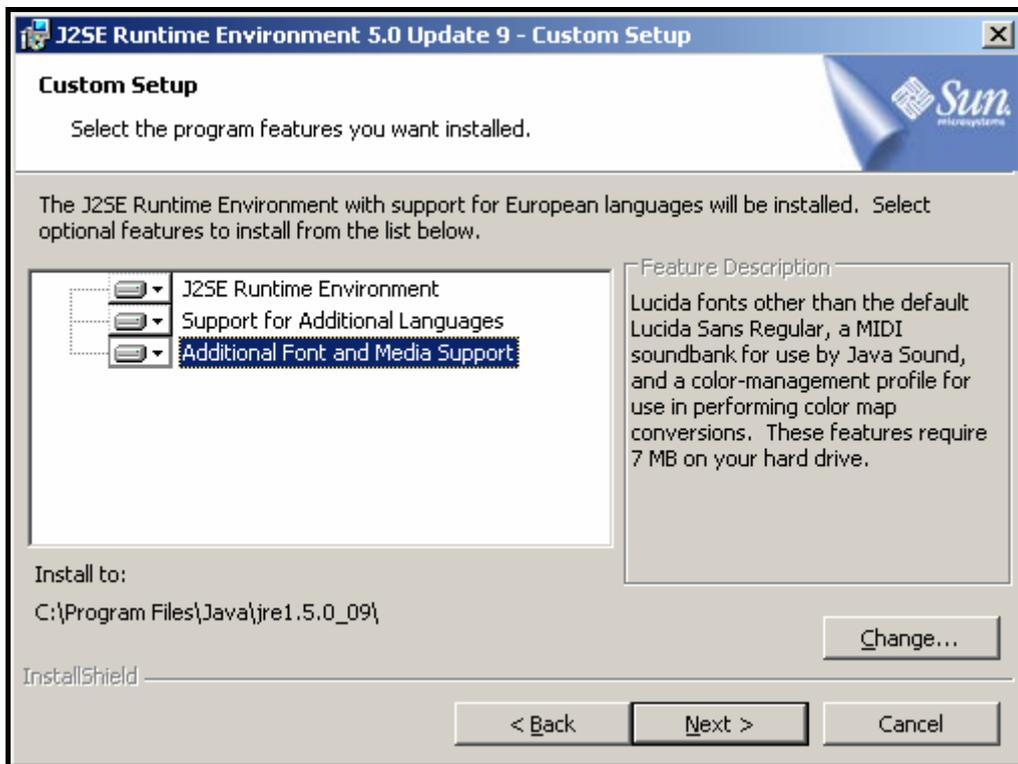
Fig. 7. Components of Java Virtual Machine installed on the computer hard drive.

7. OPERATION AND PROGRAMMING OF STAM-2 MONITORING STATION

⚠️ **The STAM-2 server program works as an ordinary application and starts after logging into the system.**

You can terminate the server program manually and then restart it. In order to terminate the server program manually, you must:

1. Hover the cursor over the server icon displayed on the system taskbar.
2. Press the right mouse button – a menu will appear.
3. Highlight the „Exit" item and press the left mouse button.
4. A window will be displayed. Enter your login and password in the window and then press the „OK" button.

Configuration of the STAM-2 server and operation of the monitoring station can be effected by means of the STAM-2 Client program.

7.1 FIRST TIME RUN OF CLIENT PROGRAM

After starting the STAM-2 Client program, the login window will open (see Fig. 8).
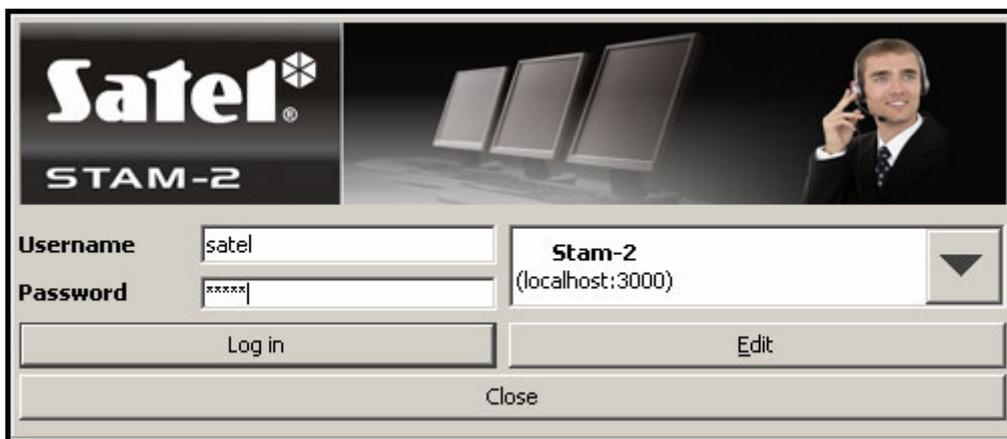
Fig. 8. STAM-2 program login window.

⚠️ **As the program is case-sensitive, make sure when logging in, that the Caps Lock has not been accidentally activated.**

7.1.1 CLIENT PROGRAM INSTALLED ON THE SAME COMPUTER AS SERVER PROGRAM

In order to log in, enter „satel" as the default password and click on the „Log in" button.

7.1.2 CLIENT PROGRAM INSTALLED ON A COMPUTER DIFFERENT FROM THAT WHERE SERVER PROGRAM IS INSTALLED

Before you log in, it is necessary to define the server parameters (address and TCP/IP port of the computer where the STAM-2 server program is installed). For this purpose, click your mouse on the „Edit" button. The „Servers" window will open, displaying the list of defined servers. You can define any number of servers for the client program to work with. By default, the „Stam-2" server is defined (see Fig. 9).
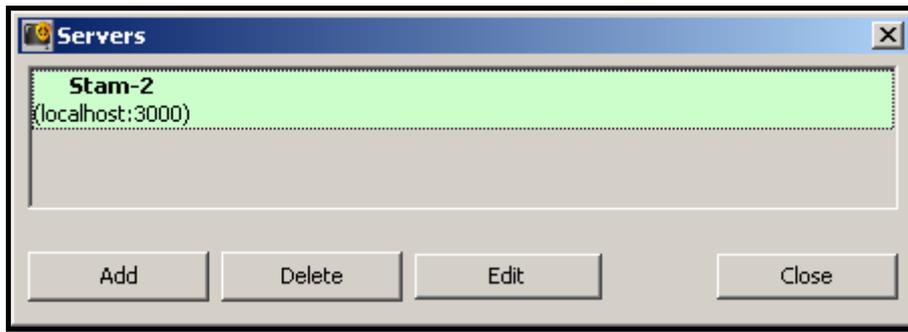
Fig. 9. „Servers" window on first-time run of the program.

Default parameters of the „Stam-2" server allow the user to log in when the STAM-2 Client program is run on the same computer as the STAM-2 Server program. You can edit the server settings (see Fig. 10) after clicking on the „Edit" button, or add a new server after clicking on the „Add" button.

Fig. 10. „Server" window for defining parameters of the server with which the client program is to work.

Having defined the server parameters, you can return to the login window. If the name of required server with which you want to communicate is not shown, click on the arrow at the server name. A dropdown list will appear, from which you should select the server the client program is to work with. If the name of required server is shown, enter the default password „satel" and click on the „Log in" button.

7.2 MAIN WINDOW OF STAM-2 CLIENT PROGRAM

After login procedure, the main window of the program will open (see Fig. 11).

Fig. 11. Main window of STAM-2 Client program

Explanations for Fig. 11:

1 Click on the icon to open a window with information on the STAM-2 program and SATEL Company, manufacturer of the program.

2 **Status board** (Alt+T) – Click on the icon (or press Alt+T) to open a window where the status of supervised sites can be checked (alarms, troubles, arm statuses, test transmissions). The window is available to all users.

3 **Event log** (Alt+H) – Click on the icon (or press Alt+H) to open the event log window. The window is available to users with the „viewing" authority level.

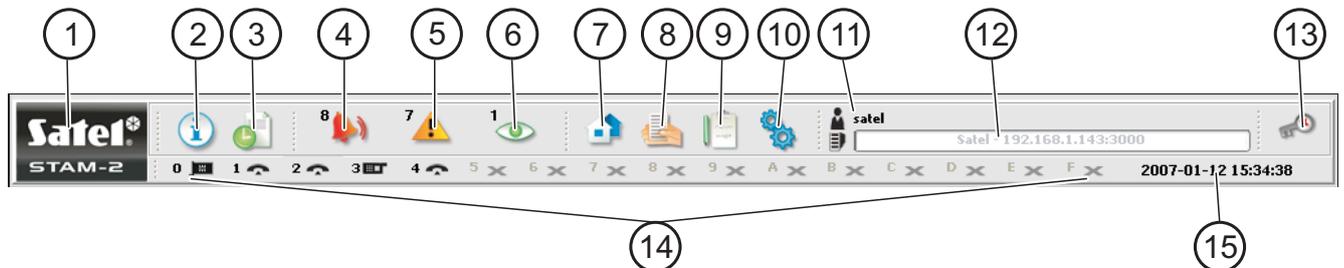**4** **Handle alarms** (Alt+1) – The icon is active when there are unhandled alarms. The number at the icon shows how many alarms are still unhandled by the user. Click on the icon (or press Alt+1) to display the windows of unhandled alarms, followed by unhandled troubles and arm status events. Available to users with the „handling" authority level.

5 **Handle troubles** (Alt+2) – The icon is active when there are unhandled troubles. The number at the icon shows how many troubles are still unhandled by the user. Click on the icon (or press Alt+2) to display the windows of unhandled troubles, followed by unhandled arm status events and alarms. Available to users with the „handling" authority level.

6 **Handle arm status events** (Alt+3) – The icon is active when there are unhandled arm status events. The number at the icon shows how many arm status events are still unhandled by the user. Click on the icon (or press Alt+3) display the windows of unhandled arm status events, followed by unhandled alarms and troubles. Available to users with the „handling" authority level.

7 **Subscribers** (Alt+A) – Click on the icon (or press Alt+A) to open the window where you can, depending on your authority level, view the list of current subscribers, edit the current subscribers, add new subscribers or remove the existing ones. The window is available to all users.

8 **Reports and documentation** (Alt+R) – Click on the icon (or press Alt+R) to open the window where you can print documentation regarding subscribers, subscriber's reports, reports on program users and station system in PDF format. The window is available to all users, but the scope of possible operations depends on the granted authority level.

9 **Notes** (Alt+N) – Click on the icon (or press Alt+N) to open the window where you can view notes created by other users or prepare notes for other user. Available to all users.

10 **Configuration** (Alt+K) – Click on the icon (or press Alt+K) to open the menu with the following functions:

Configure server (Alt+K) – The function intended to define the cards and other devices (GSM modules, VISONIC RC-4000 radio stations) supported by the STAM-2 program server. Available to users with the „server configuration " authority level.

User accounts (Alt+E) – The function makes it possible to view the list of program users, add new users, edit and/or remove the existing ones.

Available to users with the „user accounts" authority level.

Change password (Alt+P) – The function allows the currently logged in user to change the code of access to the STAM-2 program. Available to all users. It is recommended that each new user change his/her password so that the supervisor may not know the user password.

Mimic boards (Alt+S) – The function makes it possible to define the lighting mode of LEDs in the mimic boards interfacing with the monitoring station. Available to users with the „mimic boards" authority level.

11 User currently logged in

12 Data of monitoring station server.

13 Click on the icon (or press Alt+X) to open the menu with the following commands:

Log out user (Alt+L) – after the current user has logged out, a next one can log in.

Minimize (Alt+M) – minimizing the main window of the STAM-2 Client program.

Close (Alt+X) – closing the STAM-2 Client program.

14 The icons illustrate the monitoring station cards and GSM modules supported by the STAM-2 program server. They are designated by digits from 0 to 9 and letters from A to F. These characters correspond to the address of server supported card or device, saved in hexadecimal format. The icons have the following meaning:

- telephone card is working properly
- telephone card is receiving ring signal or is being configured
- telephone card has established connection with control panel
- telephone card is receiving data
- no telephone card, or trouble (to check the trouble details, refer to the „Event log" window)
- GSM module is working properly
- GSM module is receiving data (SMS or CLIP type message)
- no GSM module, or trouble (to check the trouble details, refer to the „Event log" window)
- Ethernet card is working properly
- Ethernet card is receiving data or is being configured
- no Ethernet card, or trouble (to check the trouble details, refer to the „Event log" window)

When the card is not currently connected, click on the telephone receiver card icon to go off hook. When the card connection is currently ongoing, click on the telephone receiver card icon to hang up.

A grayed out icon means that no card / device has been defined for the given address.

15 Current date.

7.3 SERVER CONFIGURATION

The first operation to be carried out after starting the monitoring station program for the first time and logging in, is configuration of the server. In order to configure the server, you must, first of all, define the devices that are to be supported by the monitoring station program. The „Cards" tab in the „Configuration" window is provided for this purpose.

7.3.1 „CARDS" TAB

Fig. 12. „Cards" tab in „Configuration" window, before defining devices.

Address – the address set in the card or assigned by default to another device (GSM module or VISONIC RC-4000 radio station). It is given in hexadecimal format (for the ease of use, decimal values are given in brackets). It is recommended that you only select boxes next to the addresses which are set in the connected cards, or to which other devices are to be assigned.

Port – the serial COM port of the computer to which the device supported by the monitoring station program is connected. Editing is possible when the adjacent „Address" box is checked.

Device – the type of device connected to the computer COM port (STAM-1 card, GSM module, VISONIC RC-4000 radio station). Editing is possible when the adjacent „Address" box is checked.

Buzzer – if this option is enabled and an event is received by the card, the card buzzer will generate an additional audible signal, irrespective of the sounds generated by the computer. The option only refers to the STAM-1 cards. Available after adding cards (automatically or manually).

Time – enter in this field the maximum time interval counted from the unsuccessful attempt of the control panel to establish connection with the monitoring station (a ring was received, but no event was received). If more failed connection attempts occur during this time and reach the number defined in the „Attempts" field, the „Failed monitoring attempt" event will be registered. If the last monitoring attempt was made by means of the DTMF system and the control panel identifier has been sent, it will be shown at the event. If the preset number of failed monitoring attempts does not occur within the defined period of time, the time counter will be reset. After another unsuccessful attempt, the time will be counted anew. Values from 0 to 255 minutes can be entered in the „Time" field. Entering 0 will disable control of the unsuccessful attempts to connect to the monitoring station. The option refers to the STAM-1 P, STAM-1 R and STAM-1 K cards. Editing is possible after cards have been added (automatically or manually).

Attempts – enter in this field the number of failed monitoring attempts which, if occur within the time period defined in the „Time" field, will result in registering the „Failed monitoring attempt" event. If the last monitoring attempt was made by means of the DTMF system and the control panel identifier has been sent, it will be shown at the event. If the preset number of failed monitoring attempts does not occur within the defined period of time, the time counter will be reset, and after another unsuccessful attempt, the time will be counted anew. Values from 0 to 255 minutes can be entered in the „Time" field. Entering 0 will disable control of the unsuccessful attempts to connect to the monitoring station. The option refers to the STAM-1 P, STAM-1 R and STAM-1 K cards. Editing is possible after cards have been added (automatically or manually).

Trouble – enter in this field the maximum time period in minutes, during which the card may receive no events. After expiry of this time, the card trouble will be reported. Values from 0 to 65535 minutes can be entered in the „Trouble" field. Entering 0 will disable control of the events receiving by the card. The option only refers to the STAM-1 cards. Editing is possible after cards have been added (automatically or manually).

Filter – enter in this field the time of filtering the card events in seconds. If several identical events are received within the defined time period (i.e. events with the same identifier and code), only the first event will be added to the event log, the other ones being omitted. Values from 0 to 2550 seconds can be entered in the „Filter" field. Entering 0 will disable the event filtering. The option only refers to the STAM-1 cards. Editing is possible after cards have been added (automatically or manually).

Ring – indicate in this field the number of rings after which the telephone receiver card is to go off hook. You can enter numbers from 1 to 9. The option refers to the STAM-1 P, STAM-1 R and STAM-1 K cards. Editing is possible after cards have been added (automatically or manually).

Information – information on the type of receiver card with the given address (TEL – telephone, TCP/IP – ethernet) or another device assigned to that address (GSM – GSM module, VISONIC – VISONIC RC-4000 radio station). Additionally, the device software version is shown. The information is displayed when the devices supported by the monitoring station program have been defined.

Config. – the button available for the STAM-1 PE and STAM-1 RE Ethernet cards and the GSM modules. Press it to open a window of extra settings (see: Additional configuration of STAM-1 PE and STAM-1 RE cards and Additional configuration of GSM modules).

Search – the button enabling automatic detection of cards connected to the computer serial COM ports (see: AUTOMATICALLY FINDING DEVICES).

Apply – the button making it possible to manually add devices supported by the monitoring station program (see: MANUALLY DEFINING DEVICES). The button becomes active on selecting the address for which the device is to be defined, or after deselecting the address to which the device was previously assigned.

AUTOMATICALLY FINDING DEVICES

The program can by itself find the cards connected to the computer serial COM ports. To do so, click on the „Search" button in the „Cards" tab of the „Configuration" window, and then select one of the 3 COM ports which is to be searched.

⚠️ **The program cannot automatically find the GSM modules and VISONIC RC-4000 radio stations.**

After the connected cards have been found, they must be appropriately configured.

MANUALLY DEFINING DEVICES

The program allows for manually adding all the supported devices. The GSM modules and VISONIC RC-4000 radio stations can only be added manually.

To manually define a device, do as follows:

1. Open the „Configuration" window, and the „Cards" tab in it.
2. Determine address of the device, checking the appropriate „Address" box. Select any unassigned address for the GSM modules and VISONIC RC-4000 radio stations, in which the address is not set.
3. Select the COM port to which the device is connected.
4. Select the type of device.
5. Click on the „Apply" button.
6. Define the „Buzzer", „Trouble" and „Filter" options for all cards. For the telephone receiver cards, determine the „Time", „Attempts" and „Ring" parameters. In case of the STAM-1 PE and STAM-1 RE cards and GSM modules, click on the „Config." button to configure additional parameters for these devices (see: ADDITIONAL CONFIGURATION OF STAM-1 PE AND STAM-1 RE CARDS and ADDITIONAL CONFIGURATION OF GSM MODULES).

ADDITIONAL CONFIGURATION OF STAM-1 PE AND STAM-1 RE CARDS
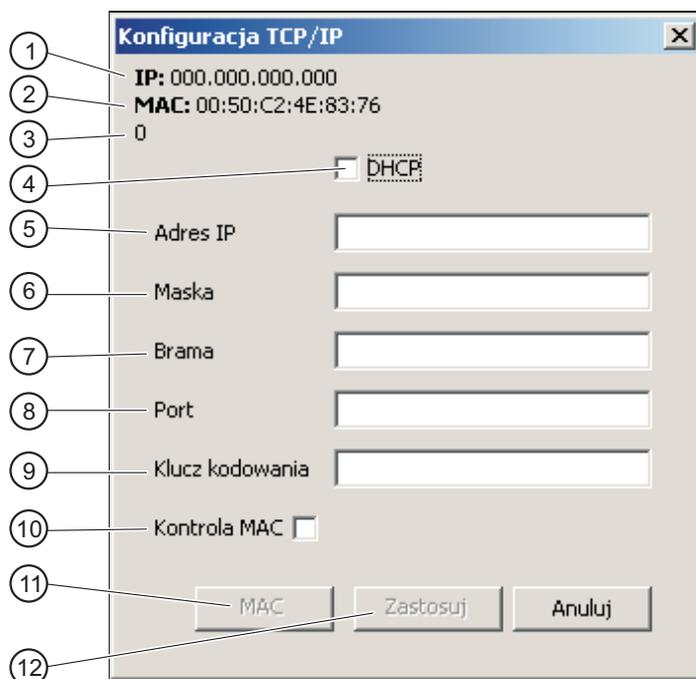
Fig. 13. Configuration window before defining card parameters.

Explanations for the TCP/IP configuration window:

1 - IP address programmed in the card.

2 - MAC card number.

3 - Number of events received by the card, but not sent to the monitoring station program yet.

4 - With the „DHCP" option enabled, the card will automatically download the data regarding IP address, subnet mask and gateway from the DHCP server.

5 - IP address to be used by the card. This field is available if the function of automatic data downloading from server has been disabled („DHCP" option).

6 - Mask of the subnetwork in which the module is working. This field is available if the function of automatic data downloading from server has been disabled („DHCP" option).

7 - Network gateway, i.e. IP address of the network device through which other network devices communicate with the Internet or other local networks. This field is available if the function of automatic data downloading from server has been disabled („DHCP" option).

8 - Number of the network port intended for communication. Values from 1 to 65535 can be entered.

9 - A string of 1 to 12 alphanumeric characters which determine the key to be used for data encrypting during communication.

10 - When the „MAC control" option is enabled, the card will only receive transmissions from the devices with defined MAC numbers. This enables the card to be protected from hacking attempts. You can define the MAC numbers after the „MAC" button is pressed.

11 - Pressing the „MAC" button will open a window where you can define MAC numbers for the devices, from which the card is to receive transmissions. Up to 256 MAC numbers can be defined. The button is available, if the „MAC control" option is enabled.

12 - The „Apply" button is available if any changes have been made in the window and enables saving the introduced changes.

ADDITIONAL CONFIGURATION OF GSM MODULES
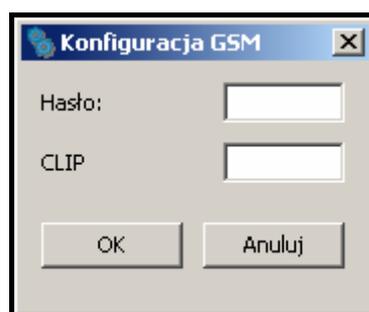
Fig. 14. Additional configuration window for GSM module.

Password – a password for communication with the GSM module connected to the COM port. In case of the GSM-4 module, the password must be identical with that programmed in the module as „DWNL code". In case of the GSM LT-1 module, enter 111111.

CLIP – a name, on the basis of which the CLIP type messages received from the given GSM module will be identified (a corresponding event code can be assigned to this name at the stage of adding / editing subscriber).

7.3.2 „INFORMATION" TAB
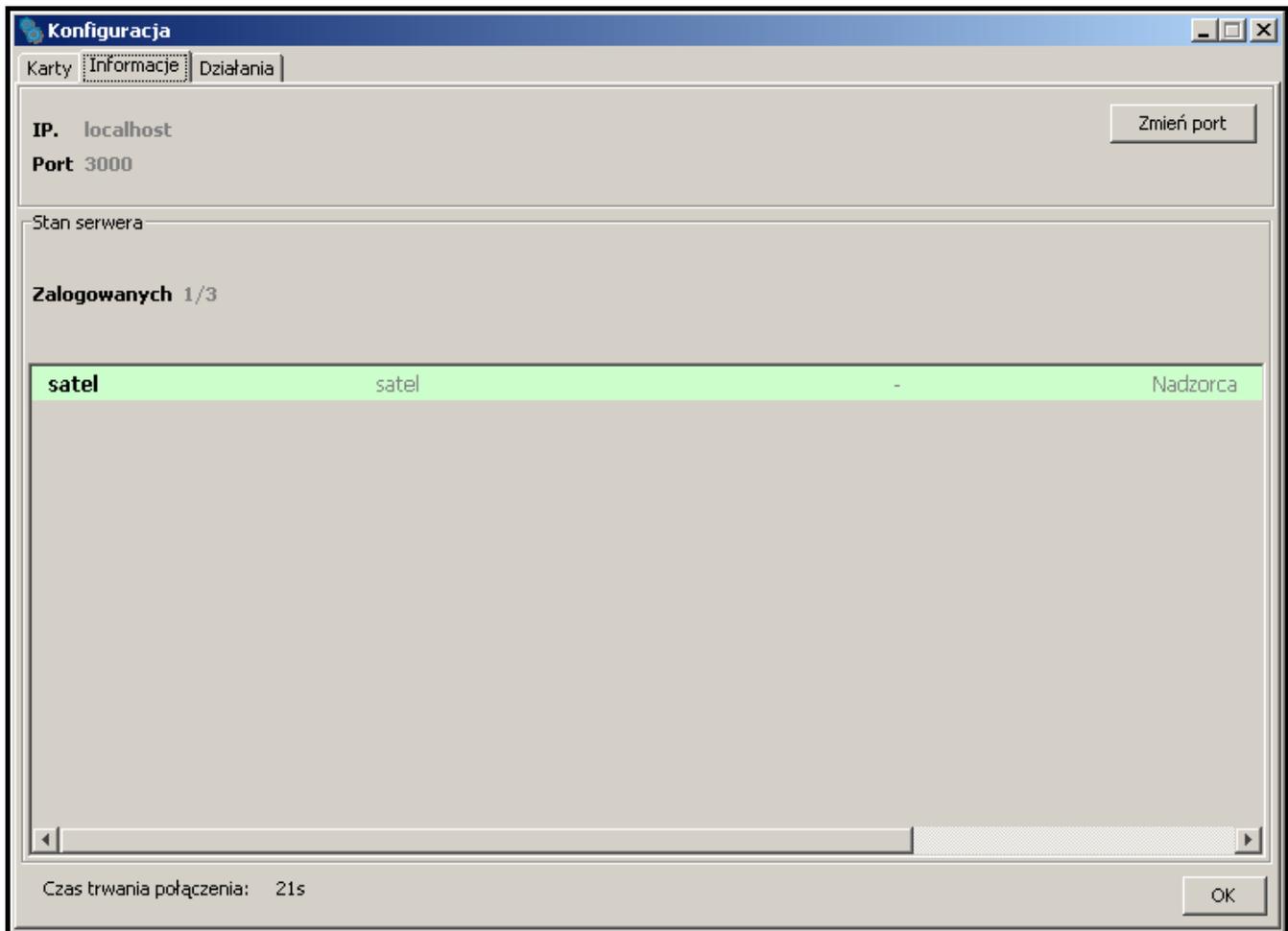
Fig. 15. „Information" tab in „Configuration" window.

The following information is provided in the tab:

- IP address of the computer with installed program of the server to which the client program is connected
- Number of the TCP/IP port through which communication is effected
- Number of users logged in
- Information on the users logged in (first and last name, address, telephone, user status, IP address of the computer from which they logged on)
- Duration of the connection to server

Change port – the button enables changing of the TCP/IP port number (see: CHANGING TCP/IP PORT).

CHANGING TCP/IP PORT

In order to change the number of TCP/IP port through which the client-server communication is effected, do as follows:

1. Open the „Information" tab in „Configuration" window.
2. Click on the „Change port" button.
3. A window will be displayed in which you should enter the new port number. It is possible to enter values from 1 to 65535.
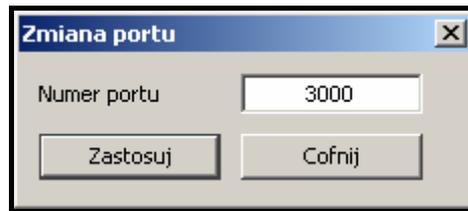
Fig. 16. Window for changing port number.

4. Click your mouse on the „Apply" button.
5. If the port is available, a window will be brought where you can accept or cancel the port change. Acceptance of the port change means that the server program will be closed and will have to be restarted. Communication between all workstations and the server will be lost. Before the next login, it will be necessary to change the server port settings in the login window (see Fig. 10).

7.3.3   „ACTIONS" TAB
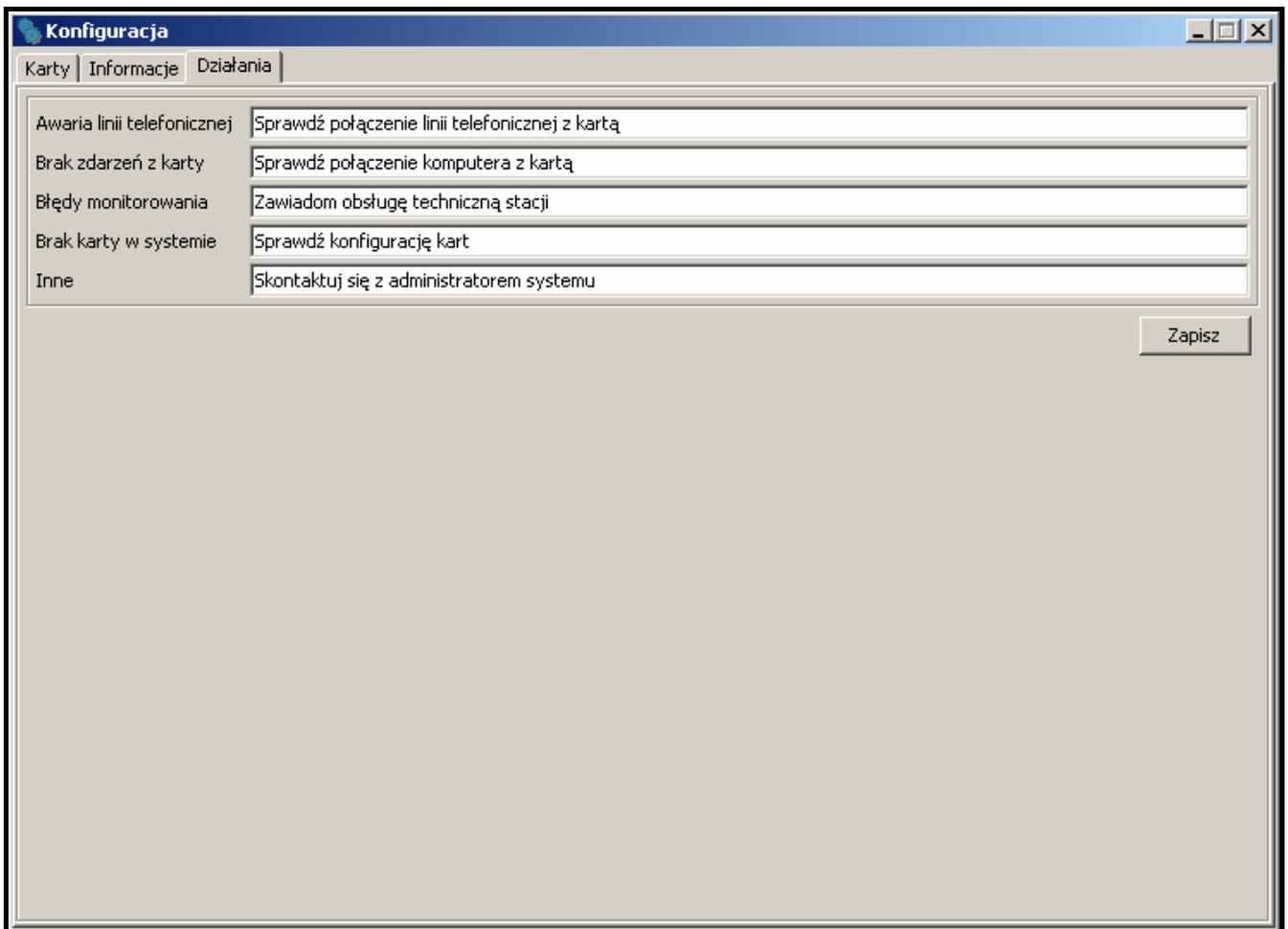
Fig. 17. „Actions" tab in „Configuration" window.

The tab allows the user to define suggested actions that should be taken by the program operator if specified events occur.

7.4 USER ACCOUNTS

The window is available to users with the „user accounts" authority level.

When the monitoring station program is started with its factory settings (first time run), there is one registered user with the name „satel", and using the password „satel", who has the „Supervisor" status and nearly all available authorities. You cannot remove this user, or change his status, or cancel his „user accounts" authority.

⚠️ **After the first run, the factory user password „satel" should be replaced with another one.**

Fig. 18. „User accounts" window at the first time run of the monitoring station program.

User – User name. Filling this field is necessary. It is recommended that the user first and last name (surname) be entered. The user name is to be entered when logging into the server program. It is saved in the event log at all events handled by this user. It will be also included in the created reports.

Address – User residence address. Filling this field is not necessary. It is recommended to fill it, so that the user can be contacted, if needed. The user address is saved in the event log at all events handled by this user.

Telephone – Number of the user's home or mobile phone. Filling this field is not necessary. It is recommended to fill it, so that the user can be contacted, if needed. The user address is saved in the event log at all events handled by this user.

Password – User password. Filling this field is necessary. The password is required to log into the server program. It must have at least 4 characters. The program is case-sensitive. After the first login, the user should change the password assigned to him by the person who added him to the user list (see: CHANGING PASSWORD).

Status – A status must be granted to each user. By default, a particular authority level is assigned to each status. One of the 3 following statuses can be chosen: „Operator", „Installer" or „Supervisor". The „Operator" is only granted the authorities of the „Event log" category. The "Installer" is given all the authorities included in the „Subscribers" category

and, additionally, is authorized to view event log, print reports and documentation. The „Supervisor" is granted all the authorities, except for the simple handling of events. The authorities possessed by the user with a particular status can be freely changed, which practically means that the status is primarily a template, useful when creating and editing users. During the use of the monitoring station program, the status will decide which of the notes sent (see: NOTES) will be received by the particular user.

Authorities – The authorities determine the scope of access to the monitoring station program. They are subdivided into three main categories: event log, subscribers and other.

- **Event log**
  - **viewing** – the user can only view the history of events (he cannot handle the events, unless he has been granted the „handling" authority level).
  - **handling** – the user can only handle events (he cannot view the events log, unless he has been granted the „viewing" authority level, but he can handle the older events by means of the „Status board" window).
  - **simple handling** – the user with the „handling" authority level can handle events in an easy way, i.e. the event will be considered as already handled immediately after the user clicks on the „Handle" button.
  - **clearing troubles** – the user can clear unhandled troubles in the „Status board" window, by clicking twice on the subscriber and opening the detailed information window (when cleared, the troubles will be considered as already handled and inactive).
  - **clearing alarms** – the user can clear unhandled alarms in the „Status board" window, by clicking twice on the subscriber and opening the detailed information window (when cleared, the alarms will be considered as already handled).

- **Subscribers**
  - **adding** – the user can add new subscribers and restore deleted ones. Unless he has been granted the „editing" authority, the user will not be able to edit the settings of added subscriber after closing the „Subscriber" window.
  - **editing** – the user can edit the existing subscribers.
  - **editing skips** – the user with „adding" or „editing" authorities can define the rules for skipping the incoming events.
  - **editing time areas** – the user with „adding" or „editing" authorities can define the „Time areas" for the subscriber.
  - **deleting** – the user can delete subscribers.

- **Other**
  - **printing documentation** – the user can print documentation regarding the monitoring station in PDF format.
  - **printing reports** – the user can print subscriber reports, reports on activity of selected program users, as well as event log and system performance statistics in PDF format.
  - **server configuration** – the user can configure the server.
  - **user accounts** – the user can add, edit and remove other users.
  - **mimic boards** – the user can define the lighting mode of mimic board LEDs.

7.4.1 ADDING NEW USER

In order to add a new user, do the following:

1. Open the „User accounts" window. An empty item in the list, intended for adding new users, will be highlighted as the active field.
2. Enter the user name.

3. Enter additional information on the user (address, telephone), so that he can be contacted, if necessary.

4. Enter the user password.

5. Select the user status.

6. Click on the „Save" button.

7.4.2 EDITING USER

In order to change the user settings, do as follows:

1. Open the „User accounts" window. An empty item in the list, intended for adding new users, will be highlighted as the active field.

2. Click on the user whose data you want to edit.

3. Make changes to the user settings.

4. Click on the „Save" button.

Note: If the user whose data have been edited is logged in, any changes regarding his name, password or authorities will take effect after logging out of the user.

7.4.3 DELETING USER

In order to delete the user, do as follows:

1. Open the „User accounts" window. An empty item in the list, intended for adding new users, will be highlighted as the active field.

2. Click on the user you want to delete.

3. Click on the „Delete" button.

4. In the window that will appear, confirm the intention to delete the user by clicking on the „Yes" button.

Note: If the user being deleted is logged in, he will be able to operate the monitoring station program until he logs out.

7.5 CHANGING PASSWORD

The function is available to all users. It is recommended that each user, after the first login, change the password assigned to him by the person who added him to the user list. In order to change the password, do as follows:

1. Open the „Change password" window.

Fig. 19. Password change window.

2. Enter the previous password in the „Old password" field.

3. Enter the new password in the „New password" field.

4. Re-enter the new password in the „Confirm password".

5. Click on the „Apply" button.

7.6 MIMIC BOARDS

The window enables configuration of the mimic boards connected to the monitoring station.
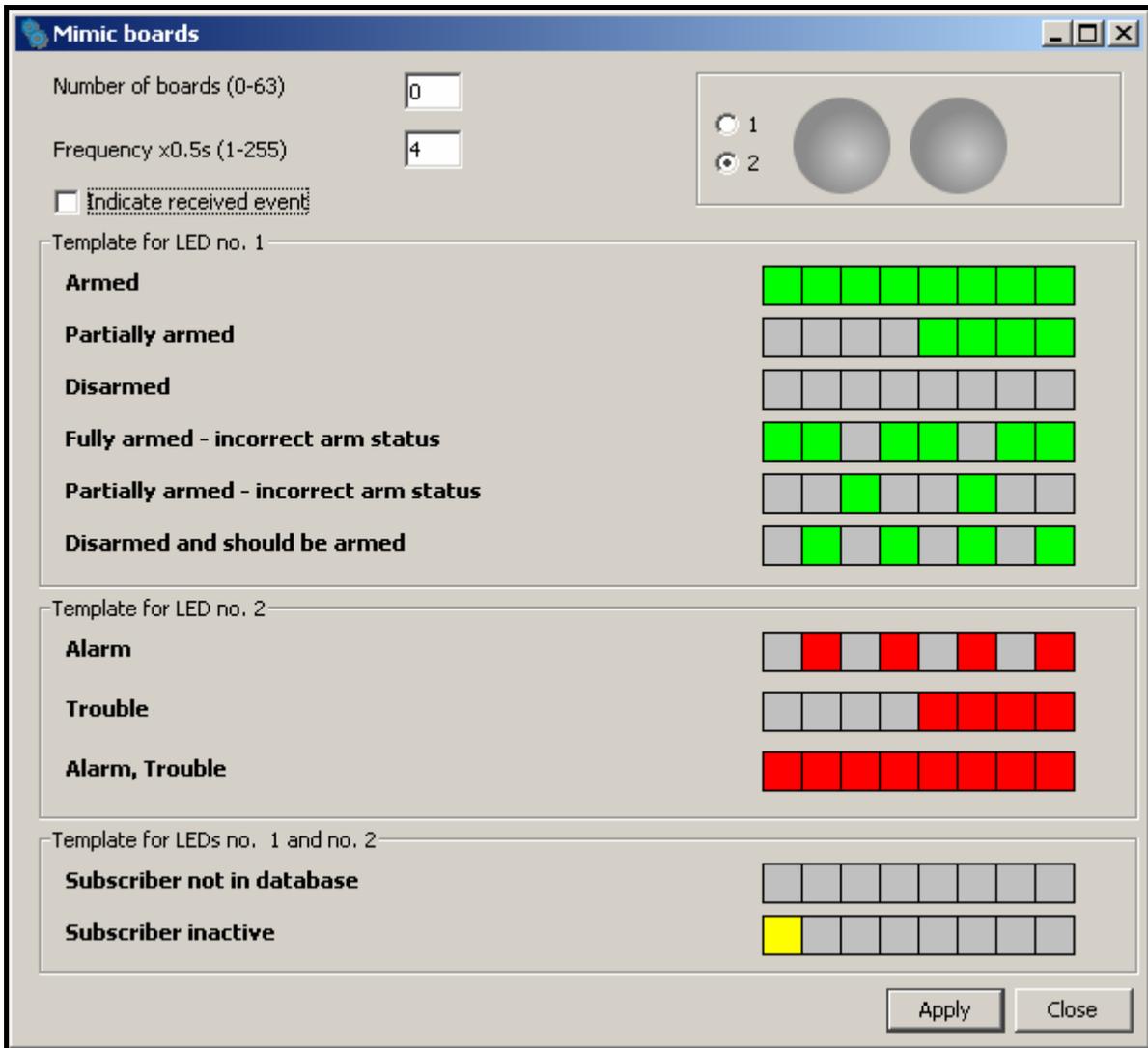
Fig. 20. „Mimic boards" on first-time run of the program.

Number of boards – enter in this field the number of mimic boards connected to the monitoring station. Up to 63 mimic boards can be connected (each board illustrates the status of 64 subscribers). Entering 0 will disable support of the mimic boards. Do not enter the greater number of boards than in reality. When you enter a smaller number of boards than in reality, only the indicated number of boards will be supported.

Frequency x0.5s – define in this field with what speed the LED lighting templates are to move. The entered value is multiplied by 0.5 seconds. You can enter values from 1 to 255 seconds.

Indicate received event – select this box if the mimic boards are to signal receiving events from the subscriber. Receiving an event will be signaled by the alternate blinking of the subscriber assigned LEDs for 2 seconds. After elapse of this time, the LEDs will indicate the subscriber's status again.

1 – select this box to see how the template will be displayed on one LED. The LED is represented in graphical form.

2 – select this box to see how the template(s) will be displayed on two LEDs. The LEDs are represented in graphical form.

Template for LED 1 – LED 1 lighting template for the following statuses:

- Armed
- Partially armed
- Disarmed
- Armed - wrong status
- Partially armed - wrong status
- Disarmed - wrong status

Template for LED 2 – LED 2 lighting template for the following statuses:

- Alarm
- Trouble
- Alarm, Trouble

Template for LEDs 1 and 2 – LEDs lighting template for the following statuses:

- Subscriber not in database
- Subscriber inactive

Click on the selected template to display it on the LED/LEDs in the upper right-hand corner of the window.

Each template is represented in graphical form on 8 fields. The LED is ON, when the field is selected. To select / deselect the required field, click on it with our mouse pointer.

Buttons:

Apply – saves introduced changes to the database and restarts mimic board LEDs.

Close – closes the window.

7.7 SUBSCRIBERS

The window is available to the users who possess the „Subscribers" category authorities („adding", „editing" or „deleting").

The window displays a subscriber list. Depending on the granted authority level, the user can add, edit or delete the subscribers.
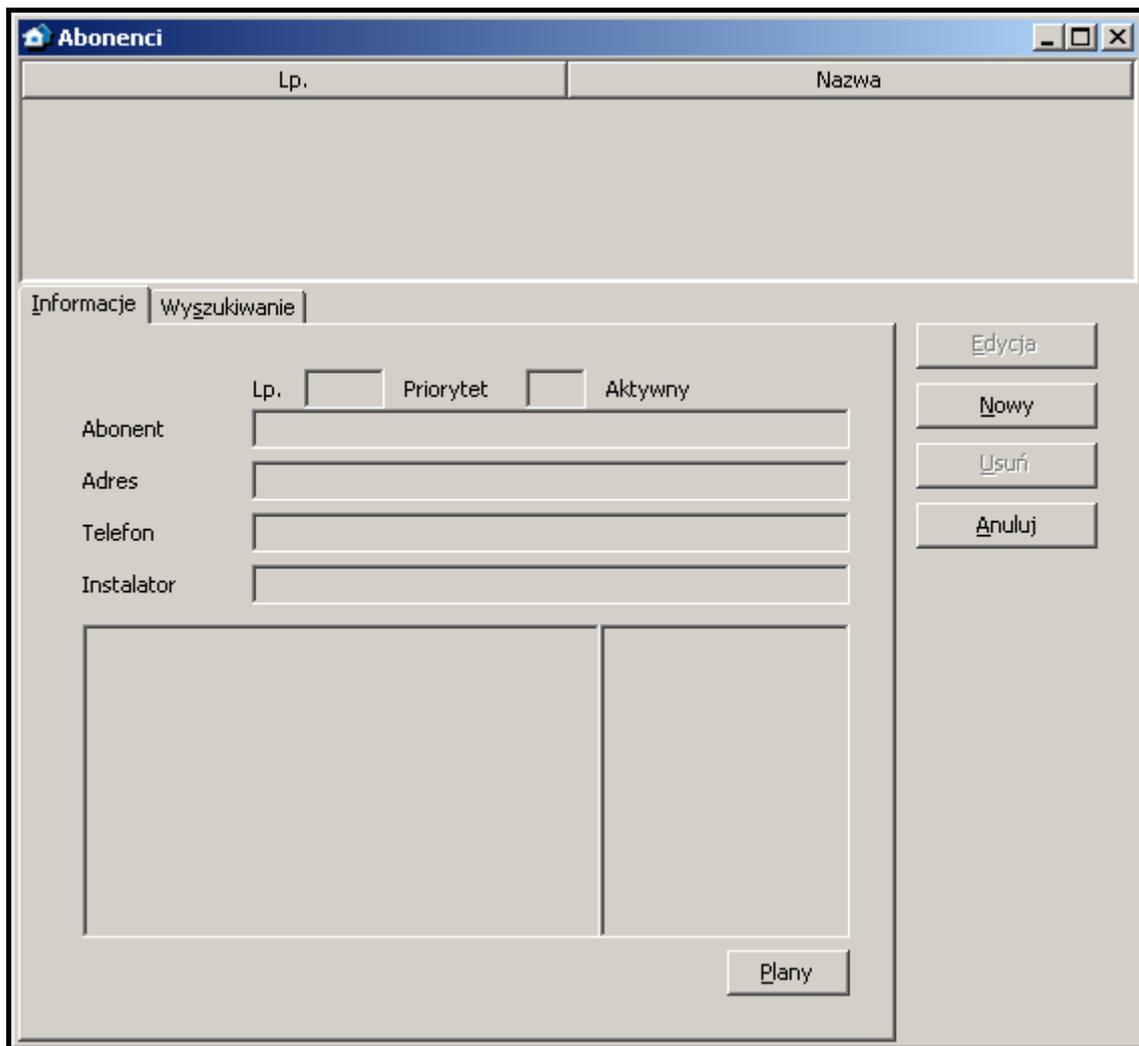
Fig. 21. „Subscribers" window with „Information" tab on first-time run of the program.

No. – subscriber's consecutive number. The number is assigned to the subscriber automatically when he is being added, but it may be changed by the user. In the „Status board" window, the subscribers are sorted by their consecutive numbers.

Name – subscriber's first and last name.

Buttons:

Edit – displayed if the user has the „editing" authority. Active after the first subscriber is added. Allows editing the existing subscribers' data and settings.

Restore – displayed after deleted subscribers are found (see: „SEARCH" TAB), if the user has the „adding" authority. Allows restoring the deleted subscriber (his setting will not be restored).

New – displayed if the user has the „adding" authority. Allows adding new subscribers.

Delete – displayed if the user has the „deleting" authority. Allows deleting subscribers.

Cancel – closes the subscribers list window.

7.7.1 „INFORMATION" TAB

No. – subscriber's consecutive number. The number is assigned to the subscriber automatically when he is being added, but it may be changed by the user. In the „Status board" window, the subscribers are sorted by their consecutive numbers.

Priority – subscriber's priority. Subscriber's priority is only meaningful when the user wants to handle unhandled events (alarms, troubles or arm status events). The events will then be displayed according to the subscriber's priority. Priority values range from 0 to 9. High-

priority events take precedence. If some subscribers have the same priority, precedence will be given to the subscriber's high-priority events which were received first, i.e. remained unhandled for the longest period of time.

Active – information on whether the subscriber is currently active or inactive. If the subscriber is inactive, events received from him require no reaction of the monitoring station operating personnel. These events are automatically saved in the event log as handled. For the inactive subscriber, neither test transmissions, nor consistence of arming/disarming with time areas are checked. The „Status board" displays no information on the inactive subscriber's status.

Subscriber – subscriber's first and last name (or company name).

Address – subscriber's address.

Telephone – subscriber's telephone number.

Installer – data of the company or person who installed the alarm security system at the subscriber's premises, or is currently responsible for maintenance and operability of the system.

Displayed below the „Installer" field is additional information on the subscriber (see: „GENERAL" TAB). The adjacent field shows a list of identifiers defined for the subscriber (see: „IDENTIFIERS" TAB).

Button:

Plans – available in case of events from the subscribers to whom the plans have been assigned (see: „PLANS" TAB). Opens the „Site plans" window.

SITE PLANS

The window displays a list of plans defined for the subscriber. Click on the required plan and press the „Preview" button to familiarize with the plan of monitored site.

7.7.2 „SEARCH" TAB

The „Search" tab makes it possible to find any subscriber (also a deleted one).

Text – the field where the character string you are searching for should be entered. The field can be left empty: if this is the case, the search will only be based on the other search criteria defined.

Where – the place where to search for the character string entered into the „Text" field. You can select the following places:

- − in names
- − in addresses
- − in installers
- − in information
- − in telephones
- − anywhere

Active – select this field if the subscriber you search for is active. By default, this field is selected.

Inactive – select this field if the subscriber you search for is inactive.

Note: If the „Active" and „Inactive" fields are selected at the same time, the search will include both categories of subscribers, similarly as when none of the fields is selected.

Fig. 22. „Search" tab (part of „Subscribers" window) on the first-time run of the program.

With identifiers – select this field if an identifier has been assigned to the subscriber searched for. By default, this field is selected. See also „IDENTIFIERS".

Without identifiers – select this field if no identifier has been assigned to the subscriber searched for.

Note: If the fields „With identifiers" and „Without identifiers" are selected at the same time, the search will include both categories of subscribers, similarly as when none of the fields is selected.

Identifiers – this field is available when the „With identifiers" field has been selected. It enables a subscriber to be found on the basis of identifier(s). If the „With identifiers" field is selected and the „Identifiers" remains blank, the search will include all subscribers who possess identifiers.

Deleted – select this field if the subscriber you are searching has been deleted. Selecting the field will block access to the fields: „Active", „Inactive", „With identifiers", „Without identifiers" and „Identifiers".

Buttons:

Search – starts searching the database. The list of subscribers who meet the defined criteria will be displayed in place of the list of all subscribers.

Clear – restores default settings of the „Search" tab and brings up the list of all users.

7.7.3 SUBSCRIBER

The window allows you to enter the subscriber's data. It will open on pressing the „Add" or „Edit" buttons in the „Subscribers" window.

Fig. 23. „Subscriber" window before entering the data. Only the „General" tab is available. The „Plans" and „Identifiers" tabs will only be available after the data are entered into the „Subscriber", „Address" and „Telephone" fields and then saved, which amounts to adding the subscriber to database. The skipping settings (on right-hand side of the window) are only available when the user has the „editing skips" authority.

„GENERAL" TAB

ID – identification number assigned automatically to each new subscriber. The number is unique and will never be assigned again, even after the subscriber is removed.

No. – subscriber's consecutive number. The number is assigned to the subscriber automatically when he is being added, but it may be changed by the user. In the „Status board" window, the subscribers are sorted by their consecutive numbers.

Priority – subscriber's priority. Subscriber's priority is only meaningful when the user wants to handle unhandled events (alarms, troubles or arm status events). The events will then be displayed according to the subscriber's priority. Priority values range from 0 to 9. High-priority events take precedence. If some subscribers have the same priority, precedence will be given to the subscriber's high-priority events which were received first, i.e. remained unhandled for the longest period of time. By default, the subscriber's priority is set to 0.

Active – the box must be checked if the subscriber is to be active. By default, the box is checked. If the subscriber is inactive, events received from him require no reaction of the monitoring station operating personnel. These events are automatically saved in the event log as handled. For the inactive subscriber, neither test transmissions, nor consistence of arming/disarming with time areas are checked. The „Status board" displays no information on the inactive subscriber's status.

Subscriber – enter the subscriber's first and last name or company name in this field. The field must be filled in.

Address – enter subscriber's address here. The field must be filled in.

Telephone – enter the subscriber's telephone number in this field. The field must be filled in.

Installer – enter in this field the data of the company or person who installed the alarm security system at the subscriber's premises, or is currently responsible for maintenance and operability of the system.

Additional information – here you can enter additional information on the subscriber.

Skipping – options available to users with „editing skips" authority. They allow you to define how to handle the alarm / trouble event codes coming from the subscriber.

>   **Skip nothing** – no alarm event will be omitted. Each of them will bring up the alarm window.

>   **Skip identical code** – having received an alarm event, the monitoring station will skip alarm events with the same identifier and code over the time period defined in the „Skipping time" field. These events will be automatically saved in the event log as handled. The event details will include information that the code was skipped.

>   **Skip codes in partition** – having received an alarm event, the monitoring station will skip alarm events with the same identifier from the same partition over the time period defined in the „Skipping time" field. These events will be automatically saved in the event log as handled. The event details will include information that the code was skipped. This option can be useful if the subscriber has a few detectors in the room, and alarms from them mean practically one alarm.

>   **Skip troubles** – having received a trouble code, the monitoring station will skip trouble events with the same identifier and code over the time period defined in the „Skipping time" field. They will be automatically saved in the event log as handled. The event details will include information that the code was skipped.

>   **Skipping time** – the time counted from the moment of receiving the alarm or trouble event code. Taken into account, if you have enabled one of the following options: „Skip identical code", „Skip codes in partition" or „Skip troubles". Values fro m 1 to 30 minutes can be entered.

>   **Simple handling** – if this box is checked, events received from the subscriber will be considered as handled immediately after the user clicks on the „Handle" button.

Button:

Save – saves data entered into the database.

„**PLANS**" **TAB**

Any number of plans can be assigned to each subscriber.

File – enter in this field the access path to the graphic file with the plan. You can indicate the access path by clicking on the „…" button. The program supports the following file types: BMP, GIF, JPG and PNG.

Description – the field where you should enter description of the plan.

Buttons:

... – enables the access path to the graphic file to be indicated.

Save – saves the selected graphic file into the database. The button is active, if the access path to the graphic file has been indicated.

Delete – deletes the selected plan. Click your mouse in the list (column on the left-hand side of the window with plan descriptions) on the plan to be deleted, and then on the „Delete" button.

Preview – allows preview of the plan selected from the list.
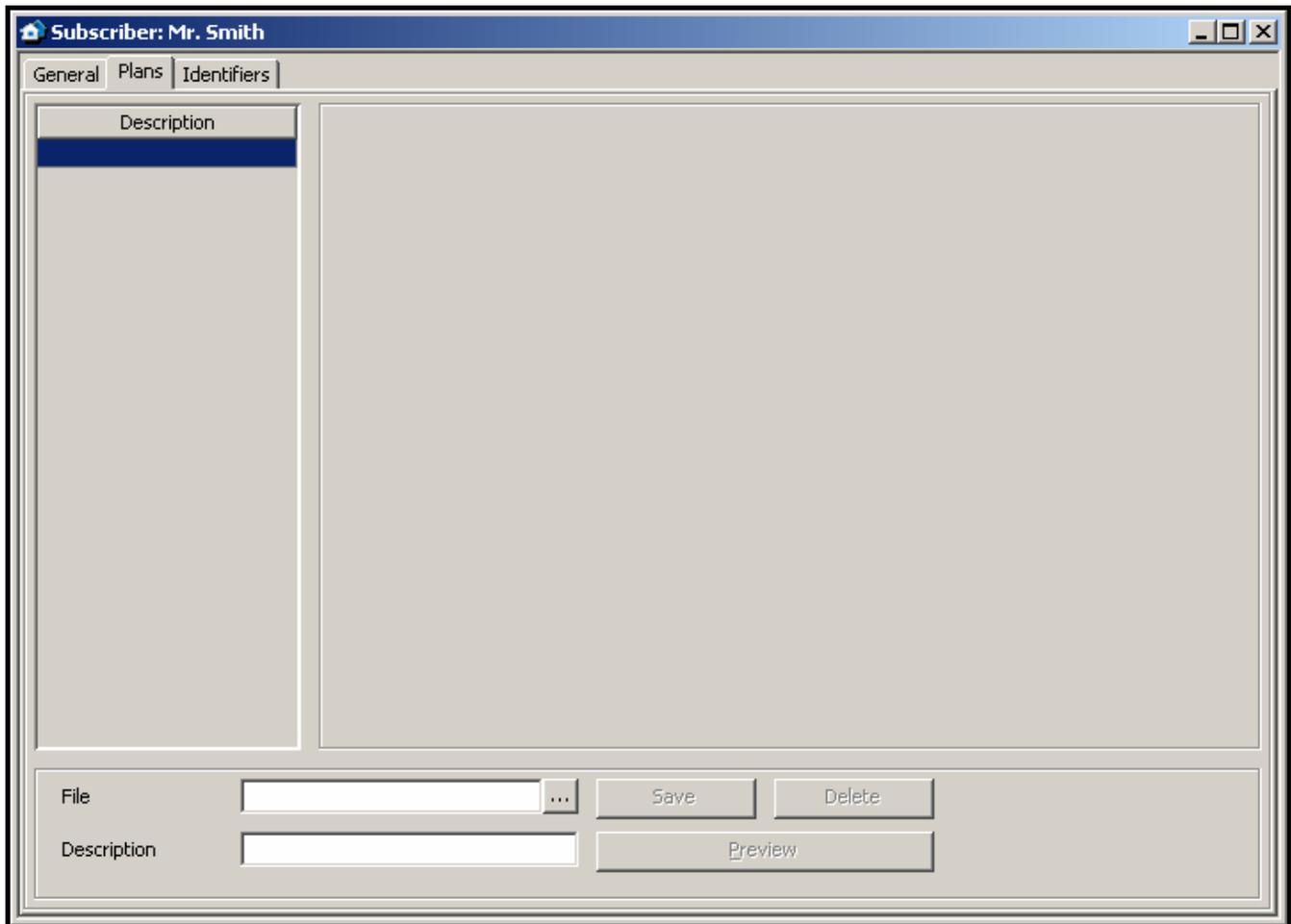
Fig. 24. „Plans" tab in „Subscriber" window, before adding a plan.

„IDENTIFIERS" TAB

The tab contains a list of identifiers defined for the subscriber. It allows for adding new identifiers, as well as editing and deleting the existing ones.

Identifier – each subscriber can be assigned any number of identifiers. The identifier has hexadecimal format (digits and letters from A to F). It cannot, however, include the digit 0 inside. See also: ADDING IDENTIFIERS and EDITING IDENTIFIERS.

Type – the subscriber-assigned identifier can be of the following type:

    Reservation – identifier is only reserved for the subscriber. Defining any codes or settings for it is impossible.

    Contact ID – identifier for transmission in the Contact ID format.

    Normal – identifier for transmission in other formats.

⚠️ **A change of the identifier type is saved automatically.**

    A change of the identifier type from „Normal" or „Contact ID" to any other will delete all the identifier settings.
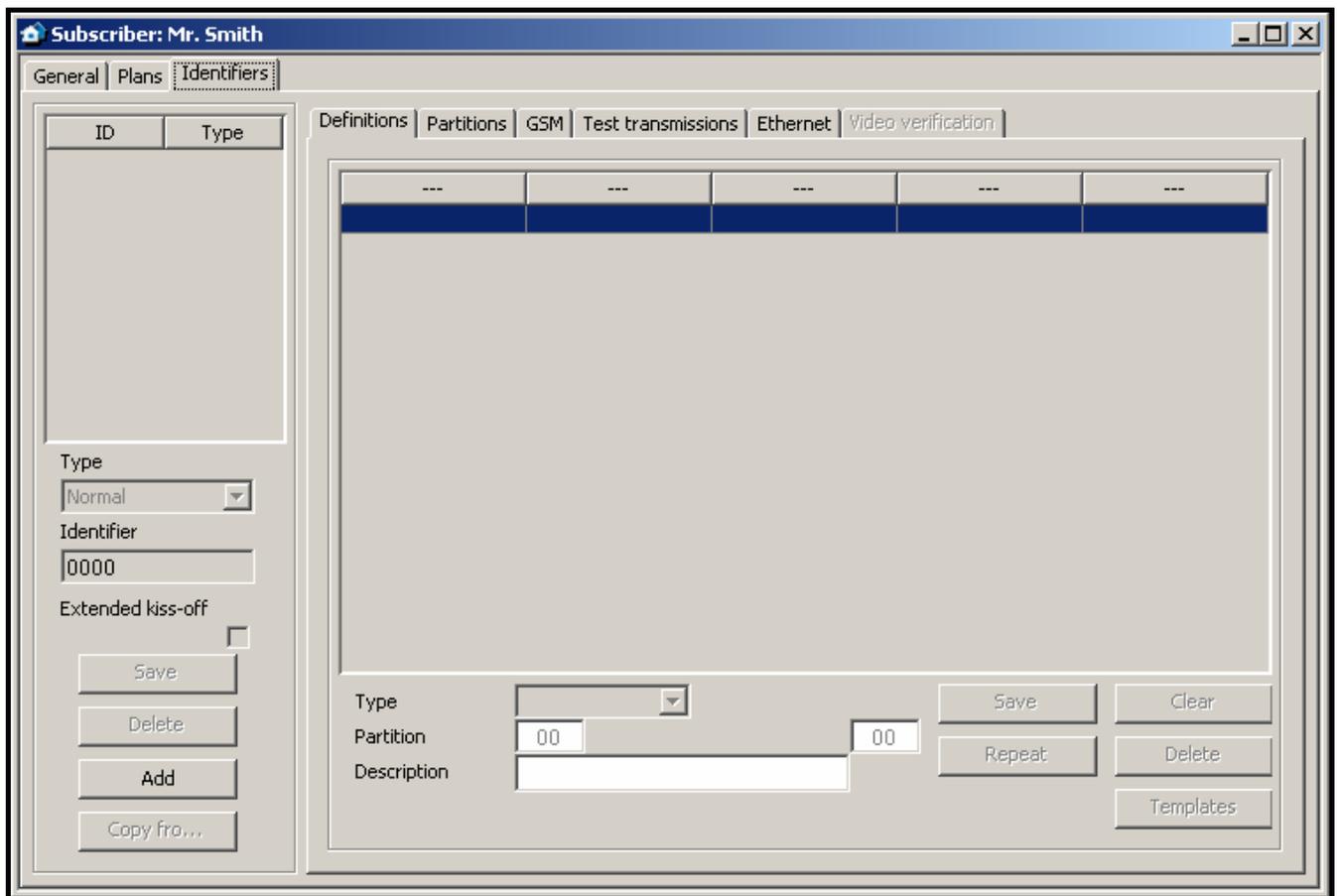
Fig. 25. „Identifiers" tab before adding identifiers.

Extended kiss-off – the option applies to the transmission of Contact ID codes via telephone lines. Some control panels require the extended kiss-off signal upon reception of the code. By default, to speed up communication, short kiss-off signal is used in the STAM-1 telephone receiver cards. The option is available after selecting the „Contact ID" identifier type.

Buttons:

Save – active after manual change of the identifier or activation of the „Extended kiss-off" option. Saves the entered data into the database.

Delete – deletes the selected identifier. Deleting the identifier will also delete all settings referring to this identifier that were entered in the tabs „Definitions", „Partitions", „GSM", „Test transmissions" and „Ethernet".

Add – enables adding new identifiers (see: ADDING IDENTIFIERS).

„DEFINITIONS" TAB FOR „CONTACT ID" TYPE OF IDENTIFIERS

The tab is available after adding the identifier and selecting the „Contact ID" type. It enables defining additional detailed descriptions for the events received in this format. Defining additional descriptions is not necessary, but it makes operation easier.

Fig. 26. „Definitions" tab for identifiers type „Contact ID" (part of „Subscriber" window) prior to defining descriptions.

Type – select in this field the type of description:

– **Zone** – the description will refer to the zone of the subscriber's security system. It will overwrite the standard zone name in all events coming from the partition defined in the „Partition" field and referring to this zone. If no partition number is entered in the „Partition" field, the name will appear in all events which refer to this zone, irrespective of from what partition they may come from.

– **User** – the description will refer to the user of the subscriber's security system. It will overwrite the standard user name in all events received from the partition defined in the „Partition" field and referring to this user. If no partition number is entered in the „Partition" field, the name will appear in all events which refer to this user, irrespective of from what partition they may come from.

– **Expander** – the description will refer to the expander of the subscriber's security system. It will overwrite the standard user name in all events coming from the partition defined in the „Partition" field and referring to this expander. If no partition number is entered in the „Partition" field, the name will appear in all events which refer to this expander, irrespective of from what partition they may come from.

Partition – enter the partition number in this field. Information entered in the „Description" field will appear at all events referring to the given zone / user / expander and coming from this partition. If the partition number is not entered, this description will appear at all events which refer to the given zone / user / expander.

Zone / User / Expander (the name dependent on the selected description type) – enter in this field the number of zone / user / expander to which the information entered in the „Description" field will be assigned.

Description – enter in this field the name of zone / user / expander (depending on the selected description type). It will appear in events referring to the given zone / user / expander.

Buttons:

Save – saves the entered descriptions into the database.

Clear – deletes all descriptions defined for the identifier.

Repeat – the button enables easy addition of a new description with parameters similar to the existing one. For this purpose, click on the description you want to copy, and then on the „Repeat" button. Having entered changes in the selected fields (a change of the zone / user / expander number or partition number is necessary), press the „Save" button.

Delete – deletes the selected description.

Dload – the button enables downloading of descriptions exported by means of the Dload64 or DloadX program.

„DEFINITIONS" TAB FOR „NORMAL" TYPE OF IDENTIFIERS

The tab is available after adding the identifier and selecting the „Normal" type. It enables the defining of event codes.

Type – enter in this field the type of edited code:

− **Alarm** – the code informs of an alarm at the subscriber's site. It requires intervention of the monitoring station operating personnel (after receiving the code, the alarm handling window will be brought up).

− **Arming** – the code informs of armed status activation. It requires no intervention of the monitoring station operating personnel, but allows to verify whether the arming occurred within the time interval defined for the „Time areas" (see: „PARTITIONS" TAB).

− **Disarming** – the code informs of armed status deactivation. It requires no intervention of the monitoring station operating personnel, but allows to verify whether the arming occurred within the time interval defined for the „Time areas" (see: „PARTITIONS" TAB).

− **Trouble** – the code informs of a trouble at the subscriber's site. It requires intervention of the monitoring station operating personnel (after receiving the code, the trouble handling window will be brought up).

− **Restore** – the code informs of the end of the previously reported trouble. It requires no intervention of the monitoring station operating personnel. For this code it is necessary to enter in the „Decode" field the code of the trouble to be restored.

− **Test** – test transmission code. It requires intervention of the monitoring station operating personnel, unless it is received according to the defined rules (see: „TEST TRANSMISSIONS" TAB).

− **Remark** – the code requires no intervention of the monitoring station operating personnel. When received, it will be saved into the event log and audibly signaled.

− **Other** – the code requires no intervention of the monitoring station operating personnel. When received, it will be saved into the event log.
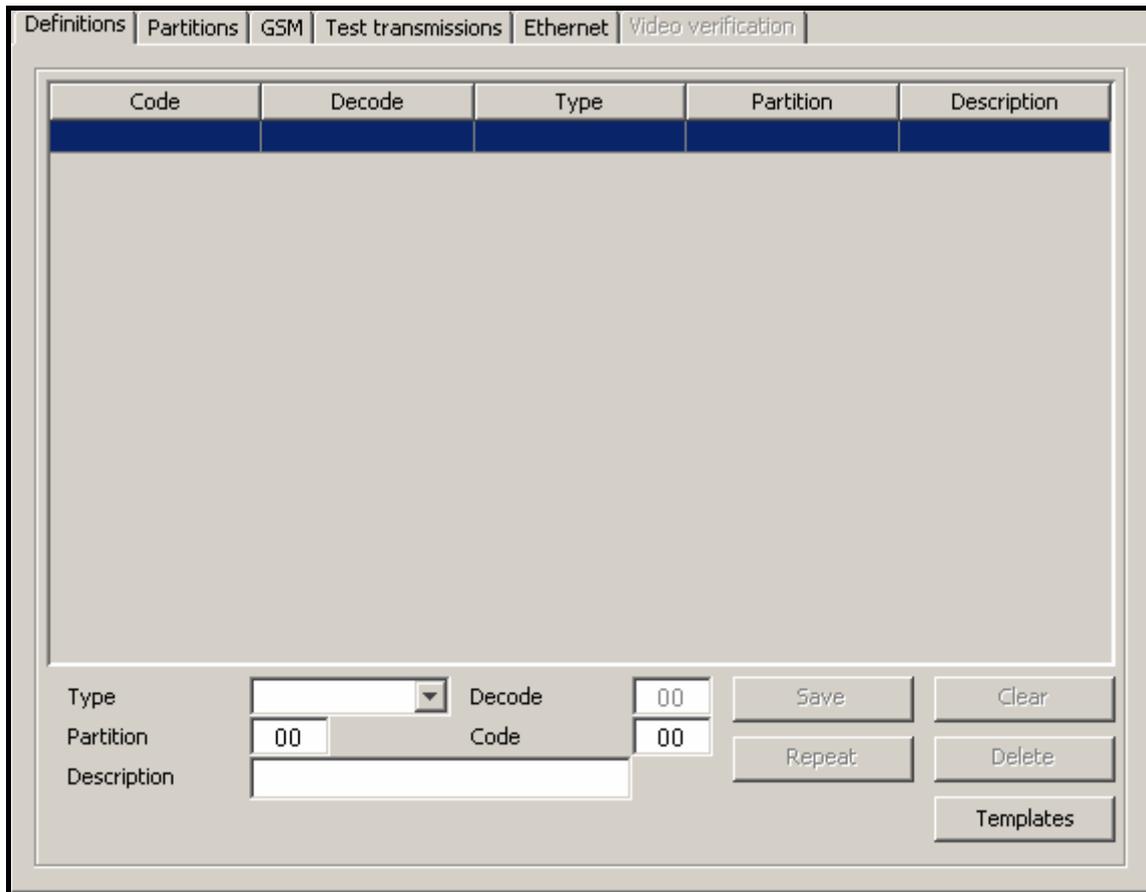
Fig. 27. „Definitions" tab for „Normal" type identifiers (part of „Subscriber" window) before codes are defined.

Decode – the field is available after selecting the „Restore" code type. Enter here the code of the trouble which will be canceled after the „Restore" code type is received.

Partition – enter in this field the number of the partition to be assigned with the code. This enables the codes to be linked to the partitions defined in the subscriber's alarm control panel. In case of certain codes, selection of the partition will affect the reaction pattern of the monitoring station. It applies to the „Alarm" type codes (see „SKIP CODES IN PARTITION" option) and the codes of „Arming" and „Disarming" type (see: TIME AREAS). In addition, for the codes of „Alarm" and „Troubles" type which come from a particular partition, it is necessary to define actions to be taken by the monitoring station personnel after the codes are received (see: PARTITION ACTIONS).

Code – enter a two-character value in the field. Digits and letters from A to F can be used. Digit 0 in the first position means entering one-digit code. Entering 0 in the second position is not recommended.

Description – enter in this field verbal description of the event to represent the entered code. The description will be shown in the „Event log" and in event handling windows.

Buttons:

Save – saves entered event codes into the database.

Clear – deletes all event codes defined for the identifier.

Repeat – the button enables easy addition of a new code with parameters similar to the existing one. For this purpose, click on the code you want to copy, and then on the „Repeat" button. Having entered changes in the selected fields (code change is necessary), press the „Save" button.

Delete – deletes the selected code.

Templates – the button enables downloading of code templates. They are included in the monitoring station program and can be found in the „templates" folder (a folder of the STAM-2 Client program). The files, which have the WZ1 extension, can be edited by means of any text editor. You can also add your own templates.

„**PARTITIONS**" **TAB**

Fig. 28. „Partitions" tab (part of „Subscriber" window) before partitions are defined.

The tab is available after adding the identifier and selecting the „Contact ID" or „Normal" type. It contains a list of defined partitions, enables defining new ones (see: Adding new partitions), as well as editing and deleting the existing ones.

Partition 00 is the default partition, created automatically for each identifier of „Contact ID" or „Normal" type. For this partition it is only allowed to define actions in case of alarm and trouble („Partition actions" tab) as well as arming / disarming at wrong time („Actions" in „Time areas" tab). These actions will be considered as default ones for all partitions for which individual actions will not be defined.

Partition – enter the partition number here. The name entered in the „Description" field will appear at all events coming from this partition.

Description – enter the partition name in this. This name will appear at all events coming from the partition with the number entered into the „Partition" field.

Arm status control – the option enables / disables verification, whether armed / disarmed status of the partition coincides with the defined time areas („areas" tab). Having checked / unchecked the box, press the „Save" button so that the change can take effect.

Buttons:

Add – adds new partition to the list.

Save – saves changes referring to the existing partition (partition number, description, „Arm status control") into the database.

Delete – deletes selected partition.

„PARTITION ACTIONS" TAB

Alarms – you can define up to 5 actions to be taken by the operator of the monitoring station program upon receipt of the alarm event from the selected partition. The action list will be displayed in the „Actions" window on pressing the „Handle" button. If no actions have been defined in case of alarm, the list of actions defined for the default partition will be displayed. The action list for the default partition should be defined.

Troubles – you can define up to 5 actions to be taken by the operator of the monitoring station program upon receipt of the trouble event from the selected partition. The action list will be displayed in the „Actions" window on pressing the „Handle" button. If no actions have been defined in case of trouble, the list of actions defined for the default partition will be displayed. The action list for the default partition should be defined.

Buttons:

Save – saves actions defined for the partition in case of alarm or trouble to the database.

Clear – deletes all actions defined for the partition in case of alarm or performance trouble.

„TIME AREAS" TAB

The „time area" is a time interval during which the partition should be armed or disarmed. The program of monitoring station will check whether the partition status corresponds to its predetermined status. If there is any inconsistence, the event window will be displayed to inform the operating personnel thereof. The window is displayed in two cases: at the beginning of the defined time interval and upon receipt of the event informing that the partition status has been changed to one which is inconsistent with the defined status (e.g. the partition has been armed when it should be disarmed, or armed when it should be disarmed). When defining the time areas, remember to leave undefined periods between the times of armed and disarmed status, when the partition status will not be monitored, so that the partition can be armed / disarmed.

Definitions – the tab contains a list of defined time areas. It enables defining new partitions, as well as editing and deleting the old ones.

- **Arm status** – select in this field whether the system is to be armed within the defined time interval, or not.

- **From** – select in this field from which day of the week the system status is to be monitored. Indicate the exact time from which the system status will be monitored.

- **To** – select in this field to which day of the week the system status is to be monitored. Indicate the exact time to which the system status will be monitored.

Buttons:

Save – saves the defined time areas into the database.

Clear – the button enables all defined time areas to be cleared.

Repeat – the button enables easy addition of a new time areas with parameters similar to the existing one. For this purpose, click on the definition of the time

area you want to copy, and then on the „Repeat" button. Having introduced changes to the selected fields, press the „Save" button.

Delete – the button enables deletion of the selected time area.

Exceptions – the tab contains a list of exceptions, i.e. time intervals within which the time area definitions will be disregarded.

- **Arm status** – select in this field whether the exception defined will refer to armed status or disarmed status.

- **[Everyday] From** – determine in this field the time from which the partition status will not be monitored everyday.

- **[Everyday] To** – determine in this field the time to which the partition status will not be monitored everyday.

- **[Valid] From** – define in this field the date from which the exception is to be effective.

- **[Valid] To** – define in this field the date to which the exception is to be effective.

- **Automatic deletion** – select this field if the exception is to be deleted on the specified day. When selected, a field will be available where you should enter exact time of the automatic deletion.

Buttons:

Save – saves the defined exception into the database.

Clear – deletes all defined exceptions.

Repeat – the button enables easy addition of a new exception with parameters similar to the already existing one. To do so, click on the exception you want to copy, and then on the „Repeat" button. Having introduced changes to the selected fields, press the „Save" button.

Delete – deletes the selected exception.

Actions – in this tab, you can define actions which should be taken by the operator of the monitoring station program when the arm status window is displayed.

- **Lack of arming** – you can define up to 5 actions to be taken by the operator of the monitoring station program when the window is brought up with information that the partition is disarmed, although it should be armed. The action list will be displayed in the „Actions" window upon pressing the „Handle" button. If for the particular partition have been defined no actions in case of such an event, a list of actions defined for the default partition will be displayed. The list of actions the default partition should be defined.

- **Lack of disarming** – you can define up to 5 actions to be taken by the operator of the monitoring station program when the window is brought up with information that the partition is armed, although it should be disarmed. The action list will be displayed in the „Actions" window upon pressing the „Handle" button. If for the particular partition have been defined no actions in case of such an event, a list of actions defined for the default partition will be displayed. The list of actions the default partition should be defined.

Buttons:

Save – saves the defined actions into the database.

Clear – deletes all defined actions.

ADDING NEW PARTITIONS

In order to add a new partition, do as follows:

1. Click on a blank field in the partition list.
2. Enter the partition number in the „Partition" field.
3. Enter the partition name in the „Description" field.
4. Select or deselect the „Arm status control", as may be required.
5. Click on the „Save" button. The new partition will appear in the list. Click your mouse on the partition and you may proceed to defining the rest of its parameters.

„GSM" TAB

The tab is available after identifier is added and the „Contact ID" or „Normal" type selected. It allows to define the subscriber's GSM telephone number and the SMS or CLIP type messages which can be received by the GSM module from the subscriber. Corresponding event codes should be assigned to these messages.

GSM telephone number – enter in this field the GSM telephone number, by means of which control panel communicates with the GSM module of the monitoring station. Based on this number, the monitoring station program will identify the subscriber. The telephone number must be preceded by the country code. The number presentation function must be enabled in the subscriber's GSM telephone.

⚠️ **Deleting the GSM telephone number amounts to deleting all settings defined for this number (SMS and CLIP type messages and codes assigned to them).**

Content – enter in this field the character string which must occur in the SMS message, or the name predefined for the CLIP type messages received from this telephone (see: Additional configuration of GSM modules). Receiving the defined SMS or CLIP message will be recognized by the monitoring station program as receiving the event code. The field is available after saving the GSM telephone number.

Fig. 29. „GSM" tab (part of „Subscriber" window) before entering the subscriber's GSM telephone number.

Code – enter in this field what kind of event code is to be generated on receiving the SMS or CLIP type message defined in the „Content" field. The field is available after saving the GSM telephone number.

Exact text – the option refers to SMS messages. If enabled, the received SMS content must precisely correspond to the character string entered into the „Content" field. If disabled, other characters may appear before and after this character string. The field is available after saving the GSM telephone number.

Buttons:

Save – saves the data entered into the database.

Delete – deletes the selected definitions from the list.

„TEST TRANSMISSIONS" TAB

The tab is available after adding identifier and selecting the „Contact ID" or „Normal" type.
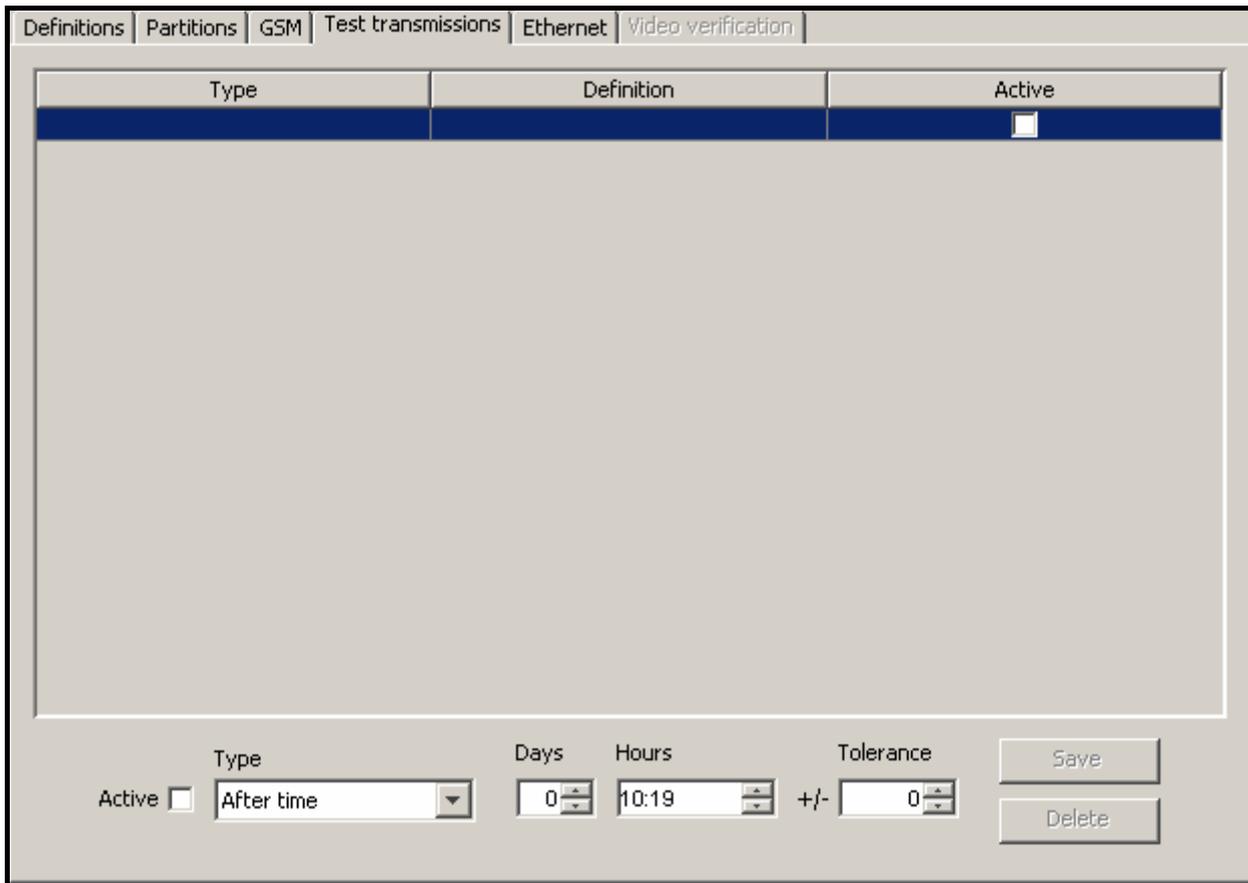
Fig. 30. „Test transmissions " tab (part of „Subscriber" window) prior to defining test transmissions for the subscriber.

Active – select this box if the monitoring station program is to monitor receiving test transmissions.

Type – select in this field the test transmission type:

– **After time** – the test transmission must be received exactly after elapse of a specified time period from the last transmission (irrespective of whether it was a test transmission, or another event was sent). If the test transmission fails to be received after defined time (taking into account preprogrammed tolerance), or is received earlier, the station program will display the trouble handling window with appropriate information.

– **On time** – the test transmission must be received every specified number of days at the defined time. If the test transmission fails to be received at the defined time (taking into account preprogrammed tolerance), or is received earlier, the station program will display the trouble handling window with appropriate information. Receiving the test transmission at another time or on another day will also result in trouble being reported. The first test transmission must be received before expiry of the time defined in the „Days" field. Receiving it is recognized as synchronization of the control panel and the monitoring station.

– **In time** – any transmission must be received within the defined time interval. The time is counted from the last transmission (irrespective of whether it was a test transmission, or another event was sent). If no transmission is received within the defined time interval (taking into account preprogrammed tolerance), the station program will display the trouble handling window with appropriate information.

Days – define in this field the number of days. The maximum value that can be entered is 31 days. In case of the „On time" transmission, entering 0 or 1 will be interpreted in

the same way, i.e. as defining transmissions to be received every day at the specified
time.

Hours – define in this field the number of hours and minutes for the „After time" and „In
time" transmissions, or the hour and minutes for the „On time" transmissions.

Tolerance – define in this field the tolerance in minutes with which the transmission can
be received. It is recommended that the tolerance be defined, as the transmission
may be received, for a variety of reasons, a little earlier or later (e.g. because of busy
status of the telephone line, the control panel was unable to establish connection, the
control panel clock out of synchronization with the monitoring station clock, etc.).
The maximum tolerance value is 120 minutes.

Buttons:

Save – saves the data entered into the database.

Delete – deletes the selected transmission from the list.

„ETHERNET" TAB

The tab is available after identifier is added and „Contact ID" or „Normal" selected. **The
tab parameters should be defined for the subscriber's system identifier.**

Fig. 31. „Ethernet" tab (part of „Subscriber" window) before entering data.

ETHM key – enter in this field a sequence of 1 to 5 alphanumeric characters identifying
the Ethernet module. It must correspond to the ETHM key defined in the subscriber's
control panel.

Card address – select in this field address of the STAM-1 Ethernet card to which the
subscriber will be assigned.

No. – consecutive number assigned automatically when you click on the „Save" button.
It can be a number from the range of 0 to 255. **One Ethernet card can support up
to 256 subscribers.**

Test period – determine in this field the time between successive communication tests.
Values from 0 to 255 seconds can be entered. Entering 0 means that the
communication test will be disabled.

Number of missing tests – determine in this field, how many unsuccessful
communication tests are required before trouble is reported (the trouble handling
window will be displayed). Values from 1 to 15 can be entered.

*Note: Caution is advisable when selecting parameters to be entered in the „Test
period" and „Number of missing tests" fields. If you enter low values in both*

fields, the frequency of reported troubles may increase, which not necessarily means any actual communication problems.

Buttons:

Save – saves entered data into the database.

Clear – deletes all data.

„**NONSTANDARD CODES** " **TAB**

Fig. 32. „Nonstandard codes" tab (part of „Subscriber" window) before defining nonstandard Contact ID codes.

The tab is available after adding identifier and selecting „Contact ID" type. It allows to define nonstandard codes of events sent in Contact ID format.

Type – select in this field the type of edited code:

  − **Alarm** – the code informs of an alarm at the subscriber's site. It requires intervention of the monitoring station operating personnel (after receiving the code, the alarm handling window will be displayed).

  − **Arming** – the code informs of arming. It requires no intervention of the monitoring station operating personnel, but allows to verify whether the arming occurred within the time interval defined for the „Time area" („Partitions" tab).

  − **Disarming** – the code informs of disarming. It requires no intervention of the monitoring station operating personnel, but allows to verify whether the disarming occurred within the time interval defined for the „Time area" („Partitions" tab).

  − **Trouble** – the code informs of a trouble at the subscriber's site. It requires intervention of the monitoring station operating personnel (after receiving the code, the trouble handling window will be displayed).

- **Restore** – the code informs of the end of previously reported trouble. It requires no intervention of the monitoring station operating personnel.
- **Test** – test transmission code. It requires intervention of the monitoring station operating personnel, unless it has been received according to the defined rules (see: „Test transmissions" tab).
- **Remark** – the code requires no intervention of the monitoring station operating personnel. When received, it will be saved in the event log and audibly signaled.
- **Other** – the code requires no intervention of the monitoring station operating personnel. When received, it will only be saved in the event log.

Code – enter in this field 4 digits, which have the Q-XYZ format, where:

- **Q** – digit 1, 3 or 6 (by default: 1 – new event or disarming, 3 – end event or arming, 6 – repeat event).
- **XYZ** – 3-character code of event.

Description – enter in this field a verbal description of the event which will be represented by the entered code. This description will be displayed in the „Event log" and in the event handling windows.

SS and CCC definition – select in this field how the last five characters of the received code should be interpreted (the whole code format is Q-XYZ-SS-CCC):

- **Partition** – SS denotes partition number, CCC will be disregarded.
- **Partition and zone** – SS denotes partition number, CCC denotes zone number.
- **Partition and user** – SS denotes partition number, CCC denotes user number.
- **User** – CCC denotes user number, SS will be disregarded.
- **Partition and expander** – SS denotes partition number, CCC denotes expander number.
- **System** – SS and CCC will be disregarded.

Buttons:

Save – saves event codes entered into the database.

Clear – deletes all event codes defined for the identifier.

Delete – deletes selected code.

ADDING IDENTIFIERS

In order to add a new identifier, do as follows:
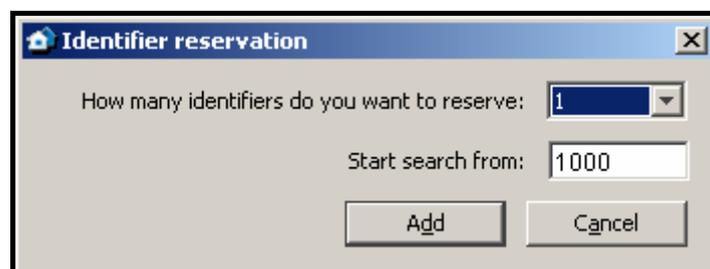
1. Click on the „Add" button.

Fig. 33. Reservation of identifiers.

2. A window will be displayed in which you must select the number of new identifiers you want to add. It is possible to add from 1 to 10 new identifiers.
3. Enter, from what value is the identifier to be searched for.

4. Press the „Add" button. The program will automatically search the database and find the identifiers which can be assigned to the subscriber.

EDITING IDENTIFIERS

To edit the existing identifier, do as follows:

1. Click your mouse on the identifier you want to edit (the column with identifier list on the left-hand side of the window). It will be displayed in the „Identifier" field.
2. Enter the new value in the „Identifier" field.
3. Click on the „Save" button. The program will check, if it possible to save the entered identifier. If it is, the changed identifier will be saved. It will retain all the settings entered for the previous identifier in the tabs „Definitions", „Partitions", „GSM", „Test transmissions" and „Ethernet".

7.8 EVENT HANDLING WINDOWS

The handling windows are available to users with the „handling" authority level.

After the monitoring station receives an intervention requiring event, the STAM-2 Server program will decide on which workstation to display the handling window. Taken into account is the number of events queued up for handling on each of the workstations. The handling window will be displayed on the workstation with the shortest queue of events waiting to be processed. If the handling window of the previously received event is currently open, the new handling window will not be displayed until it closes. If, for any reason, the window is closed without handling the event, i.e. without carrying out all the defined actions (e.g. their immediate execution is impossible, or it is recommended that they be executed later), the handling window will be displayed again after 10 minutes. Information on the events unhandled by the given user is displayed in the main window of the STAM-2 Client program (see: MAIN WINDOW OF STAM-2 CLIENT PROGRAM). A click on the selected icon („Alarm handling", „Trouble handling" or „Arm status event handling") will bring up successively the handling windows for events which have been received by the user, but still remain unhandled. The order of display depends on the subscribers' priority and the event receipt time (precedence is taken by the high-priority events which were received first, i.e. remain unhandled for the longest period of time).

Additionally, the handling window will be displayed when a user with the „handling" authority level clicks twice on an unhandled event in the „Event log" window. It enables handling the events which were received by other users.

There are 3 kinds of handling windows for 3 types of events that require intervention. The windows differ in color:

Alarm – red window. Refers to the alarm event received from the subscriber.

Fig. 34. Example of alarm handling window.

Trouble – yellow window. Refers to the trouble event, received from the subscriber or generated by the monitoring station (system).

Fig. 35. Example of trouble handling window.

Arm status – dark blue window. Refers to the event generated by the monitoring station (system), which informs of inconsistency between the actual status and the status defined for the partition (partition is armed, and should be disarmed; partition is disarmed and should be armed).

Fig. 36. Example of arm status handling window.

The handling window displays the following information:

Window heading – kind of situation that requires intervention: alarm, trouble or arm status.

When event occurred – time when event was received by the monitoring station, or the system event generated.

Event description

Event identifier and code (in case of system events, the „SYSTEM" message is displayed)

Monitored site data – information displayed in case of events received from the subscriber:

- **Partition** – partition name.
- **Expander** – expander name.
- **User** – name of the security system user.
- **Zone** – zone name.

Subscriber data – information displayed when the event is subscriber related:

- **Subscriber** – subscriber's name
- **Address** – subscriber's address.
- **Telephone** – subscriber's telephone number.
- **Installer** – data of the company or person who has installed the security system at the subscriber's site, or is at the present time responsible for maintenance and operability of the system.
- **Additional information** – displayed when the event refers to the subscriber for whom data have been entered into the „Additional information" field (see: „GENERAL" TAB in the „Subscriber" window).

Buttons:

Handle – opens the „Actions" window, unless the user has the „simple handling" authority or the simple handling of subscriber's events is permissible (see: „GENERAL" TAB in the „Subscriber" window). The event will then be handled immediately.

Alarms – the button is available to users having the „viewing" authority. It opens the „Event log" window with the tab in which alarm events received with the same identifier during the last 2 weeks will be displayed. Shown under the button is information on when the last alarm event with the same identifier was received.

Troubles – the button is available to users having the „viewing" authority. It opens the „Event log" window with the tab in which trouble events received with the same identifier during the last 2 weeks will be displayed. Shown under the button is information on when the last trouble event with the same identifier was received.

Partitions – opens the „Partitions" tab in the „Detailed information" window. Shown under the button is information on the partition current status.

Filter – the button is available to users having the „viewing" authority. It opens the „Event log" window with the tab in which events received with the same identifier over the last 2 weeks will be displayed (in case of the system events without identifier, the system events will be displayed).

Plans – available in case of events referring to the subscribers to whom the plans have been assigned (see: „PLANS" TAB). Opens the „Site plans" window.

Close – closes the window.

7.8.1 ACTIONS

The window displays the list of actions to be taken by the user who is handling the event.

Buttons:

Perform – press this button after the selected action has been carried out. A window will open in which performance of the ordered action is to be confirmed.

Give up – press this button when execution of the selected action is impossible. A window will open in which you must indicate the reason for giving up performance of the ordered action and confirm the intention to give up.

Comment – the button enables an additional comment to be added to the selected action.

Close – closes the window.

7.9 EVENT LOG

The window is available to users having the „viewing" authority in the „Event log" category. When opened, the window will display 200 recent events.

Address – address of the device by which the event was received. Events with no card address are system events, generated by the monitoring station program.

Date – date and time when the event was received.

ID – identifier with which the event was received. The system events have no identifier (except for the system events related to arm status).

Code – event code. In case of the system events, the „SYSTEM" information is displayed instead of the code. In case of the events which inform that SMS message or ring signal (CLIP type message) has been received by the GSM module, the „GSM" information is given.

Fig. 37. „Event log" window.

Description – verbal description of the event. Different types of events can be recognized by the description color:

- 🟥 (red) – „Alarm" type events.
- 🟩 (light green) – „Arming" type events.
- 🟩 (dark green) – „Disarming" type events.
- 🟧 (orange) – „Trouble" type events.
- 🟫 (brown) – „Restore" type events.
- 🟪 (violet) – „Test" type events.
- 🟦 (navy blue) – „Remark" type events and events notifying that SMS message or ring signal (CLIP type message) has been received by GSM module.
- 🟦 (light blue) – „Other" type events and system events referring to program operation.
- 🟪 (pink) – comment added by the user (see: NOTES).
- 🟨 (olive) – system events referring to arm status (see: „TIME AREAS" TAB).

If the event needs to be handled („Alarm" and „Trouble" type events and arm status system events), the color of the displayed text is black, but the whole event is highlighted in color assigned to this type of events.

Note: Displayed in the event log are also alarm and trouble events which were skipped or deleted, as well as events the execution of which, for various reasons, turned out to be impossible, hence the user gave up handling them.

Having selected the required event with your mouse pointer, click twice on it, or press the „Enter" button to:

- display the handling window in case of unhandled events (see: EVENT HANDLING WINDOWS), provided that the user has the „handling" authority
- display the window with event details in case of events which are already handled or do not require handling (see: DETAILED INFORMATION WINDOW)

Click on the event with the right mouse button to display menu with the following functions:

Information – click on this item to:

- display the handling window in case of the unhandled events (see: EVENT HANDLING WINDOWS), provided that the user has the „handling" authority
- display the event details window in case of the events which have been handled or do not require any handling (see: Detailed information window)

Filter – click on this item to display the „Filter" window.

Status board – click on this item to display the „Status board" window.

Displayed on the status bar at the bottom of the „Event log" window is additional information on the selected event. The information may include:

- System events
- Subscriber (name and consecutive number)
- Partition (name)
- Expander (name)
- User (name)
- Zone (name)
- GSM telephone number (number)

7.9.1 DETAILED INFORMATION WINDOW

Event type – information on the event type is always displayed. Additionally, a description defined for this event is given.

- **Alarm** – alarm at the monitored site.
- **Arming** – arming at the monitored site.
- **Disarming** – disarming at the monitored site.
- **Trouble** – trouble at the monitored site or at the monitoring station.
- **Restore** – end of trouble.
- **Test** – test transmission.
- **Remark**
- **SMS** – event informing that SMS message has been received by the monitoring station GSM module.
- **Telephone** – event informing that ring signal (CLIP type message) has been received by the monitoring station GSM module.
- **Other**
- **Log-in** – system event informing that user has logged in the STAM-2 program.
- **Log-out** – system event informing that user has logged out of the STAM-2 program.
- **Comment** – a comment added by the user (see: Notes).
- **Wrong arm status** – system event informing that the site arm status is inconsistent with the defined time areas.

Monitored site data – information displayed in case of events received from the subscriber.

- **Partition** – partition name.
- **Expander** – expander name.
- **User** – security system user's name.
- **Zone** – zone name.

Event data – additional information on the received event.

- **Occurrence time** – time when the event was received by the monitoring station or the system event was generated.
- **Received time** – time when the event was sent to one of the handling workstations. This information is displayed at the events which required handling.
- **By** – name of the program user to whose workstation the event was sent. This information is displayed at the events which required handling.
- **Delay** – time difference between receiving the event by the monitoring station and sending the event to one of the handling workstations. This information is displayed at the events which required handling.

Subscriber data – information is displayed if the event refers to the subscriber.

- **Subscriber** – subscriber's name
- **Address** – subscriber's address.
- **Telephone** – subscriber's telephone number.
- **Installer** – data of the company or person who installed the alarm security system at the subscriber's site, or is currently responsible for maintenance and operability of the system.

Program user data – information is displayed in case of system events (except for troubles).

- **User** – program user's name.
- **Address** – program user's address.
- **Telephone** – program user's telephone number.
- **Status** – program user's status.

Additional information – displayed if the event refers to the subscriber for whom data were entered into the „Additional information" field (see: „GENERAL" TAB in the „Subscriber" window).

Buttons:

Details – available in case of events that required handling. Opens the „Details" window.

Plans – available in case of events from the subscribers from the subscribers to whom the plans have been assigned (see: „PLANS" TAB). Opens the „Site plans" window.

Close – closes the window.

DETAILS

The window displays information on the action taken in connection with receiving an event that requires handling, and information on canceling the trouble. It may include:

- performance of defined actions
- giving up execution of defined actions
- simplified event handling
- trouble cancellation
- comment
- alarm clearing
- trouble clearing
- event skipping

7.9.2 FILTER

The filter allows to define criteria, on the basis of which events are to be displayed in a new tab in the „Event log" window. After opening, the „Event log" window will display 200 recent

events. Using the „Filter" window makes it possible to display a greater number of events and precisely specify which events are to be displayed.
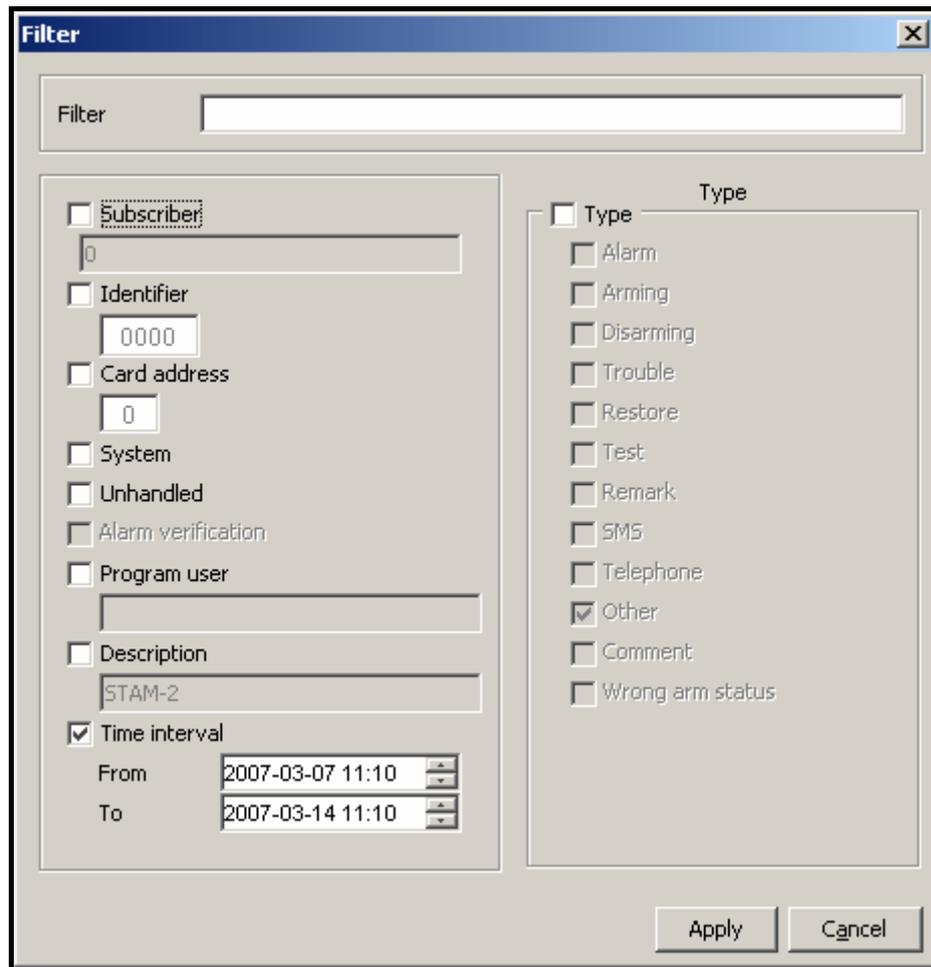

Fig. 38. „Filter" window.

Filter name – enter in this field the name to be given to the new tab in the „Event log" window.

You can select the following criteria of displaying events, by selecting the adjacent box:

Subscriber – events referring to the subscriber with a specified consecutive number. Enter the number in the field below. The events will include both those received from the subscriber and the system events generated in connection with this subscriber.

Identifier – events with a specified identifier. Enter the identifier in the field below.

Card address – events referring to the monitoring station device with a specified address. They will include both events received by the given device and the system events generated in connection with this device.

System – system events.

Unhandled – unhandled events.

Program user – system events referring to the program user. Enter the user name in the field below.

Description – events which contain a specified text in their description. This text is to be entered in the field below. If the „Description" option is selected but no text is entered into the field below, all events will be displayed.

Time range – events received within the time period defined in the fields below. By default, this option is selected, and the time range set at one week. If the option is not selected, all

the database events will be displayed (the only limitation being then the other display criteria).

Type – events of a specific type. Define the type by selecting the box next to description:

- **Alarm**
- **Arming**
- **Disarming**
- **Trouble**
- **Restore**
- **Test**
- **Remark**
- **SMS**
- **Telephone**
- **Other**
- **Comment**
- **Wrong arm status**

7.10 STATUS BOARD

The window is available to all users. Each subscriber is represented by means of a field with its consecutive number and an appropriate icon, graphically illustrating the subscriber's status. By clicking on one of the icons at the bottom of the window, the user can determine which information is to be currently displayed by means of the icons:

- alarms

- troubles
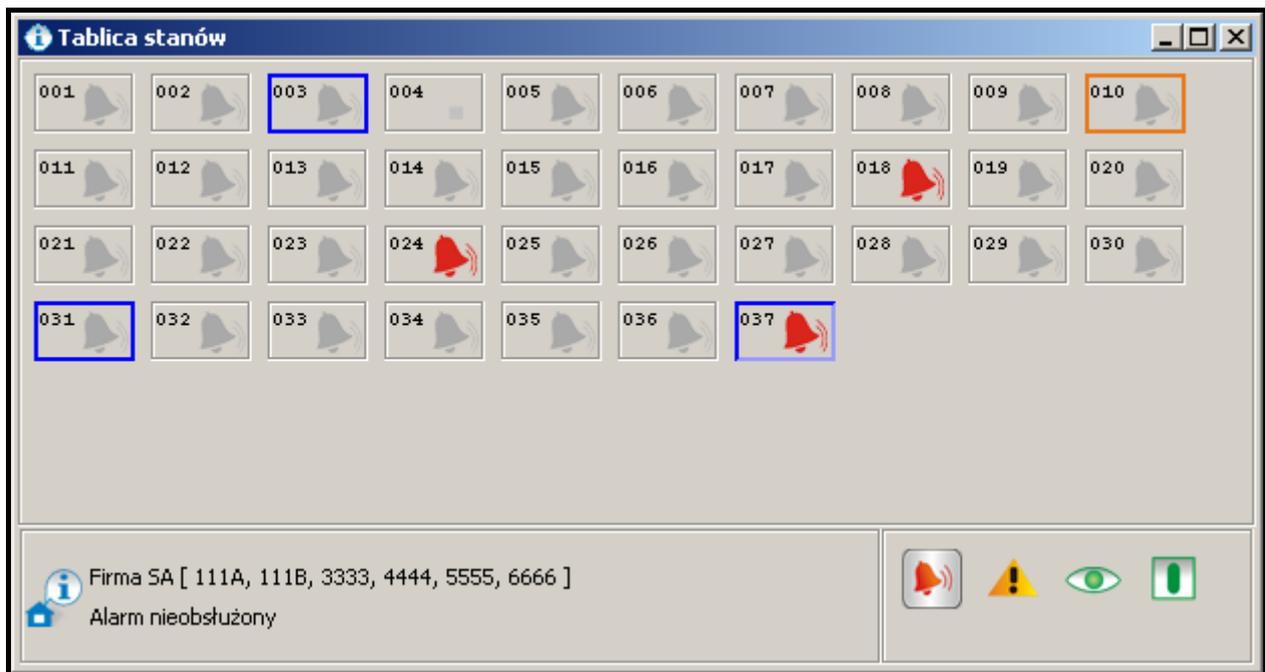
- arm statuses

- test transmissions

Fig. 39. „Status board" window with examples of subscriber statuses. Icons inform of unhandled events at subscribers Nos. 18, 24 and 37. Dark blue borders around subscriber fields Nos. 3, 31 and 37 indicate unhandled arm status. Orange border around subscriber field No. 10 indicates unhandled trouble.

Icon descriptions:

⊠ - no subscriber with this consecutive number

■ - subscriber inactive

🔔 - no unhandled alarm events from the subscriber

🔔 - there are unhandled alarm events from the subscriber

⚠ - no unhandled trouble events from the subscriber

⚠ - there are unhandled trouble events from the subscriber, but the troubles are inactive

✔⚠ - there are active troubles at subscriber's site, but events related to them are handled

⚠ - there are unhandled trouble events from the subscriber, and the troubles are active

◯ - subscriber's security system is disarmed (if the icon is flashing, the status is inconsistent with that defined in the „Time areas" tab and the system should be armed)

👁 - subscriber's security system is armed (if the icon is flashing, the status is inconsistent with that defined in the „Time areas" tab and the system should be disarmed)

👁 - security system is partially armed (if the icon is flashing, the status of at least one partition is inconsistent with that defined in the „Time areas" tab)

👁 - no arm status event has been received from the subscriber and the security system arm status remains unknown (if the icon is flashing, the system should be armed/disarmed, according to the settings defined in the „Time areas")

▯ - no defined test transmissions for the subscriber

▮ - test transmissions were received at the expected time

▯ - no test transmission

[?] - control panel and monitoring station have not been synchronized yet (no test transmission or another event was received, but the time period after which the lack of test transmission would be reported, has not expired yet)

[•] - waiting for test transmission (according to the settings, taking tolerance into account, the transmission is about to come)

A color border can appear around the icon field:

− red color – if trouble, arm status or test transmission icons are being displayed, and there are unhandled alarms.

− dark blue color – if alarm, trouble or test transmission icons are being displayed, there are no unhandled alarm, but there are unhandled arm status events.

− orange color – if alarm, arm status or test transmission icons are being displayed, there are no unhandled alarms or arm status events, but there are unhandled troubles.

The icon fields are arranged according to the consecutive number assigned to the subscribers (see: Subscribers). Using the „drag and drop" method, you can change the order in which the fields are displayed. The changes can be temporary, or can be saved when closing the „Status board" window. Saving the changes means that new consecutive numbers will be assigned to the subscribers.

Click on the icon field to display, at the bottom of the window, next to the [icon], information on the subscriber (name, identifiers) and explanations for the icon.

Click twice on the icon field, or select the required field with the mouse cursor and press the „Enter" button to display the „Detailed information" window.

7.10.1 DETAILED INFORMATION

Displayed in the upper part of the window is information on the subscriber (compare: „General" tab in the „Subscriber" window):

Subscriber [*consecutive number*]

Address

Telephone

Installer

Additional information

The following tabs are provided in the lower part of the window:

Unhandled alarms – list of alarm events received from the subscriber, which have not be handled yet.

Troubles – list of trouble events received from the subscriber, which:

− have not been handled, and no trouble restore event has been received (trouble unhandled and active),

− have not been handled, but trouble restore event has been received (trouble unhandled but inactive),

− have been handled, and no trouble restore event has been received (trouble handled but active).

Partitions – list of partitions defined for the subscriber, including information on the actual status of the given partition (armed / disarmed / unknown status), and what the status should be according to the settings defined in the „Time areas" tab (should be armed / should be disarmed / no status defined).

Test transmissions – list of test transmissions defined for the subscriber, including information on the transmission status (correct / incorrect / none).

Buttons:

Handle – available in the „Unhandled alarms" and „Troubles" tabs to users having the „handling" authority if there are unhandled events. Opens the „Actions" window.

Delete – available in the „Unhandled alarms" tab to users having the „alarm clearing" authority, and in the „Troubles" tab to users having the „trouble clearing" authority. Enables unhandled alarms / troubles to be cleared. Clearing an alarm / trouble means that the event will be considered as handled (in case of an active trouble, it will be considered as inactive).

Delete all – available in the „Unhandled alarms" tab to users having the „alarm clearing" authority, and in the „Troubles" tab to users having the „trouble clearing" authority. Allows to clear all unhandled alarms / troubles with the same identifier as the selected event.

Filter – opens the „Event log" window with the tab in which the subscriber events from the last 2 weeks will be displayed.

Plans – available in case of events from the subscribers to whom the plans have been assigned (see: „PLANS" TAB). Opens the „Site plans" window.

Close – closes the window.

7.11 REPORTS

The window is available to all users, but the scope of operations that can be done therein depends on the user's authority level. It enables printing in PDF format subscribers' reports, reports on work of selected program users, as well as event log and operation statistics of the system (users with the „report printing" authority) and monitoring station documentation (users with the „documentation printing" authority).

7.11.1 „SUBSCRIBER" TAB

The tab makes it possible to print subscribers' reports and documentation regarding subscribers.

Subscriber – the field allows to select the subscriber for whom the report or documentation is to be printed.

Documentation – select this field if documentation is to be printed.

Report – select this field if report is to be printed.

Identifiers – identifiers assigned to the subscriber:

- **All** – all identifiers assigned to the user. Click on the selected identifier to display it in the „To be printed" field and clear all identifiers from the list.

- **To be printed** – list of identifiers for which report or documentation is to be printed. Click on the selected identifier to display it in the „All" field and clear all „To be printed" identifiers from the list.

Report – options available after the „Report" field is selected. They allow to define which event types will be included in the report:

- **Alarm**
- **Arming**
- **Disarming**
- **Trouble**
- **Restore**
- **Test**
- **Remark**
- **SMS**

– **Telephone**

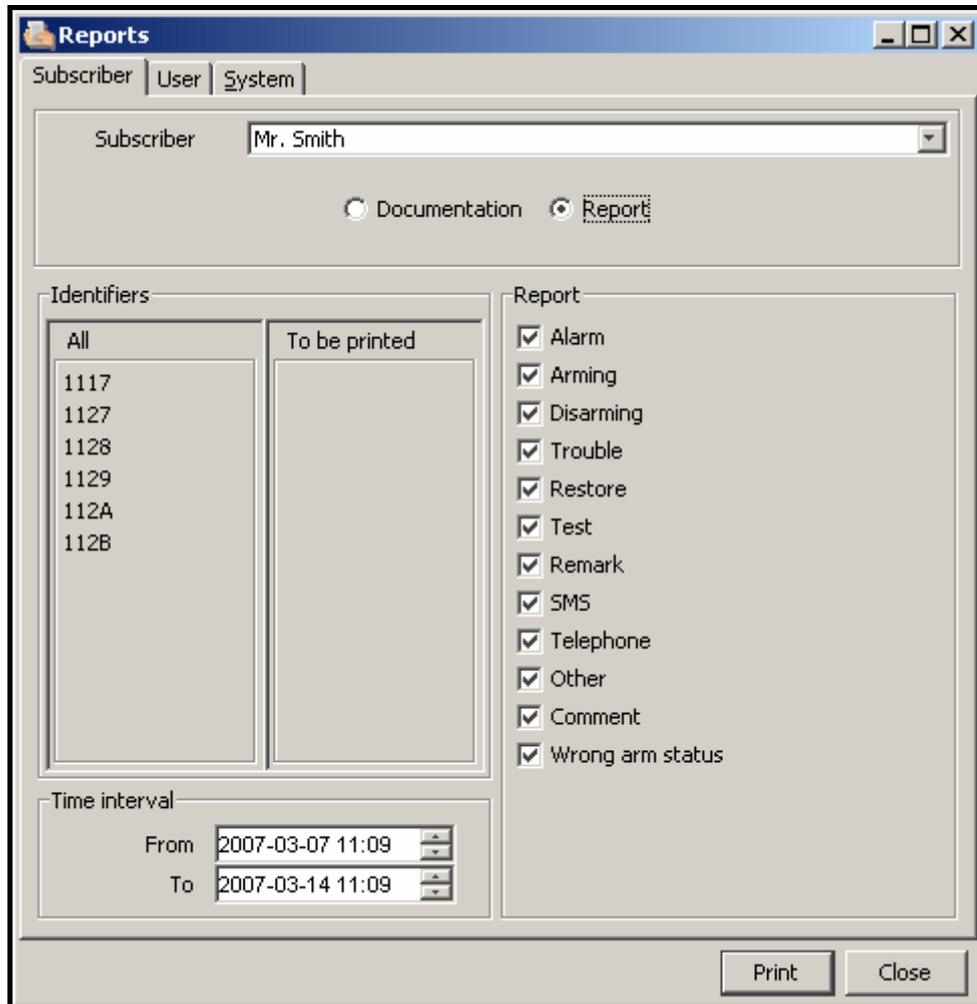– **Other**

– **Comment**

– **Wrong arm status**

Fig. 40. „Subscriber" tab in „Reports" window with „Report" field selected.

Time interval – available, after „Report" field is selected. Define the time interval of the report in the „From" and „To" fields. By default, the time range is set at one week.

Documentation – options available after selecting the „Documentation" field. Use them to determine which data will be included in the report:

– **Actions in case of alarm/trouble**

– **Additional information**

– **Identifiers list**

– **Contents of selected identifiers**

– **Partitions list**

– **Time areas definitions**

– **Skipping method**

– **Test transmission types**

– **SMS and CLIP definitions**
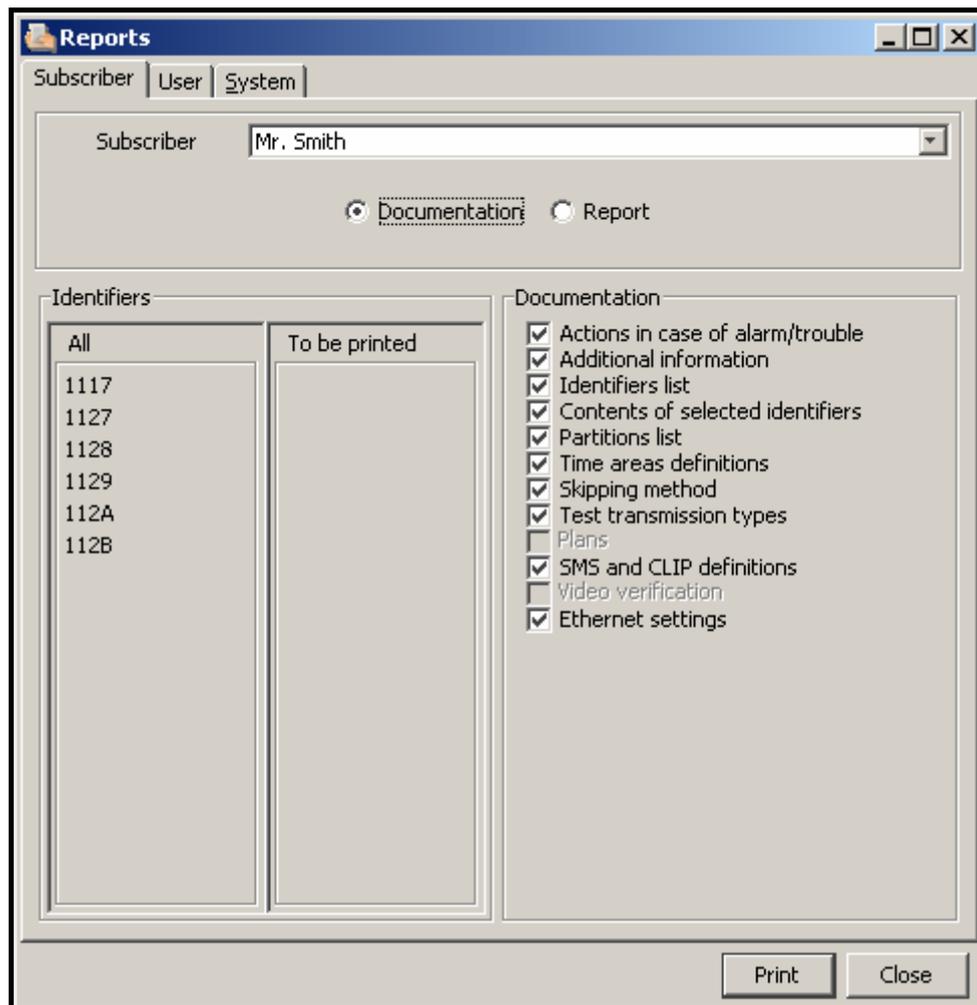
– **Ethernet settings**

Fig. 41. „Subscriber" tab in „Reports" window with „Documentation" field selected.

7.11.2 „USER" TAB

The tab makes it possible to print reports on program users' work.

User – the field allows selection of the program user to whom the report is to refer.

What to print beside information – these options enable you to define which additional information (except for the user's name, address, telephone and status) is to be included in the report:

- **Alarms handled**
- **Troubles handled**
- **Arm status events handled**
- **Shift starts and ends**
- **Comments**
- **Statistics**

Time interval – time range of the report is to be defined in the „From" and „To" fields. By default, the time range is set at one week.

Fig. 42. „User" tab in „Reports" window.

7.11.3 „SYSTEM" TAB

The tab enables printing reports on the monitoring station performance.

Report – the options make it possible to define which event types will be included in the report:

- **Alarm**
- **Arming**
- **Disarming**
- **Trouble**
- **Restore**
- **Test**
- **Remark**
- **SMS**
- **Telephone**
- **Other**
- **Comment**
- **Wrong arm status**

Time interval – time interval of the report is to be defined in the „From" and „To" fields. By default, the time range is set at one week.
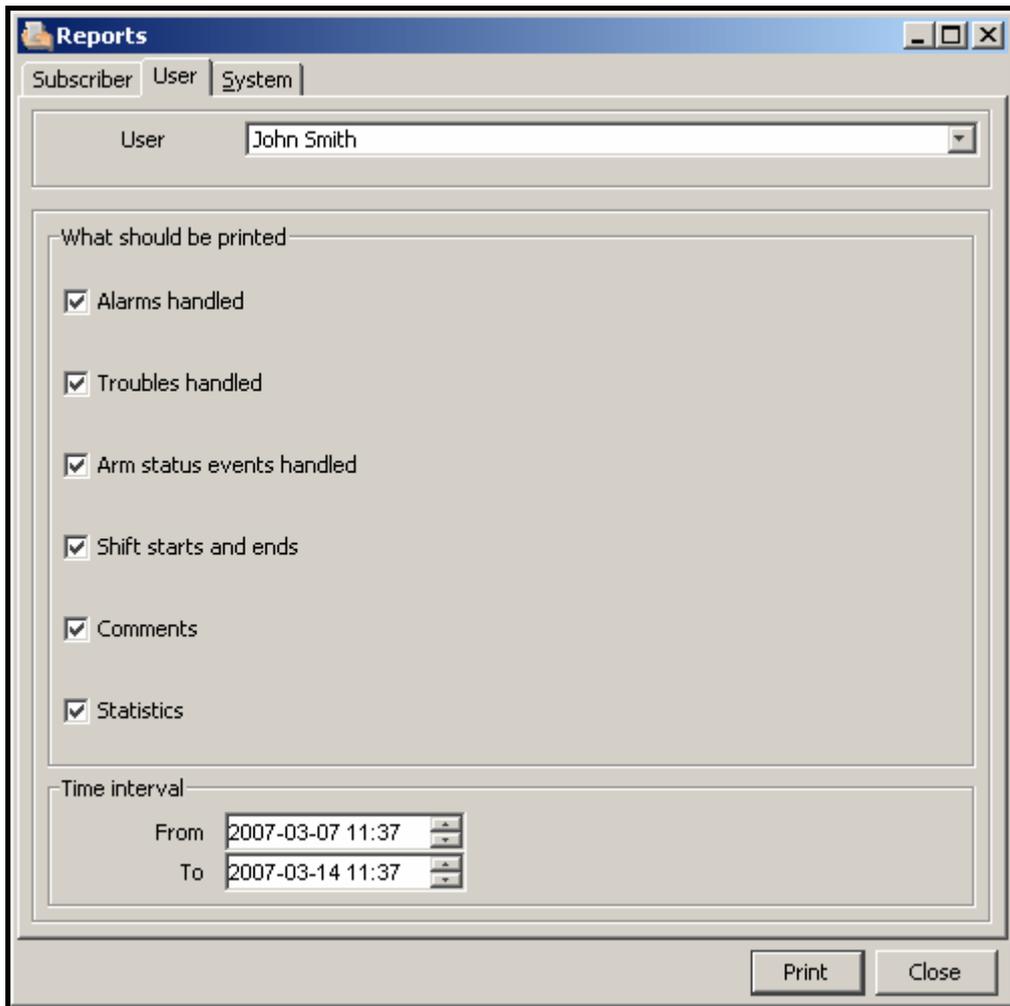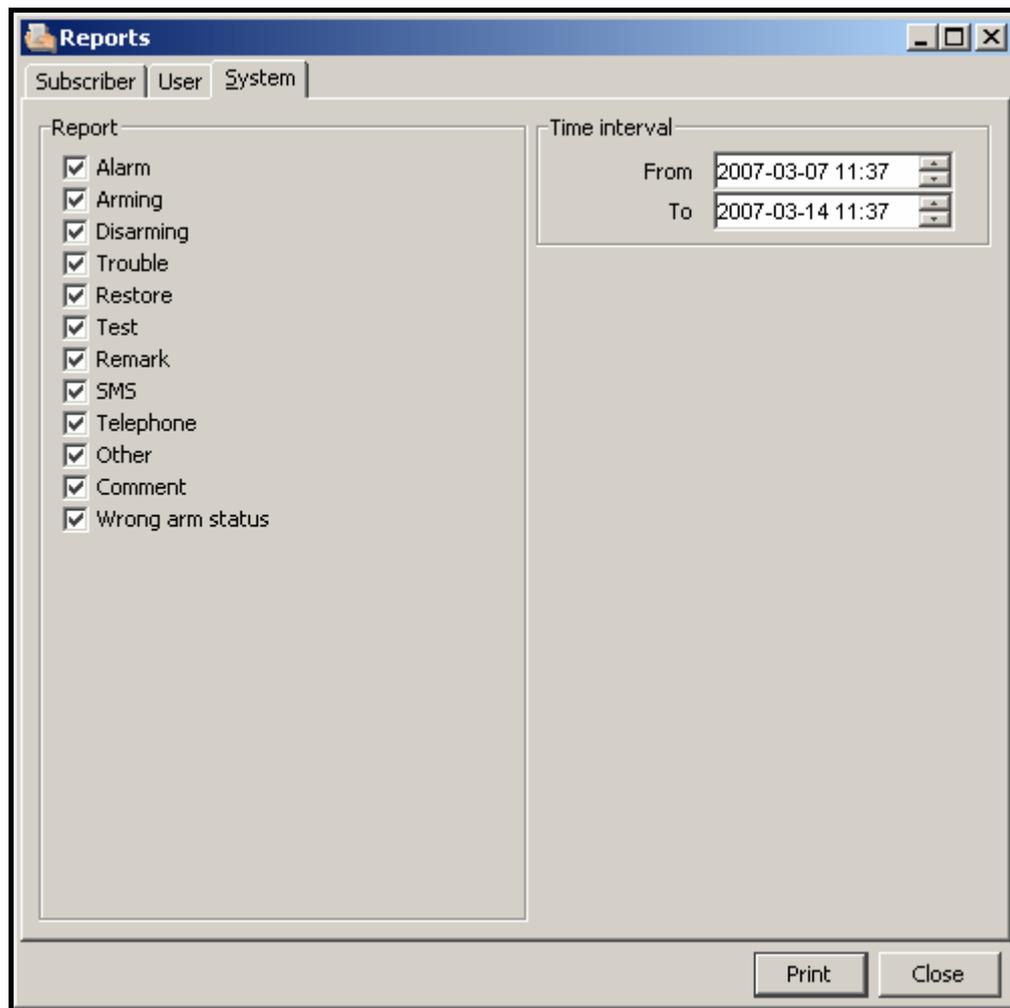
Fig. 43. „System" tab in „Reports" window.

7.12 NOTES

The window is available to all users.

7.12.1 „REVIEW" TAB

Displayed in the window is a list of notes created by other users of the program.

Buttons:

On time – the window with a list of received „On time" notes will be displayed. Click on the „Clear" button in the window to delete the notes.

Delete – deletes the selected note.

Close – closes the window.

7.12.2 „MY NOTES" TAB

The window displays a list of „Normal" type of notes created by the user, which have not been deleted. These notes can be edited or deleted. Also new notes can be created. The new note can be of one of the 3 following types:

− **Normal** – to be sent to the concrete person or a certain group of persons immediately after being created.

− **On time** – to be sent to the concrete person or a certain group of persons, but activated at the defined time during the specified time interval on the selected days of week.

− **Comment** – the note content will be saved to the event log („Comment" type event).

Buttons:

New – opens the window in which a new note can be created.

Edit – allows you to edit the already existing „Normal" type notes.

Delete – deletes the selected note.

Close – closes the window.

8. LICENSE AGREEMENT

1. SATEL sp. z o.o., a limited liability company, having its registered office at 79 Schuberta Street, 80-172 Gdansk, Poland, entered in the Register of Entrepreneurs kept by the District Court Gdansk-North in Gdansk, 7th Economic Department of the National Court Register (KRS), under KRS number 0000178400, NIP taxpayer number 584-015-40-38, share capital PLN 1,830,000 (hereinafter the "Licensor") hereby grants a nonexclusive license to use the STAM-2 program, hereinafter called the "Program", supporting operation of the computer installed base receiver card of STAM-1 P or STAM-1 PE monitoring station, hereinafter called the Device, in the following fields of use:

   1.1. loading the Program into the computer memory and replicating the Program in the computer memory;

   1.2. adapting the Program, without changing its source codes, for the Licensee's hardware platform and configuration,

   - however, exclusively for the use of the Device according to its intended purpose.

2. The License shall be granted to each Owner of the Device. The granted License may not be transferred, including sub-license, lease or rental to third parties in any way, but only with transfer of the title of ownership to the Device.

3. The License is granted against payment by the Licensee of the one-time license fee, fixed on the basis of the current price-list of the Licensor.

4. The „STAM-2 Server" program may only be installed on one computer, while the „STAM-2 Client" program - on several computers, however the „STAM-2 Client" may only be simultaneously used on the number of workstations specified in the invoice received from the Licensor.

5. The right to use the Program is defined by the hardware key and the unique LICENSE CODE which are assigned to the Licensee. The license code 1) shall determine the Licensee's authority level, as well as some options of the Program, and 2) shall be made available to third parties in no other way than together with the Device, in accordance with Item 2 above. The license code makes it possible to use the Program on the computer intended for installation of the Program. Such a code will be assigned only once. In justified cases, for example, hardware failure or replacement, or as specified below, the code may be assigned once more.

   5.1. Having installed the Program, the Licensee shall register the Program, by means of the Licensor's website, fax or mail, by sending to the Licensor the individual serial number of the hardware key assigned to the Licensee, based on which the Licensor will create a unique license code for each installation. The code will be sent to the Licensee by e-mail, or by means of anther data carrier. In order to make the Program operable, the code must be entered into the Program.

   5.2. During 30 days of the installation, the Program will work without the license code, and afterwards the hardware key will be permanently disabled by the Program. In this state, the Program will be functioning for a certain period of time and then it will be blocked. Should this happen, the Licensee must purchase a new hardware key and

install it in the Program (losing the data of supervised facilities and the history of events). In this case, the Licensee shall carry out another installation against payment, as provided for in the current price-list of the Licensor.

5.3. The Licensor shall make sure that the hardware key remains permanently in the computer on which the „STAM-2 Server" Program is running, as lack of the key will cause unregistration thereof. In such a case, to ensure further operation of the Program, the Licensee shall be obliged to purchase a new hardware key from the Licensor and carry out another installation against payment, as provided for in the current price-list of the Licensor.

6. The Licensor may make Program updates available to the Licensee, provided they are created, for a period of 12 months from the Program purchase date. After expiry of the twelve months from the Program purchase date, the updates can be provided to the Licensee against payment, according to the current price-list of the Licensor. The Licensee shall make no claims in relation to the Licensor for creating updates or upgrades to the Program. Updates and upgrades will be made available to the Licensee in accordance with the Licensor's work process and trade policy.

7. The Program shall be delivered and may only be used in the form of computer readable resultant code. In particular, the Licensee shall not be allowed to:

7.1. disassemble, decompile, translate or try to otherwise reverse engineer the source code of the Program, or create derivations of the Program or components thereof, even if such actions result from the intention to repair errors or run an inoperative Program;

7.2. remove, alter or cover copyright information and notices of intellectual property rights that are in the Program;

7.3. create derivative programs (works), make copies, translate, adapt, change layout, or otherwise modify or disseminate the Program (in electronic form or otherwise), or any copy, adaptation, transcription, or mixed version thereof;

7.4. make the Program or copies thereof available to third parties, regardless of the purpose of such actions, including the service purposes or repair of other defects, unless it is necessary for using the Program or the Device by the Licensee, according to their intended purpose, or the service or repair of defects is to be carried out by an entity authorized by the Licensor.

8. Materials for the Licensee are attached to the Program in electronic form (as Help files) only to facilitate the use of the authorized version of the Program by the Licensee. The Licensee shall have no right to use, copy, modify or disseminate the end user materials, make adaptations, transcriptions or mixed versions thereof for any other purpose without previous explicit authorization from the Licensor.

9. Any liability of the Licensor for defects of the Program and materials attached thereto, including liability under the guarantee and warranty for physical defects shall be excluded, except for the warranty for legal defects. In particular, the Licensor shall bear no liability for any damages or errors caused by the Program, both direct and consequential, loss of profit, etc. Specifically, the Licensor does not guarantee that the Program will work faultlessly in all circumstances. The Licensor guarantees no compatibility of the Program with subsequent updates or versions of the software environment the Program works in. Furthermore, the Licensor gives no guarantee as to merchantability or suitability for a particular purpose. Also, the Licensor does not guarantee that 1) the Program will meet the needs or expectations of the Licensee; that 2) the Program use will be trouble-free; nor that 3) the irregularities, if any, will be or can be rectified. The Program is delivered on the „AS IS" basis, without any explicit or implied guarantee of fitness for particular

purposes. The Licensor's liability which under mandatory legal provisions can not be excluded by this clause, shall be limited to the amount of one-time paid license fee.

10. The Licensor acknowledges that this Agreement shall not make him Owner of or grant him any ownership rights to the Program, or any related patents, copyrights, trademarks or other intellectual or industrial property rights whatsoever, except for the rights arising from the granted license.

11. The Licensor shall retain the copyrights to all copies of the Program recorded on the original data carriers, and to the subsequent copies of the Program made at any time whatsoever, irrespective of the form or data carriers on which the original or other copies were recorded.

12. This License does not mean the sale of the original or any next copy of the Program. This License shall not assign to the Licensee the title of ownership to the Program, or to the copyrights to the Program, but only the limited right to use the Program.

13. The Licensee may, without consent of the Licensor, make for his own needs one backup copy of the Program for archive purposes, however such copy may not be used simultaneously with the Program. When making the backup copy, the Licensee shall be obliged to reproduce on that copy the reservation of the Licensor's copyrights or any other suitable notices that were on the original Program. The Licensee is entitled to make copies of the user documentation. This provision does not infringe upon the Licensee's rights arising from Art. 75 of the Law on Copyright and Derivative Rights of 4 February 1994.

14. The Licensee shall make every effort to prevent infringement upon the Licensor's rights.

15. The Licensor shall have the right to terminate the license granted to the Licensee if the Licensee violates these terms and conditions of the license. If the license is terminated by the Licensor, the Licensee shall be obliged to immediately return to the Licensor the Program carriers being in Licensee's possession and remove the Program from the computer memory. Termination of the license shall not result in refund of the sum paid for the license.

16. All declarations, notices and applications made by the Parties shall only be made in written form, or else the notices and applications shall have no legal or actual effect.

17. These terms and conditions of the license constitute the exclusive basis for the rights and obligations of the Parties to the extent of the subject-matter hereof and supersede any and all previous arrangements and settlements between the Parties in this respect.

18. The applicable law shall be the Polish law. The court competent to settle disputes shall be the Court in Gdansk.

19. Installation of the Program shall mean acceptance of the terms and conditions of this Agreement by the Licensee.