Alarm Control Panel
PERFECTA
Firmware Version 1.00

SATEL
®

CE 1471

PROGRAMMING

Before you start programming, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

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

Hereby, SATEL sp. z o.o., declares that this control panel is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at www.satel.eu/ce

Service code: 12345

The following symbols may be used in this manual:

- note,

- caution.

CONTENTS

1.   Introduction

You can configure the PERFECTA alarm system by using:

- a computer running the PERFECTA SOFT program (locally or remotely),
- a keypad.

The control panel can be configured when the ACTIVE option is enabled (see USER MANUAL).

i *As required by the standards, the service access after completion of the installation has to be limited by the administrators.*

Names of parameters and options from the PERFECTA SOFT program are used in this manual. At the description of each parameter or option, you will find one of the following data in square brackets:

- name of the function which is used for configuring a parameter or option on the keypad,
- name of a parameter or option from the keypad.

2.   Configuring the system by using keypad

You can configure the alarm system by using functions available in the service mode menu.

⚠   **When the control panel is running in service mode, tamper alarms are not generated.**

2.1   Starting the service mode

1. Enter the **service code** (by default: 12345) and press [* ✆].
2. User menu appears.
3. Press [🔑|▲].
4. When the ✛ cursor shows the SERVICE MODE function, press [# ▯].
5. Service mode menu will be displayed (the ✛ cursor will show the END SM function).

2.2   Starting the service mode "from pins"

When entering the service mode in the normal way is not possible (the control panel does not support keypads, does not accept the service code, etc.), you can use the emergency procedure, so-called, starting "from pins".

1. Turn off the control panel power supply (first disconnect the AC power, and then the battery).
2. Put a jumper on the RESET pins on the control panel mainboard.
3. Turn on the control panel power supply (first connect the battery and then the AC power).
4. Wait a few seconds (until LEDs next to the RESET pins stop flashing) and remove the jumper from the RESET pins. The control panel will enter the service mode. The service mode menu will be displayed on the wired keypad with the lowest address.

i *If there is no wired keypad in the alarm system or there is no communication with the wired keypads (e.g. when the communication bus is shorted), you can get access to the service mode menu from the wireless keypad with the lowest address. Press any key on this keypad within 30 seconds of removing jumper from the RESET pins.*

The service mode menu will not be displayed, if the DISABLE SERVICE MODE option is enabled in the control panel. The "Factory settings ? 1=Yes" message will be

displayed on the keypad with the lowest address. You can press $\boxed{1}$ *to restore the factory default settings. The service mode menu will not be displayed until the factory settings are restored.*

2.3 Service mode indication

The service mode is indicated on the keypads by means of the $\boxed{\text{⸰⸻}}$ LED. The $\boxed{\text{⸰⸻}}$ LED is steady ON on the keypad on which the service mode menu is displayed, and is flashing on the other keypads. Additionally, the service mode can be signaled audibly, after the appropriate option is enabled.

2.4 Navigating through the menu and running functions

To navigate throughout the menu, you can use the arrow keys or number shortcuts. You can also combine the two methods. The cursor ✛ shows the submenu you can enter / function you can run.

2.4.1 Using the arrow keys
1. Using the $\boxed{\times|\blacktriangledown}$ and $\boxed{\wp|\blacktriangle}$ keys, find the required submenu.
2. Press $\boxed{\text{☀}|\blacktriangleright}$ or $\boxed{\text{\# }\mathbb{0}}$ to open a submenu (use the $\boxed{\text{(}|\blacktriangleleft}$ key to go back to the main menu).
3. Repeat the steps 1 and 2 until the required function is found.
4. Press $\boxed{\text{☀}|\blacktriangleright}$ or $\boxed{\text{\# }\mathbb{0}}$ to run the function.

2.4.2 Using the number shortcuts
Submenus and functions are numbered (you can find the numbers in the LIST OF SERVICE FUNCTIONS document).
1. Use the number keys to enter the number (use the $\boxed{\text{(}|\blacktriangleleft}$ key to erase the last digit).
2. The menu item designated by this number will be displayed (use the $\boxed{\text{✱ ♠}}$ key to go back to the main menu).
3. Press $\boxed{\text{☀}|\blacktriangleright}$ or $\boxed{\text{\# }\mathbb{0}}$ to open a submenu or run a function.

If the cursor ✛ indicates END SM and you want to quickly run a function, enter its number and press $\boxed{\text{☀}|\blacktriangleright}$ or $\boxed{\text{\# }\mathbb{0}}$. For example, to run the expander identification function, press successively $\boxed{2_{\text{ABC}}}\boxed{1}\boxed{\text{\# }\mathbb{0}}$.

If the cursor ✛ indicates an item different from END SM, entering a digit will add this digit at the end of the number by which the item displayed in the menu is designated. New digits are always added at the end of the number displayed (only the END SM function is not numbered). For example, if the cursor ✛ indicates a menu item with the 31 (31.EOL) number, pressing $\boxed{3_{\text{DEF}}}\boxed{2_{\text{ABC}}}$ in turn will display the 3132 (3132.Zn.32 EOL) item, not the 32 (32.SENSITIVITY) item. To display the 32 (32.SENSITIVITY) item, you should press $\boxed{\times|\blacktriangledown}$ (to move the cursor ✛ down) or $\boxed{\text{(}|\blacktriangleleft}\boxed{2_{\text{ABC}}}$ (to erase 1 and add 2).

If you remember the submenu/function number and you want to avoid mistakes, press $\boxed{\text{✱ ♠}}$ before entering the number.

2.5 Data editing

The editing method depends on the type of data. Having completed the editing, press $\boxed{\text{\# }\mathbb{0}}$ to save the changes. If you want to exit the function without saving the changes, press $\boxed{\text{✱ ♠}}$.

2.5.1   Selection from the single-choice list

In the lower line of the display, the currently selected item is presented. You can scroll the list using the ⊠▼ and ⚿▲ keys.

2.5.2   Selection from the multiple-choice list

In the lower line of the display, one of the items you can choose from is presented. You can scroll the list using the ⊠▼ and ⚿▲ keys. The following symbol is situated in the upper right corner of the display:

▣ – displayed item is selected / option is enabled,

· – displayed item is not selected / option is disabled.

Press any number key to change the currently shown symbol for another one.

If you want to see the status of all items (these can be e.g. zones, outputs, options, etc.), press ☀▶ or ☾◀. The numbers around the display allow the items to be identified. Use the ☀▶ and ☾◀ keys to move the cursor. After hovering the cursor over the selected item, you can change its status by pressing any number key. If you want to restore the previous way of presentation of the list, press ⊠▼ or ⚿▲.

2.5.3   Entering decimal values

To enter digits, use the number keys. Use the ☀▶ and ☾◀ keys to move the cursor. In some functions, the ⚿▲ key deletes the character on the left side of the cursor.

2.5.4   Entering hexadecimal values

To enter digits, use the number keys. To enter the A, B and C characters, use the 2ABC key, and to enter D, E and F, use the 3DEF key (keep pressing the key until the required character appears). Use the ☀▶ and ☾◀ keys to move the cursor. The ⚿▲ key deletes the character on the left side of the cursor.

2.5.5   Programming telephone numbers

To enter digits, use the number keys. To enter the +, *, # characters, use the 0❶ key (keep pressing the key until the required character appears). Use the ☀▶ and ☾◀ keys to move the cursor. The ⚿▲ key deletes the character on the left side of the cursor.

2.5.6   Entering names

The characters that can be entered by using the keys are presented in Table 1. Keep pressing the key until the required character appears. Long press the key to display the digit assigned to it.

Shown on the right side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke).

Use the ☀▶ and ☾◀ keys to move the cursor. The ⚿▲ key deletes the character on the left side of the cursor.

Key	Characters available after next keystroke																
1	!	?	'	`	↵	"	{	}	$	%	&	@	\	^	|	⌐	#	1
2 ABC	a	b	c	2												
3 DEF	d	e	f	3												
4 GHI	g	h	i	4												
5 JKL	j	k	l	5												
6 MNO	m	n	o	6												
7 PQRS	p	q	r	s	7											
8 TUV	t	u	v	·	■	▮	▯	↑	←	→	↓	8				
9 WXYZ	w	x	y	z	9											
0 ❶		.	,	:	;	+	-	✳	/	=	_	<	>	(	)	[	]	0

Table 1. Characters available when entering names. The upper case letters are available under the same keys (to change the letter case, press ✖▼).

2.6 Hiding the service mode

You can hide the service mode by using the 09.HIDE SM function. The control panel will remain in the service mode, but the service mode menu will not be displayed. The function can be useful e.g. when you have to leave the keypad, but you want to prevent unauthorized personnel from getting access to the service menu in the meantime. To get access to the menu again, proceed in the same way as when entering the service mode.

2.7 Exiting the service mode

Keep pressing ✱✆ until the cursor ⇥ indicates the SM END function, and then press # 🂠.

3. Configuring the system with the PERFECTA SOFT program

You can download the PERFECTA Soft program from the www.satel.eu website.

Communication between the program and the control panel is encrypted. The control panel can be programmed locally or remotely. Remote programming is only possible after the GSM/GPRS communicator settings have been configured (see "GSM phone" p. 16).

3.1 Description of the PERFECTA SOFT program

Access to the program can be password protected (see ""Configuration" window" p. 11).
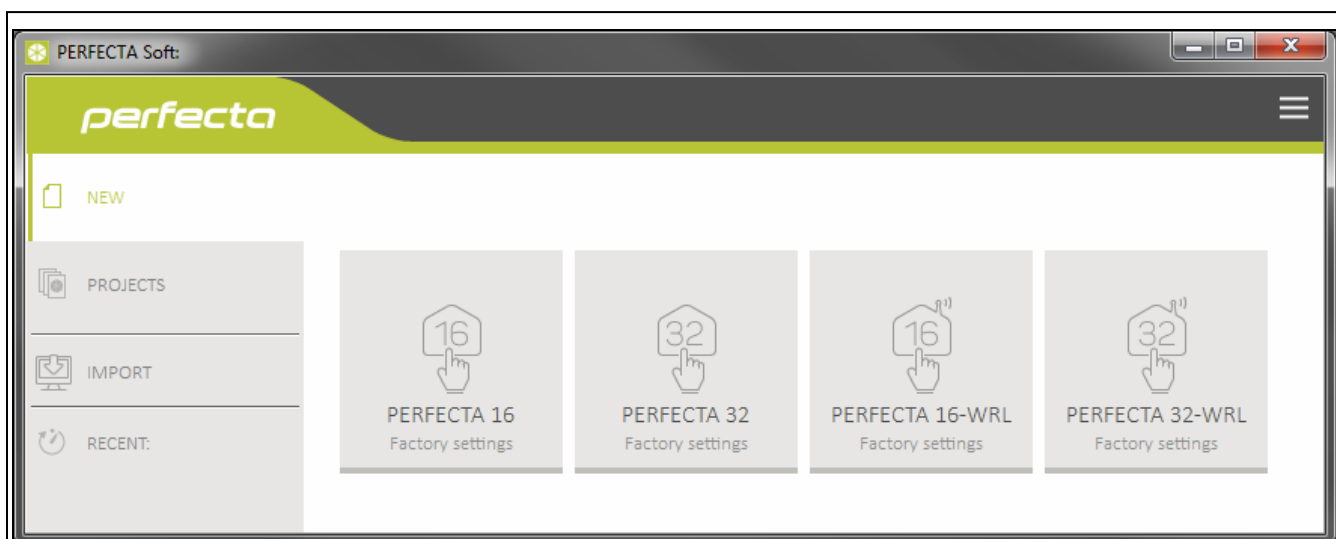
Fig. 1. PERFECTA SOFT window when the program is run for the first time.

3.1.1 Menu bar in the PERFECTA SOFT program

The menu bar is displayed in the top part of the program window. Appearance of the menu bar depends on the contents presented in the window.

Menu bar in the "Projects" tab

Fig. 2. Appearance of the menu bar when the "Projects" tab is displayed.

The search field is displayed on the menu bar. If you want to find a project file, click on the search field and start entering characters. The current view will be filtered out, based on the text entered.

Buttons

	click, if the files are to be sorted by name (the arrow next to the button indicates whether the files from A to Z or from Z to A are displayed)
	click, if the files are to be sorted by the time they were saved to disk (the arrow next to the button indicates whether the files are displayed in the descending or ascending order)
	click, if the information about files is to be presented in brief version
	click, if the information about files is to be presented in full version
	click to display additional menu.

Appearance of the menu bar when displaying the control panel data
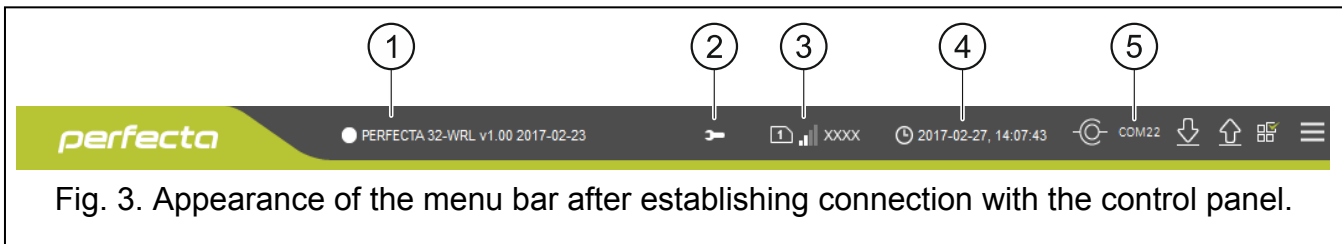
Fig. 3. Appearance of the menu bar after establishing connection with the control panel.

(1) type of alarm control panel and firmware version.

(2) icon displayed when the control panel is running in the service mode.

(3) information about the SIM card used, GSM signal level and operator of the GSM network used by the communicator.

(4) date and time according to the control panel clock.

(5) information on the way of communication with the alarm control panel:

COMn [n – number of computer COM port] – local connection,

TCP – remote connection (GPRS).

Buttons

	click to establish connection to the control panel. The button is displayed when the program is not connected to the control panel.
	click to finish connection to the control panel. The button is displayed when the program is connected to the control panel.
	click to read data from the control panel.
	click to write data to the control panel.
	click to display information on the status of partitions, zones, outputs etc. The button is active after connection to the control panel is established.
	click to display additional menu.

3.1.2   Side menu

The side menu is displayed on the left side of the program window. Appearance of the menu depends on the contents presented in the window.

The side menu before the control panel data are displayed

New – click to display the "New" tab.

Projects – click to display the "Projects" tab.

Import – click to import the file with control panel settings.

Recent – the list of recently opened files. Click on the name of the file to open it.

"New" tab

The tab displays the files with default settings of the PERFECTA control panels.

"Projects" tab

The tab displays the files saved to the computer disk, containing data of the PERFECTA control panels.

The side menu after the control panel data are displayed

After the file with control panel data is opened or connection with the control panel is established, the side menu will display buttons which open the tabs used for configuration of the control panel settings.

3.1.3   Additional menu

The additional menu is displayed after you click on ▤. Appearance of the menu depends on the contents presented in the window.

Open – click to display the "Projects" tab.

Save – click to save the control panel data to the computer disk.

Export – click to export the file with control panel data.

Connection – click to open the "Connection" window.

Configuration – click to open the "Configuration" window.
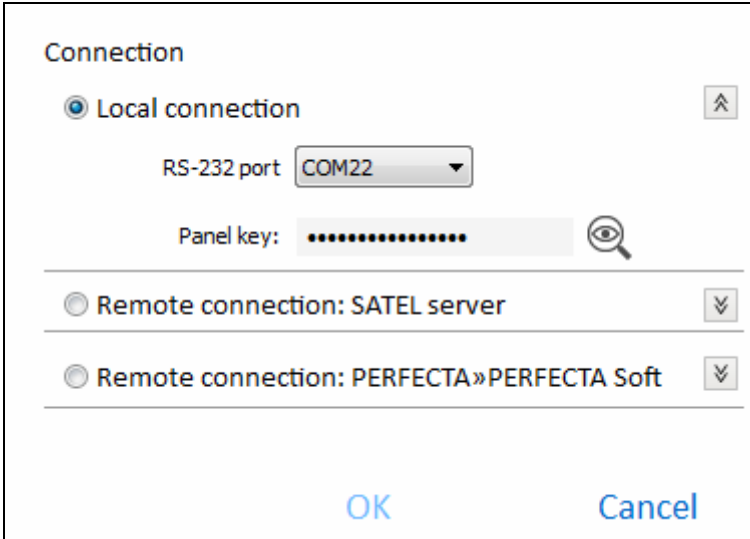
About – click to display information about the PERFECTA SOFT program.

"Connection" window

In the window, you can choose how connection with the control panel is to be established:

- if the control panel is to be programmed locally from the computer connected to the RS-232 (TTL) port on the control panel, select "Local connection",
- if the control panel is to be programmed remotely via GPRS by using the SATEL server, select "Remote connection: SATEL server",
- if the control panel is to be programmed remotely via GPRS, but the control panel is to connect directly to the program, select "Remote connection: PERFECTA>>PERFECTA Soft".

Local connection

Fig. 4. "Connection" window: local connection settings.

RS-232 port – COM port of the computer through which communication with the RS-232 (TTL) port of the control panel is to take place.

Panel key – identifier of the control panel. It must be identical to that programmed in the control panel (see p. 30).

Remote connection: SATEL server
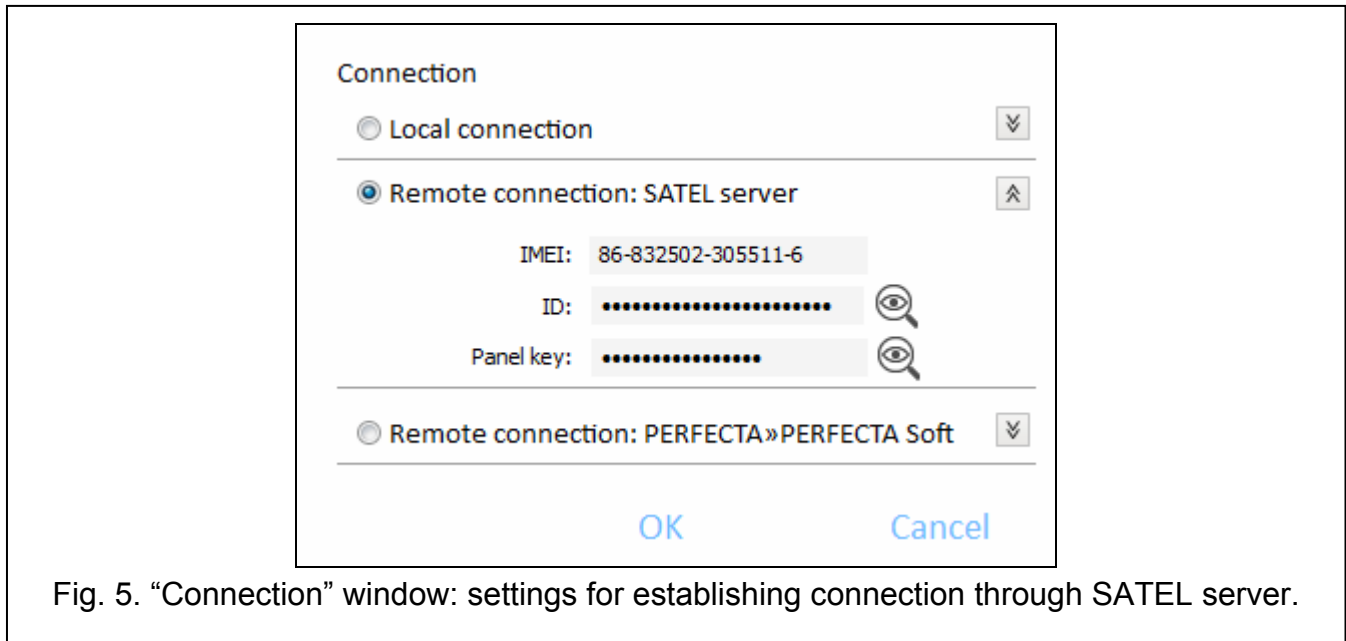
Fig. 5. "Connection" window: settings for establishing connection through SATEL server.

IMEI – individual identification number of the control panel GSM communicator.

ID – individual identification number for the purposes of communication through the SATEL server (assigned automatically by the SATEL server).

To check the IMEI number and ID number on the keypad, use the 7.IMEI/ID function (enter the user menu and press 9_{WXYZ} 7_{PQRS} in turn).

If the control panel was programmed locally before, the IMEI number and ID number will be read from the control panel data.

Panel key – identifier of the control panel. It must be identical to that programmed in the control panel (see p. 30).

Remote connection: PERFECTA>>PERFECTA Soft
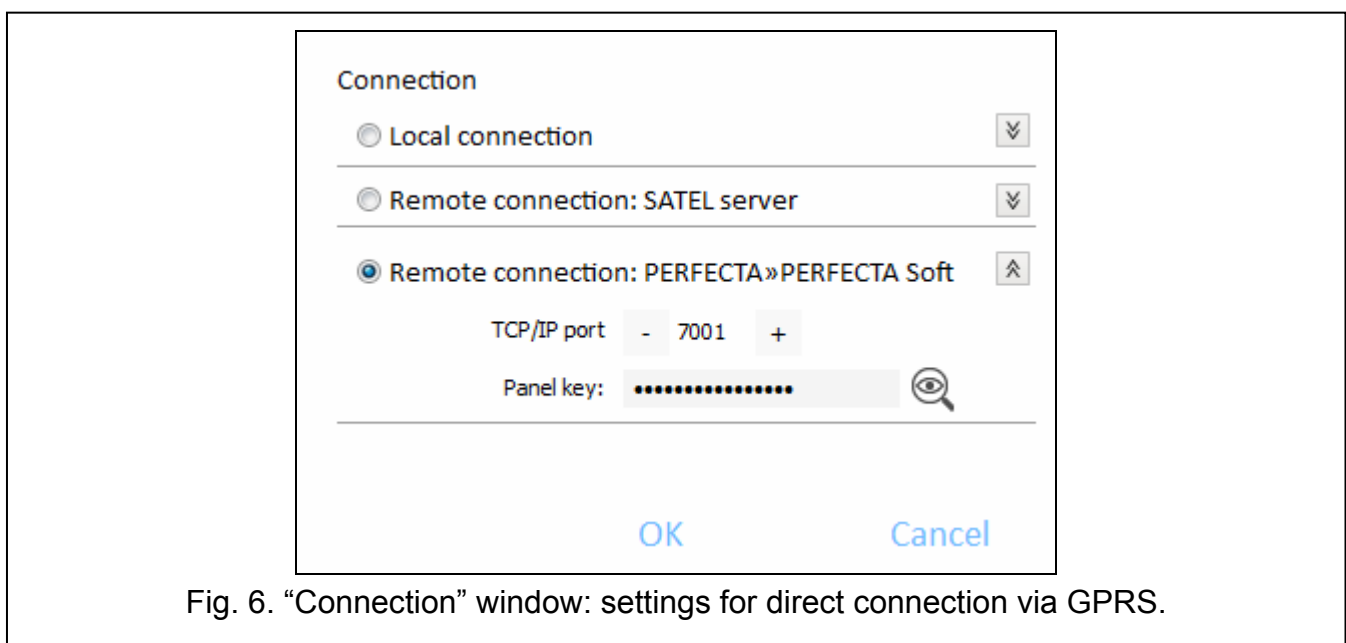
Fig. 6. "Connection" window: settings for direct connection via GPRS.

TCP/IP port – number of the TCP port used for direct communication between the control panel and the computer with PERFECTA SOFT program via GPRS.

Panel key – identifier of the control panel. It must be identical to that programmed in the control panel (see p. 30).

Buttons

OK – click to confirm the changes.

Cancel – click to close window without saving changes.

"Configuration" window

Fig. 7. "Configuration" window.
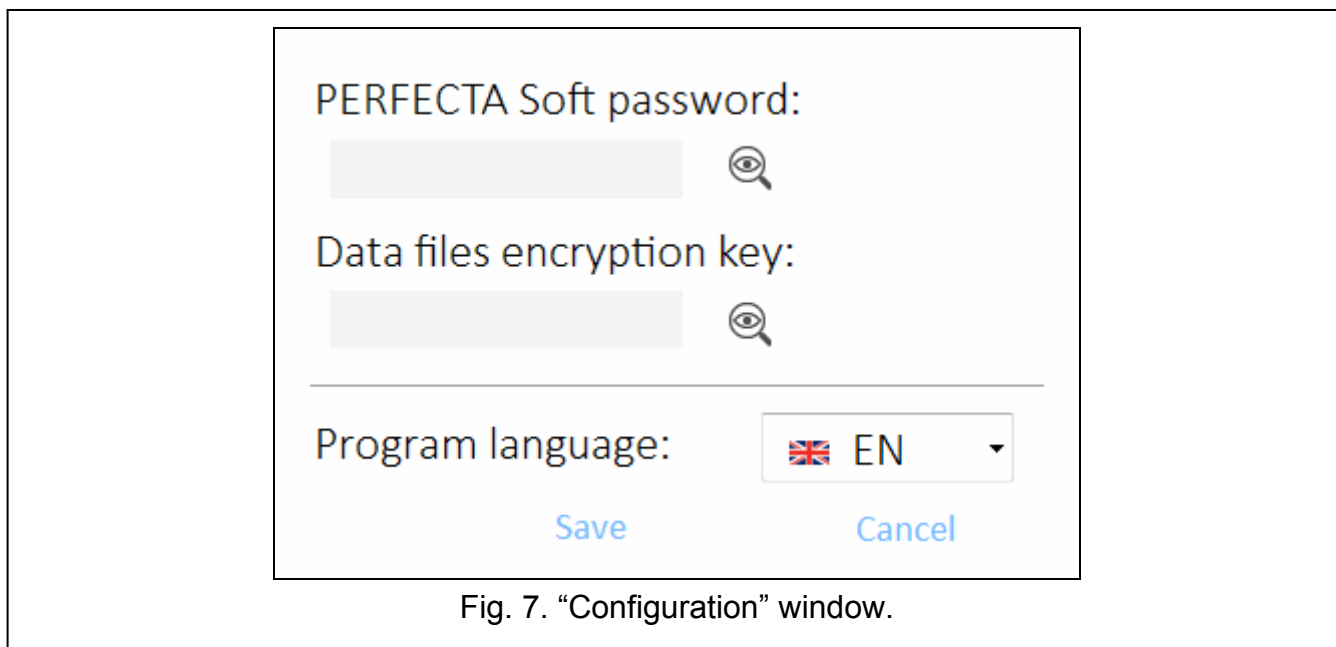
PERFECTA Soft password – if you want to protect the program against unauthorized access, you can enter the password.

Data files encryption key – if you want the files saved to disk to be additionally encrypted, enter the file encryption key. Opening the files in another PERFECTA Soft program without entering the valid key will be impossible.

Program language – you can select a program language. The program will restart after the language is changed

Buttons

Save – click to save changes.

Cancel – click to close window without saving changes.

3.2   Establishing connection between the program and the control panel

i *Establishing connection is possible, if an identical PANEL KEY has been programmed in the control panel and in the program, except for the control panel with factory settings.*

3.2.1   Local connection

1. Connect the control panel RS-232 (TTL) port with the computer port (for example, by means of the USB-RS converter offered by SATEL).
2. Open the file with control panel data (the file with default settings ("New" tab) or the file saved on the computer disk ("Projects" tab)).
3. Configure the settings required to establish local connection (see ""Connection" window" p. 9).

4. Click ⊂○⊃ on the menu bar.

5. A window will open with information that connection has been established and a prompt to read the data.

6. Click "Yes".

3.2.2 Remote connection: SATEL server

i *The PERFECTA SOFT CONN. VIA SATEL SERVER ALLOWED option must be enabled in the control panel (see "SATEL server: p. 31). By default, this option is disabled.*

1. Open the file with control panel data (the file with default settings ("New" tab) or the file saved on the computer disk ("Projects" tab)).

2. Configure the settings required to establish connection via GPRS through the SATEL server (see ""Connection" window" p. 9).

3. Click ⊂○⊃ on the menu bar.

4. A window will open with information that connection has been established and a prompt to read the data.

5. Click "Yes".

3.2.3 Remote connection: PERFECTA>>PERFECTA Soft

i *The computer running the PERFECTA SOFT program must have a public IP address.*

1. Open the file with control panel data (the file with default settings ("New" tab) or the file saved on the computer disk ("Projects" tab)).

2. Configure the settings required to establish direct connection via GPRS (see ""Connection" window" p. 9).

3. Click ⊂○⊃ on the menu bar.

4. The program will wait for connection being established by the control panel. The control panel will make an attempt to establish connection after starting the function from the keypad or receiving an SMS message.

Establishing connection after the function is started from the keypad

i *Address of the computer running the PERFECTA SOFT program and the number of port used for communication must be programmed in the control panel (see "Direct connection to PERFECTA SOFT" p. 31).*

1. Ask the authorized user to start the PERFECTA SOFT function (the function is available in user menu).

2. After the control panel connects to the computer, a window will open with information that connection has been established and a prompt to read the data.

3. Click "Yes".

Establishing connection after receiving SMS message

i *A control command, after receiving of which the control panel will make an attempt to establish connection, must be programmed in the control panel (see "Direct connection to PERFECTA SOFT" p. 31).*

The SMS message can be sent from a phone whose number is saved on the control panel (see "Phones" p. 36).

1. Send an SMS message with the following content to the number of SIM card currently used by the control panel:

   xxxx ("xxxx" – control command that initiates establishing connection with the PERFECTA SOFT program) – the control panel is to connect to the computer whose address has been programmed in the control panel,

   xxxx=aaaa:p= ("xxxx" – control command that initiates establishing connection with the PERFECTA SOFT program; "aaaa" – address of the computer running the PERFECTA SOFT program; "p" –TCP port) – the control panel is to connect to the computer whose address has been given in the SMS message and use for communication the TCP port given in the SMS message.

2. After the control panel connects to the computer, a window will open with information that connection has been established and a prompt to read the data.

3. Click "Yes".

4. Hardware

The control panel has a built-in GSM/GPRS communicator. To the control panel communication bus, you can connect additional devices that will be needed in the alarm system (keypads, zone modules and output module). The PERFECTA 16-WRL / PERFECTA 32-WRL control panel also supports wireless keypads.

4.1 Mainboard

Fig. 8. "Mainboard" tab.

4.1.1 Clock

Daylight saving time [061.DST] – the control panel can automatically adjust the clock settings due to a change from the summer time to the winter time and vice versa. The following correction schemes are available:

– no correction,

– according to the European Union rules,

– according to the United States' rules,

– correction by 1 hour according to dates,

– correction by 2 hours according to dates.

Summer time from [062.Summer from] / **Winter time from** [063.Winter from] – if the control panel clock is to be corrected by 1 or 2 hours according to dates, you should enter the dates (day, month) after the clock is changed to the summer time (moved forward) or to the winter time (moved back).

Clock correction [065.RTC adjust.] – if accuracy of the control panel clock is insufficient, its settings can be automatically corrected (by up to ±127 seconds per week).

i *When testing the clock for accuracy, the synchronization function must be disabled.*

Time synchronization

NTP server [NTP server time] – if this option is enabled, the control panel clock is synchronized with the time server.

GSM network [GSM network time] – if this option is enabled, the control panel clock is synchronized with the time of GSM network operator.

i *If the NTP SERVER and GSM NETWORK options are enabled at the same time, synchronization with the GSM network time has priority. The clock will only be synchronized with the time server if synchronization with the GSM network time fails.*

Time zone [064.Timezone] – difference between the universal time (UTC) and the zone time. The parameter is required, if the control panel clock is to be synchronized.

4.1.2 Times

AC loss report delay [123.Max.AC loss] – time during which the control panel must be without AC power before the trouble is reported. A delay in reporting the trouble prevents sending information about short-time voltage decays, having no effect on normal operation of the system.

Keypad's alarm time [124.Al.duration] – duration of alarm signaling on keypads.

Hide arm state indication after [125.Suppr.arm] – time counted from the moment of partition arming, after which the LED on keypad indicating the partition armed status goes off. If value 0 is programmed, the LED will be ON always when the partition is armed.

4.1.3 Arming

Prevent arming if not ready [Check if ready] – if this option is enabled, the control panel will perform a check during arming for any problems that may prevent arming the system. These include:

– a zone with PRIORITY option is violated in the partition,

– the 3. INSTANT, 4. DOUBLE KNOCK, 5. 24H BURGLARY, 7. 24H PANIC, 8. 24H PANIC SILENT, 9. 24 MEDICAL or 10. 24H FIRE type zone is violated in the partition which is to be armed,

– a zone is bypassed in the partition,

– there is a tamper in the partition,

– there is a trouble in the system.

The control panel checks the conditions twice:

before starting the arming procedure – the control panel will not start the arming procedure, if any problems occur (the keypad provides a forced arming option – see USER MANUAL),

after finishing the exit delay countdown – the system will not be armed (the arming procedure will end in failure), if there are any problems, which did not occur before starting the exit delay countdown.

Arm even if not ready after exit delay [Arm ExDly w.trbl] – if this option is enabled, the control panel will not check conditions after finishing the exit delay countdown (it will only check the conditions before starting the arming procedure). The option is available, when the PREVENT ARMING IF NOT READY option is enabled.

Do not arm if battery trouble [BAT low = no arm] – if this option is enabled, forced arming will be impossible in the event of battery trouble. The option is available, when the PREVENT ARMING IF NOT READY option is enabled.

Do not arm if tampered [Tamper = no arm] – if this option is enabled, forced arming will be impossible in the event of tamper. The option is available, when the PREVENT ARMING IF NOT READY option is enabled.

4.1.4 Options

Service Mode beep [SM sounds] – if this option is enabled, the service mode will be audibly signaled on the keypad.

Signal trouble state in partial arming [Trbl.in part.arm] – if this option is enabled, the [△] LED on the keypad goes off after both partitions are fully armed. If the option is disabled, the LED goes off after just one of the partitions is armed in any mode.

Lock after three incorrect codes [3wrng.codes=blk.] – if the option is enabled, after entering an incorrect code three times, the keypad will be blocked for 90 seconds. Entering an invalid code again will prolong the locking.

[i] *Entering an invalid code three times may trigger alarm (cf. the keypad ALARM 3 INCORRECT CODES option).*

Trouble memory [Troubles memory] – if this option is enabled, the control panel will also provide information about troubles that do not exist any more. You can clear the trouble memory by using keypad (when exiting the trouble review function), PERFECTA SOFT program or PERFECTA CONTROL application.

SMS notifications confirming ev. [Messaging events] – if this option is enabled, information about sending SMS notification is saved in the event log.

Zone restore events [Restore events] – when this option is enabled, information about zone restore is saved in the event log, if zone triggered alarm.

Limit number of events [Events limitat.] – if the option is enabled, events from the same source are saved into the event log 3 times only. This option does not apply to the alarms from zones.

Grade 2 [Grade 2] – if the option is enabled, the system operates in accordance with the EN 50131 standard requirements for Grade 2, i.e.:

– the keypad does not audibly signal alarms and troubles,

– the [🔔] LEDs on the keypad indicates alarms only after the user enters the code and presses [✱ ☙],

– the [△] LED on the keypad goes off after just one of the partitions is armed in any mode,

- the flashing ⚠ LED in keypad means that there is a trouble in the system, some zones are bypassed, or there has been an alarm,
- the keypad does not display alarm messages,
- the keypad display cannot be switched over to the zone status presentation mode,
- the quick arming from keypad (without entering the code) is not available,
- new access codes in the system must be composed of at least 5 digits,
- partial entering of the code is interpreted as entering an incorrect code,
- the keypad will be blocked after entering an incorrect code three times (cf. BLOCK AFTER THREE INCORRECT CODES option),
- during arming, the control panel checks for problems that prevent arming (cf. PREVENT ARMING IF NOT READY option),
- ARM EVEN IF NOT READY AFTER EXIT DELAY, DO NOT ARM IF BATTERY TROUBLE and DO NOT ARM IF TAMPERED options are interpreted as disabled,
- control panel gives information about past troubles (cf. TROUBLE MEMORY option),
- loss of communication with SATEL server will not be reported (cf. DO NOT REPORT A SATEL SERVER PROBLEM option),
- tamper of zone or expander can only be signaled by the external siren when the partition to which the zone or expander belong is armed,
- the number of alarms from the 7. 24H PANIC and 8. 24H PANIC SILENT zones is not limited (AUTO-RESET 3 option is ignored),
- arming is impossible, if the 6. 24H TAMPER zone is violated (cf. PRIORITY option),
- the warning alarm feature is enabled and the warning alarm is being signaled for at least 30 seconds (cf. WARNING TIME),
- countdown of ENTRY DELAY, DELAY and DELAY ACTIVATION TIME is running for up to 45 seconds,
- AC loss report delay can be up to 60 minutes.

Tamper alarm on internal sirens [Tmp.on int.siren] – if this option is enabled, the 1. INTERNAL SIREN output is additionally activated after triggering tamper alarm.

Tamper alarm on external sirens [Tmp.on ext.siren] – if this option is enabled, the 1. EXTERNAL SIREN output is additionally activated after triggering tamper alarm.

Backlight off on AC loss [No AC=no bcklght] – if the option is enabled, the backlight in hardwired keypads is automatically switched off in case of 230 V AC power loss.

Disable Service Mode [Block SM] – if this option is enabled, the emergency procedure of entering the service mode ("from pins") is not available (it can only be used if factory default settings of the control panel are restored).

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

Do not report wireless system jamming [No jamm. trouble] – if this option is enabled, jamming of the wireless system will not be reported.

4.2 GSM phone

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

PIN [612.PIN / 622.PIN] – PIN code of the SIM card.

i | *If a wrong PIN code is programmed, a trouble will be reported after using it. After 255 seconds the control panel will retry to use the PIN code. After the third attempt to use*

a wrong PIN code, the SIM card will be blocked. To unblock the card, enter the PUK code.

Fig. 9. "GSM phone" tab.

GPRS APN [613.APN / 623.APN] – access point name for Internet GPRS connection.

Username [614.USR / 624.USR] – user name for Internet GPRS connection.

Password [615.PWD / 625.PWD] – password for Internet GPRS connection.

DNS server [616.DNS / 626.DNS] – IP address of DNS server to be used by the module.

The GPRS parameters can be obtained from the GSM network operator.

SMS center no. [617.SMS centre / 627.SMS centre] – telephone number of the short message service center. It is used as a connecting link when sending SMS messages. If the number has been saved by the operator to the SIM card memory, it need not be programmed. Otherwise, if the control panel is to send SMS messages, it must be entered. The number must be suitable for the operator of network in which the SIM card is registered.

MCC/MNC code [618.MCC/MNC / 628.MCC/MNC] – codes of the operator of GSM network to which the SIM card is to log in. Enter in turn:

– MCC (Mobile Country Code) – country code,

– MNC (Mobile Network Code) – operator code.

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

auto [Auto MCC/MNC] – if this option is enabled and the module cannot log into the network of GSM operator defined by means of the MCC/MNC code, it will log into the available GSM network.

Lock time [63.Block SIM1 / 65.Block SIM2] – the time during which switch-over to the other SIM card is impossible. The time is counted from the moment of switch-over to the given card. For reporting, the transmission paths programmed as subsequent ones, if they require switch-over to the other card, will be skipped during the lock time countdown. Entering the value 0 means that instant switch-over to the other SIM card is possible.

Return time [64.Restore SIM1 / 66.Restore SIM2] – the time after which the other SIM card is to be used. Entering the value 0 means that automatic switch-over to the other SIM card will not take place.

i | *If two SIM cards are to be used, one of them must be treated as the priority card. It is recommended that return time equal to 0 be programmed for it.*

SMS for sending USSD code [111.USSD SIM1 / 112.USSD SIM2] – control command that will be sent in the SMS message together with USSD code. The control panel will run the USSD code and send the response received from the operator to the phone number from which the SMS message with control command was sent. You can enter up to 8 alphanumeric characters (digits, letters and special characters). You can use spaces, but at least one character must be different from space.

i | *It is not advisable to use the advanced functions available due to the USSD service if menu is presented in response to the entered code.*

The command content must be different from that of the other control commands programmed in the control panel.

The control command for sending USSD codes can be used for sending SMS messages through the control panel.

USSD codes from any number [USSD any tel.] – if this option is enabled, the control command for sending USSD codes or checking balance of the SIM card account can be sent from any phone. If this option is disabled, only from the phone the number of which is saved on the control panel (see "Phones" p. 36).

4.2.1 Pre-paid support

USSD-check balance [681.USSDchkSIM1 / 682.USSDchkSIM2] – the USSD code which is used to check balance of the SIM card account. If the code has been programmed, the user can check e.g. the account balance by using keypad.

USSD-recharge [683.USSDtopSIM1 / 684.USSDtopSIM2] – the USSD code which is used to top up the SIM card account. If the code has been programmed, the user can top up the account by using keypad. Enter $ where the top-up code is to be entered.

Minimum level [685.Min.cr.SIM1 / 686.Min.cr.SIM2] – the minimum amount of funds on the SIM card account. If the amount of funds drops below the minimum level:

– trouble will be reported,

– where the SIM card account balance is checked automatically by the control panel, information on the account balance will be sent as an SMS message to the numbers of phones for which the SMS FORW. option is enabled (see "Messaging" p. 35).

Check balance SMS [113.Chk.credit1 / 114.Chk.credit2] – the control command which can be sent in an SMS message to check the SIM card account balance. You can enter up to 8

alphanumeric characters (digits, letters and special characters). You can enter spaces, but at least one character must be different from the space.

> *i* | *The command content must be different from that of the other control commands preprogrammed in the control panel.*

Check balance at [687.hh:mm SIM1 / 688.hh:mm SIM2] – time at which the control panel will check the SIM card account balance every day.

4.3   Keypad

Fig. 10. Tab with settings for the wired keypad.

Name [28.Names] – individual name of the keypad (up to 16 characters).

Alarm in part. [22.Partitions] – the partition in which alarm will be triggered in the event of keypad tamper (opening of enclosure or loss of communication).

4.3.1   Options

Show partition 1 status [Show part.1] – if this option is enabled, the keypad LEDs and display indicate the status of partition 1. The keypad will indicate the status of partition 2 only after entering code by the user who has access to partition 2.

Show partition 2 status [Show part.2] – if this option is enabled, the keypad LEDs and display indicate the status of partition 2. The keypad will indicate the status of partition 1 only after entering code by the user who has access to partition 1.

Quick arm - partition 1 [Quickarm part.1] – if this option is enabled, quick arming (without user authorization) of the partition 1 is possible.

Quick arm - partition 2 [Quickarm part.2] – if this option is enabled, quick arming (without user authorization) of the partition 2 is possible.

Show code entering [Show code enter.] – if this option is enabled, entering the code is presented on the keypad display by asterisks.

Quick control [Quick control] – if this option is enabled, the users can control the outputs by using the number keys. The 15. CONTROLLED outputs must be assigned to the keys (see: "Quick control of outputs" p. 30).

Key 7 - troubles review [Troubles review] – if this option is enabled, the users can press $\boxed{7_{PQRS}}$ and hold down for 3 seconds to view the troubles.

Key 8 - chime on/off [Chime on/off] – if this option is enabled, the chime signal can be enabled/disabled by means of the $\boxed{8_{TUV}}$ key (the key is to be pressed and hold down for about 3 seconds).

Key 9 - change disp. mode [Disp.mode change] – if this option is enabled, the users can use the $\boxed{9_{WXYZ}}$ key to toggle between the normal display mode and the zone presentation mode (the key is to be pressed and hold down for about 3 seconds). The option is not available for the wireless keypad.

Alarm 3 incorrect codes [3 wrng codes al.] – if this option is enabled, entering incorrect code three times will trigger the alarm.

MEDICAL alarm [Medical alarm] – if this option is enabled, pressing the $\boxed{0\ \mathbf{0}}$ key for approx. 3 seconds will trigger the medical (auxiliary) alarm.

FIRE alarm [Fire alarm] – if this option is enabled, pressing the $\boxed{*\ \Psi}$ key for approx. 3 seconds will trigger the fire alarm.

PANIC alarm [Panic alarm] – if this option is enabled, pressing the $\boxed{\#\ \mathbb{C}}$ key for approx. 3 seconds will trigger the panic alarm.

Silent PANIC [Silent panic] – if this option is enabled, the panic alarm triggered from the keypad will be a silent one (without loud signal). The option is available, if the PANIC ALARM option is enabled.

4.3.2   Display and keys

Date/time format [210.ClockFormat] – mode of presentation of time and date on the display.

LCD backlight [26.LCDbacklight] – mode of keypad display backlighting.

Keypad backlight [27.KEYbacklight] – mode of keypad keys backlighting.

$\boxed{i}$ *Backlighting of the display and keys on the wireless keypad works differently than that on the wired keypad (see PRF-LCD-WRL keypad manual).*

Auto backlight [29. Autolight] – if the backlight of display or keys goes on automatically, you can define whether and what event will additionally turn on the backlighting:

Not present – backlighting will be turned on only by pressing any key.

Zone violation – backlighting will be turned on additionally in the event of zone violation (select the zone).

Entry delay in part. – backlighting will be turned on additionally in the event of starting the entry delay countdown in the partition (select the partition).

The AUTO BACKLIGHT parameter is not available for the wireless keypad.

4.3.3   Chime

The keypad can audibly signal violation of selected zones. If the zone is armed, violation will not trigger the CHIME signal.

The wireless keypad signals the CHIME from zones not more frequently than once every 30 seconds. In the inactive mode, the CHIME from zones is only signaled if the WAKE-UP option is enabled.

4.3.4   Volume

[251.Keys] – volume level of the beeps generated during keypad operation (key pressing, confirmation of performed operation, etc.).

[252.Chime] – volume level of the beeps generated after zone violation (CHIME).

[253.Entry delay] – volume level of the entry delay beeps.

[254.Exit delay] – volume level of the exit delay beeps.

[255.Fire alarm] – volume level of the fire alarm beeps.

[256.Burg.alarm] – volume level when signaling burglary, panic and medical (auxiliary) alarms.

[257.Warn.alarm] – volume level when signaling warning alarms.

[258.New trouble] – volume level when signaling troubles.

4.3.5   Wireless keypad PERFECTA 16-WRL / PERFECTA 32-WRL

For the wireless keypad, additional parameters and options are available.

Filter [1272.Filter] – the time counted from receiving of the transmission from the keypad. After it has elapsed and no other transmission is received, trouble will be reported.

Wake-up [Wake up] – if this option is enabled, the CHIME from zones will also be signaled in the inactive mode, while an alarm or start of entry delay countdown will start the active mode.

If the WAKE-UP option is enabled, the keypad will be awaiting for transmissions with information on events. As a result, the energy consumption will be growing and the battery life will be considerably reduced.

Wireless keypad initial greeting [218.Connect msg] – message displayed on the PRF-LCD-WRL keypad after wake-up. The message is the same for all keypads.

User can replace PRF-LCD-WRL battery [Usr.replaces BAT] – if this option is enabled, the users can replace battery in the PRF-LCD-WRL wireless keypads (for 3 minutes after the code is entered and confirmed with the $\boxed{* \; \maltese}$ key, the status of tamper switch will not be monitored on the keypad that was used to enter the code). The option applies to all wireless keypads.

4.4   Zone module

Name [28.Names] – individual name of the module (up to 16 characters).

Alarm in part. [22.Partitions] – partition in which alarm will be triggered in the event of module tamper.

AC loss report delay [23.Max.AC loss] – time during which the module must be without AC power before the trouble is reported. A delay in reporting the trouble prevents sending information about short-time voltage decays, having no effect on normal operation of the system. The parameter is valid for the module with power supply.

Fig. 11. Tab with zone expander settings.

4.5 Output module

Fig. 12. Tab with output expander settings.

Name [2815.Ex.0F name] – individual name of the module (up to 16 characters).

Alarm in part. [2215.Ex0F part] – partition in which alarm will be triggered in the event of module tamper.

AC loss report delay [2315.AC.0F loss] – time during which the module must be without AC power before the trouble is reported. A delay in reporting the trouble prevents sending

information about short-time voltage decays, having no effect on normal operation of the system. The parameter is valid for the module with power supply.

5.   Partitions

Fig. 13. "Partitions" tab.

The partition is a separated area within the premises protected by the security alarm system. The subdivision into partitions enables arming/disarming the system only in part of the protected area, as well as limiting access to some portion of the premises to selected users. You can create 2 partitions.

5.1   Partition parameters

Part. name [18.Names] – individual name of the partition (up to 16 characters).

Exit delay [13. Exit delay] – time counted from the moment of starting the procedure of partition arming. It allows the user to leave the protected area without triggering alarm. You can enter from 0 to 255 seconds. Entering zero 0 means no exit delay time.

> *The exit delay countdown can be terminated by using keypad (see EXIT DELAY CLEARING ENABLE option) or zones of the 1. ENTRY/EXIT FINAL, 16. EXIT DELAY TERMINATOR or 17. SHUNT LOCK type.*

Warning time [14.Warn.delay] – duration of the warning alarm. You can enter from 0 to 255 seconds. Entering any value different from 0 means enabling the warning alarm feature. The alarm alerts the user that he or she has forgotten to disarm the partition. The warning alarm is triggered when:

– ENTRY DELAY time has elapsed (see: p. 25),

– DELAY time has elapsed (see: p. 26),

– 3. INSTANT or 4. DOUBLE KNOCK zone triggered alarm when ENTRY DELAY countdown was running.

The warning alarm can be signaled by keypad or 2. INTERNAL SIREN type output. It is not reported. If the partition is not disarmed during the warning alarm, the burglary alarm will be triggered.

Alarm verif. time [15.Verif.delay] – time for verification of the alarm. You can enter from 0 to 255 minutes. Entering any value different from 0 means activation of the burglary alarm verification function. The verification consists in checking whether another zone will trigger the burglary alarm within the defined period of time. If so, the verified alarm will be generated. Alarms from the 0. ENTRY/EXIT, 1. ENTRY/EXIT FINAL, 2. INTERNAL, 3. INSTANT,

4. DOUBLE KNOCK or 5. 24H BURGLARY zones are verified. The time is counted from the moment of alarm triggering by this type of zone.

Exit delay clearing enable [Fin.exit delay] – if this option is enabled, the users can terminate the exit delay countdown by using keypad (the 🔑▲, ☀▶ or 🌙◀ key is to be pressed and hold down for about 3 seconds).

Infinite exit delay [Infinit.ex.delay] – if this option is enabled, the exit delay time is infinite. It can be terminated:

– on violation of the 1. ENTRY/EXIT FINAL, 16. EXIT DELAY TERMINATOR or 17. SHUNT LOCK type zones,

– after pressing and holding down for 3 seconds the 🔑▲, ☀▶ or 🌙◀ keys on the keypad (when the EXIT DELAY CLEARING ENABLE option is enabled).

i | *If the exit delay countdown is not terminated, the partition will not be armed.*
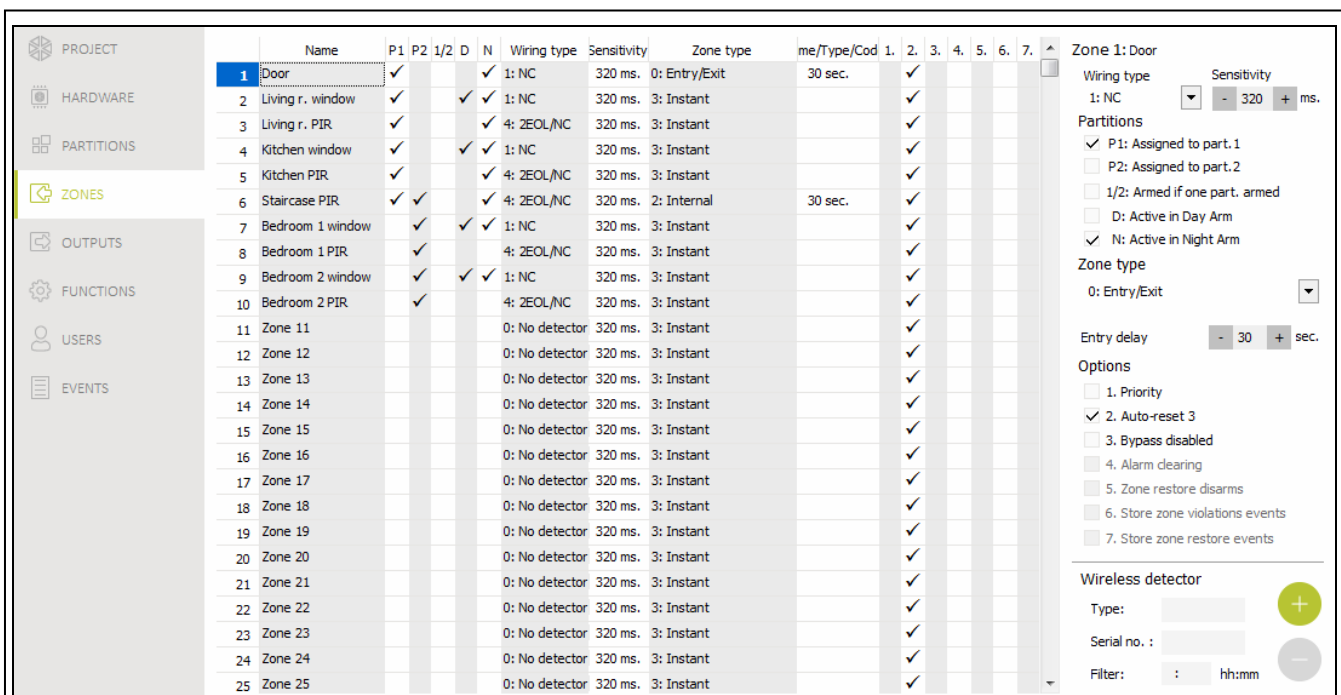
6. Zones

A zone can be assigned to one or two partitions. If the zone is assigned to two partitions, it can be armed when both partitions are armed or one of them only.

The system supports the following zones:

- hardwired – on the control panel PCB and in expanders. The number of available hardwired zones is determined by the control panel during the identification procedure.
- wireless – in the PREFECTA 16-WRL or PERFECTA 32-WRL control panel, after adding wireless detectors. The number of available wireless zones depends on the number of wireless detectors registered in the system.
- virtual – zones which do not physically exist, but are controlled by means of keyfobs.

6.1 Zone parameters and options

Fig. 14. "Zones" tab.

Name [38.Names] – individual name of zone (up to 16 characters).

Wiring type [31.EOL] – type of detector and the method of its connection:

No detector – no detector is connected to the zone,

NC – the zone supports a detector of NC (normally closed) type,

NO – the zone supports a detector of NO (normally open) type,

EOL – the zone supports a detector of NO or NC type with EOL resistor in the circuit,

2EOL/NO – the zone supports a detector of NO type with two EOL resistors in the circuit,

2EOL/NC – the zone supports a detector of NC type with two EOL resistors in the circuit,

Roller – the zone supports a roller shutter detector,

Vibration – the zone supports a vibration detector (also NC type detector).

> *i* *In case of the VIBRATION wiring configuration, opening the circuit for 200 ms or longer – irrespective of the programmed number of pulses and sensitivity (see below) – will be interpreted as violation. This solution enables a magnetic contact to be connected in series with the vibration detector.*

Sensitivity [32.Sensitivity] – depending on wiring type:

NO, NC, EOL and 2EOL – the time during which the zone must be violated, so that it can be noted by the control panel. The sensitivity is programmed in milliseconds. You can enter values from the 20 ms to 5100 ms range.

Vibration – the pulse whose duration is equal to or longer than the defined time will cause violation of the zone. You can enter values from the 5 ms to 160 ms range (every 3 ms).

Pulses [32.Sensitivity] – the number of pulses after which the zone will be violated. The parameter applies to the ROLLER and VIBRATION wiring configurations. For the VIBRATION wiring configuration you can enter values from 0 to 7 (for the value 0, the pulses will not be counted, the SENSITIVITY parameter only being taken into account). For the ROLLER wiring configuration you can enter values from 1 to 8.

Time [32.Sensitivity] – the time during which the defined number of pulses must be detected (PULSES parameter) for the zone to be violated. The parameter applies to the ROLLER wiring configuration. You can program:

30 s (keypad: press [1]) – the time counted from detecting the pulse. After the time has elapsed, the pulse counter will be reset.

120 s (keypad: press [2 ABC]) – similarly as in the event of 30 s.

240 s (keypad: press [3 DEF]) – similarly as in the event of 30 s.

for arming / disarming (keypad: press [0 ❶]) – the pulses are counted when the partition is armed or disarmed. Arming / disarming will reset the pulse counter.

Assigned to part. 1 [361.P.1 zones] – if the option is enabled, the zone is assigned to partition 1.

Assigned to part. 2 [362.P.2 zones] – if the option is enabled, the zone is assigned to partition 2.

Armed if one part. armed [365.Act.OnePart] – the option refers to the zones which are assigned to both partitions. If the option is enabled, the zone is armed when one of the partitions is armed. If the option is disabled, the zone is armed when both partitions are armed.

Active in Day Arm [364.Day active] – if the option is enabled, the zone is armed when the day armed mode is activated.

Active in Night Arm [363. Night act.] – if the option is enabled, the zone is armed when the night armed mode is activated.

Entry delay [34.Entry delay] – the time by which alarm from the zone of 0. ENTRY/EXIT or 1. ENTRY/EXIT FINAL type will be delayed. It is counted from the moment of zone violation.

During the countdown, the zones of 2. INTERNAL type act as delayed ones. You can enter from 0 to 255 seconds. Programming 0 will make the zone act as an instant one.

Delay [34.Entry delay] – the time by which alarm from the zone of 2. INTERNAL type will be delayed. It is counted from the moment of zone violation. You can enter from 0 to 255 seconds. Programming 0 means that the zone will act as an instant one.

Waiting time [34.Entry delay] – the time during which the 4. DOUBLE KNOCK type zone has to be violated again for the alarm to be triggered. It is counted from the first violation of the zone. You can enter from 0 to 255 seconds. Programming 0 means that the WAITING TIME is 30 seconds.

Delay activation time [34.Entry delay] – the time during which the 2. INTERNAL type zones act as delayed ones. It is counted from the moment of violation of the 18. ENTRY ROUTE ENABLING type zone. You can enter from 0 to 255 seconds.

Arming mode [39.Arm mode] – the armed mode activated by violating the zones of 13. ARM/DISARM or 14. ARM type. You can select full, day or night armed mode.

Trouble code [35.Trouble code] – violating of the 19. TROUBLE type zone can generate event that will be reported.

Priority [366.Priority] – if the option is enabled, arming is impossible when the zone is violated.

Auto-reset 3 [367.3 alarms] – if the option is enabled, the zone can trigger up to 3 alarms. As long as the alarm is not cleared or the partition is not armed/disarmed, violations of the zone will not trigger any alarm.

Bypass disabled [368.Bps disable] – if the option is enabled, the user cannot bypass the zone.

Alarm clearing [372.Alarm clear] – an option for the 13. ARM/DISARM and 15. DISARM zone types. If the option is enabled, together with disarming, the alarm is cleared. Violation of the 15. DISARM type zone will also clear the alarm, when the system is not armed.

Zone restore disarms [369.Shnt.disarm] – an option for the 17. SHUNT LOCK zone type. If the option is enabled, the zone restore will disarm the partition.

Store zone violations events [370.Viol.event] – an option for the 12. NO ALARM ACTION zone type. If the option is enabled, the zone violation is saved to the event log.

Store zone restore events [371.Rest.event] – an option for the 12. NO ALARM ACTION zone type. If the option is enabled, the zone restore is saved to the event log.

6.2 Zone types

0. ENTRY/EXIT – when the EXIT DELAY countdown is in progress, zone violation will trigger no alarm. When the partition is armed, zone violation will start the ENTRY DELAY countdown. The user have to disarm the partition before the ENTRY DELAY expires, otherwise, the alarm will be generated. This zone type is normally used for the detectors protecting entrances/exits (e.g. front doors).

1. ENTRY/EXIT FINAL – acts similarly as 0. ENTRY/EXIT, but the EXIT DELAY countdown will be terminated as soon as the zone is restored.

2. INTERNAL – when the ENTRY DELAY or DELAY ACTIVATION TIME countdown is in progress, zone violation will start the DELAY countdown. The user have to disarm the partition before the DELAY expires, otherwise, the alarm will be generated. When the partition is armed, but neither ENTRY DELAY nor DELAY ACTIVATION TIME countdown is running, zone violation will trigger alarm. This zone type is normally used for indoor motion detectors and internal door protection detectors.

3. **INSTANT** – when the EXIT DELAY countdown is running or the partition is armed, zone violation will trigger alarm. This zone type is normally used for outdoor motion detectors and window protection detectors.

4. **DOUBLE KNOCK** – when the partition is armed, violating a zone will result in logging the event and starting the WAITING TIME countdown. If the zone is violated again when the countdown is running, alarm will be triggered.

5. **24H BURGLARY** – zone violation will trigger burglary alarm. Use this zone type for the detectors which should be always active (e.g. glass break detectors).

6. **24H TAMPER** – zone violation will trigger tamper alarm and trouble will be reported. Use this zone type for tamper protection.

7. **24H PANIC** – zone violation will trigger panic alarm. Use this zone type for the panic buttons.

8. **24H PANIC SILENT** – zone violation will trigger silent panic alarm. The silent panic alarm is not signaled in any way, but the event code can be sent to the monitoring station. Use this zone type for the panic buttons.

9. **24H MEDICAL** – zone violation will trigger medical (auxiliary) alarm. Use this zone type for the help call buttons.

10. **24H FIRE** – zone violation will trigger fire alarm. Use this zone type for the fire detectors.

11. **DETECTOR MASK** – zone violation will report trouble (detector masking). Use this zone type for detectors with an anti-masking output.

12. **NO ALARM ACTION** – zone violation will not trigger directly any reaction of the control panel. The zone can be used to control outputs.

13. **ARM/DISARM** – when the partition is disarmed, violation of the zone will start arming procedure in the partition. When the partition is armed, zone violation will disarm the partition.

14. **ARM** – when the partition is disarmed, zone violation will start the partition arming procedure.

15. **DISARM** – when the partition is armed, zone violation will disarm the partition.

16. **EXIT DELAY TERMINATOR** – violation of the zone ends the partition exit delay countdown.

17. **SHUNT LOCK** – violation of the zone ends the partition exit delay countdown. If the ZONE RESTORE DISARMS option is enabled, the zone restore will disarm the partition.

18. **ENTRY ROUTE ENABLING** – when the partition is armed, zone violation will start the DELAY ACTIVATION TIME countdown. During the DELAY ACTIVATION TIME countdown, the zones of 2. INTERNAL type act as delayed ones.

19. **TROUBLE** – zone violation will result in trouble. You can select the type of trouble (see TROUBLE CODE parameter). Zone restore means the trouble restore.

6.3   Wireless detector PERFECTA 16-WRL / PERFECTA 32-WRL

If a wireless detector is assigned to the zone, an additional parameter is available.

Filter [1272.Filter] – time counted from the moment of receiving a transmission from the detector. After it has elapsed and no other transmission is received, trouble will be reported.

6.3.1   Wireless detectors and zone settings

Depending on the settings of the zone to which a wireless detector is assigned:

- NC, NO or EOL – the zone gives information about detector violation,
- 2EOL/NC or 2EOL/NO – the zone gives information about detector violation and tamper.

The information on tamper and tamper restore is sent by the detector in real time.

How information about violation is sent depends on the detector operating mode:

normal – the detector sends information on violation and violation restore in real time (the zone status corresponds to the detector status),

energy save (available in some detectors) – after sending information on violation, the detector will not send any further information about violations for 3 minutes (the zone will be violated for 2 seconds after the controller receives the transmission containing information on detector violation).

7. Outputs

The system supports the following outputs:

- hardwired – on the control panel PCB and in the expander.
- wireless – in the PREFECTA 16-WRL or PERFECTA 32-WRL control panel. There are 4 outputs that support wireless sirens.

7.1 Output functions

0. NOT USED

1. EXTERNAL SIREN – output activated by triggering burglary, panic or fire alarm. In the event of the fire alarm, the output is pulsating.

2. INTERNAL SIREN – output activated by triggering burglary, panic, fire or warning alarm. In the event of the fire alarm, the output is pulsating.

3. BURGLARY – output activated after alarm is triggered by the 0. ENTRY/EXIT, 1. ENTRY/EXIT FINAL, 2. INTERNAL, 3. INSTANT, 4. DOUBLE KNOCK or 5. 24H BURGLARY zone.

4. FIRE ALARM – output activated by triggering fire alarm from keypad or by the 10. 24H FIRE zone.

5. DURESS ALARM – output activated by using a code with DURESS right.

6. PANIC ALARM – output activated by triggering panic alarm from keypad or by the 7. 24H PANIC zone.

7. MEDICAL ALARM – output activated by calling medical help from keypad or by the 9. 24 MEDICAL zone.

8. ALARM – NOT VERIFIED – output activated by triggering unverified alarm.

9. ALARM - VERIFIED – output activated by triggering verified alarm.

10. TAMPER ALARM – output activated by triggering tamper alarm.

11. FIRE DETECTORS POWER SUPPLY – output for power supply of fire detectors with automatic alarm verification. The output is deactivated for 16 seconds after violation of the 10. 24H FIRE zone. If, after reactivation of the output, the zone will be violated again, fire alarm will be triggered.

12. POWER SUPPLY ON ARMED – output for power supply of the detectors which should not operate when the system is disarmed. The output is active when the system is armed (it will be activated as soon as the exit delay countdown starts).

13. ZONE VIOLATION – output activated by zone violation.

14. CHIME – output activated by zone violation, if the zone is disarmed.

15. CONTROLLED – output activated / deactivated by using zones, timers, keypad etc.

16. READY STATUS – output is active, when the system is ready for arming (no zone is violated).

17. EXIT DELAY STATUS – output is active, when EXIT DELAY countdown is running.

18. ARMED STATUS – output is active, when the system is armed.

19. TROUBLE STATUS – output is active, when there is a trouble in the system.

20. ARM/ALARM STATUS – output is active, when the system is armed (continuous mode) or when there is alarm (pulsating mode).

21. DETECTORS RESET – output is used to reset the alarm memory in detectors. It is activated on:

– starting the exit delay countdown (if the exit delay is 0 – on arming),

– starting the 3.OUTPUTS RESET user function.

22. SERVICE MODE STATUS – output is active, when the control panel is running in service mode.

23. ARM STATUS (REPORTED) – output is active, when the system is armed and information about arming has been sent to the monitoring station (if reporting is disabled, the output is active when the system is armed).

7.2 Output parameters and options

Fig. 15. "Outputs" tab.

Output name [48.Names] – individual name of the output (up to 16 characters).

Cut off time [42.Duration] – time during which the output is active. Entering 0 changes the operation mode of some outputs:

– outputs activated by triggering alarm will remain active until the alarm is cleared,

– 5. DURESS ALARM and 14. CHIME outputs will remain active until starting the 3.OUTPUTS RESET user function,

– 13. ZONE VIOLATION output will be active when the zone is violated,

– 15. CONTROLLED output will remain active until repeated zone violation, stopping timer or deactivating from keypad, etc.

Triggering zones [43.Zones] – the zones whose status has effect on the output status.

Arming modes [43.Zones] – arming modes which affect the output status.

Troubles [43.Zones] – troubles during which the output is active.

Assigned to part. 1 [451.P.1 outputs] – if this option is enabled, the output is controlled by events related to partition 1 (alarm in partition 1, clearing alarm in partition 1 etc.).

Assigned to part. 2 [452.P.2 outputs] – if this option is enabled, the output is controlled by events related to partition 2 (alarm in partition 2, clearing alarm in partition 2 etc.).

Polarity + [453.Polarity(+)] – the option defines how the outputs will operate (see the table below). If the option is disabled, the output is inverted. The option does not apply to wireless outputs.

	"–" terminal of high-current output / low-current output	
	option enabled (normal polarity)	**option disabled** (reverse polarity)
output inactive	disconnected from ground	shorted to ground
output active	shorted to ground	disconnected from ground

Table 2. Mode of output operation depending on the POLARITY + option.

Pulsed [454.Pulsed] – if this option is enabled, the output is pulsating when it is active. The option does not apply to the 1. EXTERNAL SIREN, 2. INTERNAL SIREN, 11. FIRE DETECTORS POWER SUPPLY and 20. ARM/ALARM STATUS OUTPUTS. The option does not apply to wireless outputs.

Arm/Disarm/clear sign. [455.Arm/Dis/Clr] – if this option is enabled, the output will signal:
– starting the arming procedure (if the exit delay time is 0, the system is armed immediately) – 1 pulse,
– disarming – 2 pulses,
– clearing alarm – 4 pulses,
– denial of arming or arming procedure failure – 7 pulses.

Pulse duration is about 0.3 second. Option for the 1. EXTERNAL SIREN, 2. INTERNAL SIREN, 3. BURGLARY, 4. FIRE ALARM, 5. DURESS ALARM, 6. PANIC ALARM, 7. MEDICAL ALARM, 8. ALARM - NOT VERIFIED, 9. ALARM - VERIFIED and 10. TAMPER ALARM outputs.

Triggering timers [44.Timers] – the output control timers (starting the timer activates the output). The parameter refers to the 15. CONTROLLED output.

7.3 Quick control of outputs

If the quick control of the outputs 15. CONTROLLED is to be available in keypads, the outputs of this type must be assigned to the corresponding keypad keys. One output can be assigned to each number key.

7.4 Wireless siren PERFECTA 16-WRL / PERFECTA 32-WRL

If a wireless siren is assigned to the output, additional parameters and options are available (outputs 13-16).

Filter [1272.Filter] – time counted from the moment of receiving transmission from the siren. After it has elapsed and no other transmission is received, trouble will be reported.

Signaling [1275.Al.signal.] – alarm signaling mode.

Arm/Disarm beep [1276.Acknowled.] – signaling mode for arming/disarming etc. (cf. ARM/DISARM/CLEAR SIGN. option).

Tamp. in part. [1274.Out.tamper] – partition in which alarm will be triggered in the event of siren tamper.

8. Communication

Panel key [01.PERFECTA key] – identifier of the alarm control panel. You can enter up to 16 alphanumeric characters (digits, letters and special characters). You can enter spaces, but at least one character must be different from the space. Do not program the same key for

different control panels. Communication between the PERFECTA SOFT program and the control panel is only possible, when the program key and the control panel key are identical.

i *For the control panel with factory default settings, the PERFECTA SOFT program will generate a random key that must be written to the control panel.*

Fig. 16. "Communication" tab.

8.1   SATEL server

PERFECTA Control conn. via SATEL server allowed [PERFECTA CONTROL] – if this option is enabled, it is possible to establish connection between the PERFECTA CONTROL application and the control panel through the SATEL server.

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

PERFECTA Soft conn. via SATEL server allowed [PERFECTA Soft] – if this option is enabled, it is possible to establish connection between the PERFECTA SOFT program and the control panel through the SATEL server.

i *Make sure that the SIM card tariff plan is suited to the requirements of communication via the SATEL server (GPRS connection to the server is active at all times).*

8.2   Direct connection to PERFECTA SOFT

PERFECTA Soft address [041.Address] – address of the computer running the PERFECTA SOFT program. It must be a public address. You can enter the IP address or domain name.

Port [042.Port] – number of the TCP port used for direct communication between the control panel and the computer with PERFECTA SOFT program via GPRS. You can enter values from 0 to 65535 (0=disabled).

SMS initiating connection [115.PERF.Soft] – control command which will be sent in SMS message to initiate communication between the control panel and the PERFECTA SOFT program. You can enter up to 8 alphanumeric characters (digits, letters and special

characters). You can enter spaces, but at least one character must be different from the space.

> *i* | The command content must be different from that of the other control commands preprogrammed in the control panel.
>
> In the SMS message, you can include address of the computer the control panel is to connect to, and the number of TCP port which is to be used for communication.

9. Reporting

The control panel can send event codes to the monitoring station by using the following transmission paths:

- GPRS,
- SMS messages (control panel gets no acknowledgement of event code receipt),
- GSM voice channel (the use of this transmission path is not recommended because of distortions that may occur when sending the event codes).

9.1 Reporting parameters and options

Fig. 17. "Reporting" tab.

Reporting [Monitoring] – if the option is enabled, the control panel can send event codes to the monitoring station.

Reporting mode [72.Stations] – defines how event codes are to be sent to the monitoring stations:

Station 1 or station 2 – the control panel will make an attempt to send the event code to station 1 and, if unsuccessful, to station 2.

Station 1 only – the event codes are only sent to station 1.

Station 2 only – the event codes are only sent to station 2.

Station 1 and Station 2 – the event codes are sent to both stations.

9.1.1   Station 1 / Station 2

Reporting format [738.Format / 758.Format] – format in which event codes are sent to the monitoring station:

CID – all codes – event codes are sent in Contact ID format. All events are sent to the monitoring station.

CID – selected codes – event codes are sent in Contact ID format. Only selected events are sent to the monitoring station.

SIA – all codes – event codes are sent in SIA format. All events are sent to the monitoring station.

SIA – selected codes – event codes are sent in SIA format. Only selected events are sent to the monitoring station.

Panel identifier [731.Identifiers / 751.Identifiers] [732.SIA prefix / 752.SIA prefix] – identifier of the control panel for reporting purposes. It allows the monitoring station to determine from the events are sent. For the Contact ID format, it consists of 4 hexadecimal characters (digits or letters from A to F). For the SIA format, it consists of 6 hexadecimal characters (digits or letters from A to F). Additional characters are to be put at the beginning (to enter them on the keypad, use the 732.SIA prefix / 752.SIA prefix function). If the identifier only consists of the digits 0, events are not sent.

IP format and protocol [UDP] [SIA-IP] – for reporting via GPRS, you must define:
– format: SATEL or SIA-IP (SIA DC-09 standard).
– protocol: TCP or UDP.

Monitoring station address [736.Address / 756.Address] – address of the monitoring station for GPRS reporting. You can enter either the IP address or the domain name.

Port [737.Port / 757.Port] – number of the port used for communication between the control panel and the monitoring station when reporting via GPRS. You can enter a value from 0 to 65535 (0=disabled).

SMS reporting - tel. no. [735.Tel.(SMS) / 755.Tel.(SMS)] – phone number of the monitoring station for SMS reporting.

SMS format [741.SMS format / 761.SMS format] – SMS format for SMS reporting. It must be defined as required by the monitoring station. The SMS message format, preset by default in the control panel, corresponds to the default settings of the STAM-2 monitoring station (firmware version 1.2.0 or newer) for the Contact ID format.

Audio reporting - tel. no. [734.Tel.(AUDIO) / 754.Tel.(AUDIO)] – phone number of the monitoring station for AUDIO reporting (GSM voice channel).

Reporting priority [733.Priority / 753.Priority] – if sending an event code to the monitoring station using one transmission path fails, the control panel can use another transmission path. You must specify the order of using different transmission paths by the control panel. A successful send of the event code to the monitoring station will terminate the procedure (except for the test transmissions).

i   *The control panel will only use the transmission paths for which priority is specified (they are included in the list defining the order of using transmission paths).*

In the case of SMS reporting, the control panel gets no acknowledgement of receiving the event codes by the monitoring station, hence this transmission path should be used as the last one.

The switch-over from one SIM card to the other one requires time (for example, to log onto the network), so it is better to use up all the transmission paths available for one SIM card.

The switch-over from one SIM card to the other is affected by the LOCK TIME and RETURN TIME parameters (see: "GSM phone" p. 16).

Suspend time [746.Suspen.time / 766.Suspen.time] – the time for which reporting will be suspended, if attempts fail to send an event code through all provided transmission paths. The control panel will resume the attempt of establishing connection with the monitoring station after this time expires or a next, new event occurs. Up to 30 minutes can be programmed. Programming the value 0 means that an attempt to establish telephone connection with the monitoring station will only be taken after occurrence of a new event in the system.

Advanced

SATEL station key [739.STAM key / 759.STAM key] – a sequence of characters for encrypting data sent to the monitoring station via GPRS. You can enter up to 12 alphanumeric characters (digits, letters and special characters). In the PERFECTA SOFT program, you can enable the HEX option, if you want to enter 24 hexadecimal characters (digits or letters from A to F).

GPRS key [740.GPRS key / 760.GPRS key] – a string of characters, which is used to identify the control panel for the purpose of GPRS reporting. You can enter up to 5 alphanumeric characters (digits, letters and special characters). In the PERFECTA SOFT program, you can enable the HEX option, if you want to enter 10 hexadecimal characters (digits or letters from A to F).

Send names [Names in SIA] – if the option is enabled, in the SIA format, the name of event source (zone, user, etc.) will also be sent, in addition to the event code.

National char. [National chars] – if this option is enabled, you can send in the SIA format not only ASCII characters but national characters as well.

SIA-IP account number [742.SIA-IP acct / 762.SIA-IP acct] – a string of characters, which is used to identify the control panel for the purpose of reporting in SIA-IP format. You can enter up to 16 hexadecimal characters (digits or letters from A to F).

SIA-IP key [743.SIA-IP key / 763.SIA-IP key] – a sequence of characters for encrypting data sent in the SIA-IP format. You can enter up to 16 alphanumeric characters (digits, letters and special characters). In the PERFECTA SOFT program, you can enable the HEX option, if you want to enter 32 hexadecimal characters (digits or letters from A to F).

Encryption [SIA-IP encrypt.] – if the option is enabled, the data being sent are encrypted, and the date and time are sent with event code (the monitoring station can program the date and time in the control panel). Option for SIA-IP format.

Send date & time [Timestamp SIA-IP] – if the option is enabled, the date and time are sent with event code (the monitoring station can program the date and time in the control panel). Option for SIA-IP format. It is available, when the ENCRYPTION option is disabled.

SIA-IP test report period [744.SIA-IP test / 764.SIA-IP test] – in the case of reporting in the SIA-IP format, an additional transmission can be sent at specified intervals to check communication with the monitoring station. You can program a number of days, hours, minutes and seconds between the transmissions. Entering zeros only means that no additional transmission will be sent.

9.1.2 Test transmissions

ℹ️ *The test transmission is sent using all transmission paths included in the list that defines the order of using transmission paths (cf. REPORTING PRIORITY parameter).*

At [791.At] – if the test transmission is to be sent regularly at a specified time, you must define every how many days and at what time. As for the number of days, 0 is interpreted as 1 (test transmission will be sent every day).

When armed [793.Armed] – if the test transmission is to be sent at regular intervals when the system is armed, define every how many days, hours and minutes.

When disarmed [792.Disarmed] – if the test transmission is to be sent at regular intervals when the system is disarmed, define every how many days, hours and minutes.

Test transmissions regardless of events [Independ.test] – this option refers to the test transmissions sent at regular intervals (see WHEN ARMED and WHEN DISARMED parameters). If this option is enabled, the time is counted from the last test transmission. If the option is disabled, the time is counted from the last transmission, irrespective of whether it was a test transmission, or a code of another event was sent.

9.1.3 Events selection

If the CID – SELECTED CODES or SIA – SELECTED CODES reporting format is selected, define which events are to be sent to the monitoring station.

10. Messaging

The control panel can send notifications about alarm system events by means of:

- voice messages – the voice messages which are to be used for notification should be saved to the control panel by using the PERFECTA SOFT program,
- SMS messages – the content of SMS messages is automatically generated by the control panel.

10.1 Parameters and options of the messaging

Fig. 18. "Messaging" tab.

10.1.1 Phones

In the control panel, you can enter data of 8 telephones which will be notified of events in the alarm system. At the same time, users of these phones can control the alarm system by using SMS messages.

Name [88.Names] – individual name of the telephone number (up to 16 characters).

Telephone no. [81.Numbers] – the telephone number.

SMS [83.SMS msg.] – if this option is enabled, the phone is notified by SMS messages.

AUDIO [82.AUDIO msg.] – if this option is enabled, the phone is notified by voice messages.

Listen in [85.Listening-in] – if this option is enabled, the given phone can be used to listen in to what is happening in the premises (the phone user can call the number of the SIM card used to listen in or can listen in after the voice message is played).

SMS forw. [84.Unknown SMS] – if this option is enabled, unknown SMS messages received by the control panel are forwarded to the phone number (e.g. information received from the GSM network operator).

Listening-in time [86.List.durat.] – the time during which the phone users can listen in to what is going on in the premises. The time is counted from answering the call by the control panel or from playing back the voice message.

10.1.2 AUDIO messaging

AUDIO messaging [AUDIO messag.] – if this option is enabled, the control panel can notify the users of events by using voice messages.

Event assignment

For the events of which the control panel is to notify, you must define:

- the telephone numbers to be notified,
- the number of the voice message to be used for notification of this event.

10.1.3 AUDIO messages

Repeat twice [Double v.message] – if this option is enabled, voice message is played back twice.

Managing the voice messages

The PERFECTA SOFT program allows you to manage the voice messages that will be used for notification. Up to 16 voice messages can be saved on the control panel. Total duration of all the voice messages must not exceed 131 seconds.

Content of the message – text of the voice message. The text entered can be converted into a voice message by using the text-to-speech converter (voice synthesizer).

Duration – duration of the voice message.

Total – information on total duration of the voice messages.

- click to play back the selected voice message.

- click to import the .WAV type file which is to be used as the selected voice message.

- click to delete the selected voice message.

- click to convert the message text into a voice message. In the field below the button, you can select the voice synthesizer installed on the computer that will be used to convert the text.

- click to read the voice messages from the control panel.

- click to save the voice messages to the control panel.

10.1.4 SMS messaging

SMS messaging [SMS messaging] – if this option is enabled, the control panel can notify the users of events by using SMS messages.

SMS notifications confirming ev. [Messaging events] – if this option is enabled, information about sending SMS notification is saved to the event log.

Event assignment

The following options are available for each telephone:

Partition 1 / **Partition 2** – if this option is enabled, the phone will be notified of events that occurred in the given partition (the events of which the phone will be notified are defined in other options).

Alarms – if this option is enabled, the phone will be notified of alarms.

Arming/disarming – if this option is enabled, the phone will be notified of arming / disarming and alarm clearing.

Zone bypasses – if this option is enabled, the phone will be notified of bypassing / unbypassing zones.

Troubles – if this option is enabled, the phone will be notified of troubles.

Used functions – if this option is enabled, the phone will be notified of the functions used.

System events – if this option is enabled, the phone will be notified of system events.

11. SMS control

The alarm system can be controlled by means of SMS messages containing appropriate control commands. The SMS messages should be sent to the number of the currently used SIM card. You can program 16 control commands.

11.1 Parameters and options of SMS control

SMS [118.SMS control] – control command which can be sent in the SMS message to run the function assigned to the command. You can enter up to 8 alphanumeric characters (digits, letters and special characters). You can enter spaces, but at least one character must be different from the space.

i | *The content of control commands must vary. If the content of two different commands is identical, the control panel, having received the SMS messages, will execute only one function anyway.*

The content of one control command must not be inserted into the content of another command.

Function [119.SMS funct.] – the function that will be started after the control panel receives an SMS message containing the control command.

Any tel. no. [1110.Any number] – if this option is enabled, the control command to run the given function can be sent from any phone. If the option is disabled, only from the phone whose number is saved on the control panel (see: "Phones" p. 36).

Fig. 19. "SMS control" tab.

12. Timers

The timer compares the time to that of the control panel clock and executes the selected function at the programmed time. Using the timers, it is possible to control the armed mode of partitions and the 15. CONTROLLED outputs. You can program 8 timers.

12.1 Parameters and options of the timers

TIMER n [59.Active] – if the option is enabled, the timer is enabled (n=timer number).

Name [58.Names] – individual timer name (up to 16 characters).

Partition 1 [55.Partition 1] / **Partition 2** [56.Partition 2] – the arming mode that will be activated in the partition when the timer will start.

Mon / Thu / Wed / Tue / Fri / Sat / Sun

You can program individual timer operating parameters for every day of the week.

ON – timer start time on the given day of the week (hour:minutes).

OFF – timer stop time on the given day of the week (hour:minutes).

Everyday

The everyday settings apply to only those days of the week for which no individual parameters have been programmed.

ON – timer start time every day (hour:minutes).

OFF – timer stop time every day (hour:minutes).

		From	To	ON	OFF
PROJECT	☑ TIMER 1 Name: Timer 1				
HARDWARE	Partitions controll				
PARTITIONS	Partition 1: full arm ▼ Partition 2: --- ▼	Exception 1 xxxx-12-24	xxxx-12-26	14:00	06:00

Fig. 20. "Timers" tab.

Exception

An exception is the period of time when the timer is started and stopped at times different than those defined by the settings for each day of the week and the everyday settings. 4 exceptions can be programmed for a timer.

From – the date from which the given exception is valid (year-month-day).

To – the date to which the given exception is valid (year-month-day).

ON – the timer start time when the exception is valid (hour:minutes).

OFF – the timer stop time when the exception is valid (hour:minutes).

12.1.1 Editing the timer parameters

You can program only the start time or the stop time for the timer. The hour or minutes may remain undefined (e.g. if you enter a value from beyond the range (more than 23 for the hour or 59 for the minutes), it will be changed into xx). For example:

xx:45 – the timer will be started / stopped every hour throughout the day (at 0:45, 1:45 etc.),

11:xx – the timer will be started / stopped every minute between 11.00 and 11:59.

You must program both dates for an exception (FROM and TO). One or two of the date components may remain undefined (e.g. if you enter a value from beyond the range (more than 2099 for the year, 12 for the month or 31 for the day)). For example:

xxxx-12-25 – the exception will be valid from / to 25 Dec. each year,

xxxx-xx-12 – the exception will be valid from / to 12th day of each month in each year,

xxxx-03-xx – the exception will be valid from the beginning of March each year (same as xxxx-03-01) / to the end of March each year (same as xxxx-03-31),

2018-xx-05 – the exception will be valid from / to 5th day of each month in 2018,

2018-xx-xx – the exception will be valid from the beginning of 2018 (same as 2018-01-01) / to the end of 2018 (same as 2018-12-31),

2018-06-xx – the exception will be valid from the 1st of June 2018 (same as 2018-06-01) / to the 30th of June 2018 (same as 2018-06-30).

As you can see from the above examples, how you interpret the dates depends on whether the unidentified value is the beginning (FROM), or the end (TO) of the exception.

13. Control panel firmware update

ℹ️ *When the firmware update is running, the control panel does not execute its normal functions.*
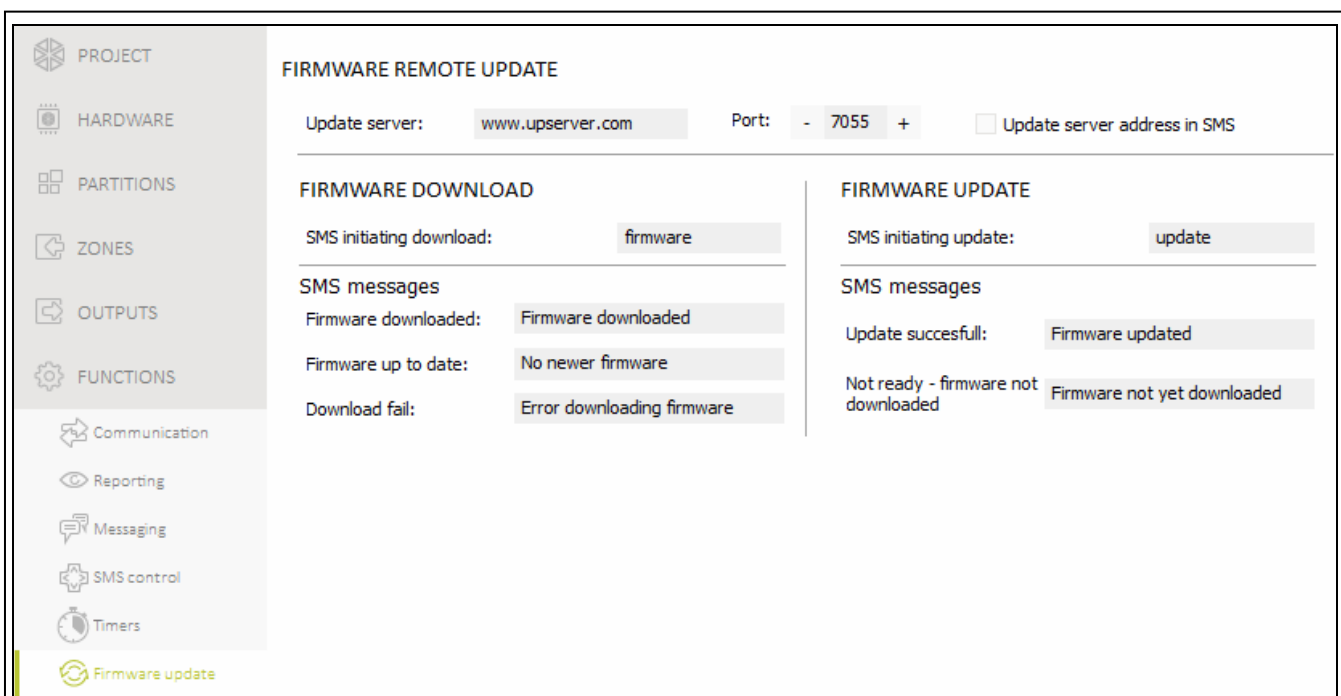
13.1 Local update

1. Download the update program for control panel firmware from www.satel.eu.
2. Connect the control panel RS-232 (TTL) port with the computer port
3. Run the update program for control panel firmware.
4. Click on the [icon] button.
5. When a prompt window is displayed asking you whether to continue the firmware update, click "Yes". The firmware of control panel will be updated.

13.2 Remote update

Remote update of the control panel firmware is made possible by the UPSERV update server, which is included in the SATEL product portfolio.

13.2.1 Remote update parameters and options

Fig. 21. "Firmware update" tab.

Update server [051.Address] – address of the UPSERV update server. You can enter the IP address or domain name.

Port [052.Port] – number of the TCP port used for communication with the UPSERV update server. You can enter values from 0 to 65535 (0=disabled).

Update server address in SMS [FW adr.from SMS] – if this option is enabled, you can enter server address and port number in the SMS message initiating the firmware download from the update server. If the message contains no address or port number, the control panel will use the preprogrammed settings.

Firmware download

SMS initiating connection [116.Download FW] – the control command which can be sent in the SMS message to initiate firmware download from the UPSERV update server. You can enter up to 8 alphanumeric characters (digits, letters and special characters). You can enter spaces, but at least one character must be different from the space.

i | *The command content must be different from that of the other control commands preprogrammed in the control panel.*

SMS messages

The control panel sends out an SMS notification on how the new firmware download has proceeded. The notification is sent to the telephone from which the SMS message initiating the firmware download was received. The message content may consist of up to 32 characters.

Firmware downloaded [1111.FW d-loaded] – the message to be sent by the control panel after completion of the firmware download from the UPSERV update server.

No newer firmware [1112.FW notfound] – the message to be sent by the control panel, if it turns out, after connecting to the update server, that there is no new firmware.

Download fail [1113.FW error] – the message to be sent by the control panel, if attempts to download the new firmware fail.

Firmware update

SMS initiating update [117.Update FW] – the control command which can be sent in the SMS message to initiate update of the control panel firmware. You can enter up to 8 alphanumeric characters (digits, letters and special characters). You can enter spaces, but at least one character must be different from the space.

i | *The command content must be different from that of the other control commands preprogrammed in the control panel.*

SMS messages

The control panel sends out an SMS notification on how the firmware update has proceeded. The notification is sent to the telephone from which the SMS message initiating the firmware download was received. The message content may consist of up to 32 characters.

Update successful [1114.FW updated] – the message to be sent by the control panel after completion of the firmware update.

Not ready – firmware not downloaded [1115.FW not upd.] – the message to be sent by the control panel, if the firmware update is not possible, because the new firmware version has not been downloaded.

13.2.2 Procedure of remote update for control panel firmware

i | *The SMS messages that initiate new firmware downloading and firmware updating can only be sent from the phone whose number is saved on the control panel (see "Phones" p. 36).*

1. Send to the number of SIM card currently used by the control panel an SMS message containing control command to initiate firmware download from the UPSERV update server. If the UPDATE SERVER ADDRESS IN SMS option is enabled in the control panel and you want the control panel to connect to an update server other than that indicated in the control panel settings, the message should look like this: **xxxx=aaaa:pp=** ("xxxx" – control command; "aaaa" – server address (IP address or domain name); "pp" – port number).

i | *If an SMS message containing the firmware download initiating command is re-sent when the new firmware downloading is in progress, the control panel will indicate in reply the download progress (percentage value).*

2. Completion of the new firmware download will be indicated by the control panel with an SMS message.

3. Send an SMS message containing the control command to initiate the control panel firmware update.

4. Completion of the control panel firmware update will be indicated by the control panel with an SMS message.

14. Users

There can be 15 users in the system. To simplify the procedure of adding / editing a user, the control panel makes available:

- user schedules,
- default functions of keyfob buttons.

14.1 User schedules

The user schedule defines the user rights. The control panel offers 5 user schedules. When adding or editing a user, one of the user schedules is selected.

i | *Changing the rights in user schedule results in a change of rights of all the users to whom that schedule was assigned.*

14.1.1 Parameters of the user schedule

Schedule name [121.Schedules] – individual name of the user schedule (up to 16 characters).

Right [121.Schedules] – defines which functions are available to the user. The following rights are available:

Arming – the user can arm the system.

Disarming – the user can disarm the system.

Alarm clearing – the user can clear alarms.

DURESS – a special right that allows to define in the system a code which, if used, will trigger a silent alarm (which is signaled in no way, but the alarm code is sent to the monitoring station). The alarm will be triggered in the partition in which alarm would be triggered in the event of tamper of the keypad used for code entering.

Zone inhibition – the user can inhibit the system zones by means of the INHIBIT function.

Zone isolation – the user can isolate the system zones by means of the ISOLATE function (the ZONE INHIBITION right is additionally required).

Change access code – the user can change own access code (CHANGE CODE function).

Users editing – the user can add, edit and delete users (USERS function).

Control – the user can control the outputs by means of the OUTPUTS CTRL. function.

Tests – the user can run the functions available in the TESTS submenu (except for the ID CHANGE function).

Service access – the user can run the SERVICE ACCESS and PERFECTA SOFT functions.

Changing panel ID – the user can run the ID CHANGE function (the TESTS right is additionally required).

Fig. 22. "Users" tab.

14.2 Default functions of keyfob buttons

You can define which functions can be started by using the new keyfob. When adding / editing a user, you can change the keyfob settings to make the functions suitable for the needs and rights of the user.

Changing the default functions has no effect on the settings of keyfobs which are already added to the users.