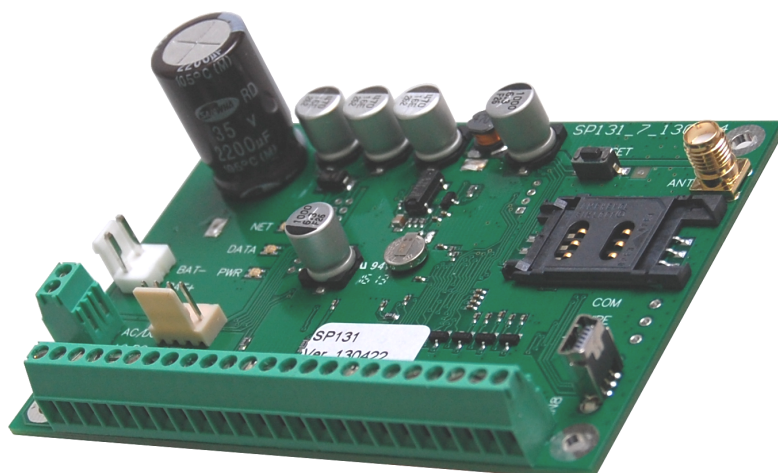




Security Module SP131

User Manual

Contents

SAFETY REQUIREMENTS	3
DESCRIPTION OF THE SECURITY MODULE SP131	6
COMPATIBLE MODULES	8
TECHNICAL PARAMETERS	9
PACKAGE CONTENTS	9
MODULE COMPONENTS	10
TERMINAL BLOCK DESCRIPTION	10
LIGHT INDICATION	10
SETTING UP	11
SETTING UP GUIDELINES	11
WIRING DIAGRAMS.....	12
SETTING UP OPERATION PARAMETERS OF THE MODULE	14
CONNECTING TO A COMPUTER USING A USB CABLE	14
CONNECTING TO A COMPUTER VIA GPRS.....	15
SOFTWARE SPCONFIG	16
SETTING THE MAIN SECURITY MODULE PARAMETERS	16
USER CODE MANAGEMENT	18
ZONE TYPE CUSTOMIZATION.....	19
SMS TEXT CUSTOMIZATION	20
CUSTOMIZATION OF PGM OUTPUTS OPERATION	20
CUSTOMIZATION OF CMS REPORTING PARAMETERS	21
CUSTOMIZATION OF OS ANDROID OR MOBILE PHONE REPORTING PARAMETERS.....	22
CUSTOMIZATION OF NON-ZONE EVENT PARAMETERS	23
REGISTRATION OF YG DATA BUS MODULES	23
REGISTRATION OF MCI DATA BUS MODULES	23
EVENTS LOG	24
RESTORATION TO DEFAULT FACTORY SETTINGS.....	24
MODULE OPERATION FIRMWARE UPGRADES	24
SECURITY SYSTEM CONTROL	25
CONTROL BY SMS MESSAGES	25
CONTROL USING THE PROTEGUS KEYPAD	26
CONTROL USING THE PARADOX KEYPAD.....	28
ANNEX 1. DESCRIPTION OF ZONE TYPES.....	30
ANNEX 2. OPERATION MODES OF PGM OUTPUTS	31
ANNEX 3. WARRANTY AND LIMITATION OF LIABILITY	33

Safety Requirements

Please read this manual carefully before using the module.

Module may be set up and maintained by qualified personnel having the knowledge of GSM equipment operation and safety requirements. Module must be disconnected from external power supply source before starting the set up!

Module should be set up in locations with restricted access and in safe distance from any sensitive electronic equipment. Module is not resistant to vibration and other mechanical effects, dampness or hazardous chemical environment.



Casings, transformers, batteries and programming devices must comply with LST EN60950 safety requirements.

The module is powered either by 16-24 V DC source or via 16-18 V II class voltage transformer from 220 V 50 Hz AC power grid. 12 V/7 Ah (or higher capacity) battery must be used in order to ensure standby power supply. Current consumption depends on the load of all connected external devices.

An automatic bipolar fuse must be installed to safeguard from a current overload in the electricity supply circuit. Release contacts must be $\geq 3\text{mm}$ apart. The fuse must be mounted in a location well known to the maintenance personnel.

The device may be disconnected from the electrical grid:

- by switching the automatic fuse off (from AC power grid);
- by unplugging the terminals (from the battery).

Definitions

Alarm (security system, alarm system) - interconnected safety devices which comprise the burglary and fire alarm system of the premises.

ARM – a security mode which covers all zones in the premises. Alarm system will react to events in any of the zones.

Auto ARM function – this function protects from an accidental shutdown of the alarm system.

Bell Squawk function – a type of function that will sound a short siren when the alarm system is being armed or disarmed.

BYPASS function – a type of function that allows to temporarily turn off the control of a protected zone, e.g. for a single alarm system actuation period.

Central Monitoring Station, CMS - the location where messages from the protected object alarm system are sent via existing wired and wireless communication channels and where appropriate actions are taken in response.

Data Bus (multi-functional/two-wire) – subsystem which allows to transfer the data from one component of the security system to another.

DISARM – a type of a security mode which covers only a part of zones in the premises. Alarm system will react only to *Fire*, *Silent* and *24 hour* zone events while the other will be ignored.

Door Chime function – a type of function that will sound a short buzzer when the entry door is being opened or closed even if the alarm is disarmed.

Driver - a computer program which operates or controls a particular type of device that is connected to a computer.

Entry Delay – a delay of the alarm system activation in order to enter the premises and turn off the alarm, e.g. to enter the password using the keypad. Alarm system will not react to *Delay*, *Interior* and *Interior STAY* zone events during the countdown.

EOL (End of Line) – a type of a circuit connected to outputs **ZNx** and **COM**. The value of circuit resistance is predetermined in a normal state. Event signal is conditioned on the change of value of circuit resistance exceeding permissible limits. Usually, a resistor of suitable denomination is connected at the end of such circuit stub and *NC* or *NO* sensors are used to form event signals in the circuit.

Event (event signal) - any external effect which forms an electrical signal and causes security module (control panel) to react, e.g. an electrical signal in the sensor monitoring zone may appear due to the alteration in temperature and cause a change exceeding permissible limits of value of resistance in the electric circuit, connected to the terminals **ZNx** and **COM**.

Event Log function – this function allows to register and save detected events (according to the time of their occurrence).

Exit Delay – a delay of alarm system activation in order to freely leave the premises after the alarm activation command is sent, e.g. by entering the password using the keypad. Alarm system will not react to *Delay*, *Interior* and *Interior STAY* zone events during the countdown.

Expansion Module – an external interface which allows to increase the number of security module inputs.

GSM modem – a component of the system which allows to operate in a mobile network.

Interoperable Module - a type of module that can be connected to module data bus (two-wire YG or single-wire MCI).

NC (*Normally Closed*) – a type of a circuit connected to terminals **ZNx** and **COM**. Electric circuit between contacts is closed in a normal state, i.e. resistance in the circuit or in between contacts is low. Event signal is conditioned on the change of value of circuit resistance exceeding permissible limits.

NO (*Normally Open*) – a type of a circuit connected to terminals **ZNx** and **COM**. Resistance in the circuit or in between the contacts is high, i.e. the circuit is open. Event signal is conditioned on the change of value of circuit resistance below acceptable limits.

Port forwarding – a technology which allows to connect remote devices to a specific computer or a service within a private local-area network.

Restoration (restoration signal) – a reset of electrical circuit (circuit resistance), connected between module terminals **ZNx** and **COM**, to the original (normal) state before the zone event signal.

Router – a device which connects computer networks and carries out the data routing function, i.e. makes network routing maps and tables.

Security Module (module) – a control unit which manages the alarm system of the protected object and allows the user to select a desired security mode by call, using the keypad or another type of control. In case of an event the module turns on the siren, the flash or another alarm device according to the settings. A message is sent via the integrated communicator to the centralized monitoring panel, user's mobile phone or it may react to the alarm signals in a different way.

SLEEP - a type of a security mode of the premises when the alarm system protects only the outside of the premises and allows movements inside, i.e. ignores Interior *STAY* and *Instant STAY* zone events. When this mode is on, the breach of *Delay zone* immediately triggers the alarm without starting the **Entry Delay** countdown.

STAY - a type of a security mode of the premises when the alarm system protects only the outside of the premises and allows movements inside, i.e. ignores Interior *STAY* and *Instant STAY* zone events. When this mode is on, the breach of *Delay zone* starts the **Entry Delay** countdown.

Terminal – a module element intended for electrical connection (contact) with other devices.

Zone (secured zone, sensor zone) - a space, a medium or a surface whose physical or chemical properties are controlled by the sensitive element of the sensor. When an irregularity is detected (i.e. secured zone is breached), the sensor triggers an event signal.

Zone Type - a special predetermined algorithm according to which the module starts to work if the zone event is detected.

Note. Signal input and output terminals are denoted by acronyms **ZNx** or **PGMx**. x symbolizes any of the input or output sequence numbers.

Description of the Security Module **SP131**

Module **SP131** is a burglary and fire alarm control panel with an integrated GSM modem which can transmit event messages to central monitoring station via GPRS connection and SMS messages, to the mobile phone of the user by SMS or to *OS Android* device with an application "Proteagus". Sent messages are encoded in *Contact ID* protocol codes. Features:

- **Alarm control using the most convenient device for the user.**

Module can be armed/disarmed using these devices:

- *UAB Trikdis Proteagus SK130LED W/B* keypads; or
- *Paradox* MG32LED, K636, MG10LED keypads;
- *OS Android* phone with an application "Proteagus";
- Phone (by call);
- Phone (by SMS);
- *iButton* key;
- Code or another electrical switch.

- **Setting the operation parameters using a USB.**

All operation parameters can be set using MS Windows OS computer with a program **SPconfig** by connecting the module to a computer using a USB cable. 5V voltage from USB cable is sufficient for setting the parameters. Set parameters are stored in the memory of the module for a storage period.

- **Management of operation parameters and the module from central monitoring station.**

It is not only possible to change all the operation parameters of an already set up and operating module, but also to turn off the control (bypass) of a desired zone, change the output status of a desired PGM, arm and disarm the alarm, and even update the firmware. This feature is useful for organizing, e.g. cash machine protection.

- **Multi-functional data bus MCI.**

Module has a singlewire multi-functional data bus **MCI** which automatically recognizes and registers connected compatible devices (maximum 4):

- Additional transmitting module (T10C, E10C or G10) which transmits all event messages of the security system to central monitoring station in parallel either by VFH radio (T10C), Ethernet (E10C) or GSM/GPRS (G10).
- *iButton* key scanning device **W131**;

- **Two-wire data bus YG (also called YEL/GRN).**

Module has a data bus **YG** which automatically recognizes and registers connected compatible devices (maximum 12):

- *Proteagus SK130LED W/B* or *Paradox* MG32LED, K636, MG10LED keypads;
- ZN input expanders **CZ8**

- **8 zones (can be expanded up to 32).**

Module has eight terminals **ZN1–ZN8** for connecting sensor controlled external circuits.

- Number of zones can be expanded up to 32 by using **CZ8** expanders. Up to 12 various expansion modules can be connected to **YEL/GRN** data bus, e.g. 4 keypads and 8 zone inputs expanders and likewise.
- An external circuit of any type (*NC*, *NO* or *EOL*=2.2 kΩ) can be connected to any of the terminals.
- Any of the **ZNx** circuit inputs can be monitored as **ON/OFF**, **Delay**, **Interior**, **Interior STAY**, **Instant**, **Instant STAY**, **24 hours**, **Fire** or **Silent** zone. Zone types vary depending on the module operation after the event and appearance of the restoration signal (see Annex "Description of Zone Types").

- **Fire zone.**

- Any of the module **ZNx** inputs can be set to *Fire* zone and be connected to a four-wire fire (smoke) sensor.
- Two-wire fire (smoke) sensor can be connected to the input **ZN8** (default *Fire* zone). If needed, the sensor can be reset using the keypad or by SMS.

- **4 PGM outputs.**

Module has four programmable output terminals **PGM1–PGM4** for connecting module controlled external circuits. Every output can be set to operate in any of 14 operation modes (see Annex "Operation Modes of PGM Outputs").

- **Remote control of PGM outputs.**

Output state can be controlled remotely by SMS or telephone call if the mode of any of the **PGMx** outputs is set to **Remote Control by SMS** or **Remote Control by DIAL**. This function helps to remotely control various devices (gates, watering pump, cooler, etc.) without changing security mode of the premises.

- **Event message forwarding to central monitoring station of any security service company.**

The module sends messages to central monitoring station (CMS) via GPRS and/or by SMS. Sent information matches *Contact ID* protocol codes. PING signals are used periodically for connection control with central monitoring station receivers.

Module sends messages to central monitoring system via GPRS connection main IP receiver address IP-1. The messages will be reported to a station receiver backup address IP-2 in cases of connection failure.

If sending fails to both, the main and backup IP receivers, the module will send a coded *Contact ID* message by SMS to the SMS receiver of the station.

- **Event messaging to a mobile phone.**

Event messages can be sent to 5 mobile phones. Texts of events are written in either Lithuanian or Latin alphabet. It is possible to customize the list of events in which the messages will be sent.

- **Event messaging to OS Android device.**

Module can be set to send a special format SMS messages to OS Android device with an installed app **PROTEGUS**. **PROTEGUS** will convert your OS Android device to a user-friendly, informative and cost effective (depends on cost of SMS) security system control and management console.

PROTEGUS can be used as an easy-to-use widget for checking the status of the alarm system, and arming or disarming it. The widget enables to arm or disarm the system in just a couple of seconds. Additional relevant information will be readily available.

Note. When choosing payment plans for Smart Phone and module SIM card GSM connection services **pay close attention** to the pricing of SMS messages.

- **Module Calls**

Besides sending an SMS message, module can also call two mobile phones if a specified event occurs, e.g. burglary. Events when a call is desired can be specified when setting the parameters of the module. This function is useful in cases when an important event occurs and the SMS sound is disabled.

Note. The alarm call has higher priority than security system or PGM output control call. When module is calling to a user phone, all the incoming calls are rejected and commands controlled by call are not executed. It is **highly recommended** to configure the security system to either make alarm calling or be able to be controlled by call, but not both at the same time.

- **System status messages**

Module sends messages not only about robbery, fire and other hazards, but also about system operation and power supply failures (*AC fail* and *Low battery*) to desired addresses. It also informs on who, when and how (keypad or mobile phone) armed or disarmed the alarm system, etc. Connection *Test* messages are sent to central monitoring station in set *Test Time* or *Test Period*.

- **Bell Squawk function.**

Module may sound a short siren indicating arming and disarming of the alarm system.

- **Door Chime function.**

Module may sound a short buzzer indicating that entry door is being opened or closed (breach of **Delay** zone) even if the alarm system is disarmed (**DISARM** mode).

- **BYPASS function.**

Control of a protected zone can be temporarily turned off, e.g. for a single alarm system actuation period in order to arm the alarm system even if the protected zone is breached.

- **Auto ARM function.**

This function protects from an accidental shutdown of the alarm system. If the security system is disarmed remotely and during the time for entry into the premises none of the secured zones are breached, the module will automatically rearm to a previous **ARM / STAY / SLEEP** mode.

- **Event Log function.**

Module registers and stores all recorded events. Events log can be read using the program **SPconfig**. Events are registered according to the time of their occurrence which is counted by the internal clock of the module.

- **Main power supply by AC or DC power source**

Module and the entire alarm system can be powered by standard 16-18V AC power supply source or by 16-24V DC power supply source. The latter feature is useful when the protected premises are not connected to the electricity network and the security system must be powered by an independent source of energy (e.g., solar power). Power supply voltage is monitored. Central monitoring station and the user (depending on the settings) will be informed in cases of faults in the power supply system.

Compatible Modules

These modules can be wired to a two-wire YG (also YEL/GRN) or a singlewire MCI data bus of the module.

<i>Product code</i>	<i>Data bus</i>	<i>Description</i>	<i>Current consumption</i>
CZ8	YG	Input expansion module (up to 8 zones)	50 mA
W131	MCI	Interface with <i>iButton</i> key code scanning device	30 mA
T10R	MCI	Radio transmitter which sends messages in VHF radio frequencies	50 mA on standby 1000 mA in transmission mode
E10C	MCI	Ethernet communication which sends messages via internet networks	60 mA on standby 100 mA in transmission mode
GM10	MCI	GSM communicator which sends messages via GPRS	60 mA on standby 120 mA in transmission mode
PROTEGUS SK130LED W/B	YG	Touchscreen LED keypad with white or black glass surface (16 zones)	60-150 mA
Paradox K636	YG	LED keypad (10 zones)	50-100 mA
Paradox MG10LEDV and MG10LEDH	YG	LED keypad (10 zones)	50-100 mA
Paradox MG32LED	YG	LED keypad (32 zones)	50-150 mA

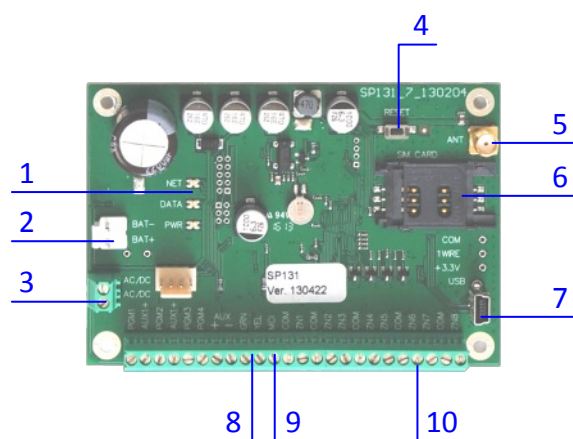
Technical Parameters

Power supply voltage	AC 16–18 V, DC 16–24 V
Power consumption (module only, without external devices)	80 mA on standby Up to 150 mA (while transmitting data)
Standby power supply	12 V / 7 Ah battery
Battery charging current	Custom 0,1-2,0 A stabilized current
Connected external devices power supply	DC 13.6 V in between terminals [AUX+] and [COM]. Current up to 1,1 A
GSM modem SIM900R frequency	GSM EGSM 900 MHz and DCS 1800 MHz
Power supply failure thresholds:	Main power supply source voltage is lost/restored, Backup power source voltage is lower than 11,5 V, Backup power source voltage is restored to 12,6 V
ZN terminals (inputs)	8 programmable; Custom <i>NC</i> , <i>NO</i> or <i>EOL</i> =2,2 kΩ circuit type;
	Number of ZN inputs (expandable up to 32)
Number of data bus expansion modules	Up to 14 (including keypads)
PGM terminals (outputs)	4, field-effect transistor NO terminal commutates up to 30 V / 1,5 A between COM terminal
Number of passwords	up to 40
<i>Entry Delay</i> and <i>Exit Delay</i> times	Custom duration (0-255 seconds)
Siren sound duration	Custom duration (0-9999 seconds)
Connection protocols	TCP/IP or UDP/IP via GPRS; SMS
Message encoding	<i>Contact ID</i> protocol codes
SMS messages to the user	To 5 mobile phones according to selected event type
Calls to the user	To 2 mobile phones according to selected event type
Operation environment	From -10 °C to 50 °C when relative air humidity is 80 % at +20 °C
Dimensions	130 x 65 x 25 mm

Package Contents

Security Module SP131	1 pc
Battery connection wire	1 pc
2,2 kΩ resistors	8 pcs
Plastic distance holder	4 pcs

Module Components



1. Network and operation light indication
2. Standby power supply connector
3. Terminal block for main power supply source connection
4. RESET button
5. GSM antenna connector
6. SIM card holder
7. USB socket for configuring the module
8. Two-wire YEL/GRN data bus terminals
9. Singlewire MCI data bus terminal
10. Terminal block for external outputs

Terminal Block Description

<i>Terminal</i>	<i>Description</i>
AC/DC+ AC/DC-	Terminals for connecting the main power supply source AC 16-18 V or DC 16-24 V
AUX+	Terminals for connecting the keypad(s), signalling-devices and various sensors powered by +13,6 V voltage
BAT+/ BAT-	Terminals for connecting the standby power supply source, e.g. 12 V, 7 Ah battery
COM	General terminal for the keypad(s), signalling-devices and sensors
YEL	Terminal for connecting external device (keypad) circuit YEL (yellow wire)
GRN	Terminal for connecting external device (keypad) circuit GRN (green wire)
MCI	Terminal for connecting of <i>iButton</i> scanning device W131 and/or another transmitting module
ZN1-ZN8	Terminals for connecting external circuits of the sensors. Terminal ZN8 can be used for two-wire fire (smoke) sensors.
PGM1-PGM4	Programmable terminals (outputs) for connecting various signalling and control devices

Light Indication

<i>LED</i>	<i>Activity</i>	<i>Indication</i>
"Network" indicates connectivity status to the GSM network	OFF	SIM card read error
	Green frequently flashing	SIM card PIN code error
	Green flashing	Connecting to GSM network
	Green ON	Module is connected to GSM network
	Yellow ON	Message is being sent
"Data" indicates data transfer	Yellow flashing	Number of flashes represent GSM signal strength (up to 10)
	Green ON	Unsent messages present in module memory
	Green flashing	Messages are being sent and received
"Power" indicates power supply status and programming mode	Green flashing	Power supply voltage is sufficient
	Yellow flashing	Power supply voltage is not sufficient (< 11,5 V)
	Green and yellow flashing in turns	"Boot loader" mode
	All OFF	Power supply is off or the voltage of the battery is lower than 9,5 V

Setting Up

Setting Up Guidelines

1. Make a rough sketch of the premises to get an idea of where the module, keypads, signalling devices and other devices are to be set up. According to the evaluation of the premises and their protection requirements select the type and the number of sensors as well the places where they should be placed accordingly.
2. It is recommended to use the factory settings of the module when developing your alarm system. In order to check the factory settings of the module use the program **SPconfig**. The factory settings and their values can be seen in the windows of the program **SPconfig**. It is not necessary to connect the module to the computer.

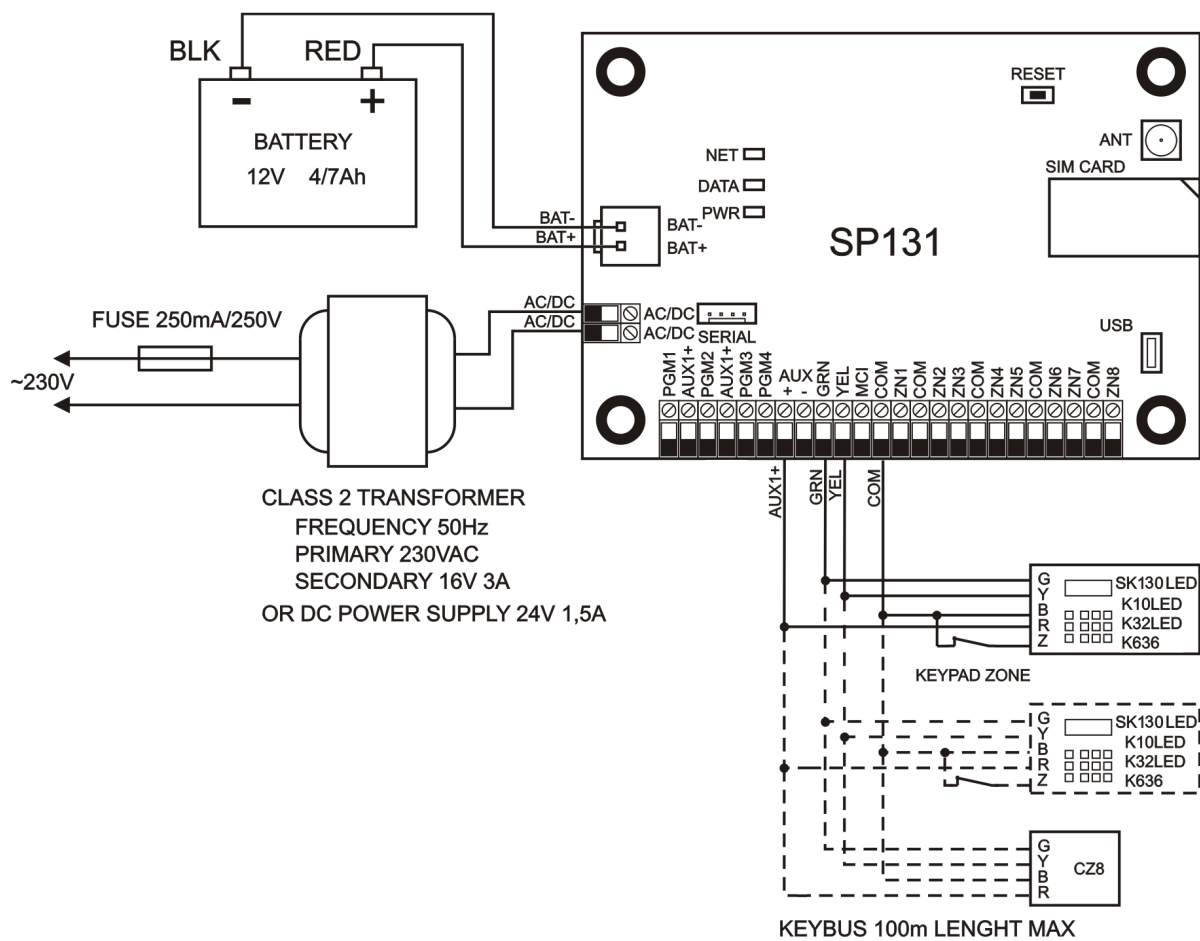
However, if there is a need to change the factory settings according to the requirements of the premises, see the section **Setting Up Operation Parameters of the Module**.

Note. Default factory settings remain in the memory of the module even if it is stored unpowered for long periods of time.
--

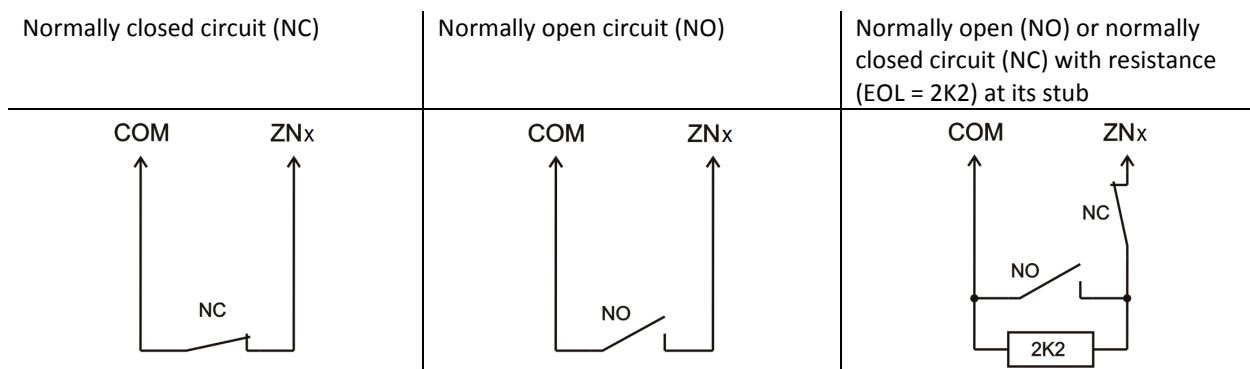
3. Secure the module plate with the plastic distance holders into a plastic or metal mounting case with an integrated battery or power supply source. If a metal case is selected, do not forget to ground it during the set up.
4. Screw the 2.5 m long GSM antenna to the antenna connector with a magnetic or adhesive pad. Insert the SIM card (registered to GSM network provider) into the SIM card holder.
5. In order to connect external devices, e.g. door and wall mounting tampers, magnetic door contacts, fire sensors, a siren, etc. follow the wiring diagrams of both, this manual and the manual of the device to be connected to this module. Correctly connected keypads, extenders, transmitters, etc. will be recognized and registered to the system automatically by SP131.
6. Insert the standby power supply battery into the mounting case. Connect its wires to the module terminal for the standby power supply BAT+ / BAT-;
7. Connect the main power supply wires to AC/DC+ and AC/DC- terminals;
8. Turn on the main power supply. Security system will send E305 (system reset) event message. If there are additional devices connected to YEL/GRN and MCI data buses of the module SP131, security system will send R333 (Expansion Module Restore) event message. E760 (PING) event message will be sent to central monitoring station IP receiver. This message will enable communication control with the module SP131.
9. Check security system operation and transmission of messages. In order to check the system transmission of event messages, breach the protected zone or input the system arming password using the keypad triggering the transmission of the event message.
10. If needed, module operation parameters can be set and changed even when the alarm system is set up, connected and in operation.

Note. After the operation parameters are set, we highly recommend to reset the module, i.e. either press RESET button or unplug and replug the power supply.
--

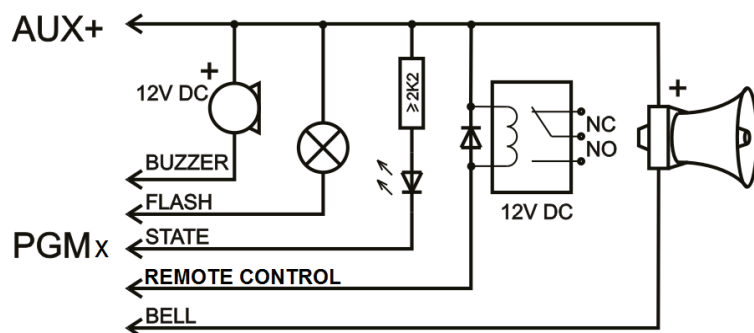
Wiring diagrams



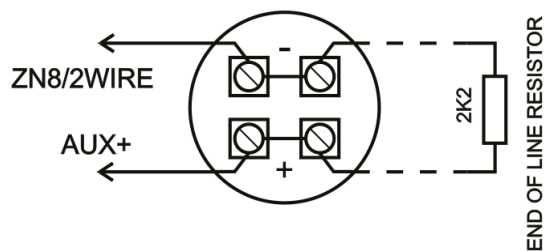
Zone connection



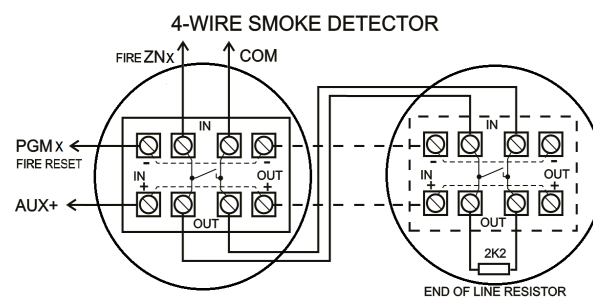
Signalling (control) devices



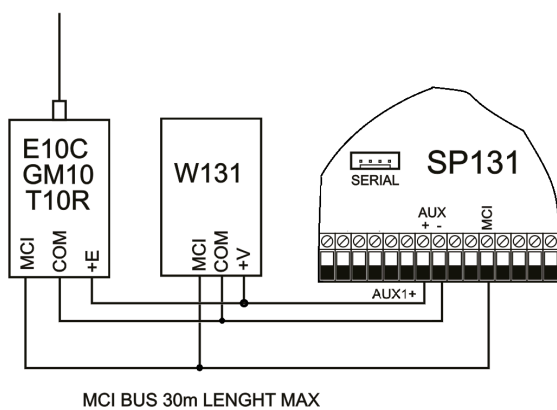
Two-wire fire (smoke) sensor



Four-wire fire (smoke) sensor



Transmitter and interface W131



Setting Up Operation Parameters of the Module

Module operation parameters are set using the computer program **SPconfig** which runs on *MS Windows* OS. You can find the program on the website www.trikdis.lt.

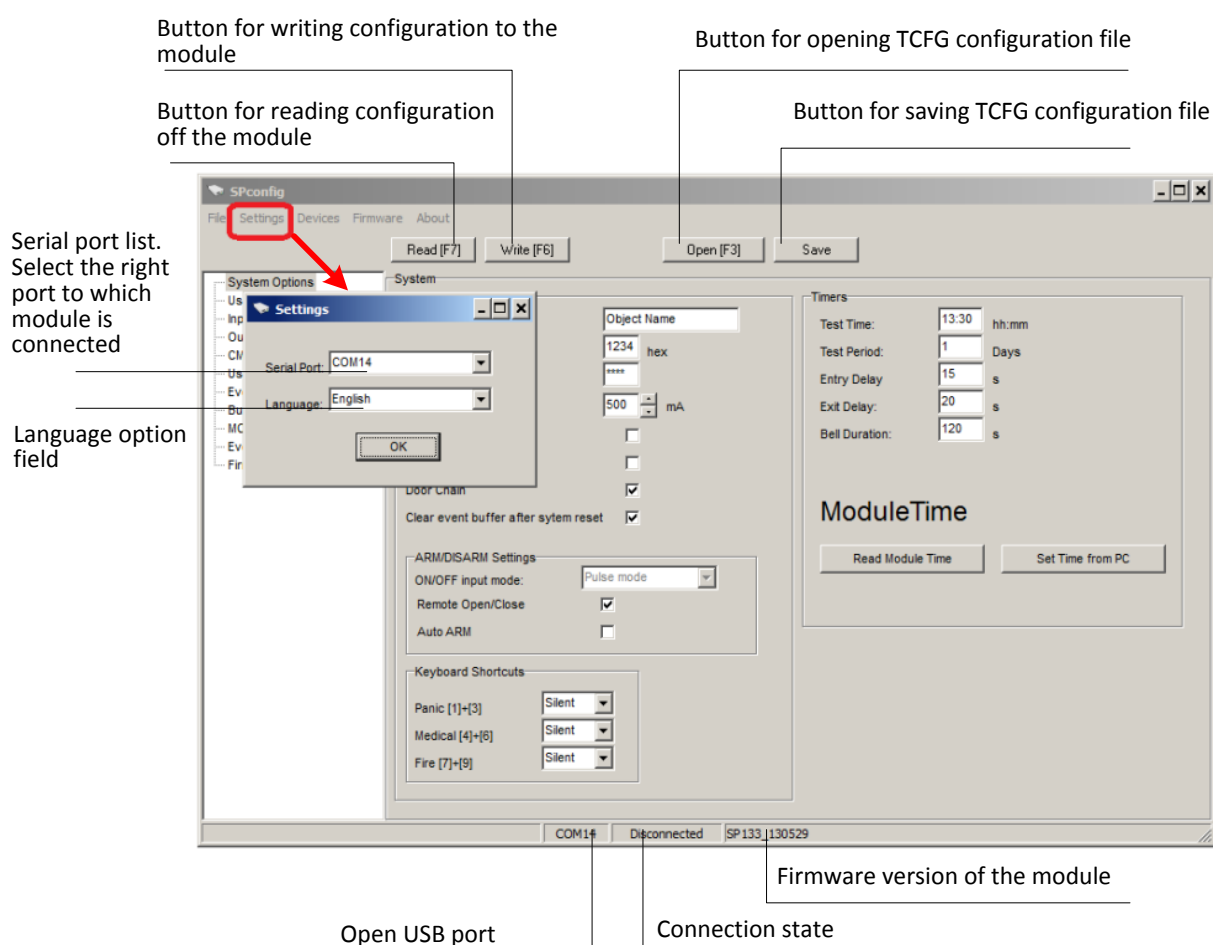
Connecting to a computer using a USB cable

1. Connect module to the computer using a USB cable. Module does not require additional power supply during the programming.

Computer must have a USB driver installed. If the module is connected to a computer for the first time, *MS Windows* OS should open the window *Found New Hardware Wizard* for installing USB drivers. Download file *USB driver.zip* from the website www.trikdis.lt and extract it. In the wizard window select the function *Yes, this time only* and click *Next*. After the window *Please choose your search and installation options* opens click *Browse* and select the location where the file *USB_COM.inf* was extracted to. Follow the remaining installation wizard instructions to finish the USB driver installation.

Note. Computer has to be connected to the internet network for proper USB driver installation!

2. Start the program **SPconfig**;
3. Choose the command **Settings** in the menu bar and select the port to which the module is connected in the **Serial port** list. Click **OK**.
A specific port appears only once the module is connected to a computer and the USB driver is installed properly.
4. Select the preferred language in the **Language** option field. Click **OK**.
5. Choose the command **Devices** in the menu bar and make sure it is set to **SP131/SP133**. Default factory settings will be shown in **SPconfig** windows and the status bar will display information about the module.
6. System is ready for configuration even if in the status bar of program window is indicating *Disconnected*. For more, see section *Setting Up Operation Parameters using SPconfig*.
7. When desired parameters and functions are set press **Write [F6]** and the new configuration will be sent to module **SP131**.
8. When configuration is finished, turn off the program **SPconfig** and unplug the USB.



Connecting to a computer via GPRS

In order to program the module **SP131** remotely via GPRS several conditions have to be met:

1. SIM card inserted into the module has to support a GPRS service. In order to activate the GPRS service contact your network provider.
2. Module **SP131** has to be connected to an already installed **IPcom** program (must be v.1.10 or newer) on a Windows OS computer with internet connection. Installation file for **IPcom** can be found on www.trikdis.lt.

Connection to program **IPcom**

1. Install the program **IPcom** (v1.10 or newer version) on the Windows OS computer and start it. In order to configure **IPcom** to receive module signals correctly refer the user manual.
2. Configure computer network LAN in a way that module **SP131** signals are forwarded to a dedicated **IPcom** port. For information on port forwarding please refer to your router user manual.
3. In order to open up a GPRS connection session send an SMS message containing the code below to the SIM card number of the module **SP131**.

PSWxxxxxx _ 10 _ xxx.xxx.xxx.xxx#yyyy#

Here:

PSWxxxxxx – initial command and the six-digit remote access code;

10 – a command code for setting an IP address;

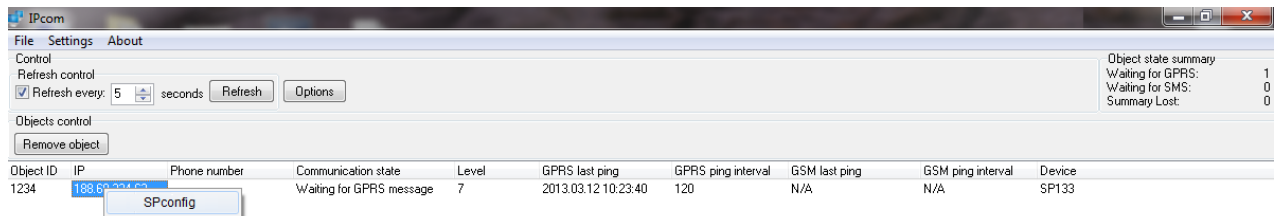
xxx.xxx.xxx.xxx – external IP address of computer LAN;

yyyy – number of the **IPcom** port;

_ - space between the values. Spaces are necessary in marked places.

- the end mark of values. Do not forget to end an IP address and the port number with this mark.

4. If the SMS message is sent correctly and configuration of LAN and **IPcom** was successful, the module should appear in **IPcom** window not for long after.
5. Open the window of **IPcom** and right click on the data row. After the **SPconfig** icon appears, left click on it to launch **SPconfig**.



6. When **SPconfig** starts click **Read [F7]** to read the present configuration of the module. The reading process will be displayed in a progress bar. Data exchange may take up to a minute.
7. Set the desired module operation parameters values. Refer to the section **Software SPconfig**.
8. In order to enter the values to the module click **Write [F8]**.
9. After the configuration is finished close the program **SPconfig**.
10. In order to close the GPRS session between the module and **IPcom** send another SMS to the same module **SP131** SIM card number with IP and port values of zero:

PSWxxxxxx _ 10 _ 000.000.000.000#0000#

Software *SPconfig*

It is recommended to use the default factory settings set in the module when developing your alarm system and change them only when needed.

Setting the main security module parameters

General parameters of the module can be set under **System Options** in the program *SPconfig*.

Object name

Account number
0001-FFFF

PIN code of SIM card. If there is no set PIN code on SIM card leave the default value.

Charging current of battery. Possible values 100-2000 mA. Set according to recommendation of battery manufacturer.

1

2

3

4

5

Bell Squawk activation. If activated short bell signals will be formed then Arming (one short signal) and Disarming (two short signals) the security system.

Checkbox to activate the **Buzzer** signal formation everytime the door is opened in **DISARM** mode.

1

Bell Squawk: ☐

Set Zn8 as 2-Wire ☒

Door Chime ☒

Clear event buffer after sytem reset ☒

Zone 8 set as 2-wire zone. If box is checked it will be possible to reset 2-wire fire sensor with keypad or SMS.

Checkbox to activate the event buffer clearing after every reset.

Switch mode **Pulse** or **Level** selection for **ON/OFF** zone depending on switch type. If **Remote Open/Close** is marked the **Pulse** mode will be set automatically

Enable Arm/Disarm by phone call. If enabled PGM control by call and calling to user functions will be disabled

2

ARM/DISARM Settings

ON/OFF switch mode: Pulse mode

Remote Open/Close ☒

Auto ARM ☐

Checkbox to activate the automatic arming function of the security system. If **Delay** zone is not activated in set **Entry Delay** time after phone call to disarm the control panel, the module will automatically switch back to previous mode, for example ARM mode

Keyboard Settings **3**

Panic [1]+[3]	Audible
Medical [4]+[6]	Audible
Fire [7]+[9]	Audible

Emergency mode selection. If Audible mode is selected the message will be sent and keypad sound will be formed. If Silent mode is selected the message will be sent, but keypad sound will not be formed.

Test Time

Timers **4**

Test Time:	13:30	hh:mm
Test Period:	0	Test Disable
Entry Delay:	15	s
Exit Delay:	20	s
Bell Duration:	120	s

Test period. 0-99 days. If 0 is set, the test messages will not be sent.

Entry delay time.
0-255s

Exit delay time.
0-255s

Bell duration time. 0-9999s

Button for setting module time to
PC time

Panel Time **5**

Read Panel Time	Set Time from PC
-----------------	------------------

Button for reading internal
clock of the module

User code management

Menu directory **Users** is for entering telephone numbers, names and user codes of up to 40 users who will be able to control the security system.

The screenshot shows the SPconfig software window. On the left is a tree view with 'System Options' expanded and 'Users' selected. The main area displays a table with the following columns: Type, User Name, User Tel., User Code, and iButton Code. The table contains three rows: 'Master' with 'Master Name', 'USER 2' with 'User1 Name', and 'USER 3' with an empty name field. The 'User Code' column has four asterisks in the first two rows and is empty in the third. The 'iButton Code' column contains '000000000000' for the first two rows and is empty for the third. Above the table are buttons for 'Read [F7]', 'Write [F6]', 'Open [F3]', and 'Save'.

Type	User Name	User Tel.	User Code	iButton Code
Master	Master Name		****	000000000000
USER 2	User1 Name		****	000000000000
USER 3				000000000000

User number

Section for entering name of the user. The name of the user will be included in SMS message

Section for entering a user code

Section for entering user telephone number which will be allowed to ARM/DISARM the security system remotely. Telephone number must be entered with international country code but without "+" (plus) sign, for example 37061111111

Type	User Name	User Tel.	User Code	iButton Code
Master	Master Name		****	000000000000
USER 2	User1 Name		****	000000000000
USER 3				000000000000

Section for iButton key codes.

If there is an iButton code in the section and interface W131 with iButton scanner connected to the module, security system can be armed and disarmed with iButton key.

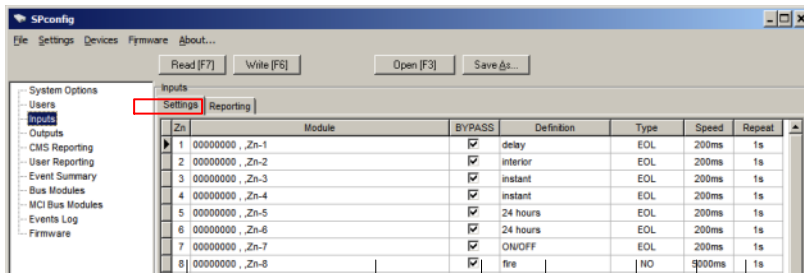
iButton key code register

1. The module will automatically record *iButton* code to the Master user when the old code is 000000000000. If there is another code, enter all zeros to iButton Code section of the master user.
2. Touch the *iButton* key reader with *iButton*.
3. Automatically recorded *iButton* code can be transferred to other User box by using CTRL+C (copy) commands CTRL+V (paste).
4. For security reasons *iButton* Code of Master user has to be changed to 100000000000 or other code to prevent another key scan.
5. Press **Write (F6)** in *SPconfig* and *iButton* key will be saved in the memory of module.

Note. If there is a need to remove *iButton* code from the system, enter the 000000000000 instead of it.

Zone type customization

Zone properties can be set in the **Settings** tab under the directory **Inputs**.



Zone serial number, 1-32

Module or expansion module registration number and zone serial number

Marked zone can be bypassed. Bypass can be activated by keypad or with special Android OS application

The module will not react to disturbances in a protected zone if their recurrence period is shorter than set in this section

The module will not react to disturbances in a protected zone if their duration will be shorter than set in this section

Selectable input type. EOL, NO or NC

Selectable zone type

Double-click the left mouse button on an zone parameters row to open a table intended for setting parameters for the desirable zone.

Selectable zone type

Selectable input type

Event code in *Contact ID* format. Changes automatically if another zone type is set, or can be set manually

SMS text to user if zone is violated. Text can be changed manually

Physical module of the zone

SMS text to user if zone is restored. Text can be changed manually

Enable Alarm reporting

Enable Restore reporting

Marked zone can be bypassed

The module will not react to disturbances in a protected zone if their duration will be shorter than set in this section

The module will not react to disturbances in a protected zone if their recurrence period is shorter than set in this section

SMS text customization

SMS text can be customized in the directory **Inputs** under the tab **Reporting**.

Zone serial number, 1-32

Event code in *Contact ID* format

Enable Alarm reporting

Alarm SMS text. If there is a need, text can be changed manually

Restore SMS text. If there is a need, text can be changed manually

Enable Restore reporting

Zn	CID	Alarm	SMS Text on Alarm	Restore	SMS Text on Restore
1	134	☒	Input1 Alarm	☒	Input1 Restore
2	136	☒	Input2 Alarm	☒	Input2 Restore
3	132	☒	Input3 Alarm	☒	Input3 Restore
4	132	☒	Input4 Alarm	☒	Input4 Restore
5	110	☒	Input5 Alarm	☒	Input5 Restore
6	133	☒	Input6 Alarm	☒	Input6 Restore
7	409	☒	Input7 Alarm	☒	Input7 Restore
8	110	☒	Input8 Alarm	☒	Input8 Restore

Customization of PGM outputs operation

Desirable output operation mode can be set under the menu directory **Outputs**. Every mode is described in the Annex of this manual.

Note: If any of the PGM outputs is set to **Remote Control by DIAL** mode, functions which enable to arm/disarm the alarm system by call and a warning call function will be disabled.

Drop-down list invoked by double press of left mouse button presents PGM output operation options. PGM1-4 output signal ON (active state) is a closed type circuit in respect of common terminal COM

Area for setting the parameters of remotely controlled output.
After receiving a control message or call, the output state of the Remote Control outputs will change to opposite. When level mode is selected the output state will not change to opposite until it receives another remote control command. If pulse mode is selected the output state change to opposite will last only for the set time in Pulse Time (0-9999s) box

ID	Name	Out definition
1	PGM1	Bell
2	PGM2	System State
3	PGM3	Ready
4	PGM4	Disable

Remote PGM Control
PGM Control Mode: Pulse mode
Pulse Time: 10 s

Customization of CMS reporting parameters

Parameters of GPRS and/or SMS reporting to central monitoring station of the module can be set in the directory **CMS Reporting**. Precise values of parameters should be provided by the person in charge of the central monitoring station and by the GSM/GPRS provider.

Program table to set the communication parameters for the **Backup** channel. The parameters are set the same way as in **Primary** channel table

Communication type

For **GPRS** communication:
Remote IP 1 – IP address of the monitoring station server.
Domain 1 – if monitoring station doesn't have a static ip, the domain name can be used.
Port 1 – port number of IP receiver at the monitoring station
For **SMS** communication:
SMS Tel 1 – the phone number of the SMS receiver at the monitoring station

1

2

3

SMS Tel 3 - the phone number of the second backup SMS receiver at the monitoring station

GPRS settings

APN: gprs.net

Login:

Password:

DNS1: 0 0 0 0

DNS2: 0 0 0 0

1

Access point name for connecting to the GSM network of operator

User name for connecting to the GSM network

Password for connecting to the GSM network

Address of internet name server

Section for selecting transmission protocol TCP/IP or UDP/IP

TCP/UDP/IP settings

Transport Protocol: TCP

Backup reporting after: 3 Attempts

2

The number of attempts before module switches to backup channel, 0-999

6-digit encryption key for messages. This key has to be identical to a decryption password entered in a server program **IPcom**

Settings

Encryption Key: 123456

Return To Primary After: 3 min

GPRS PING Time: 30 s

SMS PING Time: 600 s

3

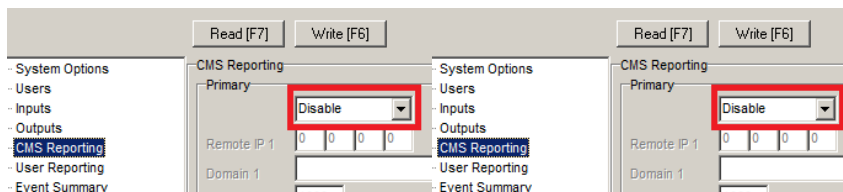
The set time for the module return from **Backup** to **Primary** reporting channel, 0-999 min

Time interval according to which the module sends signals **PING** for checking connection 30-9999 s. In order to activate **PING** sending mark the near placed markbox

Customization of OS Android or mobile phone reporting parameters

Parameters of GSM mobile phone reporting can be set in directory **User Reporting**.

Note: Messages are first sent to central monitoring station and only then addressed to the users. If needed, messages can be sent to the mobile phone of the user only and **CMS Reporting** can be disabled in the section **Communication type** by checking the option **Disable**.

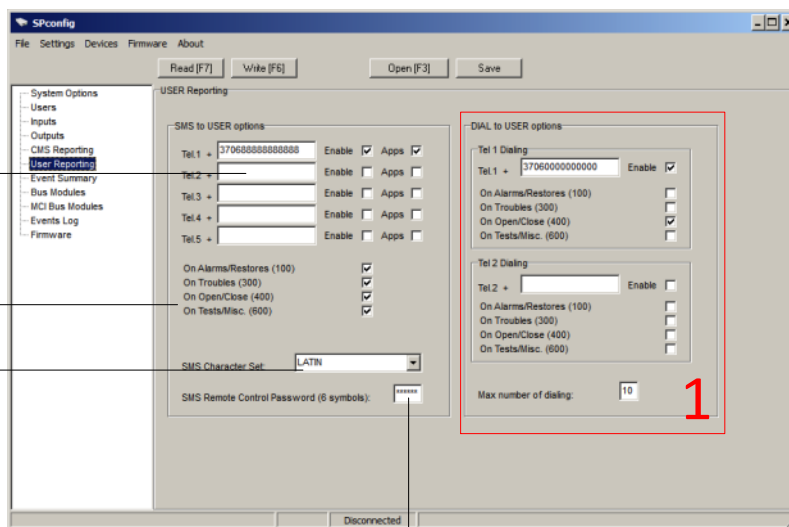


If there is a need for notifications to be sent to GSM phone, phone number has to be entered in international format without "+" sign.

Enable checkbox has to be ticked. For OS Android application **Apps** checkbox has to be ticked too.

Tick the specific events for getting notifications of them

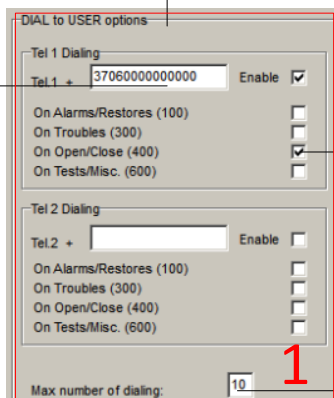
Desired SMS encoding



6-digit password for remote control and configuration of the module by SMS messages. Default value 123456. **It is highly recommended to change it**

The alarm call has higher priority than security system control call or PGM output control call. It is highly **recommended** to configure the security system either to make alarm calling or be able to be controlled by call, but not the both at the same time

For notification calls enter GSM phone number in international format without "+" sign. To enable notification calls to entered GSM phone number tick **Enable**



Tick the specific events for getting notification call

A number of attempts to make a call to the User. If set to dial two times or more and a call is rejected after 15 seconds from the start of it, the module will not call anymore. Call time 60 seconds

Customization of *non-zone* event parameters

Directory *Status Event Summary* presents a list of other - non-zone - events in case of which the module sends messages to the user with indicated *Contact ID* codes and/or customized texts.

ID	Name of Status Event	Enable	Code	Text in User SMS
1	Periodical test	☒	602	Periodical test
2	GSM level	☒	660	GSM level
3	Open	☒	400	Open
4	Close	☒	400	Close
5	System Reset	☒	305	System Reset
6	Remote Open	☒	407	Remote Open
7	Remote Close	☒	407	Remote Close
8	Armed STAY	☒	441	Armed STAY

Event

Enable CMS and User Reporting

Notification SMS text.
Text can be changed manually

Contact ID code of the event

Registration of *YG* data bus modules

Directory *Bus modules* presents a list of expansion modules connected to two-wire YEL/GRN data bus and registered by *SP131* module, e.g. keypads or input expanders.

ID	Module SN	Hardware	Zn	PGM
0	00000000		8	4
1	13012002	Keypad K32LED	1	0
2	00000000		0	0
3	00000000		0	0
4	00000000		0	0
5	00000000		0	0

Module number

Module serial number

Name of the module

Outputs number of the module

Inputs number of the module

Registration of *MCI* data bus modules

Directory *Bus Modules* presents the list of expansion modules which can be connected to MCI data bus. *SP131* automatically registers the modules when they are physically connected and powered.

ID	Module SN	Module Type	Device FW
1	00000000	Not Available	
2	00000000	Not Available	
3	00000000	T10 RF transmitter	
4	00000000	E10C Ethernet module	
5	00000000	G10 GSM module	
6	00000000	W131 1-Wire Dallas Bus Adapter	
7	00000000	Not Available	
8	00000000	Not Available	
9	00000000	Not Available	

Module number

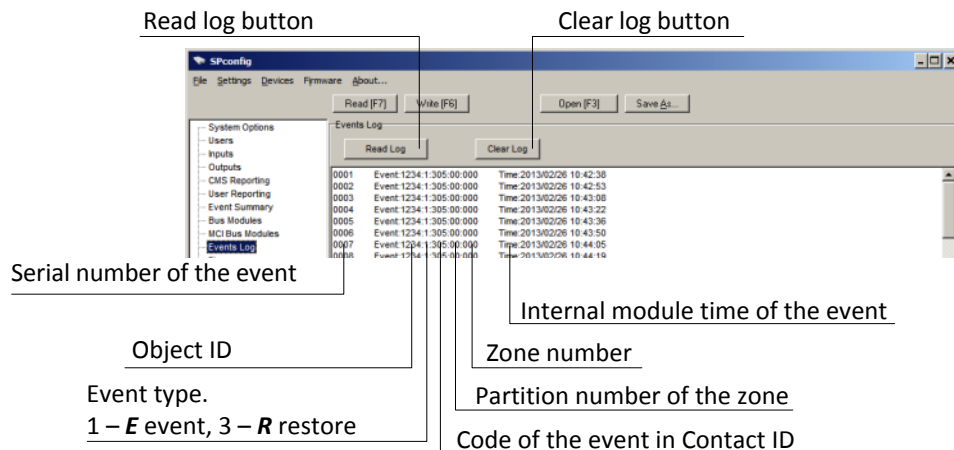
Module serial number

Module name/type.
Select the module which will be connected to MCI data bus

Firmware version of the module

Events log

Directory **Events Log** presents the list of registered events.



Restoration of default factory settings

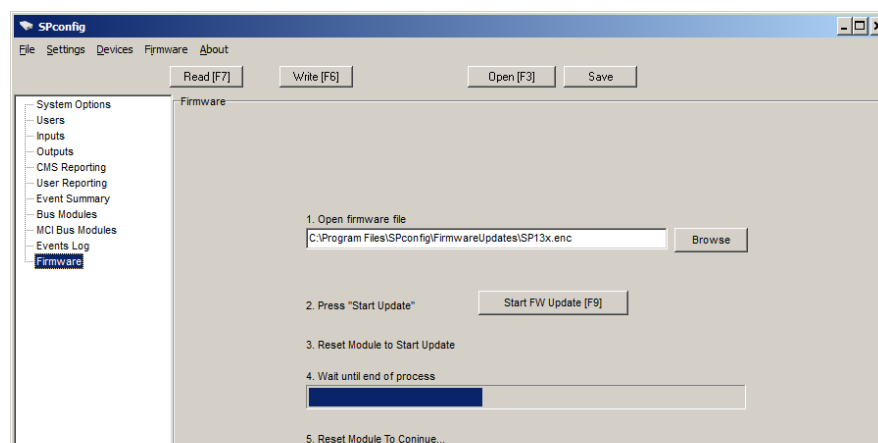
Parameters are restored to default values automatically after the firmware update of the module. Factory settings can also be restored manually:

1. Restart program **SPconfig**.
2. Connect the module as described in section **Connecting to a computer using a USB cable**.
3. Click **Write [F6]** to record the factory settings into the memory of module **SP131**.
4. If needed, re-enter the parameters (see. **Software SPconfig**) and click **Write [F6]** to record the new parameters into the memory of the module.

Module operation firmware upgrades

Firmware of module **SP131** can be updated once the manufacturer releases an update:

1. Download the newest version of the program **SPconfig** from the website www.trikdis.lt.
2. Connect module **SP131** to the computer using a USB cable. Open **SPconfig** directory **Firmware**, click **Browse** and select the file **SP13x.enc**.
3. Click **Start FW Update [F9]**. Press **RESET** button at the back of the module. It will begin an update process. Press **RESET** button again once the progress bar fills up.
4. After the firmware update all parameters of the module will be set to default. If there is a file of set parameters, open it using the program **SPconfig** and enter it into the module.



Security System Control

Control by SMS messages

Security system can be controlled by SMS, but only some parameters of the module can be changed by SMS. All module parameters can only be changed using the program *SPconfig*. In order to change the desired parameter of the module, send an SMS message with the following text:

PSW[Password] space [Command code] space [Command content]

Note: Change the default password (123456) to a new one known only by you, e.g. for 111111, send an SMS message with the following text:

PSW123456 98 111111

Every SMS message should be started with capital letters PSW and a 6-digit remote access code.

The symbol „ _ „ indicates a space in the SMS message text.

Module will send an SMS message – a response to the request – to the phone, from which the request was received.

SMS text	Description
PSW000000 _ 97 _ 3	Module will send an SMS message about the status of PGM outputs.
PSW000000 _ 97 _ 4	Module will send an SMS message about the state of inputs and power supply status.
PSW000000 _ 97 _ 5	Module will send an SMS message about GSM network connectivity level and module the IMEI number.
PSW000000 _ 97 _ 6	Module will send an SMS message about module firmware version and the IMEI number.
PSW000000 _ 50 _ N	N th output state will be changed to the opposite, if the N th output is set to "Remote Control by SMS". N values: 1, 2, 3, 4.
PSW000000 _ 5N _ 0	N th output state will be changed to OFF, if the N th output is set to "Remote Control by SMS". N values: 1, 2, 3, 4.
PSW000000 _ 5N _ 1	N th output state will be changed to ON, if the N th output is set to "Remote Control by SMS". N values: 1, 2, 3, 4.
PSW000000 _ 59	Reset of two-wire fire (smoke) sensors connected to IN8 input.
PSW000000 _ 10 _ xxx.xxx.xxx.xxx#yyyy#	To set the first IP address and port number. xxx.xxx.xxx.xxx IP address yyyy Port number
PSW000000 _ 11 _ xxx.xxx.xxx.xxx#yyyy#	To set the second IP address and port number. xxx.xxx.xxx.xxx IP address yyyy Port number
PSW000000 _ 12 _ APN#LOGIN#PSW#ENC#PING#	To set APN, six-digit encryption key for GSM connection and the interval of PING messages. Enter the corresponding values received from the network provided instead of acronyms in the example and use # as the end mark, e.g. <i>PSW000000 12 banga#... .</i> If the network provider does not require APN, user LOGIN or password PSW, the SMS message should look like this: <i>PSW000000 12 banga###123456#180#</i>
PSW000000 _ 96 _ yyyy/mm/dd#hh:mm#	To set the date and time of the module. yyyy - year, mm - month, dd - day, hh - hour, mm - minutes.
PSW000000 _ 98 _ 999999	Set a new password. 999999 new code (six 0-9 digits)
PSW000000 _ 99	Module restart.
PSW000000 _ 80 _ NN _ S	Turn on BYPASS mode for zone NN. NN values: zone number 01 – 32. S values: 1 – BYPASS on, 0 – BYPASS off.
PSW000000 _ 60 _ S	Change the system status: S values: 0 – <i>Disarm</i> , 1 <i>ARM</i> , 2 <i>STAY</i> .

Control using the *Protege*s keypad

1. **ARM.**

Note. Security system cannot be armed if any of the zones is breached.

[4 3 2 1]

Enter the User code using the keypad.

After entering the User code the time countdown **Exit Delay** for leaving the premises and closing the door will start.

The keypad indicator [ARM] will start flashing while countdown **Exit Delay** is in progress. After that, indicator [ARM] will be constantly on. A short siren will be sounded indicating that the security system is armed if **Bell Squawk** function is enabled.

2. **ARM in STAY mode.**

Note. Security system cannot be armed in STAY mode if any other than *Interior STAY* or *Instant STAY* zone is breached.

At least one zone has to be set to **Interior STAY** or **Instant STAY** mode, otherwise, command STAY will not be carried out.

[] + [4 3 2 1]

Press [] and enter the User code using the keypad.

After entering the User code the time countdown **Exit Delay** for leaving the premises and closing the door will start. Keypad indicators [ARM] and [STAY] will light up once security system is armed.

Breaches of **Interior STAY** and **Instant STAY** zones will be allowed in STAY mode. The time (**Entry Delay**) countdown will start for entering the premises and disabling the alarm if **Delay** zone is breached.

To disable the mode enter the User code, e.g. [4321].

3. **ARM in SLEEP mode.**

Note. Security system cannot be armed in SLEEP mode if any other than *Interior STAY* or *Instant STAY* zone is breached.

Note. At least one zone has to be set to **Interior STAY** or **Instant STAY** mode, otherwise, command SLEEP will not be carried out.

[] + [4 3 2 1]

Press [], enter the User code using the keypad and do not breach **Delay** zone, e.g., do not open the exit door.

The security system will be armed in SLEEP mode. Keypad indicator [ARM] will light up and [STAY] will start flashing once security system is armed.

Breaches of **Interior STAY** and **Instant STAY** zones will be allowed in SLEEP mode. **Delay** zone will be protected as an **Instant** type zone when breached, e.g. once the entry door is open **Entry Delay** countdown will not start - the security system will be alarmed and event messages will be sent immediately.

To disable the mode enter the User code, e.g. [4321].

4. **DISARM.**

[4 3 2 1]

Once the premises are entered in either ARM or STAY mode, **Entry Delay** time countdown for entering the User code (e.g. [4321]) using the keypad will start.

The User code (e.g. [4321]) must be entered using the keypad in order to disarm the security system if it is armed in either STAY or SLEEP mode and you are inside of the premises.

Two short siren signals will be sounded indicating that the security system is disarmed if **Bell Squawk** function is enabled.

Keypad indicator [OFF] will light up once the alarm system is disarmed.

5. Bypass function.

Security system may be armed even if a zone is breached. Zone control may be disabled for a single alarm system actuation period.

[] + [4 3 2 1] + [1 2] + [O K]

Press [] and enter the User code before disarming the security system. Indicator [BYP] will start flashing. In order to disable another zone control repeat previously described actions. Press [] again, enter the User code, enter the two-digit zone number and press [OK]. Indicator [BYP] will light up. Arm the security system according to the description. Security system will ARM even if a zone is breached.

6. Bypass function OFF.

Repeat the same actions as described in section **Bypass function**.

7. Changing the Master code.

Master code may be edited, but cannot be deleted.

[] + [1 2 3 4] + [0 1] + [X X X X] + [X X X X] + [O K] + [C] + [C]

Press . Enter the Master code (default - 1234). Zone indicators of serial numbers of those users whose codes are already entered will light up. Enter a two-digit Master code serial number [01] and then enter a new four-digit Master code twice. Press [OK] and then [C] twice.

8. Entering new User codes.

[] + [1 2 3 4] + [0 2] + [X X X X] + [X X X X] + [O K] + [C] + [C]

Press . Enter the Master code. Zone indicators of serial numbers of those users whose codes are already entered will light up. Enter a two-digit user serial number, e.g. [02] and enter a new four-digit User code. Press [OK] and then [C] twice.

9. Deleting User codes.

[] + [1 2 3 4] + [0 2] + [] + [O K] + [O K]

Press . Enter the Master code. Zone indicators of serial numbers of those users whose codes are already entered will light up. Enter a two-digit serial number (e.g. [02]) of the User whose code is to be deleted. Press . A sound signal will be heard and an indicator of the serial number of the deleted User code will turn off. Press [OK] twice.

10. Clearing the alarm system memory.

[C] – 3 s e c . , [C]

Keypad indicator [MEM] will light up and breached zones indicators will start flashing rapidly after the security system has been breached. Same indications are kept when the security system is disarmed.

In order to clear the memory press and hold down [C] for 3 seconds. Press [C] again once indicator [MEM] starts flashing.

11. Resetting two-wire fire (smoke) sensors

[] – 3 s e c .

Two-wire sensors can be reset by pressing and holding the key [] for 3 seconds.

12. To exit the programming mode, erase or edit incorrectly entered values, always use the key [C] .

13. Emergency Keys.

Panic – press and hold key [1] for 3 seconds.

Auxiliary – press and hold key [4] for 3 seconds

Fire – press and hold key [7] for 3 seconds

Control using the *Paradox* keypad

1. **ARM.**

Note. Security system cannot be armed if any of the zones is breached.

[4 3 2 1]

Enter the User code using the keypad.

After entering the User code the time countdown **Exit Delay** for leaving the premises and closing the door will start.

The keypad indicator [ARM] will start flashing while countdown **Exit Delay** is in progress. After that, indicator [ARM] will be constantly on. A short siren signal will sound indicating that the security system is armed if **Bell Squawk** function is enabled.

Alarm system will be armed in *STAY* mode if at least one zone in the system is set to *Interior STAY* or *Instant STAY* mode and doors are not opened (*Delay* zone breached) during the **Exit Delay** time countdown.

2. **ARM in STAY mode.**

Security system cannot be armed in *STAY* mode if any other than *Interior STAY* or *Instant STAY* zone is breached.

At least one zone has to be set to **Interior STAY** or **Instant STAY** mode, otherwise, command *STAY* will not be carried out.

[S T A Y] + [4 3 2 1] + [E N T E R]

Press [STAY], enter the User code using the keypad and press [ENTER].

After entering the User code the time countdown **Exit Delay** for leaving the premises and closing the door will start. Keypad indicator [ARM] will light up and [STAY] will start flashing once security system is armed in *STAY* mode.

Breaches of **Interior STAY** and **Instant STAY** zones will be allowed in *STAY* mode. The time (**Entry Delay**) countdown will start for entering the premises and disabling the alarm if **Delay** zone is breached.

To disable the mode enter the User code, e.g. [4321].

3. **ARM in SLEEP mode.**

Note. Security system cannot be armed in *SLEEP* mode if any other than *Interior STAY* or *Instant STAY* zone is breached.

Note. At least one zone has to be set to **Interior STAY** or **Instant STAY** mode, otherwise, command *SLEEP* will not be carried out.

[S T A Y] + [4 3 2 1] + [E N T E R]

Press [STAY], enter the User code using the keypad and do not breach **Delay** zone, e.g., do not open the exit door.

Alarm system will be armed in *SLEEP* mode if **Delay** zone is not breached during the **Exit Delay** time. [STAY] and [ARM] will light up once the security system is armed.

Breaches of **Interior STAY** and **Instant STAY** zones will be allowed in *SLEEP* mode. **Delay** zone will be protected as an **Instant** type zone when breached, e.g. once the entry door is open **Entry Delay** countdown will not start - the security system will be alarmed and event messages will be sent immediately.

To disable the mode enter the User code, e.g. [4321].

4. **DISARM.**

[4 3 2 1]

Once the premises are entered in either *ARM* or *STAY* mode, **Entry Delay** time countdown for entering the User code (e.g. [4321]) using the keypad will start.

The User code (e.g. [4321]) must be entered using the keypad in order to disarm the security system if it is armed in either *STAY* or *SLEEP* mode and you are inside of the premises.

Two short siren signals will be sounded and keypad indicator *OFF* will light up indicating that the security system is disarmed if **Bell Squawk** function is enabled.

5. Bypass function.

Security system may be armed even if a zone is breached. Zone control may be disabled for a single alarm system actuation period.

[B Y P] + [4 3 2 1] + [1 2] + [E N T E R]

Press [BYP] and enter the User code before disarming the security system. Indicator [BYP] will start flashing. Enter a two-digit serial number of the zone to be bypassed and press [ENTER]. Indicator [BYP] will light up. In order to disable another zone control repeat previously described actions. Press [BYP] again, enter the User code, enter the two-digit zone number and press [ENTER]. Arm the security system according to the description. Security system will ARM even if a zone is breached.

6. Bypass function OFF.

Repeat the same actions as described in section **Bypass function**.

7. Changing the Master code.

Master code may be edited, but cannot be deleted.

[⏻] + [1 2 3 4] + [0 1] + [X X X X] + [X X X X] + [E N T E R] + [C L E A R] + [C L E A R]

Press [⏻]. Enter the *Master* code (default - 1234). Key will start flashing and [1] will light up. Enter a two-digit *Master* code serial number [01] and then enter a new four-digit *Master* code twice. Press [ENTER] and then [CLEAR] twice.

8. Entering new User codes.

[⏻] + [1 2 3 4] + [0 2] + [X X X X] + [X X X X] + [E N T E R] + [C L E A R] + [C L E A R]

Press [⏻]. Enter the *Master* code. Key will start flashing and number keys indicating serial numbers of the users whose codes are entered will light up. Enter a two-digit user serial number, e.g. [02] and enter a new four-digit User code. Press [ENTER] and then [CLEAR] twice.

9. Deleting User codes.

[⏻] + [1 2 3 4] + [0 2] + [S L E E P] + [C L E A R] + [C L E A R]

Press [⏻]. Enter the *Master* code. Key will start flashing and number keys indicating serial numbers of the users whose codes are entered will light up. Enter a two-digit serial number (e.g. [02]) of the User whose code is to be deleted. Press [SLEEP]. A sound signal will be heard and an indicator of the serial number of the deleted User code will turn off. Press [CLEAR] twice.

10. Viewing and clearing the alarm system memory.

[M E M] + [C L E A R]

Key [MEM] will light up and number keys indicating serial numbers of breached zones will start flashing rapidly once the security system has been breached. Same indications of breached zones are kept when the security system is disarmed.

Press [MEM] in order to clean the memory. It will start flashing and number keys indicating serial numbers of breached zones will light up. Press [CLEAR].

11. Resetting two-wire fire (smoke) sensors

[C L E A R] a n d [E N T E R]

Two-wire sensors can be reset by pressing and holding keys [CLEAR] and [ENTER] at the same time. Two-wire fire (smoke) sensors connected to the input ZN8 will be reset.

12. To exit the programming mode, erase or edit incorrectly entered values, always use the key [CLEAR].

Annex 1. Description of Zone Types

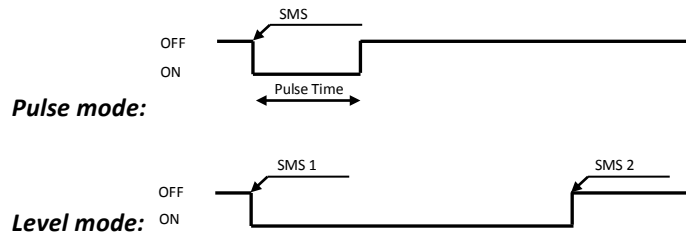
<i>Zone type</i>	<i>Module operation after the event in the circuit</i>
ON/OFF	Security system can be armed and disarmed by breaking the input circuit. Security system will arm after the specified period of time (Exit Delay) during which secured premises can be left. Entry Delay countdown for disarming the alarm system will start once the zone is breached and the alarm system is armed. Set by default to input ZN7, EOL;
Delay	Exit Delay time will start and the alarm system will arm after the set Exit Delay time period once the User code is entered in order to arm the security system. Bell and Flash signals will be sounded and messages will be sent if the zone is breached. Entry Delay countdown will start if the zone is breached when the alarm system is armed. Alarm system must be turned of, otherwise, Bell and Flash signals will be sounded and messages will be sent. Set by default to input ZN1, EOL;
Interior	Bell and Flash output signals will be immediately sounded and messages will be sent if the zone is breached when the alarm system is armed. Zone breaches are allowed during the Entry Delay and Exit Delay time. Set by default to input ZN2, EOL;
Interior STAY	Operates the same way as Interior, however, when the arming mode STAY is enabled, the module will not react to the breaches in input circuits.
Instant	Bell and Flash output signals will be immediately sounded and messages will be sent if the zone is breached when the alarm system is armed. Set by default to input ZN3 and ZN4, EOL;
Instant STAY	Operates the same way as Interior, however, when the arming mode STAY is enabled, the module will not react to the breaches in input circuits.
24 hours	Constant input circuit control. Bell and Flash output signals will be immediately sounded and messages will be sent if the zone is breached when the alarm system is armed. Set by default to input ZN5 and ZN6, EOL;
Fire	For connecting two-wire and four-wire fire sensors. Bell and Flash output signals will be immediately sounded and messages will be sent if the zone is breached when the alarm system is armed. Set by default to input ZN8, NO;
Silent	Constant input circuit control. Messages will be sent immediately, however, Bell or Flash output signals will not be sounded when the zone is breached while the security system is disarmed.

Annex 2. Operation Modes of PGM Outputs

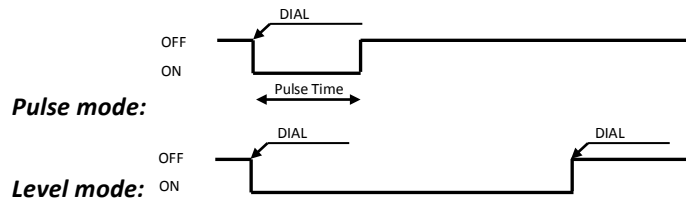
Function of a PGM output	Output signal
Bell	Output for connecting a sound-emitting (siren) device. A continuous or a wailing <i>PGMx</i> output signal is sounded once a signal from input <i>ZNx</i> is received. Set by default to output PGM1.
Buzzer	Output for connecting a sound-emitting (siren) device. A wailing signal is sounded during Exit Delay time. A continuous signal is sounded during Entry Delay time or once the zone is breached.
Flash	Output for connecting a light-emitting device. A continuous signal is sounded when the alarm is armed and a wailing signal is sounded when it is breached.
System State	Output for connecting a light-emitting indicator of the alarm system status. A continuous signal is sounded when the alarm is armed and a wailing signal is sounded during Entry Delay and Exit Delay times. Set by default to output PGM2
Ready	Output for connecting a light-emitting indicator of the input status. A continuous signal is sounded when all <i>ZN</i> inputs are in order. Set by default to output PGM3.
AC OK	Output for connecting an indicator of power supply by AC source status.
Battery OK	Output for connecting an indicator of power supply by battery status.

Remote Control by SMS

Output which can be controlled by SMS message. This output is for connecting electrical devices which will be controlled by SMS message.

**Remote Control by DIAL**

Output which can be controlled by call. This output is for connecting electrical devices which will be controlled by call.

**ARM/DISARM**

Output for connecting an indicator of the alarm system status. A continuous signal is sounded when the security system is armed.

**Alarm Indication**

Output for connecting a status indicator. A continuous signal is sounded once the alarm system is breached.

**Lost Primary Channel**

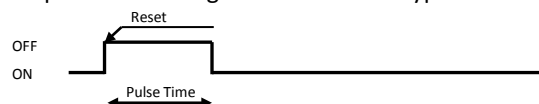
Output in which a continuous signal is sounded once a connection to a central monitoring station is lost.

**Lost Secondary Channel**

Output in which a continuous signal is sounded once a standby connection to a central monitoring station is lost.

**Fire Sensor Reset**

Output for resetting an indicator of keypad commands to fire sensors.



Annex 3. Warranty and Limitation of Liability

The manufacturer provides a 24 month warranty. Warranty coverage period begins on the date of product purchase, issue of an invoice or signing of a fiscal receipt.

- Manufacturer is not liable in cases of burglary, fire or any other losses suffered in the premises of the Buyer and/or the User and does not recompense for any direct or indirect damages incurred thereof.
- Manufacturer is not liable for device malfunction if device is not set up or used according to the user manual.
- Manufacturer is not liable for device malfunction if such occurs due to the loss of GSM/GPRS/Internet connection or faults in service provider network.
- Manufacturer is not liable in cases of GSM/GPRS/Internet service disconnection or restriction and does not recompense the device Buyer and/or the User for any direct or indirect losses incurred thereof.
- Manufacturer is not liable in cases of electricity supply disconnection or restriction and does not recompense the device Buyer and/or the User for any direct or indirect losses incurred thereof.