EN

Control panel PulsON Alarm 4G

Installer's manual

ALARM SYSTEM
PulsON Alarm 4g v.1.0

☎ ✉

www.pulsonalarm.pl

NSS Sp. z o.o. ul. Modularna 11 (Hala IV), 02-238 Warszawa
tel. +48 882 481 935, e-mail: kontakt@pulsonalarm.pl
NIP: 521-312-46-74

Update: 3.11.2022

TABLE OF CONTENTS

Introduction **5**
General information about the system 5
Compatible devices 5
Purpose of the system 5
Technical specifications **6**
Technical specifications 6
Mainboard description 6
Pinout description 7
Power supply performance on the motherboard 7
Menu navigation 8
System programming 8
Characteristics of bus connections 9
Adding and addressing bus devices 9
System manipulator installation 9
Connection of detection lines 10
Recognizing faults 11
Signal power measurement for GSM and Wi-Fi 12
Resetting to factory settings 13
Description of control panel functions **13**
System **13**
General settings.......... 13
Parameterization selection 14
Timers 15
Service settings 15
Partitions **16**
Input/output times 16
Lines **16**
Assigning lines to partitions 18
Types of line parameterization 18
Night line" function 18
Method of signaling an alarm from a supervisory line 18
Zone response time 18
Blocking capability 18
TX transmission delay 18
BELL delay 19
Gong 19
Dual fire verification 19
Alarm verification 19
Violation counter 19
Violations over time 19
Forced arming 19
Violation verification 19
Bell lock 19
Manipulators **20**
Settings 20
Keypad options 20
Schedules **22**
Outputs **23**
Output type 23
Operation time of an output 23
Partition assignment 23
Event types depending on Action Type 23
Communication **26**
GSM 26
TCP/IP 26
Monitoring 26
Cloud 27
SMS notifications 27

Event groups 27
Communication options 28
Users 29
Users 29
Access code options 29
Codes 29
Clip 30
Monitoring station 31
Alarms 31
Arming/disarming – users 31
Arming/disarming – general 31
Manipulators 31
Warnings 31
Lines 31
Expansion modules 31
SMS settings 31
Diagnostics (PC only) 31
Update 29
Local update 29
Remote update 29
LOG 29
Appendices 32
Appendix 1 – LCD/C keypad 32
Appendix 2 – LCD/T keypad 33
Appendix 3 – Manipulator installation 34

INTRODUCTION

General information about the system

The hybrid alarm system PulsON Alarm 4G is an innovative solution based on modern technologies. The basic function of the alarm system is to ensure the safety of property and people staying in the protected facility by informing the user and / or security about a potential threat. The main element of the system is the PulsON Alarm 4G alarm control panel, which continuously controls the operation of all peripheral devices, provides connectivity with the cloud and an alarm monitoring station. The control panel constantly supervises the detection lines and key parameters of the system operation.

The PulsON Alarm 4G control panel, the PulsON EXP8 / 1 expansion modules and the PulsON LCD / C and PulsON LCD / T keypads meet the requirements of the EN-50131 standard for Grade2.

Compatible devices

The PulsON Alarm 4G alarm system, via the communication bus, can work with the following peripheral devices:

Manipulators:
PulsON LCD/C
PulsON LCD/T
Line expansion module:
PulsON EXP8/1

System purpose

The PulsON Alarm 4G alarm system was designed to protect small and medium-sized facilities. The unit is designed for continuous operation, in rooms with low dustiness, in a neutral environment, with an ambient temperature of 0°C to + 50°C and a relative air humidity of 5% to 95% without condensation.

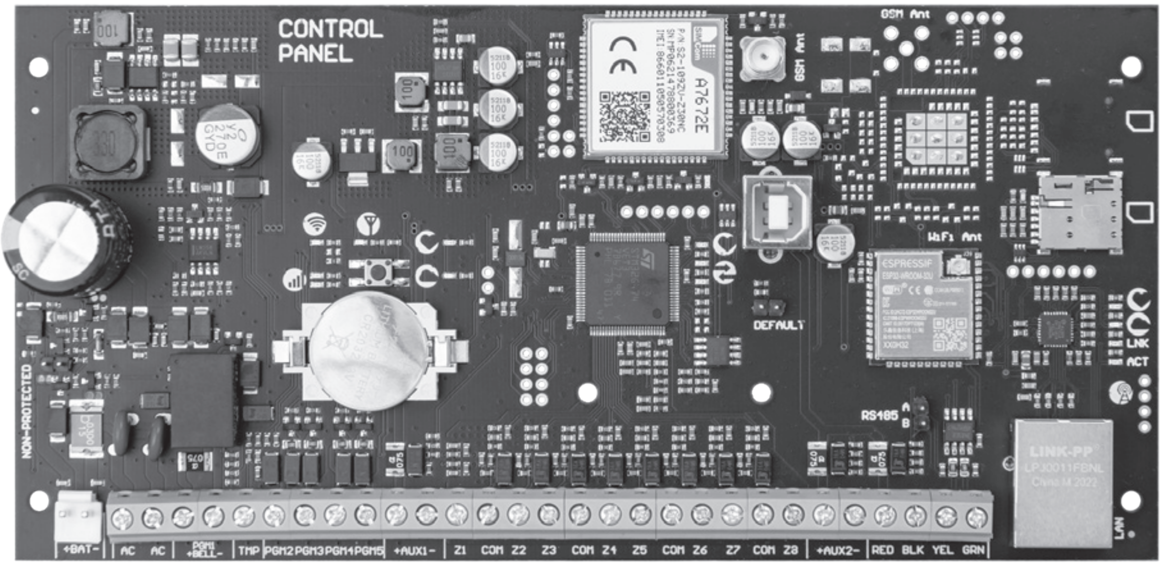
TECHNICAL SPECIFICATIONS

Technical data

	PulsON Alarm 4G
Number of lines on the control panel mainboard	8
Maximum number of lines	80
Maximum number of line expansion modules	7
Number of outputs on the control panel board	1+4
Maximum number of outputs	12
Maximum number of subsystems	8
Maximum number of keyboards	8
User codes	101
Wi-Fi module on the control panel board	YES
IP module on the control panel board	YES
GSM module on the control panel board	YES

Table 2

Mainboard description



ikon	name	Diode color	description
C	Heartbeat	Red	The diodes are signaling the correct operation of the systems (the processor and the systems responsible for IP and GPRS communication). If the system is working properly, the LEDs should flash approximately once per second
⇄	Communication	Green	The LED signals correct communication on the data bus. When working properly, the LED is blinking with a very high frequency
	Communication with SimCom	Yellow (2×) under the SimCom module	The diodes are signaling correct communication with the SimCom module. Yellow LEDs blink regularly when working properly
C	Cloud	Blue	The LED informs that the control panel is connected to the cloud server
Wi-Fi Ant	Antenna WiFi	–	Icon showing where to connect the WI-FI antenna
GSM Ant	Antenna GSM	–	Icon showing where to connect the GSM antenna

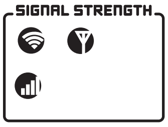
	Signal strength measurement section		This section is described in detail in the GSM and Wi-Fi signal strength test chapter
NON-PROTECTED	Funkcja „non-protected”	–	A function designed to protect the battery against deep discharge (below 10.5V). If the jumper is: • Removed – the battery protection function is active • Established – the battery protection function is inactive – in the absence of AC, the battery may be discharged to extremely low values
DEFAULT	Factory settings	–	Jumper for restoring the default settings of the control panel. A description of the restoring procedure can be found in the section Control panel reset to factory settings

Table 3

Pinout description

The table below describes all the screw terminals available on the control panel mainboard.

Clamp	Description
+ BAT -	Battery connector intended to support the control panel operation in case of 230V AC power failure
AC	Main power supply terminal of the control panel. The control panel should be powered with alternating voltage of 16V, 40VA.
+BELL- (PGM1)	Relay output controlling the alarm siren. The mass is displayed at the moment of its activation. The circuit is supervised.
TMP	Control panel tamper terminal, the normal state is shorted to ground.
PGM2-5	Universal transistor outputs, OC type. The mass is displayed at the moment of its activation.
+AUX1-	First auxiliary power supply rated 0.5A.
Z1 - Z8	Detection line terminals for connecting detectors.
+AUX2-	Second auxiliary power supply, rated 0.5A.
RED, BLK, YEL, GRN	Communication bus used for communication with keypads and expansion modules. The RED and BLK terminals are the power supply, the load capacity of the bus devices power supply circuit is 0.5A. The YEL and GRN terminals are used for data exchange between the control panel and devices connected to it.

Table 4

Power supply performance on the motherboard

The power supply on the mainboard supplies power to external devices via the AUX outputs, control panel modules installed on the bus, and to charge the battery. The sum of currents consumed by these devices must not exceed the power supply capacity. If devices with higher current consumption are used, they should be supplied from an additional buffer power supply and its status (lack of mains and low battery) should be monitored using inputs in the control panel.

Power supply parameters:

– current efficiency	2,5A
– AUX1 output load capacity	0,5A
– load capacity of the AUX2 output	0,5A
– bus load capacity	0,5A
– low battery status notification	11V
– battery disconnect / system shutdown	10,5V

MENU NAVIGATION

PulsON LCD/C

PulsON LCD/T

To navigate the menu on the main screen and in the user and installer menu, use the navigation arrows on the buttons 2 (up), 0 (down), 4 (left) and 6 (right), and the buttons OK (confirm) and ↩ (return to the previous screen), while to move the cursor to the right or left, hold down the 4 (left) or 6 (right) buttons for about 2 seconds. In order to delete the text, hold down the key ↩ for about 2 seconds.

When entering names and descriptions from the keyboard, with keys 2 and 0 (arrows up and down), we change the size of the letters: key 2 to capital letters, 0 to small letters. Press and hold the button until the letter size changes.

System programming

The control panel can be programmed by the system installer by means of a keypad or a computer with the Windows7 or newer operating system installed. Programming requires the Pulson Alarm Configurator program and a USB cable with a B-type plug.

⚠ **ATTENTION!**
The Pulson Alarm Configurator program only works with Windows operating system.

Programming the system is possible (in accordance with EN50131 Grade2) only after prior authorization for programming by the system user. The user allows programming by logging in to the keypad and selecting from the menu the **Settings** section, then the **Allow service** option and indicating the time necessary for the installer / service technician to carry out work on the system. During the service, the installer code allows you to log into the keypad.

Default access codes:	
Main user code:	**8888**
Installer code:	**4321**

When the installer is in the installer menu or has an active connection with the configuration program, it is not possible to operate the system:

- The system does not generate any alarms (including priority ones from the 24h zone and from keypads);
- Schedules are skipped;
- On all keypads, except for the one from which the installer carries out service, the message “programming in progress” is displayed;
- No partition can be armed (keypad, application, key zone);
- It is not possible to generate any type of alarm in the system (we block the generation of alarms, including 24h alarms, tampers, etc., e.g. if we open a detector or control panel housing).

It is not possible to program the control panel from the keypad and the PC configurator at the same time.

⚠ **CAUTION!**
Each time after changing the control panel settings using AlarmConfiguration or the keypad, it is recommended to restart the system: wait 10 seconds from making the changes to the control panel, turn off the mains and battery power, wait 10 seconds, and then turn on the control panel power supply again.

CHARACTERISTICS OF BUS CONNECTIONS

All 4 control panel terminals must be connected to the bus clamps in the extension modules and manipulators. The cable used for connections should have a minimum cross -section of 0.5 mm2. The maximum length of the cable used to connect the module to the communication bus is 305 m.

It is not recommended to build buses on a circular topology.

Adding and addressing bus devices

Each device connected to the system bus must be assigned its unique address by means of a DIP switch. System keypads and expander modules have a separate, independent addressing. This means that Manipulator1 and Expander1 can have the same address set by DIP switch and it does not cause any conflict. Devices of the same type must be assigned different addresses.

Device	Address	Line range	PGM range
Central	1 = ON, 0 = OFF	1-8	1-5
Expander 1	0000	9-16	6
Expander 2	1000	17-24	7
Expander 3	0100	25-32	8
Expander 4	1100	33-40	9
Expander 5	0010	41-48	10
Expander 6	0101	49-56	11
Expander 7	0110	57-64	12
Manipulator 1	0000	65-66	-
Manipulator 2	1000	67-68	-
Manipulator 3	0100	69-70	-
Manipulator 4	1100	71-72	-
Manipulator 5	0010	73-74	-
Manipulator 6	0101	75-76	-
Manipulator 7	0110	77-78	-
Manipulator 8	1110	79-80	-

Table 1

After connecting all devices to the bus, **start the Bus scan** from the installer menu or the PC program.

⚠ **ATTENTION!**
Setting the same address on similar devices (for example - for two keyboards) or no bus scanning after changing the addresses of devices on the bus results in the wrong operation of these devices (not taking a valid code, not performing functions, lack or erroneous display of the system status).

SYSTEM MANIPULATOR INSTALLATION

System manipulators are suitable for surface mounting. The detachable keypad base should be attached with the screws provided by the manufacturer. The use of other screws may damage the manipulator.

Slide the button keyboard onto the mounted base from the top.

Hook the touch keyboard to the lower or upper hooks in the base and press it into the base's hooks on the other side.

In the holes on the side walls of the manipulator's base, we can screw one locking screw, two screws, or not screw them in at all.

The touch keypad has a cleaning lock function that locks all buttons on the keypad for 20 seconds. During this time, it is possible to clean the touch surface of the manipulator without the risk of generating unwanted events / alarms.

To activate the keypad lock, simultaneously press and hold these buttons for 2 seconds OK and ↩.

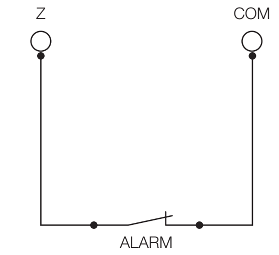
CAUTION!
The alarm system installation and all adjustments, changes and maintenance activities should be performed only by suitably qualified installers.
Incorrect installation may cause injury to people and animals, and damage to property, for which the manufacturer is not responsible.
Connection to the electrical system must be made in accordance with the applicable standards and legal regulations..

Connection of detection lines

In the PulsON Alarm 4G system, there are four types of parameterization of detection lines

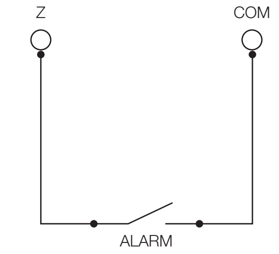
- NC
- NO
- EOL (1k, 1.1k, 2.2k, 2.7k, 3.3k, 3.74k, 4.7k, 5.6k, 6.8k, 6.98k, 10k)
- DEOL (1k, 1.1k, 2.2k, 2.7k, 3.3k, 3.74k, 4.7k, 5.6k, 6.8k, 6.98k, 10k)

NC



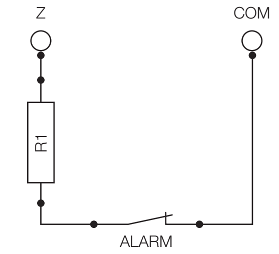
State	Value
Normal // line closed	0Ω
Violation // line open	∞

NO



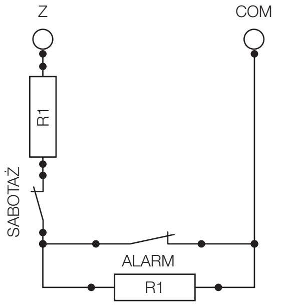
State	Value
Normal // line open	∞
Violation // line closed	0Ω

EOL



State	Value
Normal // line closed	R1 Ω
Violation // line open	∞
Line fault // Short Circuit	0Ω

DEOL



State	Value
Normal // line closed	R1 Ω
Violation // line open	R1 + R2 Ω
Line fault // line shorted	0Ω
Line tamper // line broken	∞

Recognized faults

The system monitors the system parameters on an ongoing basis. If any irregularities are detected, information about the trouble is displayed on the keypad, and an appropriate reporting code is sent to the alarm monitoring station.

Fault	Cause	Solution
Bus fault	Bus line interrupted or loose in the terminals. Short circuit in the bus line. Incorrect addressing of the manipulators. Failure to scan the bus.	Check the connection and continuity of the bus cables. Check the addressing or verify detection of keypads and expanders in the installer. Enable bus scan. Check which keyboard or module is causing the problem.
AUX1 failure	A short circuit or overload in the power cord of the devices connected to the output No.1.	Disconnect devices connected to the output and check if voltage appears. If so, remove the cause of the short circuit or overload. Look for the device that causes the output to short-circuit. Replace cable, correct connections.
AUX2 failure	A short circuit or overload in the power cord of the devices connected to the output No.2.	Disconnect devices connected to the output and check if voltage appears. If so, remove the cause of the short circuit or overload. Look for the device that causes the output to short-circuit. Replace cable, correct connections.
BELL output malfunction	A broken or loose cable in the Bell terminals connected to the device output. No 2.2 kOhm resistor on the device connected to the output. Faulty device connected to the output. Defective output relay.	Replace cable, correct connections. Connect a 2.2 kOhm resistor in the device connected to the output. Check that the device is functional. Check the output relay: connect the computer to the control panel with the AlarmConfiguration program and enable / disable the BELL output in the Diagnostics / Outputs tab.
Time Loss	The control panel did not have the time update from the NTP server within two days. No connection to the server. The server's IP address has changed. Wrong IP configuration of the Wi-Fi modem. Freezing of the router.	Check that the NTP server is specified. Change the NTP server. Check internet connections. Change time server. Restart the control panel. Check if the control panel has access to the Internet. Check the router and Wi-Fi coverage. Check the Ethernet cable.
Battery missing	Battery voltage is below 10.7V. The battery has been disconnected. No battery. Return at a voltage of 11.5V.	Connect a battery with a voltage higher than 10.5V. Check that the connectors at the battery and the control panel board are properly connected. Check the message after a few charging hours.
Low battery voltage	The battery was discharged below 11.2V. Return at 12V.	The battery is discharged or damaged. Connect the 230V power supply. If the facility's power was turned off before, check the battery voltage after a few hours of charging. Change the battery charging current setting to 0.7A. If the fault persists, replace the battery with a new one.
No AC	There is no voltage at the AC terminals. Broken track on the control panel board. The transformer is not working. Blown fuse in transformer. Power failure in the building.	Check if there is 230V power supply in the building and at the transformer input. Check the fuse in the transformer housing. Check the voltage at the transformer output. Replace fuse and / or transformer.

Line fault	The EOL or DEOL line is shorted to ground. Wrong type of line parameterization or resistance in installer programming selected.	Check connections at the control panel and in the detector. Check the cable. Change the line parameterization settings.
Lack of activity	The zone has not been violated within the set time interval, which means a long-term absence of people in the vicinity of the detector or a faulty device connected to the line. Broken wire in case of NO line.	Check the device connected to the detection line. Check the correctness of connections in the device and in the PBX. For the NO line, check the cable for patency. Verify the programmed time of inactivity.
Bus voltage low	Bus voltage low. Too many bus powered devices. Bus too long.	Check the efficiency of the control panel power supply. Use additional buffer power supplies. Increase the cross-section of the bus wires.
Service mode	The need for periodic inspection / maintenance of the system. The interval is programmed by the installer.	Perform a periodic inspection of the system. Disable the periodic review message in AlarmConfiguration.
Service fault	Triggering fault or tamper 5 times within 2 hours.	Find out what caused the service fault. Correct the fault. Restart the control panel. Reset the time in System / Service Settings / Time Reset.
No GSM / GPRS coverage fault	No coverage on the GSM module.	Connect the GSM 900MHz / 1800MHz antenna. Reposition the antenna. Restart the control panel.
Keyboard lock	A wrong code was entered three times (this is not a fault).	Wait 90 seconds and enter the correct code.

Table 5

To delete the defects indicated by the system, log in to the keyboard with the user code or installer, with the ok key to enter the menu, select the Fault Review screen and delete faults by pressing the OK key for several seconds. The faults will be deleted, but will be displayed again if the issue causing their occurrence has not been resolved.

⚠ **ATTENTION!**
With the fault of the monitoring station, re -attempt to make a connection takes place every 20 minutes. By using the options for deleting faults, (user menu/defects review/deletion of faults OK key) you can delete the connection fault and then the control panel will try to connect to the monitoring station immediately.

MEASUREMENT GSM and Wi-Fi signal strength test

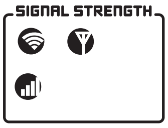


Figure 2

On the motherboard there is a section used to measure the strength of the WiFi and GSM signal.

To measure the signal strength, use the switch located in the “signal strength” field above the control panel memory backup battery to select the signal you want to measure - Wi-Fi 🛜 or GSM 📡. A blue LED will light up when an option is selected.

The signal strength will be presented on the LEDs next to the icon symbolizing range 📶, according to the table below.

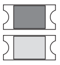
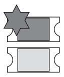
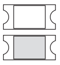
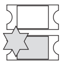
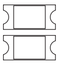
Signal strength	LEDs	Description
Nearly 100%		**Green and yellow LEDs are on continuously**
75%		**Green LED flashes, the yellow LED is on continuously**
50%		**The yellow LED is on continuously**
25%		**The yellow LED flashes**
No coverage		**No LED is on**

Table 6

In parallel with the signal force using the LED on the control panel, after pressing the switch on the board, signal strength and access to services is shown in decibels on the cental panel manipulators. The -64 dB to -78 dB signal is about 50% of the range. Below the value -82 dB, the signal is weak (less than 25%) and this may cause the lack of connection to the GSM network. Value -115 dB or larger and the inscription „No Service" prevents the control panel from connecting to the GSM network.

Each time after removing the SIM card from the socket, restart the control panel (turn off the network and battery power for a while). Putting the SIM card on the working control panel does not log in to the GSM network.

⚠ **ATTENTION!**
The Wi-Fi control module only supports the frequency of 2.4 GHz.
The Wi-Fi module requires the use of a separate antenna with the U.FL IPX connector. The Wi-Fi antenna is independent of the antenna to the GPRS module. Antenna for Wi-Fi should be purchased separately.

Reset the control panel to factory settings

The control panel can be reset to factory settings using the "Default" jumper on the main board. To restore factory settings, follow the instructions below.

1. Disconnect the AC power and the battery
2. Put the "Default" jumper
3. Connect the AC power and wait about 20 seconds
4. Disconnect AC power and remove the "Default" jumper
5. Connect the battery and apply AC power
6. The control panel is ready for operation

⚠ **ATTENTION!**
If the „Deleting settings to remove users" option in the control panel is enabled, all users of the system will be permanently deleted when performing the above procedure.
If the „Reset lock to factory settings" option is enabled, the control panel reset by means of the on-board jumper will not be possible.

DESCRIPTION OF THE CONTROL PANEL FUNCTIONS

The PulsON alarm system software has been designed in such a way as to give the installer the greatest possible configuration possibilities, so that he can adapt the system to the object specification and customer expectations.

Below is a list of all options that have been implemented in the alarm system.

The chapters in the manual reflect the arrangement of the options in the installer menu as well as in the "Alarm-Configuration".

BUS SCANNING

Start scanning

After connecting the modules, even before programming the control panel, scan the system devices.

List of modules

After scanning the bus, you can check the keyboard and expanders in the system here.

SYSTEM

The System section contains all the control panel parameters that define the operation of the entire system.

General settings

Compliance with the norm EN-50131:Grade2

Enabling EN-50131 compliance will change the following settings:

1. Quick arming – OFF
2. Allow arming in fault time – OFF
3. Time to enter – maximum 45s
4. Presentation of partition status – OFF
5. Allow the site without asking the user – OFF

Default: NO

Quick arming

If the function is enabled, holding a closed padlock on the keypad will arm all partitions assigned to the keypad without entering the user code.

Default: NO

⚠ **WARNING!**
When this option is enabled, the system does not comply with the requirements described in the EN50131 standard in the scope of Grade2.

Lock possible

The function determines whether it is possible to bypass (temporarily disarm) zones in the system for the time of supervision. Defining which zones will be blockable is performed in the „Zones” section in installer programming.

Default: YES

Wrong code – information to ARC

If the function is enabled, entering an incorrect code 3 times on the keypad will result in sending information about the event to the ARC.

Default: NO

Wrong code – keypad lock

If the function is enabled, entering an incorrect code on the keypad three times will activate the keypad lock. The keypad lock lasts 90 seconds. Only after the blocking time has elapsed, it is possible to enter the correct code.

Default: YES

BELL signaling when arming / disarming

If the function is enabled, the system will indicate arming the system with one short beep on the BELL output, disarming with two beeps and with alarm in memory, disarming with three double beeps.

Default: NO

Loud panic alarm

If enabled, using the panic button on the system keypad will trigger a loud alarm.

Default: NO

Quiet exit delay countdown when arming in night mode

If the function is enabled, when arming the partition in night mode, the keypad will not signal the exit delay countdown with the built-in buzzer.

Default: YES

Factory reset lockout

If the function is enabled, it will not be possible to restore the factory default settings of the system using a jumper on the control panel board.

Default: NO

Factory reset removes users

Disabling the function preserves the users and their rights in the event of a system reset to factory settings.

Default: YES

Allow arming during trouble

Enabling the function allows the system to be armed during any trouble.

Default: NO

⚠ **WARNING!**
When this option is enabled, the system does not comply with the requirements described in the EN50131 standard in the scope of Grade2.

Parameterization selection

EOL resistor

The value of the EOL resistor used in the EOL line configuration (with a single resistor). • Normal condition = EOL • Alarm = ∞ • Fault = 0Ω	1k, 1.1k, 2.2k, 2.7k, 3.3k, 3.74k, 4.7k, 5.6k, 6.8k, 6.98k, 10k (2,2k by default)

DEOL resistor

The value of EOL resistors used in the DEOL line configuration (with a double resistor). • Normal condition = 1xEOL • Alarm = 2xEOL • Tamper = ∞ • Line Fault = 0Ω	1k, 1.1k, 2.2k, 2.7k, 3.3k, 3.74k, 4.7k, 5.6k, 6.8k, 6.98k, 10k (2,2k by default)

Custom line response time

A parameter that specifies the custom line response time. Range 1ms-600ms	Range 1-600 milliseconds. (domyślnie 30ms)

Battery charging current

Parameter specifying the maximum current that can be consumed by the charging battery.	0.36A, 0.7A, 1.6A (0.36A by default)

Clocks

BELL signaling time

A parameter that defines the cut-off time of the BELL output (siren output) in the event of an alarm.	Range 0-120 minutes. (default is 4 minutes)

AC loss delay

A parameter specifying the delay in sending information on AC power failure to the monitoring station	Range 0-120 minutes. (default 60 minutes)

Line stabilization time

A parameter that defines the time from recovery of the control panel voltage until detector operation stabilization. During this time, alarms from all zones will not be generated.	Zakres 0-255 sekund. (domyślnie 10 s)

Smartline timezone

After a single violation of a zone with the „intelligent” partition option enabled, it does not generate an alarm, the system starts counting the verification time. If another line is violated with the „intelligent” option on, only then an alarm event is generated.	Range 0-255 seconds. (default 10 s)

Sequential detection timezone

After violation of a zone with sequential detection, the partition goes into alarm, the verification time starts counting down, but does not send an event to the ARC. If another violation occurs within the programmed time, the event is only sent to the ARC.	Range 0-255 seconds. (default 0 s)

Time zone

A parameter that allows you to select a time zone corresponding to the location of the control panel.	Default is UTC + 1

Summertime

This function enables automatic switching of the control panel clock to summer time.	

NTP server

Time synchronization server address.	

Sabotage sound

The function defines how the tamper of the alarm system will be signaled.

• Silent	Just a silent alarm
• Bell	Activation of the output defined as BELL
• Buzzer	Buzzer only activation in manipulators
• Bell i buzzer	Activation of the output defined as BELL and Buzzer in keypads
BELL-Armed, Buzzer-Disarmed	Depending on the arming of the system
• BELL – armed, Silent – disarmed	Depending on the arming of the system

Cichy,
• Bell,
• Buzzer,
• Bell i buzzer,
• BELL-Armed, buzzer-disarmed
• BELL – armed, Silent – disarmed
(by default "BELL-Armed, Buzzer-Disarmed")

Service settings

It is possible to remind the user of the necessity to carry out periodic service visits for maintenance and test the system by the installer.

The service visit interval determines the time after which information will be generated in the system (in the form of a service fault).

Options:
- Off
- 6 months
- 12 months
- 24 months (disabled by default)

PARTITIONS

Partitions are logically separated parts of the secured object that are subject to arming at different times or situations than the other partitions in this object. In relation to the system, a partition is defined by zones, outputs, keypads and users assigned to it. Partitions can be separate parts or optionally have common parts.

Activate partitioning

The alarm system can be divided into 8 independent partitions. In order to enable partitioning, in the installer menu, next to the selected partition, switch the "Active" option to YES.

CAUTION!
If we divide the system into several partitions, and then turn off some partitions, be sure to remove / deselect all lines that were originally assigned to these partitions. To do this, first include these partitions in AlarmConfiguration, uncheck any marked zones assigned to these partitions, and then disable unused partitions again. This is necessary for the correct handling of active partitions.

Choosing the communication path

Each partition can send alarm signals to one or more monitoring stations (maximum 8). To enable monitoring to the monitoring station, select the ARC (monitoring station) to which alarm signals are to be sent and configure the connection to the station in the communication-monitoring section.

Entry / exit times

Entry time 1

Entry time 1 is a parameter closely related to the Delayed 1 zone and defines the time that the system user has to enter the premises (disarming the system). If the entry delay time ends without disarming, an alarm will be generated.

Entry time 2

Entry time 2 is a parameter closely related to the Delay 2 zone type and defines the time that the system user has to enter the premises (disarming the system). If the entry delay time ends without disarming, an alarm will be generated.

Exit time 1

A parameter that specifies the time that the user has to exit the site. The exit delay time is assigned to the keypad.

Exit time 2

A parameter that specifies the time that the user has to exit the site. The exit delay time is assigned to the keypad.

Special exit time

Time for exit counted down when using a key type zone or a mobile application to arm.

LINES

Line reaction types

Line reaction types define how the line will behave. There are 22 different line types available in the system. To be able to program zone related functions, first select the zone reaction type (for an Unused zone, zone programming is not possible).

Not used

The unused zones in the system should be programmed as unused zones. This type of zone is not visible in the system, its violation does not cause any system reaction.

Delayed 1

Violation of the zone Delayed 1 when arming the partition starts the entry delay 1 countdown – if the system is not disarmed during the entry delay, an alarm event will be triggered.

Delayed 2

Violation of the Delay 2 zone while arming the partition starts the Entry delay 2 countdown – if the system is not disarmed during the entry delay, an alarm event will be triggered.

Internal

An internal zone becomes delayed if a delay zone is first violated. Otherwise, it works like an instant zone when armed.

Immediate

When armed, the zone immediately triggers an alarm.

24h fire

Violation of this line will trigger an immediate loud alarm: BELL output (switchable 3 seconds / 3 seconds), signaling on all keypads, a fire icon is displayed next to the appropriate partition in the mobile application, the zone violation is recorded in the event log. (See also: Dual Fire Verification).

24h break-in

Violation of this line will immediately trigger a continuous BELL alarm, signaling on all keypads, the Shield icon will appear in the mobile application, the line violation is recorded in the event log.

24h gas

Violation of this line will trigger signaling on all keypads (fast signaling every 1 second) and an entry in the event log about gas detection. There is no information in the mobile application.

24h CO2

Violation of this line will trigger signaling on all keypads (fast signaling every 1 second) and an entry in the event log about the detection of carbon monoxide. There is no information in the mobile application.

24h temperature

Violation of this line will immediately trigger a continuous BELL alarm, signaling on all keypads, and an entry in the event log about exceeding the temperature, if the temperature exceeds the threshold programmed in the temperature detector.

24h flood

Violation of this line will immediately trigger a continuous BELL alarm, signaling on all keypads, and an entry in the event log about flooding.

24h tamper

Violation of this zone will result in an immediate triggering of the continuous BELL alarm, signaling on all keypads, and an entry in the event log. Attention! Violation of this type of zone when the control panel is in the service mode does not cause any system reaction and can be used to carry out service work without triggering alarms.

24h no alarm

Violation of the zone does not trigger an alarm, only an entry is added to the event log. Information about the violation of this line is not sent to the mobile application.

24h definable

Function being prepared for future use.

Output control

The zone does not generate any alarm event, its violation is not recorded in the event log. The line serves only to control the PGM output. When programming, a line of this type must be associated with an Output (the Line tracking event type and the line number).

Momentary key on / off

A momentary violation of NC, NO and EOL zones causes alternate arming / disarming of the partition to which the zone is assigned.

Permanent switch on / off

Violation of the zone causes permanent arming / disarming of the partition to which the zone is assigned. NC and EOL zone: closed = system disarmed; violated, in tamper or in trouble = system armed. For NO lines: closed = system armed; zone open = system disarmed.

Momentary key arming

A momentary violation of NC, NO and EOL zones will arm the partition to which the zone has been assigned.

Momentary key to disarm

A momentary violation of NC, NO and EOL zones will disarm the partition to which the zone has been assigned.

24h panic

Violation of this zone will result in an immediate triggering of the continuous BELL alarm, signaling on all keypads, and an entry in the event log.

24h burglary

Violation of this zone will result in an immediate triggering of the continuous BELL alarm, signaling on all keypads, and an entry in the event log.

Assigning Zones to Partitions

Possibility to assign a line to a given partition / subsystem. A zone can be assigned to several partitions. In this way, we create a common zone.

⚠ **CAUTION!**

If we divide the system into several partitions, and then turn off some partitions, be sure to remove / deselect all lines that were originally assigned to these partitions. To do this, first include these partitions in AlarmConfiguration, uncheck any marked zones assigned to these partitions, and then disable unused partitions again. This is necessary for the correct handling of active partitions.

Types of line parameterization

Defining the type of line parameterization. The types are available as described on pages 10 and 11.

“Night line” function

Zones with “night” function enabled will be automatically blocked during arming in night mode.

Signaling an alarm from a detection line

Silent

Violation of a zone with the Silent signaling function selected does not cause a loud alarm. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Bell

Violation of a zone with the BELL signaling function selected causes a loud alarm. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Buzzer

Violation of a zone with the Buzzer signaling function selected will generate acoustic signaling only on keypads. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Bell and Buzzer

Violation of a zone with a selected Bell and Buzzer signaling function generates a loud alarm and triggers acoustic signaling in keypads. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Bell arming / buzzer disarming

Violation of a zone with the Bell signaling function selected – arming / buzzer – disarming generates a loud alarm during supervision, and in the case of a disarmed system, it only triggers acoustic signaling in keypads. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Buzzer arming / silent disarming

Violation of a zone with the selected signaling function Buzzer arming / silent disarming, in the case of a system in supervision, triggers acoustic signaling in keypads, and in the case of a disarmed system, it does not trigger any sound signals. Information about the alarm is recorded in the event log and the appropriate reporting code is sent to the monitoring stations.

Line response time

Fast

Line response time 100ms.

Slow

Line response time 400ms.

User time

The response time is defined in the System / General / Custom zone response time tab.

Lockable

The option determines whether the zone can be bypassed while arming by the user.

Transmission delay (TX)

Time of delay of transmission to the monitoring station, expressed in seconds. If the alarm is cleared during this time (disarming the partition to which the zone is assigned), the system will not send information about the alarm to the ARC.

BELL delay

BELL output delay time, expressed in seconds.

Gong

If this option is enabled, each violation of a zone with the gong function enabled will generate a beep on the keypad, if the gong function has also been enabled in the keypad settings.
For the user to enable / disable the gong sound, in the Keypad options tab, the function Enabling / disabling the gong function should be assigned to the function key F1-F6.

Double fire verification

Fire alarm verification function - if an alarm from the 24h fire zone is detected, the voltage on the power supply output of the smoke detectors will be removed for 3 seconds, if after restarting the detectors, they re-detect the threat, a loud alarm will be immediately generated and the event reporting code will be sent to the monitoring stations.

Alarm verification

Defining the method of alarm verification.

Sequential detection

A violation of a zone with the “sequential detection” option turned on during the supervision period generates an alarm, but information about the alarm is not sent to the ARC. Only the next violation of the line with the sequential detection on will cause the appropriate reporting code to be sent to the ARC. (See also: Sequential Detection Timezone on the System Tab).

Multiple violations

The first violation of a line during the supervision with the “multiple violations” option enabled does not generate an alarm, only the next violation of the same line generates an alarm. The option is related to the “Counter of violations” and “Violations in time” parameters.

Intelligent line

After a single violation of a zone with the “intelligent” partition enabled, no alarm is generated, the system starts counting the verification time. If another line is violated with the “intelligent” option on, only then an alarm event is generated. (See also: Intellizone Timezone on the System Tab).

Violations Counter

The option determines how many line violations are needed to generate an alarm - this option is related to the “Violations during time periods” parameter.

Violations during time periods

The option defines the time in which a line violation must occur in order to trigger a loud alarm - the option is related to the “Violations counter” parameter.

Force Arming

The option defines whether it is possible to arm the system when a detector line is violated.

Violation Verification

The function makes it possible to detect possible damage or malfunction of the detector. If the detector is not violated within the defined time period, the system will generate a trouble.

Violation Verification – Time

Parameter related to the function “ Violation Verification“.

Violation Verification – Days

Parameter related to the function “ Violation Verification“.

Bell Lock

A parameter that defines after how many alarms from a given line will be blocked from triggering the loud signaling.

TX Lock

A parameter that defines after how many alarms from a given line the transmission to ARC will be blocked (this option protects the ARC against sending a large number of alarm events from damaged detectors).

MANIPULATORS

Settings

Name

Keypad name – the programmed name will be displayed in the system log, mobile application, etc.

Assigning to subsystems

The partitions assigned to the keypad will be displayed on the keypad screen - if this option is enabled.

Buzzer -> Bell

If enabled, the buzzer on the keypad will mimic the operation of the Bell output (siren output).

Gong

If the function is enabled, each violation of a zone with the “gong” function on will trigger a short buzzer signal in the keypad. In order for the user to enable / disable the gong sound, one of the function keys (F1-F6) must be programmed in the keypad options as “Enable / disable the gong function”.

Assignment of exit times to the keypad

Choosing which exit delay time (set in the Partitions tab) will be counted down when individual partitions are armed.

Manipulator options

Fire button active

If the function is enabled – the keypad fire alarm button is active.

Panic button active

If the function is enabled, the panic alarm button on the keypad is active.

Medical button active

If the function is enabled, the medical alarm button on the keypad is active.

Function buttons

The keypad has 6 function buttons, which are designed to make it easier for the user to operate the system.
The function buttons make it easy to start the most frequently used functions in the system. They are a kind of keyboard shortcuts which trigger a specific reaction of the system in accordance with the settings programmed by the installer.
To recall the action assigned to a function button, press and hold for 1 second the button with the f symbol and the number of the function button 1-6.

Function key programming options available

Button not used	No response to button selection
Check for faults	After pressing the button, the user will go to the fault checking menu after entering the user code
Line blocking	Selecting the button results in moving to the zone bypassing menu after entering the user code
Fully arming all partitions assigned to the code	Selecting the button causes complete arming of all partitions assigned to the user code
Night arming of all partitions assigned to the code	Selecting the button causes night arming of all partitions assigned to the user code
Activation of the PGM 1… 12 output	Selecting the button will activate the PGM output defined as an operational output – after providing the user code
Enabling / disabling~ the gong function	Selecting the button will enable / disable the gong function in the keypad
Programming user codes	Selecting the button results in moving to the access code programming menu after providing the user code with appropriate authorizations
Select Partition 1… 8	Selecting the button and entering the correct user code takes you directly to the partition screen

Presentation of entry time

The function determines whether the entry delay will be displayed on the keypad – on the partition screen.

Presentation of time to leave

The function determines whether the exit delay will be displayed on the keypad – on the partition screen

Partition status presentation

The function determines whether the status of partitions assigned to the keypad will be displayed on the keypad main screen.

LCD blank

If the function is enabled, the LCD display will not display any content 5 seconds after the last operation on the keypad.

LED blanking

If the function is enabled, the information LEDs will go off 5 seconds after the last operation on the keypad.

The AC diode blinks when the ~ 230V power supply is off

If the function is enabled, the AC LED on the keypad will blink in the event of AC power failure.

Buzzer does not indicate a fault

If the function is enabled, the buzzer will not signal any system failure.

Keyboard blanking during supervision

If the function is enabled, the keypad backlight, LCD display and LEDs will go out after arming all assigned partitions.

Brightness

Defining the brightness of the keypad backlight. Range 0-5.

Buzzer

Defining the buzzer volume when using the joystick buttons. Range 0-5.

LCD backlight time

Parameter defining the keypad backlight timeout. Range 000-999 seconds.
000 = infinite backlight time (backlight does not turn off).

SCHEDULES

The schedules enable automatic, clock-controlled arming (including arming in night mode) and disarming of partitions as well as control of utility outputs. Two schedules must be used to obtain the on / off operation.

Active

Before changing the settings, check the Active option for the given schedule.

Hour, Minutes

Enter the time (hours and minutes) for the expected response.

Days of the week

Mark the days of the week on which the reaction is to be triggered.

Action type

Select the expected operation of the control panel from the drop-down menu.

Object number

Select the partition or output number depending on the selected action type.

OUTPUTS

Output type

Timed NO

Timed (Pulse) – NO (monostable, normally open)

Timed NC

Timed (Pulse) – NC (monostable, normally closed)

Fixed NO

Fixed – NO (bistable, normal open)

Fixed NC

Fixed – NC (bistable, normally closed)

Output cut-off time

A parameter that defines the PGM output cut-off time. Only valid for time outputs. Range from 1 to 9999 seconds.

Allocation to a partition

Select the partitions from which events will trigger the exit action. Partition selection cannot be made for System and Line actions.

Types of events depending on the type of action

According to the System

- Bell
  Alarm signaling output. It will be activated in the event of an alarm in the system.
- Power supply for fire detectors
  The output is active in the normal state (NC). It is used to power resettable fire detectors. The output is reset after the fire alarm is reset.
- Fault
  The output will activate if any fault occurs with the system.
- Time Loss
  The output will activate if there is a problem with the clock in the system.
- No ~230V power supply
  The output will activate in the event of AC power failure.
- Battery failure
  The output will be activated if the battery voltage drops below 11V
- Bus failure
  The output will be activated if the control panel loses communication with any module installed in the system.
- Bell failure
  The output will be activated if the siren is not connected to the BELL outpu.

- GSM failure
  The output will be activated if the GSM module cannot be logged into the network.
- No GSM coverage
  The output will be activated when there is no GSM network coverage.
- No GPRS coverage
  The output will be activated when there is no GPRS network coverage.
- Jamming GSM / GPRS
  The output will be activated in case of a sudden drop in GSM / GPRS signal strength.
- Communication error
  The output will be activated in the event of a problem with the connection to the SM receiver and the control panel does not receive the KISSOFF signal within the programmed time and number of attempts.
- Service failure
  The output will be activated in the event of a need for a periodic service visit.
- Fault Group – Connectivity
  The output will be activated if there is a communication fault in the system – GSM fault, GPRS range fault, GSM range fault, Trouble – jamming, Communication fault
- Fault group – power
  The output will activate if there is a power related fault in the system – AC Fault, Battery Fault, AUX Fault.
- Tamper alarm
  The output will be activated if a tamper alarm occurs in the partition assigned to the output.
- Keypad tamper alarm
  The output will be activated if a tamper alarm occurs in the partition assigned to the output (e.g. when the keyboard is torn off a wall).

According to Partition

- Utility output
  User-controlled output (from the keypad level, mobile application and via CLIP notifications). Related to the Users / Clip tab. Only after selecting / enabling this output function, cells related to the added output will be added to the CLIP menu. Up to this point, you can only enter the telephone number in the CLIP tab, but you cannot assign any output reaction.
- Utility output – schedule
  User-controlled output (from the keypad, mobile application) or schedule. This type of output is not controlled by CLIP notifications.
- Burglar Alarm
  The output will activate if a Burglar Alarm occurs in the partition assigned to the output.
- Panic alarm
  The output will activate when a panic alarm occurs in the partition assigned to the output.
- 24h line alarm
  The output will be activated if an alarm from any 24h zone occurs in the partition assigned to the output.
- Fire alarm
  The output will activate when a fire alarm occurs in the partition assigned to the output.
- Verified alarm
  The output will activate if a verified alarm occurs in the partition assigned to the output.
- Keypad panic alarm
  The output will activate when a panic alarm is generated from the keypad.
- Keypad fire alarm
  The output will activate when a fire alarm is generated from the keypad.
- Keyboard medical alarm
  The output will activate when a medical alarm is generated from the keypad.
- Duress alarm
  The output will activate if a duress code is used.

- System status – armed
  The output will be activated if the partitions assigned to it are armed – regardless of arming mode (total / night).
- System State – Armed in Exit Mode
  An output will activate if all assigned partitions are armed in exit mode.
- System State – Night Armed
  The output will activate if all assigned partitions are armed in night mode.
- System status – disarmed
  The output will activate if all partitions assigned to it are disarmed.
- Entry delay time
  The output is active during the entry delay period.
- Exit delay time
  The output is active during the exit delay period.
- Wrong code
  The output will be activated after 3 attempts to enter the wrong code. The deletion will take place after entering the correct access code.

According to the line

- Line alarm
  The output will be activated when an alarm occurs from the indicated zone.
- Line tracking
  The output shows the status of the detector line.
- Line number
  Parameter defining the line number in case of selecting the Action Type – Same as line.

COMMUNICATION

GSM

GPRS

For communication via the cellular network, an APN access point must be set. The default APN, Username and APN Password for most operators is "internet".

SIM

In the SIM section it is possible to enter the PIN code of the sim card. If the card is to work without entering the PIN code, disable this option on the SIM card using an external device (mobile phone), insert the prepared card into the control panel socket, and do not enter any values in the "SIM card PIN code" box in the program.

TCP/IP

IP

Transmission medium selection:

- Ethernet
- Wi-Fi

If you select Wi-Fi, enter the network name and password in the SSID and Wi-Fi Password sections

Connection type

- DHCP Enabled
  If the option is enabled, the IP address and other network parameters will be automatically downloaded from the router.
- IP
  The current IP address of the control panel must be entered.
- Mask
  You must enter the current Netmask.
- Gateway
  You must provide a Default Gateway.

- DNS1
  Primary DNS must be entered.
- DNS2
  Backup DNS must be provided.

Monitoring

Name

Name of the monitoring station - the programmed name will be displayed in the system log, mobile application, etc.

Channel

Selection of the transmission channel for establishing connection with the alarm monitoring station.

GPRS only	communication to the cloud will be established only via GPRS
LAN (Wi-Fi)	One communication path – always LAN / Wi-Fi
SMS	One communication path – always SMS
LAN(Wi-Fi)/GPRS	Two communication paths – priority LAN / Wi-Fi and GPRS replacement
GPRS/ LAN(Wi-Fi)	Two communication paths – priority GPRS replacement LAN / Wi-Fi
LAN(Wi-Fi)/GPRS/SMS	Three communication paths – priority LAN / Wi-Fi replacement GPRS – SMS in case of unavailability of the previous two
GPRS/ LAN(Wi-Fi)/SMS	Three communication paths – priority GPRS replacement LAN / Wi-Fi – SMS in case of unavailability of the previous two

Kissoff Time

The time during which the control panel waits for confirmation that the alarm signal has been received by the receiver.

Number of attempts

The number of communication attempts made when no confirmation signal was received from the receiver.

Basic IP

IP address of the alarm monitoring station receiver.

Backup IP

IP address of the alarm monitoring station receiver used when the primary receiver is unavailable.

Port

Receiver port.

Partition 1 to 8 – Object Number

Enter the object number (DL) – four digits, in accordance with the Contact ID format.

Telephone for SMS communication

Specify if SMS reporting code reporting is used.

Type

Select the communication protocol: TCP or UDP.

Events

Select the events that will be reported to the given monitoring station.

Cloud

Connection type

Selecting the connection method through which to connect to the cloud server:

TCP / IP only	communication to the cloud will be established only via the Ethernet / Wi-Fi module
GPRS only	communication to the cloud will be established only via GPRS
IP/GPRS	communication will be established first over the Ethernet / Wi-Fi module. GPRS is a backup track
GPRS/IP	communication will be established first over the GPRS module. Ethernet / Wi-Fi is a backup path.

Cloud address

In order to use the mobile application, the cloud settings must be properly configured. By default, the control panel uses the manufacturer's cloud to connect to the address **nss.pulsonalarm.pl** on port **8883**.

Cloud port

The port used to connect to the cloud server.

SMS notifications

The purpose of SMS notifications is to inform the user about the occurrence of a specific event in the alarm system.

Phone number

Phone number of the person for SMS notifications. There is no need to enter a prefix.

Assigning to Partitions

Defining from which partition the given user is to receive information about events.

Event groups:

Arming

SMS reporting on partition arming.

Disarming

SMS reporting on partition disarming.

Alarms

Partition alarm SMS reporting.

Sabotage

SMS reporting on system tamper.

Faults

SMS reporting about system faults.

Communication options

Periodic transmission test

Enter the time during which the periodic test of transmission to ARC will be carried out.

Loading default report codes

It is recommended that you load the default report codes whenever you change line types.

USERS

Users

User Name

User name – the programmed name will be displayed in the system log, mobile application, etc.

Assigning to Partitions

Select which partition the user will be able to manage.

Code

The code to be used by the user. Asterisks show if the code is entered, but the code itself is invisible.

Set the code

Possibility to enter the code to be used by the user.

⚠ **ATTENTION!**
When facing a threat, the user can use the action code under coercion. The use of the action code under the compulsion to disarm the system, causes the system disarming and simultaneously generating a quiet alarm and notification of the monitoring station. The code under coercion is like the user code, but the value of the last digit should be increased by 1.

Access Codes options

Active

Only active codes have access to the system.

Arming

The function defines whether the user is allowed to arm the system.

Disarming

The function defines whether the user has the right to disarm the system.

Line blocking

The function defines whether the user has the right to bypass the line.

Access from the mobile application

The function defines whether the user has access to the mobile application.

Controlling the outputs

The function defines whether the user can control the outputs. The control concerns only the outputs defined as operational outputs.

Supervisor code

The function defines whether a given user has the right to exercise supervision over the system. The supervisor code has permissions similar to the master user – it can add new users and edit the existing ones, excluding the master user.

Maintenance code (cleaners)

The function defines whether the given user has the maintenance rights. The maintenance code can disarm the system only once a day, it can arm an unlimited number of times.

Turn on the time scheme

The time scheme allows you to restrict user access to certain times and days of the week. After selecting / enabling the time schedule, select the days of the week and the time in which the time schedule will run.

QR code

This function allows you to display and scan the QR code needed to log in to the user in the mobile application.

Codes

Master user code

Master user code. The master user has the highest possible access rights in the system. Has access to all partitions, can add new users and edit the properties of the existing ones.

Installer code

The installer code is active only if the master user has authorized the service and programming of the system (User menu / Settings / Allow service / How many hours).

Code length

Parameter specifying the length of access codes. 4, 6 or 8 digit codes are possible. After selecting a given value, all codes in the system must have the same length.

Clip

The CLIP function makes it possible to activate the output programmed as the “Utility output” by calling the SIM card number in the control panel. Function related to the tab Outputs / Partition / Usable output. The cells related to the added output will be added to the CLIP menu only after selecting / enabling the Function Output function for any of the control panel outputs. Up to this point, you can only enter the telephone number in the CLIP tab, but you cannot assign any output reaction.

Active

Mark the given relation: telephone number – output so that the control is possible.

Phone

Enter the telephone number from which the output will be controlled.

Output

Select reaction of the output to the received CLIP. You can choose to enable, disable and switch (from current to opposite state).

MONITORING STATION

The tabs offer event codes in the Contact ID protocol and the option to select events for SMS notifications.

Alarms

The following alarm event codes are provided: panic, fire, medical, duress, control panel tamper, panic.

Arming / Disarming – Users

Codes of events related to arming and disarming the system by individual users are provided.

Arming / Disarming – General

Codes of events related to arming with the key line, auto-arming and quick arming are provided.

Manipulators

The codes of events related to the tamper, keypad lock and bus fault are provided.

Warnings

Codes of events related to power failure, siren failure, battery failure, AUX outputs, receiver failure as well as incorrect code and programming mode are given.

Lines

Codes of events related to alarms, faults, interlocks, tampers and inactivity of detection lines are given.

Extension modules

The codes of events related to the tamper and the expansion module bus fault are provided.

SMS settings

You can choose which notifications from the event group: alarms, arming / disarming, zones, warnings, expansion modules, keypads will be sent to the user as SMS messages..

DIAGNOSTICS (PC ONLY)

Diagnostic functions are only available from AlarmConfiguration program.

Lines

The tab allows you to test the lines existing in the system in real mode. To test, turn on the “Line test” button in the upper part of the window. The current status of the zone will be displayed in the STATUS column.

Modules

The tab will display information on the control panel modules connected in the given system. Next to the module name, information about its current status, supply voltage and firmware version is provided.
The UPDATE button allows you to download a newer software version to the control panel and modules. Relevant files will be made available, if necessary, by the technical support of the control panel manufacturer.

CAUTION!
Updating the control panel software is only possible when the alarm system is fully disarmed. It is not possible to perform any actions in the alarm system during the update. The update progress is shown on the keypad as a percentage.
It is also possible to remotely update the control panel firmware. The update is carried out by the installer after obtaining the user’s consent. The user agrees to allow service access to the control panel by activating this function from the keypad. The user should enter the user code, press the OK / Menu button, use the arrows to move to the Settings tab and confirm with OK. Then, select the Allow service option and select the appropriate one in a given situation from among the displayed periods, confirming the selection with the OK button. Access for the website may be granted for 1, 2, 4 or 8 hours, 1 day or for an unlimited period. Confirmation of the selection will be a message on the keypad indicating the current period of service access to the control panel and the Finish option, by means of which the user can at any time disable the installer’s access to the control panel programming options.

Above the list of modules, there is the control panel serial number, which identifies the control panel when logging into the servers. The installer can use the Blockade function to remotely block the control panel utility functions. The control panel operation becomes then impossible, until it is unblocked by the installer. The lock can be activated remotely at any time or a time limit can be programmed in advance, after which the lock will be activated automatically.

Outputs

The tab makes it possible to test the outputs existing in the system in real mode. In order to test the outputs, press the ON and / or OFF buttons. The current status of the output will be displayed in the STATUS column.

ATTENTION!
In case of a failure of the device connected to the tested output, the displayed status may not correspond to the actual operation of the device at the output.

UPDATE

Local update

The tab will display information about the headquarters modules that are connected in a given system. At the name of the module, information about its current status, supply voltage and firmware version is given. The UPDATE button allows you to upload a newer version of the software to the control panel and modules. Appropriate files will be made available if necessary by technical support of the control panel manufacturer.

Remote update

The remote update shows a list of systems supported by the installer and allows you to select a system for remote software update. In this tab you can also change the language of the configuration program.

ATTENTION!
The control panel software update is only possible with a completely disarmed alarm system. During the update it is not possible to perform any activities in the alarm system. The update progress is shown on the manipulator as a percentage. A remote control panel software is also possible. The update is carried out by the installer after obtaining permission from the user. The user agrees to the Service Access to the Control Panel by including this function from the manipulator. The user should enter the user code, press the OK/Menu button, go to the Settings tab and confirm with the OK button. Then select Allow the service and select the appropriate in a given situation from among the periods displayed, confirming the selection with the OK key. Access to the website can be granted for 1, 2, 4 or 8 hours, 1 day or for an unlimited period. Confirmation of the selection will be the message on the manipulator providing the current period of the website access to the Control Panel and the end option, with which the user can turn off the installer's access to the programming of the Control Panel at any time.

Above the list of modules there is the Serial number of the Control Panel, identifying the control panel when logging in to the servers. The installer can use the blockade function to be used to remotely block the functioning functions of the Control Panel. The control panel operation then becomes impossible until the installer is unlocked. The lock can be turned on remotely at any time or program the time limit after which the lock will turn on automatically.

LOG

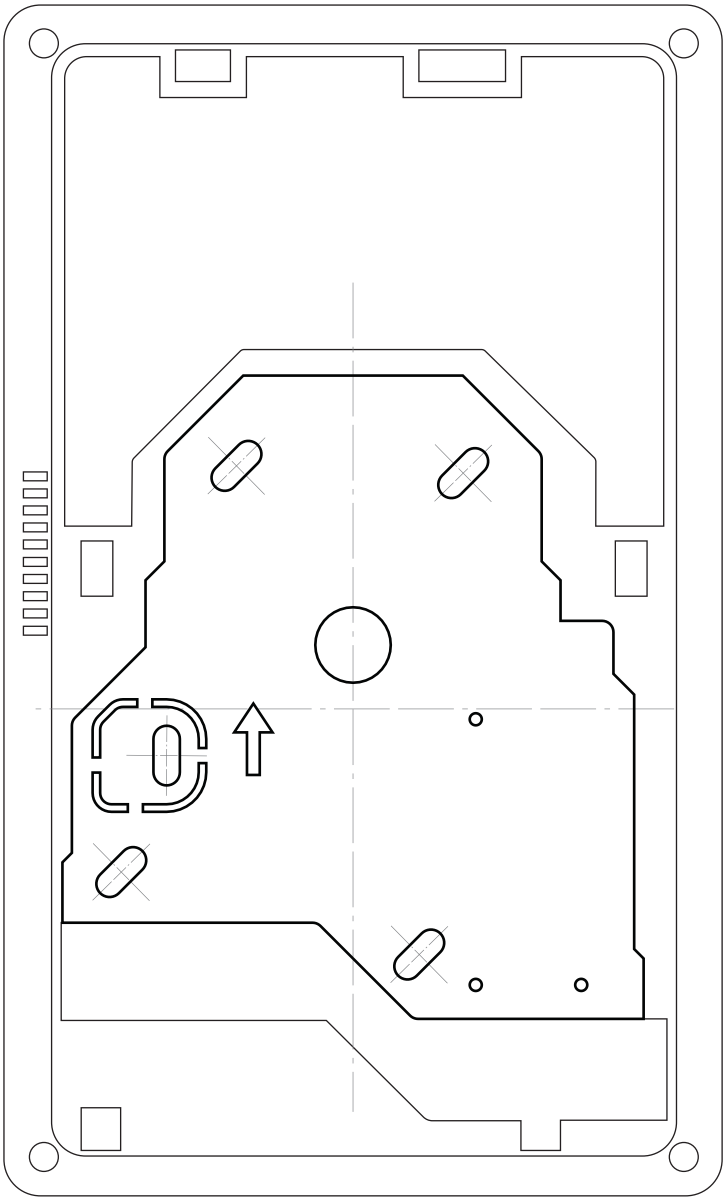
Log is a tab where you can read events that took place in the alarm system.

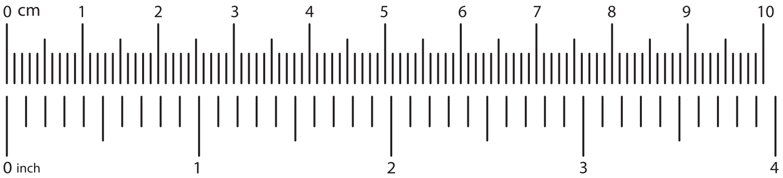
With the “load” button, download events from the control panel. With the select File/folder button, indicate the place to save file with events and save by pressing a button with this name.

Events can also be read directly from the keyboard - you should log in with the user code or installer, press the ok menu key and select an event register. To read the details of the event, press the OK key on any event. Next, you can scroll with the arrow cursor (buttons 2 and 0).

APPENDIX 1 – INSTALLATION TEMPLATE

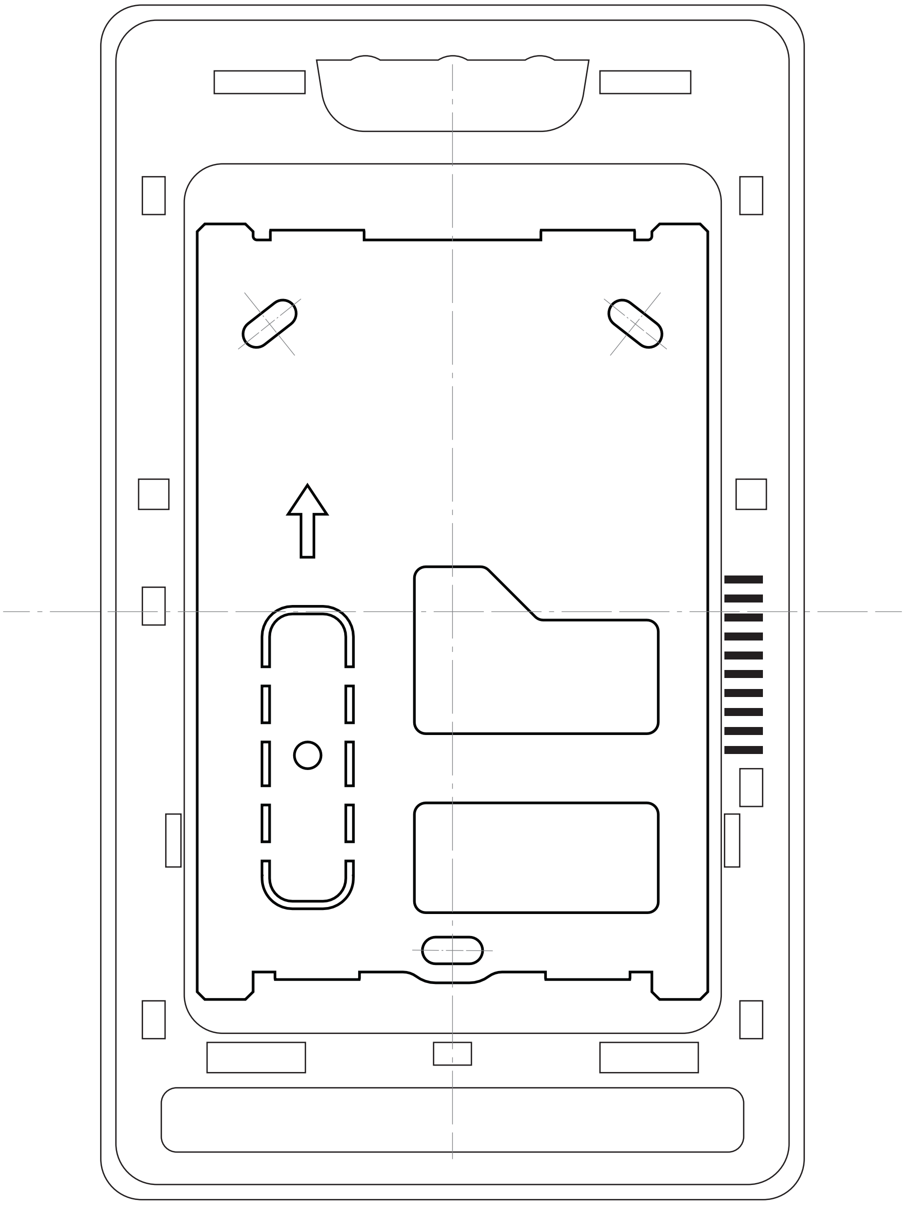
Manipulator LCD/C

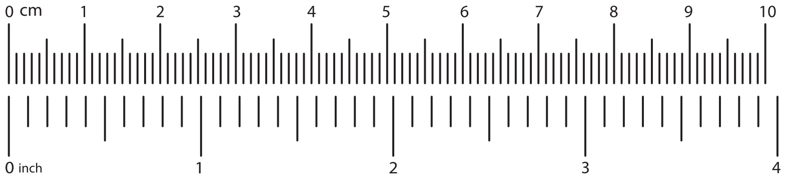




APPENDIX 2 – INSTALLATION TEMPLATE

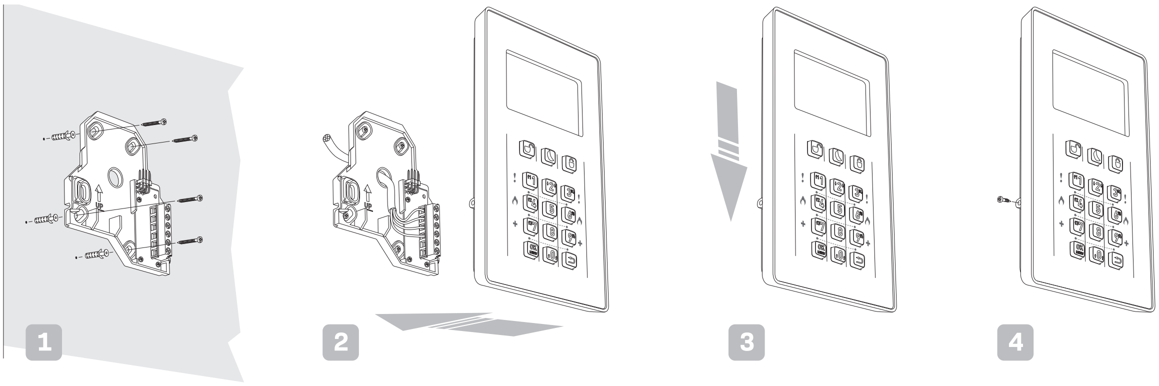
Manipulator LCD/T



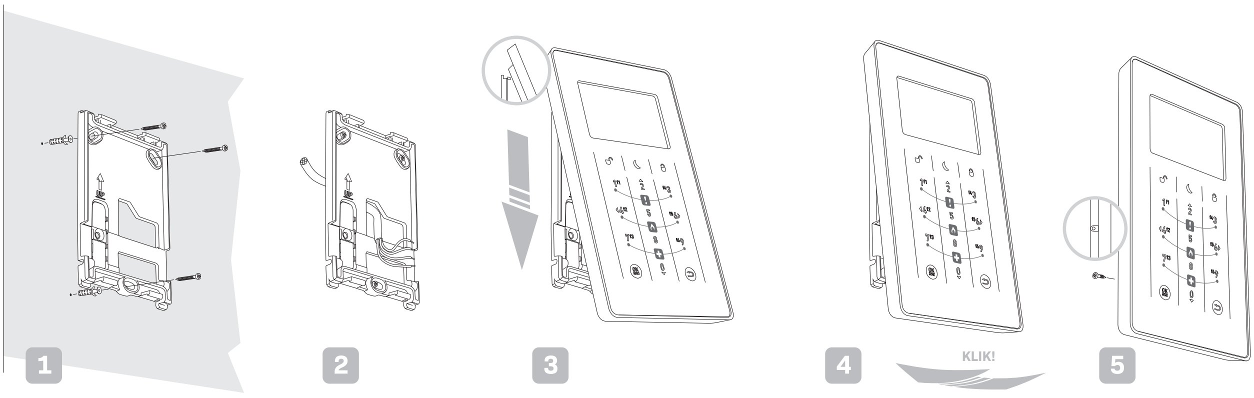


APPENDIX 3 – METHOD OF INSTALLATION FOR LCD/C AND LCD/T KEYPADS

Manipulator LCD/C



Manipulator LCD/T



PulsON
ALARM

NSS Sp. z o.o.
ul. Modularna 11 (hala IV)
02-238 Warszawa

Update: 3.11.2022