TOPKODAS

PROGATE

Installation & Programming Manual

Cellular Gate controller PROGATE

Multifunctional device: access control + security + home automation

This manual includes steps to install, set up and use your system.

DESCRIPTION

PROGATE is gate controller - **access control system** with **relay output** and **programmable selectable inputs or outputs.**

The module PROGATE supports up to 800 users for remote control purpose.

PROGATE GSM gate controller can remotely control automatic gates and other equipment as well provides the high level of protection residential homes and any place where high security and automation is essential.

Users can control the gate and other equipment with SERANOVA application, phone calls and SMS messages. The controller can recognize up to 800 user phone numbers. A user control schedule and counter for how many times a specific user can control the system can be set for the controller. The GSM controller can send SMS messages up to 8 administrators informing when inputs and outputs are activated and restored (the text of the SMS messages is customizable).

The controller is capable of sending event messages to the receiver of a security company.

PROGATE designed to be easy to use. Once installed, module can be programmed remotely via GPRS connection or via USB using SERA2 configuration software.

FEATURES

- **Network**
  - 2G or 4G LTE modem
- **Remote control**
  - With Android/IOS/WEB application SERANOVA.
  - With SMS messages.
  - With phone call
- **Notifications**
  - Push Notifications to Android/IOS application SERANOVA.
  - SMS messages.
  - Autodial phone call
- **Reporting events to Central Monitoring Station (CMS)**
  - Communication via SIA IP DC-09 standard protocol
- **Outputs**
  - RELAY
  - I/O1 (1A)
  - I/O2 (1A)
  - 1W, 10mA, Max Voltage 3.3V!
- **Inputs**
  - IN1, IN2 0-30V
  - I/O1, I/O2 0-30V
  - 1W - 1-wire bus Up to 32 sensors, temperature, humidity etc.
  - Digital input max 3.3V
- **Events log** buffer. 3072 events
- **USERS** Up to 800 app/iButton/ RFID keycard/code.
- Wiegand keyboard.
- In-field firmware upgradeable via USB or Remote using SERA2 software

DOWNLOAD SERANOVA APP

GET IT ON Google Play

Download on the App Store

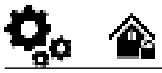
The meaning of icons in the manual:

Automation part	Security system's part	Very important	Important	About the manual

Contents

1 GENERAL INFORMATION

1.1 Specifications



Parameters of built-in GSM module:

- Quad-band (850/900/1800/1900 MHz)
- *Optional 3G ,4G LTE bands*
- Transmitting power
  - GSM/GPRS power class:
    - EGSM900: 4 (33dBm±2dB)
    - DCS1800: 1 (30dBm±2dB)
  - EDGE power class:
    - EGSM900: E2 (27dBm±3dB)
    - DCS1800 : E1 (26dBm+3dB/-4dB)
  - LTE power class: 3 (23dBm±2.7dB)
- Sending of SMS messages
- Receiving of calls and dialing
- Mobile Data via GPRS/LTE network

Module control via:

- Android, iOS, Web, SERANOVA app
- SMS message 800 users
- Short call DIAL 800 users
- Maxim-Dallas iButton key (iButton DS1990A – 64 Bit ID)) 800 users.
- Wiegand keypad code or RFID keycard or key fob 800 users

Outputs:

- RELAY , 1 A 30 V DC, 0,5 A 125 V AC
- I/O1,I/O2 - Open Drain (1A) 30V
- 1W (10mA Max voltage 3.3V)! (Programmable selectable input or output)
- All outputs can be controlled via short call DIAL or via SMS message, mobile, web app. This feature may be used for gate opening.
- Output alarm parameters may be programmed.
- Programmable algorithms for outputs operation: Access Control,CTRL/SMS/DIAL, SIREN, BUZER, ARM state, inverting, pulse mode

Inputs:

- Analog inputs In1, In2: 0-30V
- Analog inputs I/O1, I/O2: 0-30V (Programmable selectable input or output)
- SMS text for input alarm and restore
- Burglary alarm zones. Input type NC/NO/EOL/EOL+TAMPER 5.6K + 5.6K
- Algorithm for zones operation: delay, interior, instant, 24 hours, silent, fire
- Response time;
- Time of additional response;
- Commutation of selected output

Wiegand interface D0/D1:

DATA0/DATA1, RFID reader, Keyboard.

1-Wire bus Digital I/O 1W:

- Programmable optional digital input or output
- Max. Voltage 3.3V
- Dallas 1-Wire Bus, DS18b20, DS1990A
- Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321
- The total length of the bus up to 100m.

Aux power source +5V:

Used to power 1-Wire Bus sensors, DS18b20, DS1990A, Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321

- Voltage 5V
- Current limit 100mA

Power supply voltage:

- DC 10-30V
- AC 12-24V
- Min 0.5A
- Max. Allowed ripple DC voltage 100mV

Consumption current:

- In standby mode less than 50 mA.
- In dialing or SMS/GPRS sending mode less than 300 mA.

Events Log:

Nonvolatile flash events log 2048 events

Environmental parameters:

- Storage temperature range from -40 to +85 ºC / -40 to 185 ºF
- Operational temperature range from -30 to +75 ºC / from -22 to 167 ºF
- Max relative humidity under +40 ºC / 104 ºF 95%

Package weight 90g

Module weight: 70g

Overall dimensions of the module:

73x62x26mm

1.2 Used definitions and terms


Term	Description
Alarm Log	Contains information about alarms that are currently active on the system or information about alarms that have been raised and then resolved on the system. This log can be useful in analyzing problems and trends in the system.
Arming/Disarming	A process of enabling/disabling system's security.
Authorized user	It is a person whose mobile phone's number is entered in PROGATE module. Several authorized users with the same rights may be entered into the module.
Backup battery	The secondary power source of the system. In case of a main power failure, the backup battery will take over.
Bell squawk	If enabled, the siren/bell indicates the completed system arming and disarming process (except the arming in STAY mode). After the system is successfully armed, the siren/bell will emit 2 short beeps and 1 long beep after the system is disarmed. By default, the parameter is disabled.
Bypass/Activate Zone	Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. The zone will remain bypassed until the system is disarmed. Zones can only be bypassed and activated when the system is not armed.
Caller ID	Caller's identification
COM	Negative power supply terminal.
Configuration	Programming of the settings, which will define the operation of the item. For example, user's telephone numbers, set-up of periodicity for sending SMS message, input names etc.
CMS	Central monitoring station
DIAL	The system makes a call to the number specified.
Diagnostic Tool	When using Configuration tool software, you may monitor system inputs/ outputs, view changes of peripheral devices, instantly configure necessary options, for example, enabling/disabling PGM outputs, etc.
Entry Delay	The system initiates the entry delay countdown if a Delay type zone is violated. The countdown is indicated by short beeps emitted by keypad buzzer and by steady beep emitted by system's buzzer. The indication is intended to advise the user that the system should be disarmed. If the system is disarmed before the entry delay expires, no alarm will be caused.
EOL	(End of line resistor) input type with resistor.
Event	The information that the user receives.
Event Log	A list of system events that is uploaded from the device‘s memory to the configuration software for further analysis. The system logs all information about system configuration, system actions and info messages.
Exit Delay	A period of time intended for user to leave the secured area. The system begins the countdown after the arming process initiation.
Fault	A specific problem or error that prevents the system from working properly. The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault and send SMS text message notification to the listed user phone number.
iButton key	A unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. The module supports up to 800 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.
Installer	a person provided with INST (installer's) password
Master/User Code	Allows to carry out system arming/ disarming as well as minor system configuration and control
Normally closed (NC)	It is a switch that passes current until actuated.
Normally open (NO)	It is a switch that must be actuated to pass current.
Periodic Test Event	Provides the following information on alarm system: date & time, status (armed/disarmed), GSM signal strength, mains power supply status, temperature value measured by primary and secondary temperature sensors (if any).
Pull-up resistor	Is that it weakly "pulls" the voltage of the wire it is connected to towards +V (or whatever voltage represents a logic "high").
PGM output	A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system or if the user has initiated the PGM output state change manually.
Ping period	Sets period of time defining how often the module sends ping data packet to the server.
Service messages	ARM/DISARM, test, resetting of the system.
SSR	Solid State Relay
SMS forward	System can re-sent all incoming SMS messages to the specified users. It is useful if the GSM operator of the inserted SIM card sends some useful information (SIM card validation or payment account status and etc.) or it is necessary to monitor all incoming SMS messages by specified user.
User	It is a person being aware USER password.
Zone	Detection devices such as motion detectors and door contacts are connected to the alarm system's zone terminals.
Zone state/status	Zone status is a position of a certain zone being enabled or disabled. Meanwhile, zone state points out the condition of a certain zone, which can either be violated (i.e. In case of alarm) or restored.
+V	Positive power supply terminal.

1.3 Package content

Table 1 Standard package content

PROGATE module – 1 pcs

Shipping Package - 1 pcs

Package content may be vary without a notice. Ask the seller before buying!

Table 2 Additional, under request package content

Mini USB cable

Cellular Antenna 2.5 dBi L-Type SMA Connector

4G LTE Antenna 3dBi SMA male Adhesive Mount 2m Cable

4G LTE Antenna 7dBi SMA male Magnetic 2m Cable

iButton DS1990A-F5+ key

iButton probe with LED indicator

Plug-in type Switching Power Supply 12V/1A AC/DC

Wiegand keypad & RFID reader

1.4 General view of the module

Figure 1 General view of the module PROGATE

1	**ANT**	GSM antena connector
2	**SIM**	Nano SIM holder. Push- Push Type
3	**USB**	Mini USB programming connector
4	**REG (yellow)**	See table below
5	**DATA**	See table below
6	**PWR (green)**	See table below
7	**RELAY (blue)**	See table below
8	**I/O Connector**	Power supply and inputs, outputs connector.

! Do not locate SIM card with force, because you may damage SIM card holder

1.5 Meaning of LEDs and contacts

Table 3 Meaning of LEDs

Name	Indication variations	Meaning
PWR (green)	Watchdog blinking, on 50ms, and turns off after 1000ms.	The module is functioning.
	Off	The module is out of order or no voltage
REG (yellow)	Lights continuously	Modem has been registered to the network
	Flashes, remains lit for 50ms, turns off for 300ms	Modem is being registered to the GSM network.
	Blinking fast, remains lit for 50ms turns off for 50ms	PIN code of SIM card error. PIN code request should be removed
	Off	Modem failed to register to the network.
DATA (red)	Lights continuously	The memory of the module contains unsent reports
	Off	Data status is OK. All reports has been send.
RELAY (blue)	ON/OFF	Relay switched ON/OFF

Table 4 Terminal block. Contacts.

Name	Optional functions and Description	
AC/DC	DC	10-30V
	AC	12-24V
	Max	0.2A
NC, C, NO	Relay Output 1A 30 V DC, 0.5A 125 V AC	
I/O1-I/O2	Programmable functions	Input with pull up resistor 10K to the VD+
		Open drain output 30V/1A
		Analog voltage input 0-30V
	Max available voltage	30V
IN1/D0 … IN2/D1	Programmable functions	Input/Zone with pull up resistor 10K to the VD+. Used for gate position or security sensors
		Can be configured NC/NO/EOL/EOL+Tamper
		Wiegand interface. Inputs D0 and D1 used for wiegand RFID reader, keypad
	Max available voltage	30V
COM	Negative supply terminal for keyboard(s), indicators and sensors.	
1W	Programmable functions	Digital output (Max 3.3V)
		Digital input (Max 3.3V)
		Dallas 1-Wire bus. For iButton DS1990A and temperature sensors DS18B20
		Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
	Max available voltage	+3,3V
	Max available current	10mA
+5V	Power supply for external temperature, humidity sensors	
	Max available voltage	+5V
	Max available current	100mA

2 WIRING & INSTALLATION

This Installation & Programming manual provides the basic installation, wiring and programming information required to program the module PROGATE and connect all third party devices to the module.

Before beginning installation, make sure that you have the necessary components:

1. USB Mini-B type cable for configuration.
2. Cable consisting of at least 4 wires for connecting the controller.
3. Flat-head 2.5 mm screwdriver.
4. External GSM antenna if reception is weak in the area.
5. Activated nano-SIM card (can have turn off PIN code requests).
6. Instruction manual for the automatic gate to which the GSM gate controller is about to be connected.

Order the necessary components separately from your local retailer

2.1 Fastening

Mounting on DIN rail

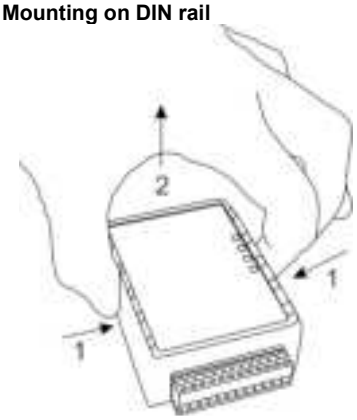


Figure 2 remove the top lid

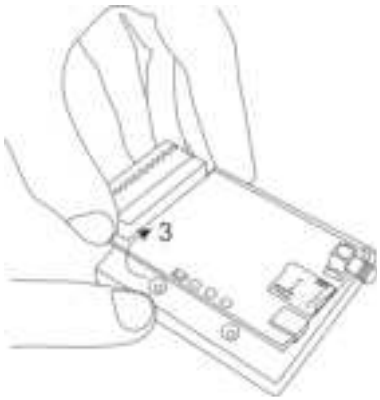


Figure 3 Remove the PCB board

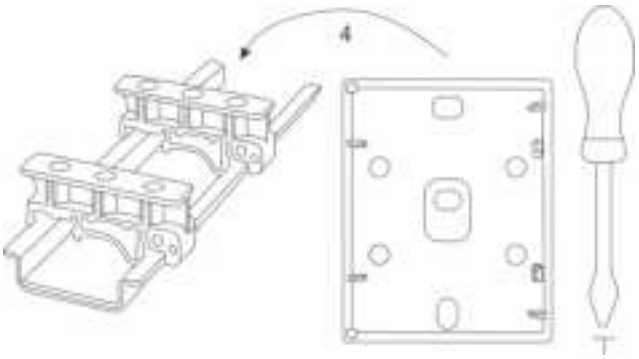


Figure 4 Fasten DIN rail adapters to the base of the case

Fasten the base of the case in the desired place using screws

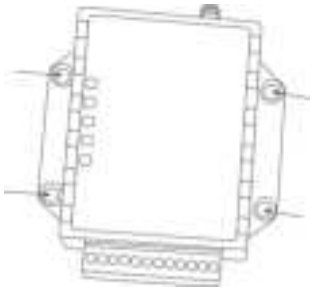
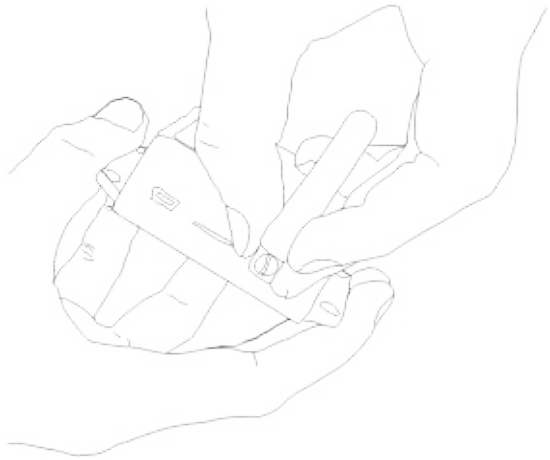
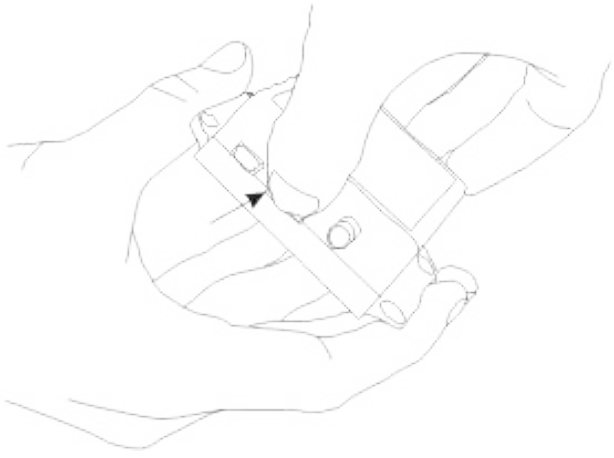


Figure 5Fasten the base of the case

2.2 Preparation



Screw the GSM antenna



Insert SIM Card

2.3 Wiring PROGATE to the gate control unit

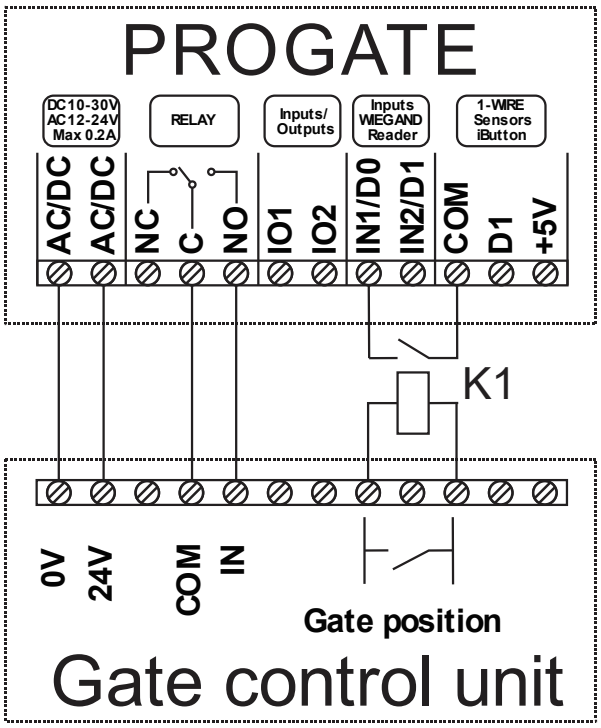


Diagram 1General connection

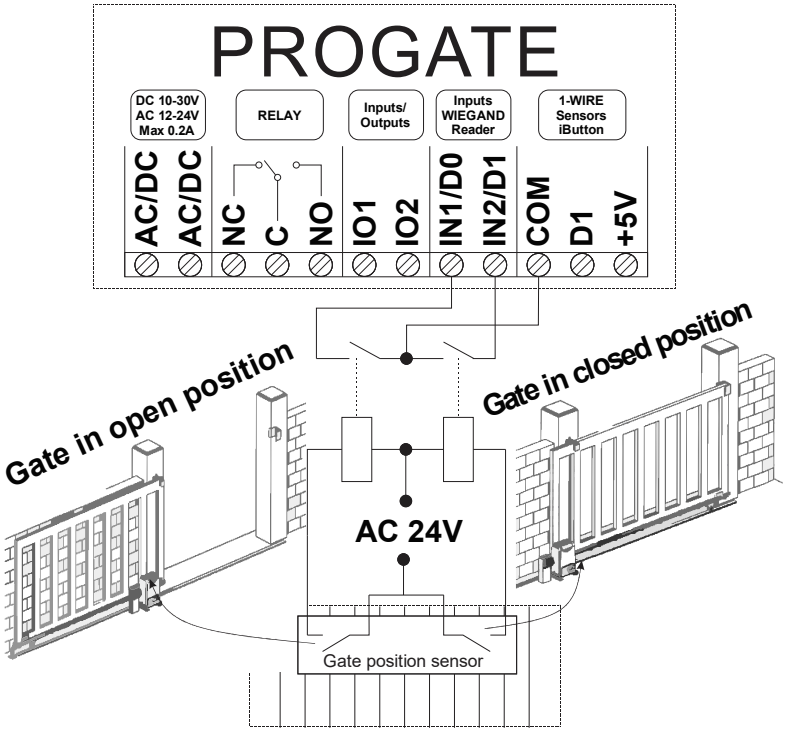


Diagram 2Connection with dual gate position sensor to detect fully open and fully closed gate status

Please note that AC relays must be used if the voltage is AC. Depending on the gate voltage, use 12 V AC or 24 V AC.

Automatic gates have a gate control input. The PROGATE relay can be connected to this input to open and close the gate with a pulse or steady (latch) signal.
Automatic gates shall normally have a gate position sensor output which indicates when the gate is closed and when it is open. The gate status output may be a voltage output or a relay output. In the diagram, relay K1 is connected to the voltage output of the automatic gate. Intermediate relay K1 is triggered when the gate is open and the input PROGATE IN1 is triggered. The gate position sensor signal gives precise information about the status of the gate (when the gate is closed and when it is open). The gate status can be displayed in SERANOVA

More information:

Quick start PROGATE: https://www.topkodas.lt/Downloads/media/Manuals/PROGATE_QS_EN.pdf
Quick start SERANOVA APP: https://youtu.be/Benf6xKcnjM
Quick start Control via call, SMS: https://www.topkodas.lt/Downloads/media/Manuals/PROGATE_Control_sms_call_QS_EN.pdf

3 QUICK START

3.1 Preparation

- Screw on the gsm antenna.
- Insert the SIM card in the SIM card holder. (Ensure that PIN request function is disabled. Ensure that mobile internet service (mobile data) is enabled if mobile app or IP connection with CMS will be used)
- Connect power supply.
- Wait for the controller to register to the GSM network

3.2 Control with free short call

The first one to call the controller will become the system administrator/owner. The controller automatically rejects the call and turns on the RELAY output for 2 seconds and will be the only one who can administer and control the controller with free short call, SMS commands. When calling PROGATE for the first time, the phone number is stored in the module memory automatically. This means that it will be possible to control the first output of RELAY with a short, free call. If this is enough, PROGATE can be installed without additional configuration.

3.3 Control with SERANOVA (Android/iOS) app

With the **SERANOVA** app, users will be able to control gates and other devices remotely, as well as administer users, view system status and push notifications, and view a log of all events.

3.3.1 Steps to get started with SERANOVA

To use the **SERANOVA** app or the **SERA2** remote connection. The **[SERA cloud service]** needs to be activated by using the **SERA2** or SMS command e.g. INST000000␣010␣1. *By default* **[SERA cloud service]** *service is activated*.

Imortant! *If there is no data plan on your SIM card.* ***[SERA Cloud service]*** *must be deactivated. Using* ***SERA2*** *or SMS command:* INST000000␣010␣0 *Otherwise the module will stop working due to a lost data connection.*

SMS command to set APN DATA/GPRS/LTE network settings. Some networks require exact APN name to be entered, otherwise data connection will not work. Network APN can be configured using SERA2 via USB or following SMS command:
INST000000␣008␣APN#LOGIN#PSW# where: APN=the name of network APN default=”internet”, LOGIN=login leave empty if not used; PSW =password leave empty if not used.
e.g.INST000000␣008␣internet### where APN=’internet’; no LOGIN; no PSW

1. Install the app. Scan a QR code with your phone or start it on the web.

Free WEB SERANOVA app https://seranova.eu/login
SERANOVA website https://www.topkodas.lt/SERANOVA-app/

Launch As Web App

SERANOVA

GET IT ON Google Play

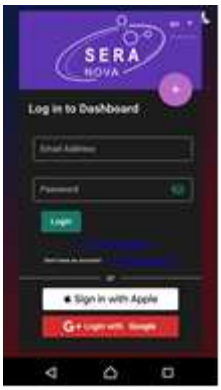
Download on the App Store

SERANOVA app for iPhone iOS: https://apps.apple.com/app/SERANOVA-smart-home/id1596644632?platform=iphone
Android SERANOVA app: https://play.google.com/store/apps/details?id=com.SERANOVA.cloud&hl=en&gl=US

2. **Create account**. If you already have account, log in, if not, register as a new user
3. To add a system, it is necessary to know the IMEI of the device. The IMEI of the device can be obtained in the following ways:
   - Make a first call to the device. The first caller to the system becomes the owner and administrator. SMS will be received from PROGATE with the IMEI. Copy the IMEI. IMEI is used as UID of the module. This IMEI will allow you to connect to the free SERANOVA app.
   - Send IMEI requested SMS command to the number of the SIM card inserted into the controller. IMEI request SMS: INST000000␣100␣1 the sender will receive SMS respond with full device information including IMEI
   - The IMEI of the device can also be read via USB using the configuration program SERA2
4. **Add new system to the app**
   - Enter the IMEI (UID) you copied from the SMS or SERA2 system information
   - Enter App Key. Default 123456.
   - **Enter user access code.** Default 123456. **Without a user access code, the system cannot be operated. The user access code is used by the system as a user ID and password.**
   - Phone number of system
   - Enter system name.
   - Press save
5. **How to add a new user**
   - New users must download the SERANOVA app. Create an account, login with his email and password
   - System owner or administrator goes to SERANOVA> Menu> Users> **[Add new User]**
   - To enable a user to log in to the system, the owner must enter the user's email and user code (with which the system will be operated. This is the user ID and password). This is enter the user email that was used to create the SERANOVA account. Enter User code (Default 1234), Phone number, Set Output for control, User privileges: admin or user

Enter a valid email address of a user who already has a SERANOVA account. The system will be automatically added to the user's account. If the user is added without a valid SERANOVA account email. The user can create a SERANOVA account later and add the system manually.

1.Install SERANOVA app
2.Create account



3.Log In
4. The first person to call the PROGATE SIM card number becomes the owner and administrator.

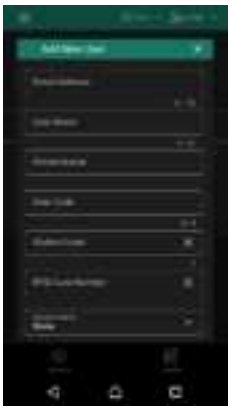
5. PROGATE sends a message with the IMEI
6. Enter the IMEI and App Key (Default 123456), **Enter User access code (Default 123456)**

7. The system is now manageable

8. Go To SERANOVA> Menu> Outputs. Edit settings

9. Select pulse or level

10. Go to SERANOVA> Menu> Users> Add New User
Owner or administrator can add other users or administrators



11. The email with which the user created the SERANOVA account must be entered. Also enter the unique user code. They cannot be repeated as the user code will be used by the system as user ID and password

How to add additional system (unlimited number) to SERANOVA app:
Go to SYSTEMS, Choose Add new system and enter the controller Unique ID (IMEI) number. IMPORTANT: When adding the controller to SERANOVA app:

1. The **[Sera Cloud Service]** must be turned on.
2. The power supply must be connected
3. Device must be registered in to network and have mobile data plan
4. Set valid **APN** of the network. (default: 'internet')

More help how to setup device and app could be found here:

3.4 Control with SMS messages

Control the RELAY output with this SMS command:
Activate or deactivate selected output
USER123456␣021␣N#ST

021= command code
(Activate or deactivate selected output N)
N = output number
ST= output mode:
0 – deactivated output, 1- activated output

E.g. send SMS: USER123456␣021␣1#1 to activate OUT1.

Output pulse activation for the time interval
USER123456␣022␣N#TIME#
022= command code,
N = output number 1-32;
TIME = 0-999999 Time interval in seconds for the output activation.

e.g. USER123456␣022␣2#5# Activate OUT2 for 5 seconds

3.5 Configuration methods

It is possible to configure device in following methods:

1. **SERA2** software via **USB**
2. **SERA2 remote** connection
3. **SERANOVA** app
4. **SMS** text messages. For more details, see: *8 SMS Commands for remote control and configuration*

SERA2 software via USB

SERA2 software is intended for PROGATE configuration locally via USB port or remotely via 2G/3G/4G network. This software simplifies system configuration process. SERA2 software is free, which you can download from our website: topkodas.lt

SERA2 remote connection

The system will NOT transmit any data to monitoring station while configuring the system remotely via 2G/3G/4G TLE network connection. However, during the remote connection session, the data messages are queued up and will be transmitted to the monitoring station after the configuration session is over.

SMS text messages

In order to configure and control the device by SMS text message, send the text command to the PROGATE SIM card from one of the listed administrator phone numbers.

System Access codes

Table 5 Default passwords and explanation

Password	Default	How to find and how to change	Explanation
Administrator password	123456	SERA2> System Options> Access	System administrator password enable to read/write configuration of the module
Installer code (for SMS control and configuration)	000000	SERA2> System Options> Access	This code allows to send SMS commands with INST identification as well it allows you to enter programming mode, where you can program all features, options, and commands of the module via SERA2 if system administrator is allowed.
SMS User code (for SMS control and configuration)	123456	SERA2> System Options> General system options	This code allows to send SMS commands with USER identification. Note: to control system the USER phone number must be authorized as well
SIM card PIN	1234	SERA2> GSM Communications> Network/SIM Card	It is automatically ignored if pin request in SIM card is disabled
App Key	123456	SERA2> GSM Communications> Sera Cloud Service	[APP Key] is used for [SERA Cloud service] This code is used for remote connection to the module via cloud service from SERA2 or SERANOVA app.

3.5.1 SERA could service

SERA Could Service – is used for remote connection to device via internet using SERA2 or SERANOVA app.

Imortant! *If there is no data plan on your SIM card.* ***[SERA Cloud service]*** *must be deactivated. Using* ***SERA2*** *or SMS command:* INST000000_010_0 *Otherwise the module will stop working due to a lost data connection.*

To connect to device using **[SERA Could Service]** is need to have UID=**IMEI** of device and **AppKey (Default 123456)**

1. **Change default App Key (Default 123456).** SERA2> GSM Communication> Sera Cloud Service
2. **Enter App Key for the remote connection via SERA2.** Go to SERA2> Settings Enter the same App Key as in the SERA2> GSM Communication> Sera Cloud Service
3. To establish a remote connection with the device, the **App Key** of the device and the **SERA2** or **SERANOVA** must match.

Figure 6 GSM Communication> Sera Cloud Service> App Key

3.5.2 Configuration using SERA2 software

With SERA2 software you can change the controller's settings (if default settings are not enough)

- Download and Install and open free SERA2 configuration & Diagnostic software: https://www.topkodas.lt/Downloads/SERA2_Setup.exe
- Connect the controller to a computer using a mini USB cable.
- The program will automatically recognize the connected device and will automatically open the controller configuration window.
- [Menu > Read] will read configuration of device and show current settings of device.
- [Menu > Write] will save the settings made in the program to the device.
- [Menu > File > Save] will save the settings into a configuration file. You can upload the saved settings to other Devices later. This allows to quickly configure multiple devices with the same settings.
- [Menu > File > Open] will allow to choose a configuration file and open saved settings.
- If you want to revert to default settings, go to Update in the command line and update FW. Or press [Menu->File->Restore Default]

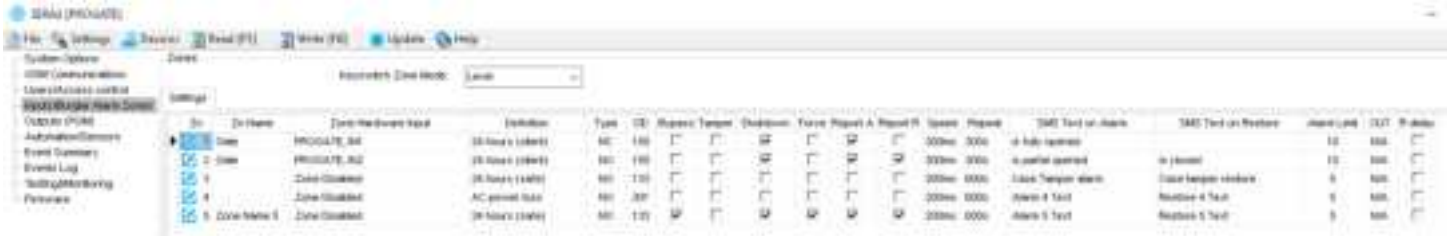


Figure 7SERA2> Inputs/ Burglar Alarm Zones

Figure 8SERA2> Outputs (PGM)

Figure 9SERA2> Users/ Access control

3.5.3 Installer and User passwords

Installer password for remote and SMS configuration. Installer Password (default: 000000). This password used for remote configuration or for configuration via SMS messages with INST code
SMS USER password for remote control or for control via SMS messages. SMS user password (default: 123456). The password used for remote control of the module or control of the module via SMS messages with USER commands.
For more information about SMS commands see: *8 SMS Commands for remote control and configuration*

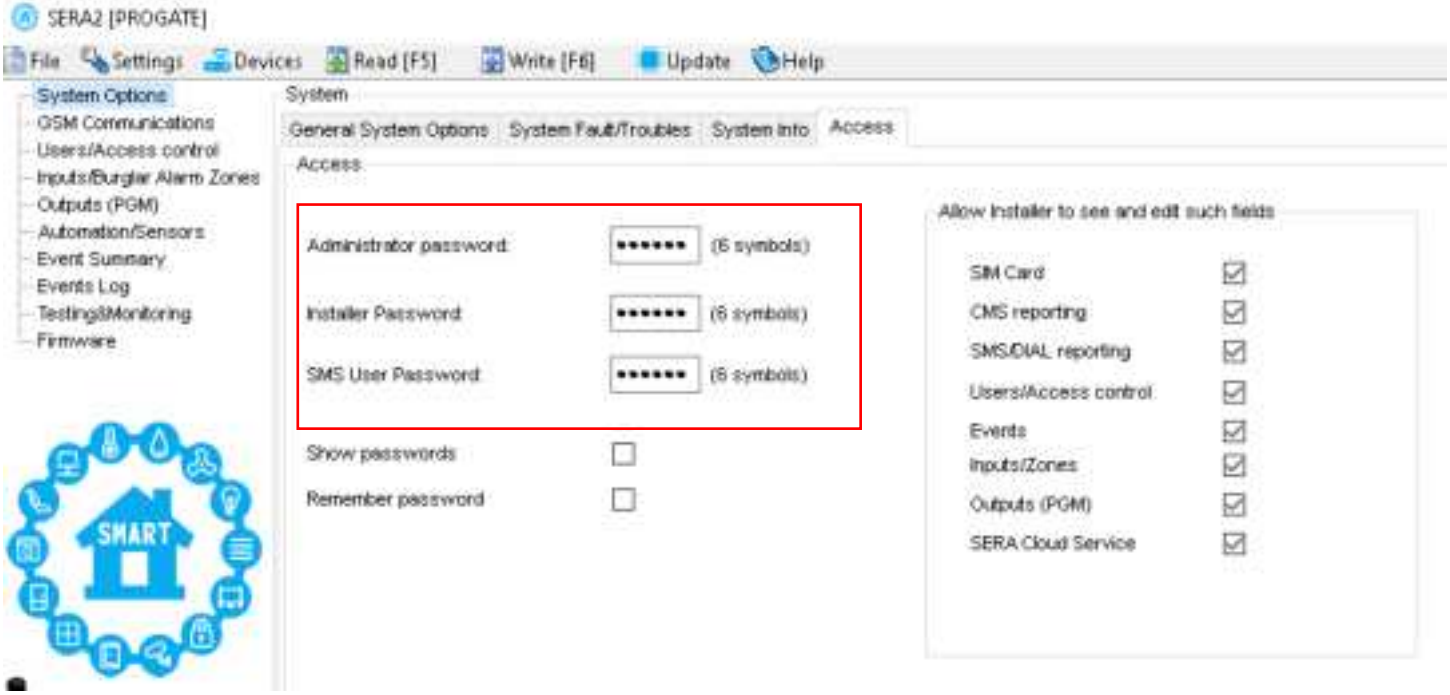


Figure 10System Options> General System Options

3.5.4 User codes for access control via keypad and SERANOVA app

Each user must have a unique user code for authorization and user identification.
The user has to enter valid code to control the system via the keypad or the SERANOVA app.
Master Code for access control via keypad. Default Master Code: 1234 or 123456

1. Select 6 or 4 digits user access code format. SERA2> System Options> General System Options>User Access Code Format
2. Enter 6 or 4 digits codes in the SERA2> Users/ Access control > Keyb Code

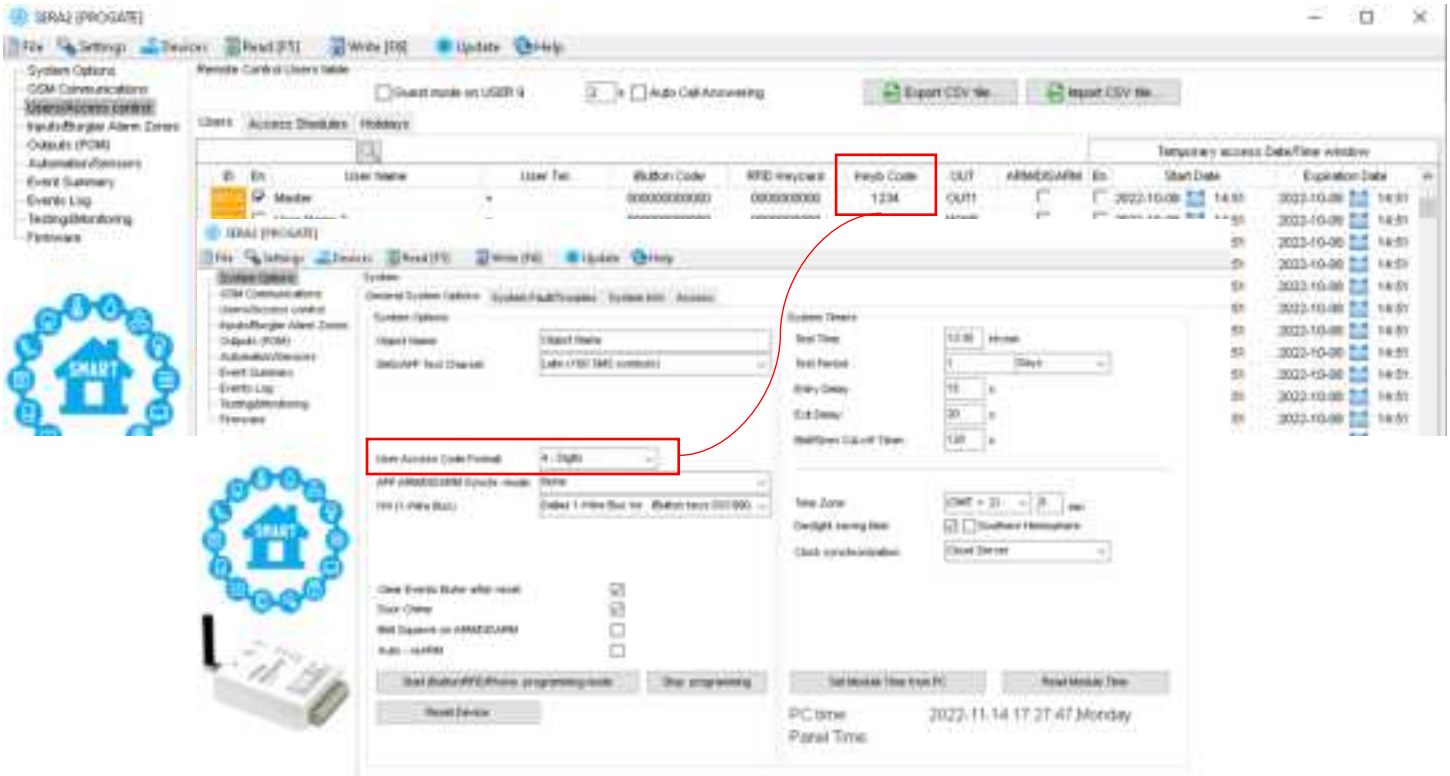


Figure 11User/ Access control and System Options> General System Options

4 Wiegand Keypad & RFID Card Reader, iButton Probe Wiring

Wiegand keypad specifications:
Wiegand Terminals: **D0 / D1**
26bit Wiegand (Default);
8bit key press code

1W - 1-Wire Maxim-Dallas interface is used for iButton DS1990A keys or temperature sensors.

iButton keys (iButton DS1990A – 64 Bit ID)) can be used to access control. Up to 800 iButton keys can be assigned to the system for authorization.

The First iButton key is automatically added to the configuration memory by touching it to the reader. Without the need to send any SMS. The system will notify about successfully recording of the key into memory by shortly beeping twice via buzzer. The system will automatically assigns control function (ARM/DISARM) and Relay Output.

The first key is the main key (MASTER)

The total length of the 1-Wire bus is up to 100 m. Depending of cable quality, and environment noise.

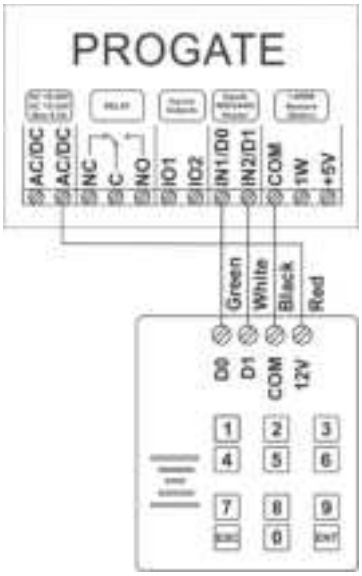


Figure 12 Wiegand keypad wiring

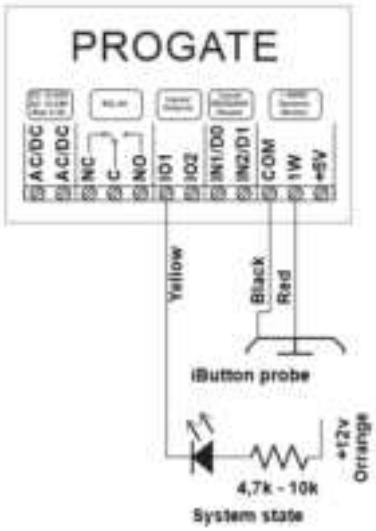


Figure 13iButton connecting diagram

Figure 14 iButton connection diagram

iButton probe LED is without resistor. External 4.7k – 10k resistor required depending of power voltage

4.1.1 Enter iButton, RFID, Phone numbers to the memory of the module

First steps:

- Connect iButtons or RFID reader to the module.
- Insert SIM card;
- Screw GSM antenna;
- Connect power supply;
- Connect the module to the computer.

Possible configurations methods:

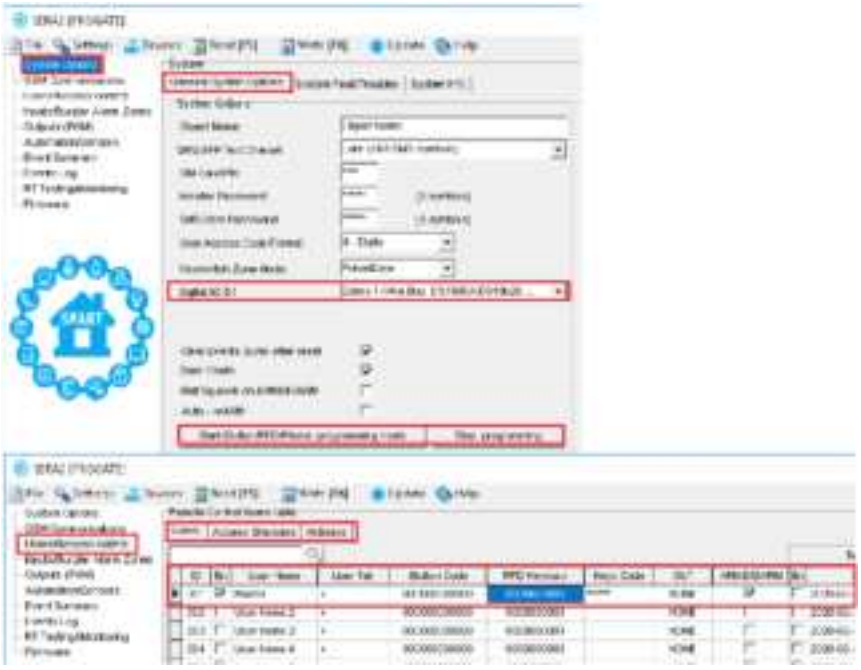
1. Start automatic learning mode via mini USB cable (SERA2 software).
2. Start automatic learning mode via SMS command INST000000␣063␣1
3. Enter Keycard numbers manually via mini USB cable (SERA2 software).
4. Start automatic learning mode remotely via SERA2 software.

If you want to edit existing configuration,

- Read configuration press [Read]
- Edit settings
- Write edited configuration press [Write]

Start automatic learning mode via mini USB cable (SERA2 software).

Go to SERA2> System Options> General system Options.
Select Dallas 1- Wire Bus (for iButton keys)
Press [Write]
Press [Start iButton/ RFID/ Phone programming mode]
Go to SERA2> Users/ Access control window.
Touch RFID keycards, iButton keys to the reader.
RFID keycard, iButton key numbers will appear in the list.
Go to System Options> General system Options and
To finish press [Stop programming]
Edit additional setting in the Users/ Access control window.
Press [Write]
Go to RT Testing & Monitoring> Hardware.
Press [Start Monitoring]
Go to RT Testing & Monitoring> Security Alarm Panel/ Access



Start the automatic key programming mode by SMS command

Send SMS message: INST000000␣063␣1
You will receive the message: iButton/RFID/Caller ID Learning Mode is Switched ON
Touch RFID keycards to the RFID reader.
Sent the message: INST000000␣063␣0
You will receive the message: iButton/RFID/Caller ID Learning Mode Stopped

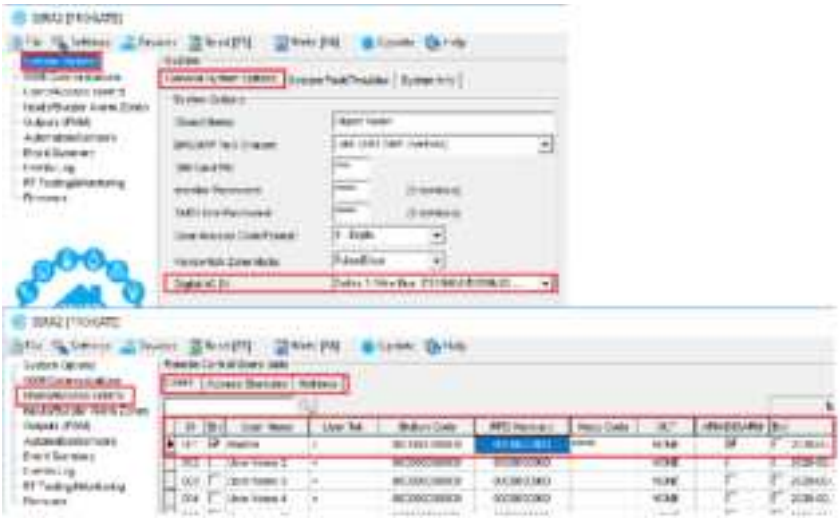
INST000000␣063␣S
INST = Install. Configuration of the parameters.
000000= Installer's password
␣= Space character
063= command code (iButton keys learning/deleting mode)
␣= Space character
S=iButton keys entering/deletion mode.
- 0- Disable iButton keys learning mode,
- 1- Enable iButton keys learning mode,
- 2- iButton keys deleting mode,

Delete these keys from memory, which will be touched to the reader.

!	**Before activating the RFID learning mode via SMS, the module must have the appropriate System Options> General System Options settings**

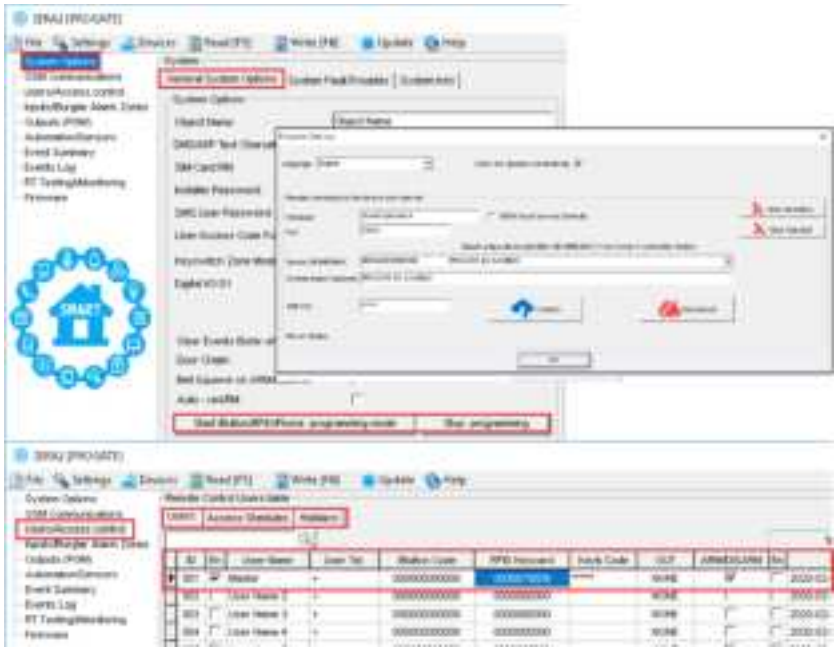
Enter Keycard numbers manually via mini USB cable (SERA2 software).

Go to SERA2> System Options> General system Options.
Select Dallas 1- Wire Bus (for iButton keys)
Press "Write"
Go to SERA2> Users/ Access control.
Enter RFID keycard, iButton key numbers
Edit other settings
Press "Write"
Go to RT Testing & Monitoring> Hardware
Press "Start Monitoring"
Go to Security Alarm Panel/ Access"
Touch the keycard to the RFID reader and iButton keys to the probe



Start the automatic key programming mode remotely via SERA2 software.

Start SERA2 software
Press "Connect remotely" button
Enter required parameter.
(Default App Key is 123456)
Press "Connect"
Go to SERA2> System Options> General system Options.
Select Dallas 1- Wire Bus (for iButton keys)
Press “Write”
Press "Start iButton/RFID/Caller ID Learning Mode"
Touch RFID keycards, iButton keys to the reader
Press "Stop programming" button
Or wait until the learning mode will stop automatically



Refer to: Users & Access Control programming details.

5 OUTPUTS

The module PROGATE has:

- 1 **RELAY** output.
- 2 open drain **I/O1** and **I/O2** (1A/30V).
- 1 output: **1W** (10mA, Max Voltage 3,3V) for LED, solid state relays control. ! Max voltage 3,3V
- All outputs can be controlled via short call DIAL, SMS message, RFID, iButton and SERANOVA app. This feature may be used for gate opening
- Automatic Schedules, holidays
- Programmable algorithms for outputs operation: Access Control /CTRL/SMS/DIAL, SIREN, BUZZER, ARM state, Zones OK, Light Flash, inverting, pulse mode

The output toggles to its set up state when a specific event has occurred in the system. The output can be used to open/ close garage doors, activate lights, heating, watering and much more.

If the output is not in used, it must be disabled. Once the output is disabled, it can no longer be turned ON or OFF unless it is enabled again.

It is possible to instantly turn ON an individual output for a determined time period and automatically turn it OFF when the time period expires.

5.1.1 Output PGM wiring. Bell, Relay, Led Wiring

Output switch to ground when activated from the module. Connect the positive side of the device to be activated to the VD+ terminal. Connect the negative terminal to the selected output.

1. Connect devices to the selected outputs as shown in the figures below. For sound signaling we recommend to use siren DC 12V up to 1500mA. It is recommended to connect the siren to the system by using 2 x 0,75 sq. mm double insulation cable. Auxiliary BUZZER is recommended to be installed inside the premises not far from the entrance. Buzzer operates together with the main siren also when the system starts calculating the time to leave the premises and the time till alarm response of the security system after entering the premises (see clause 7.1). It is possible to use buzzer of hit point PB12N23P12Q or similar modified piezoelectric 12V DC, 150mA max Buzzer.

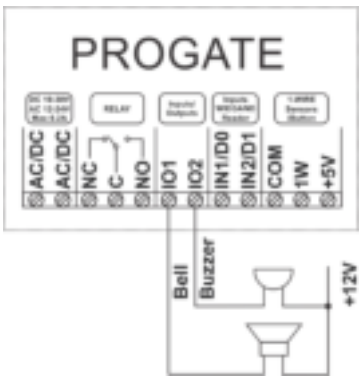


Figure 15 Bell, buzzer connection to I/O1, I/O2

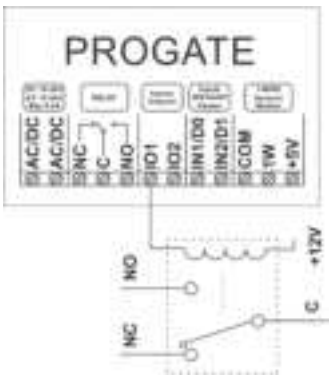


Figure 16 Relay connection to , I/O1, I/O2

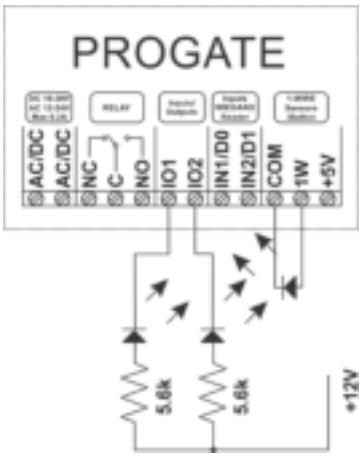


Figure 17 LED connection toI/O1, I/O2

Output mode: timer, steady, pulse count.

The output action can **automatically switch ON or OFF under the following conditions:**

- **System armed or disarmed, -**
- **Alarm begins or stops, -**
- **Temperature falls below the set MIN value,**
- **Temperature rises above the set MAX value,**
- **Zone violated, Zone restored.**

The user can also set a custom text, which will be sent by SMS text message to user phone number when the automatic PGM output action is carried out.

Set output's parameters step by step:

1. Open SERA2 > Device >PROGATE> Outputs
2. Enter the required parameters.
3. If the output is not in used, it should be disabled
4. Press "Write" icon.

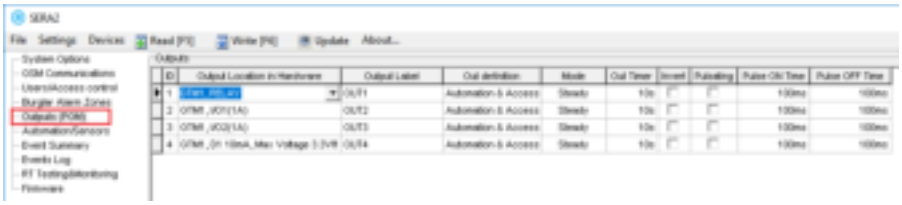


Figure 18Outputs (PGM) window

If you want to edit existing configuration,

- You have to read it (press "Read" in the command line)
- Edit settings
- Write edited configuration (press "Write" in the command line)

5.1.2 Output programming

Quick start outputs

1. Install SERA2 software. For more information look at
1.
2. Connect the module to the computer via mini USB cable. Device> PROGATE
3. Go to Outputs (PGM) window in the SERA2 software
4. Parameters of the selected output should be set:

output operation description (OUT definition): disable, bell, buzzer, flash, system state, ready, automation/ CTRL, AC OK, battery OK, ARM/ DISARM, alarm indication, lost primary channel, lost secondary channel, fire sensor, RH sensor trouble.

5. State type: flash, timer, steady mode.
6. If necessary output operation might be inverted.
7. Write configuration by pressing write icon

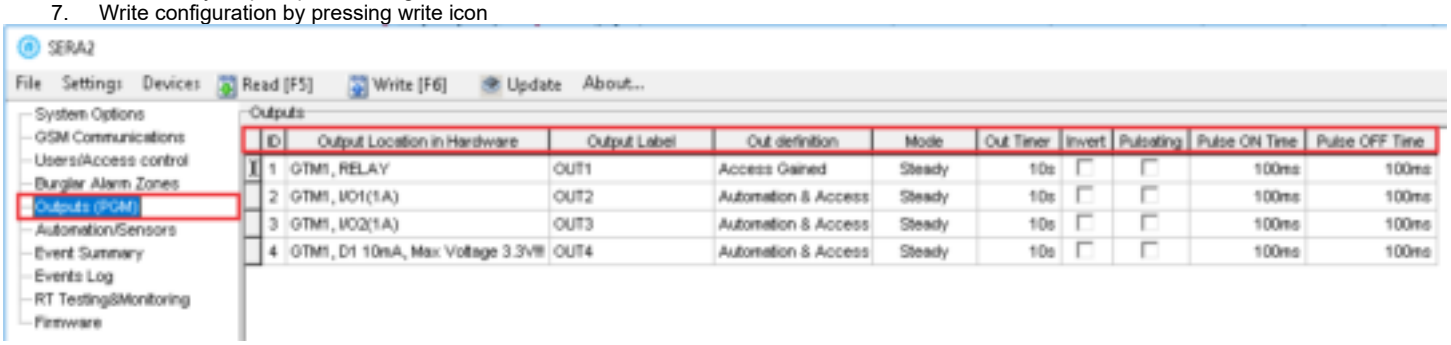


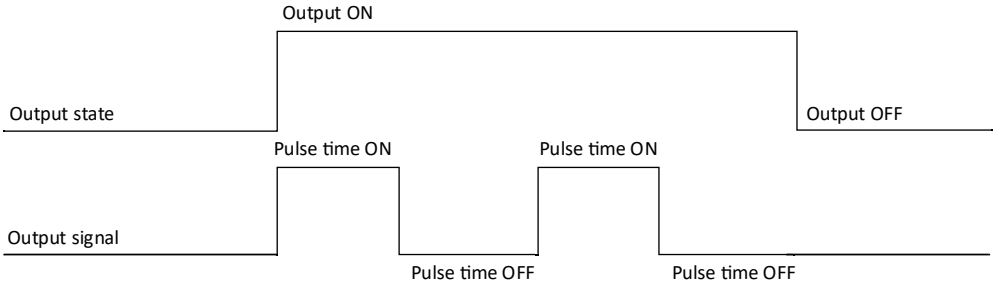
Figure 19 Outputs (PGM) window

If you want to edit existing configuration,

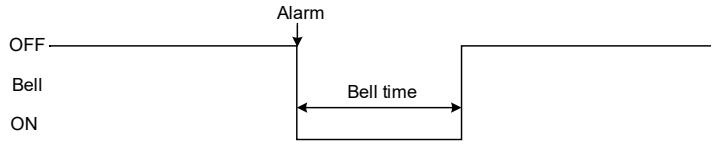
- You have to read it (press “Read” in the command line)
- Edit settings
- Write edited configuration (press “Write” in the command line)

Outputs can be set as timers.

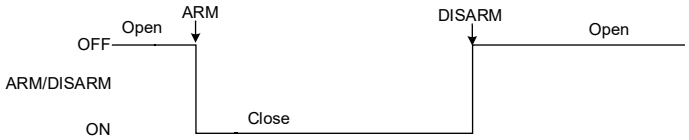
1. When output is activated for “Out Timer” time interval,
2. Relay contact start changing state from ON (pulse time ON) to OFF (Pulse time Off)
3. This cycle will repeat until output is deactivated.



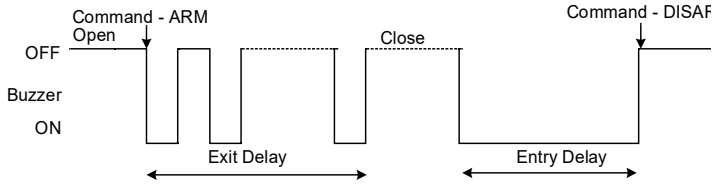
Bell: Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.



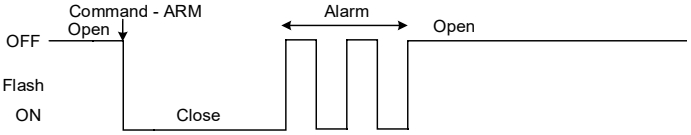
ARM/DISARM: Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.



Buzzer: Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.

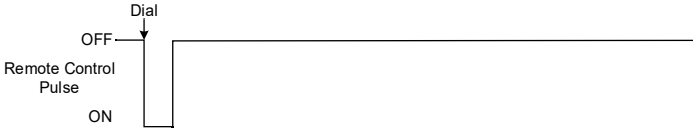


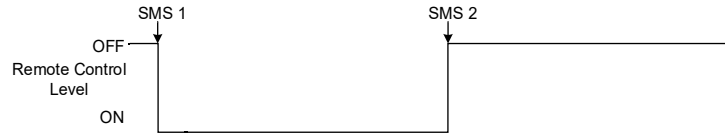
Flash: Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



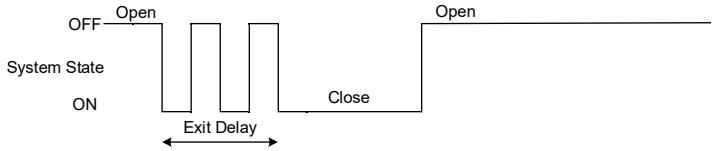
Remote Control: Output designed for connection of electrical devices which will be controlled by SMS message or phone call a) control by SMS message

Remote Control b) control by phone call

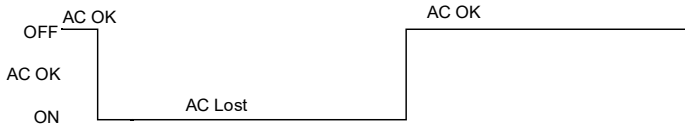




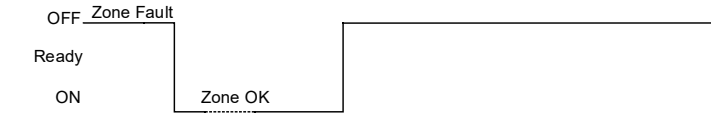
System State: Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.



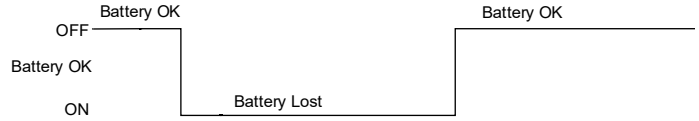
AC OK: Output for connection of indicator about control panel supply from alternating current



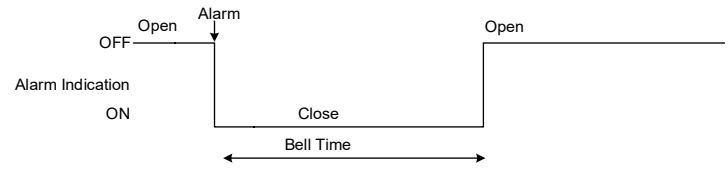
Ready: Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.



Battery OK: Output for connection of indicator about control panel supply from battery.

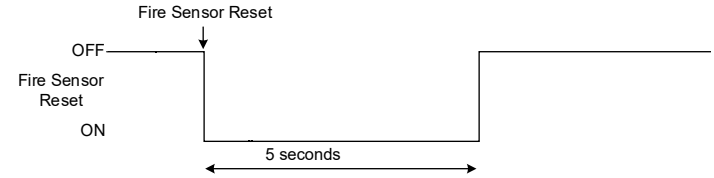


Alarm indication: Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.

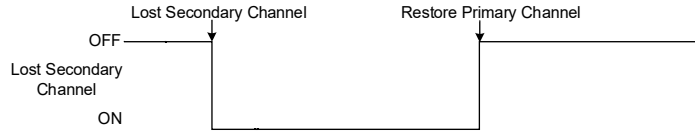


Lost Primary Channel: Output where a continuous signal is generated when communication with primary channel was lost.

Fire Sensor Reset: Output for reset of fire sensor operation. Its status changes 5 sec. and returns to the initial one.



Lost Secondary Channel: Output where a continuous signal is generated when communication with secondary channel was lost.



5.1.3 Access control output with logging

If you want to edit existing configuration,

- You have to read it (press “Read” in the command line)
- Edit settings
- Write edited configuration (press “Write” in the command line)

Set output definition to [**Access Gained**] . SERA2>Outputs

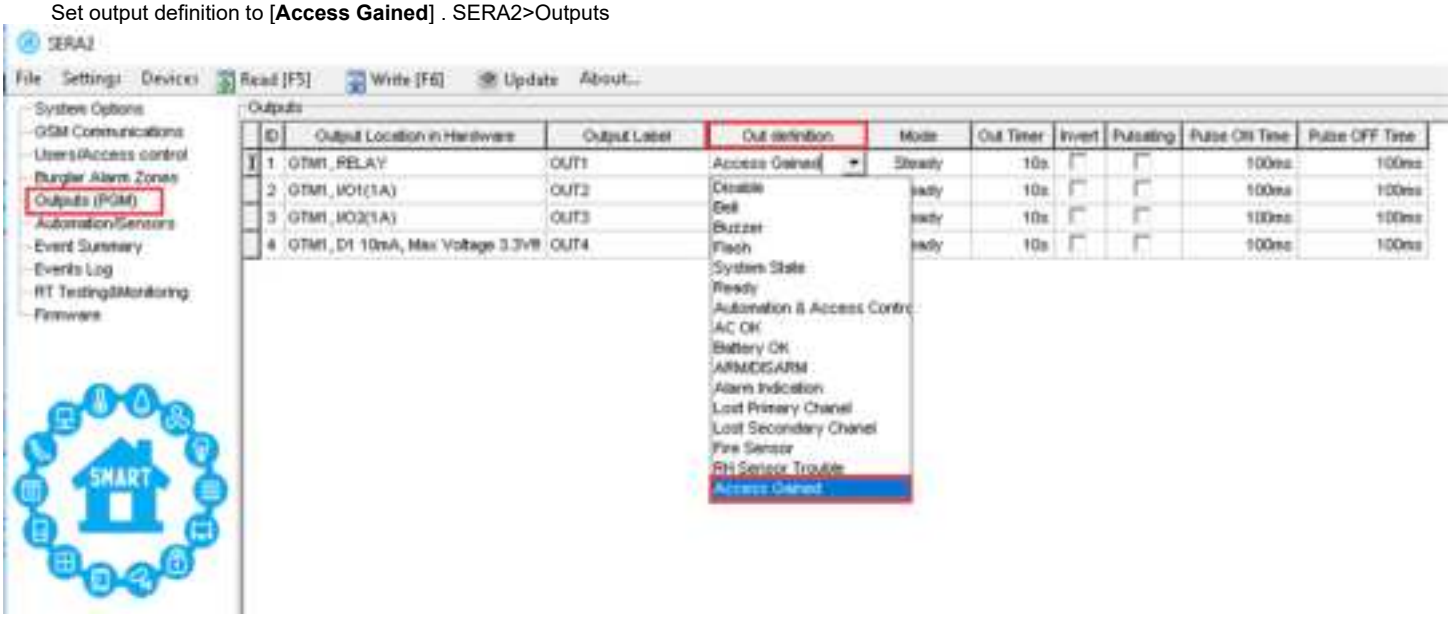


Figure 20Outputs (PGM) window

This output could be controlled as fallowing:

- **If the user has right to ARM/DISARM system, it always has access to this output.**
- **If the user has not the right to ARM/DISARM the system** (field near ARM/DISARM is not marked (SERA2> User/ Access control)), **the user can access this output only if system is Disarmed.**

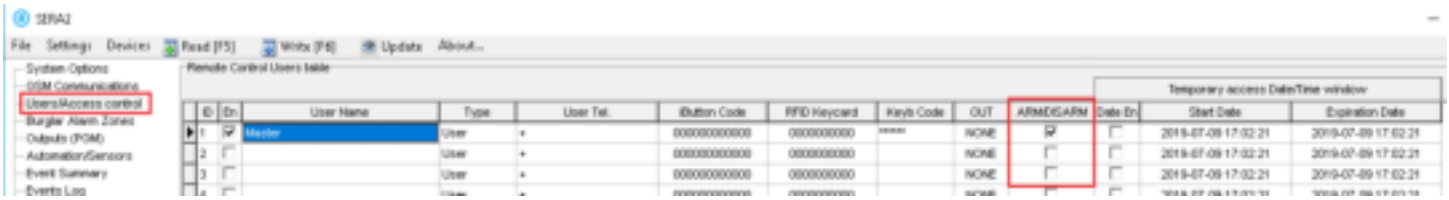


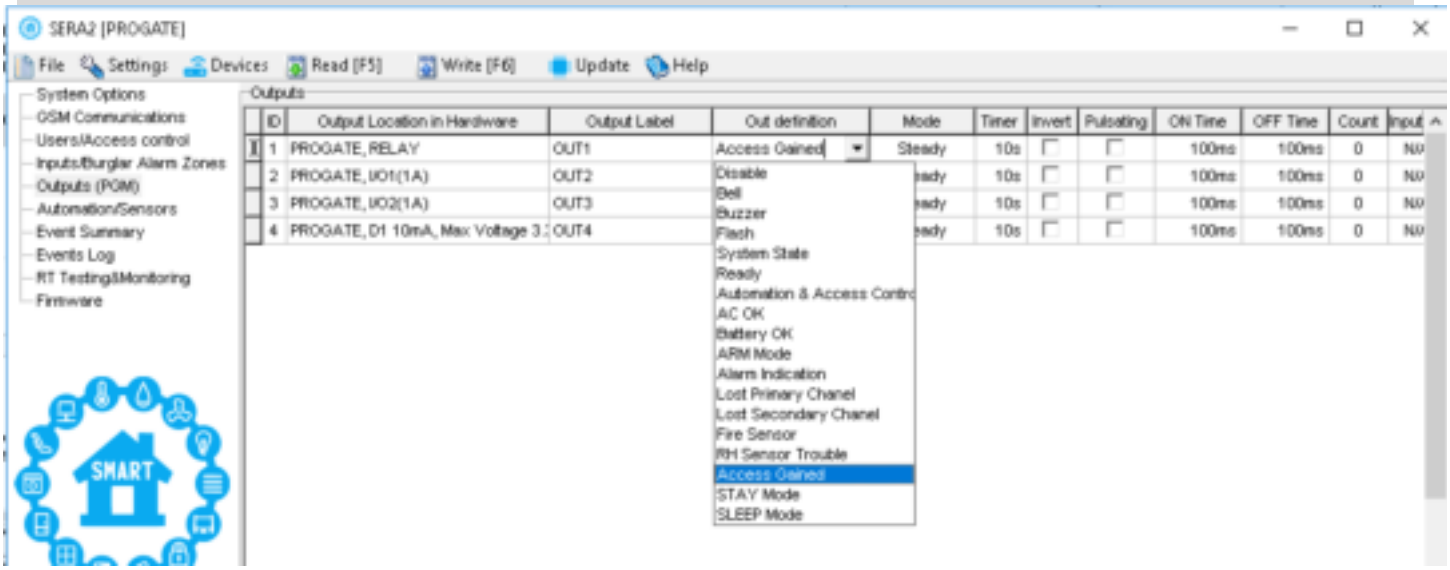
Figure 21User/ Access control window

- If access is granted by user, 421 event Access granted is stored into the log. If not Access denied event 422 is stored to the log (SERA2> Events Log)
- if output will have definition [**Automation / CTRL**] it also can be controlled by user in any way but it will not generate 421 and 422 events

Event log e.g.

1853	Event:1234:1:401:01:001	Time:2017-08-20 14:42:36	Note: , Open by User, User:001, Name:Master
1852	Event:1234:1:422:00:001	Time:2017-08-20 14:41:41	Note: , Access Gained by, User:001, Name:Master
1851	Event:1234:1:406:01:001	Time:2017-08-20 14:41:27	Note: , Cancel, User:001, Name:Master

Outputs can be controlled in Outpus> Out definition> select “Access Gained”



8. If you need to control outputs by short call or SMS, go to SERA2> Users/ Access control window and enter phone numbers of users, who will be able to control selected outputs via free short call.
9. Write configuration by pressing [Write]

Figure 22Users/ Access control window

- In order to control big power alternating current equipment, it is comfortable to use solid state relays.
  Refer to: Outputs. Bell & PGM programming

6 INPUTS

The module PROGATE has:

- 2 analog inputs (In1, .In2 (0-30V)) for analog sensors connection. Or can be used as security system‘s zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- 2 programmable analog inputs (I/O1, I/O2(0-30V) for analog sensors control or using as security system‘s zone with selectable type: NC/NO/EOL/EOL+TAMPER
  Wiegand interface, RFID reader, Keyboard.

- 1 programmable digital inputs (D1(Max voltage 3.3V)) used for:
  - Dallas 1-Wire Bus. To connect temperature sensors DS18b20 or iButton key DS1990A,
  - Aosong 1-Wire bus Humidity Sensor AM2302, DHT22, AM2305, AM2306,

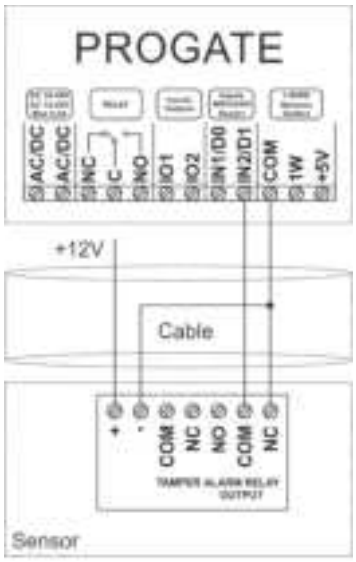
6.1 Input / zones wiring EOL NO NC

The module PROGATE has:

- In1, In2, I/O1, I/O2 Can be used as inputs to detect Gate position or security system‘s zones with selectable type: NC/NO/EOL/EOL+TAMPER.

It is recommended to use standard motion, fire, and glass breaking sensors. For powering of sensors we recommend to use standard 6-8 wires cable for, designed for installation of security system.

- Connect sensors to module the as is shown in connection diagrams below
- Set the required parameters
- Write configuration by pressing [Write] button



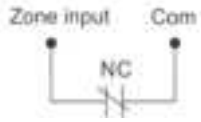


Figure 23NC Contacts, No EOL

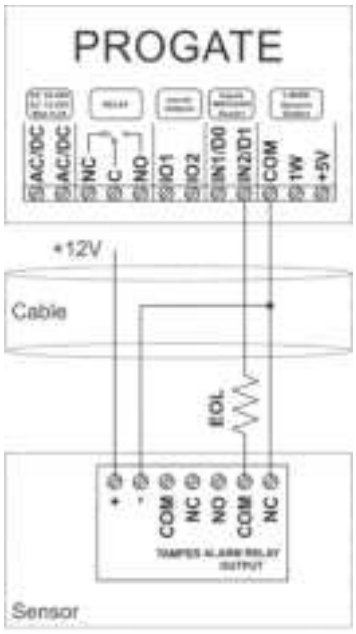
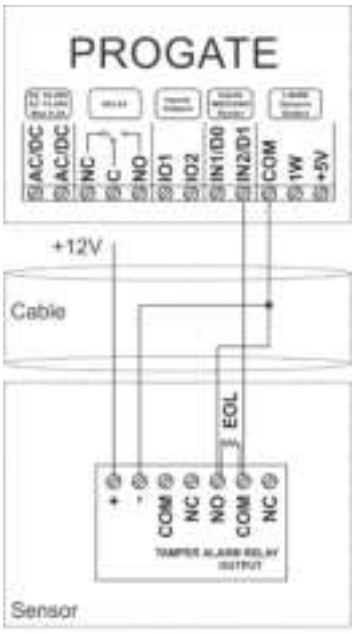


Figure 24 NC, With EOL



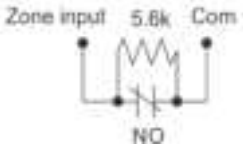
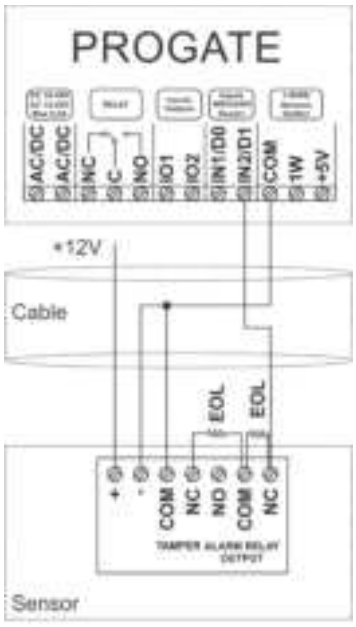


Figure 25 NO, With EOL



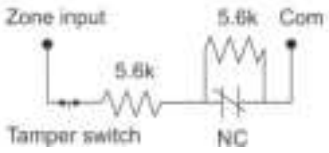


Figure 26NC With EOL Wire Fault Recognition

All inputs has pull up resistors 10k

Refer to: Zones programming

7 SERA2 configuration software

In order to configure and control the system by SMS text message, send the text command to the PROGATE phone number from one of the listed user phone numbers. More

SERA2 software configuration tool is intended for the module PROGATE configuration locally via USB port or remotely via GPRS network. This software simplifies system configuration process by allowing to use a personal computer in the process.

We recommend programming the module PROGATE with SERA2 software

2. Open the folder containing installation of the software SERA2. Click the file „SERA2 setup.exe“
3. If installation directory of the software is OK, press [Next]. If you would like to install the software in the other directory press [Change], specify other installation directory and then press next>.
4. Check if the correct data are entered and press Install
5. After successful installation of the software SERA2, press [Finish]

Start the software SERA2. Go to „Start“> „All programs“> „SERA2“> „SERA2 “

Or go to installation directory and click „SERA2.exe“.

Figure 27Sera2 software

Connection of the module to your PC

Power supply: DC 10-33V, AC 12-24V, Max 0.2A. The module should have inserted SIM card (with replenished account and removed PIN CODE REQUEST). Module must be connected to the PC via mini USB cable

Work with the software SERA2

If you are sure that the module is fully connected to PC and power supply, please go to Devices > PROGATE

Figure 28 Command line

Each time after configuring the module press Write 5 icon thus the software SERA2 will write configuration changes into the module! Wait until progress bar line will indicate that the configuration has been written successfully

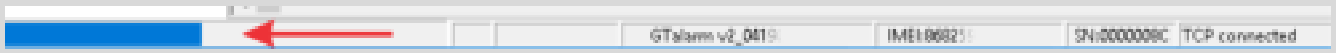


Figure 29 Progress bar

After configuration of the module, all settings may be saved at PC. It enables to save time, when next time the same configuration will be used – it will not be necessary again to set the same parameters. If you want to save that is already recorded by the module, firstly you must read configuration of the module**. Press Read 4 icon. In order to save configuration go to File 1 then press "Save As" or "Save".** Enter configuration parameter in the displayed table and press „OK“

In order to start saved configuration go to File then press Open. It allows to copy the same programmed content into as many modules as required.

If you want to receive software updates, go to Settings and mark "Check for Updates Automatically". When new update will be available, the program will inform you, and you have to start the update. After that you have to connect the module to the computer via mini USB cable. You have to write this update to the module PROGATE by pressing "Update" in the bottom line in SERA2 software.

Figure 30Go to „Update“ in the command line

If you want to update the module manually, got "Update" in the command line

If you need to contact the seller with the questions about the configuration, you have to:

Press "Read" icon first to read the configuration from the module, the press "File>Save us" and save the configuration.

Save the Events Log file and send these files with the question to the seller.

These steps will let better understand the problem and will reduce the time to find the solution.

Figure configuration at the same time 31Unlimited number of modules

An unlimited number of modules can be configured remotely on the same computer at the same time. The configuration reading and writing speed does not decrease because the processes are running in parallel. Many SERA2 programs could be opened and used at the same time.

7.1 General system options programming

The module can send a trouble report and restrict arming if some of selected troubles [Restrict ARM] exist during close event.

System Options > General system Options

The general system options settings let you control system options, system general settings, systems timers, let you program iButton keys and reset the module.

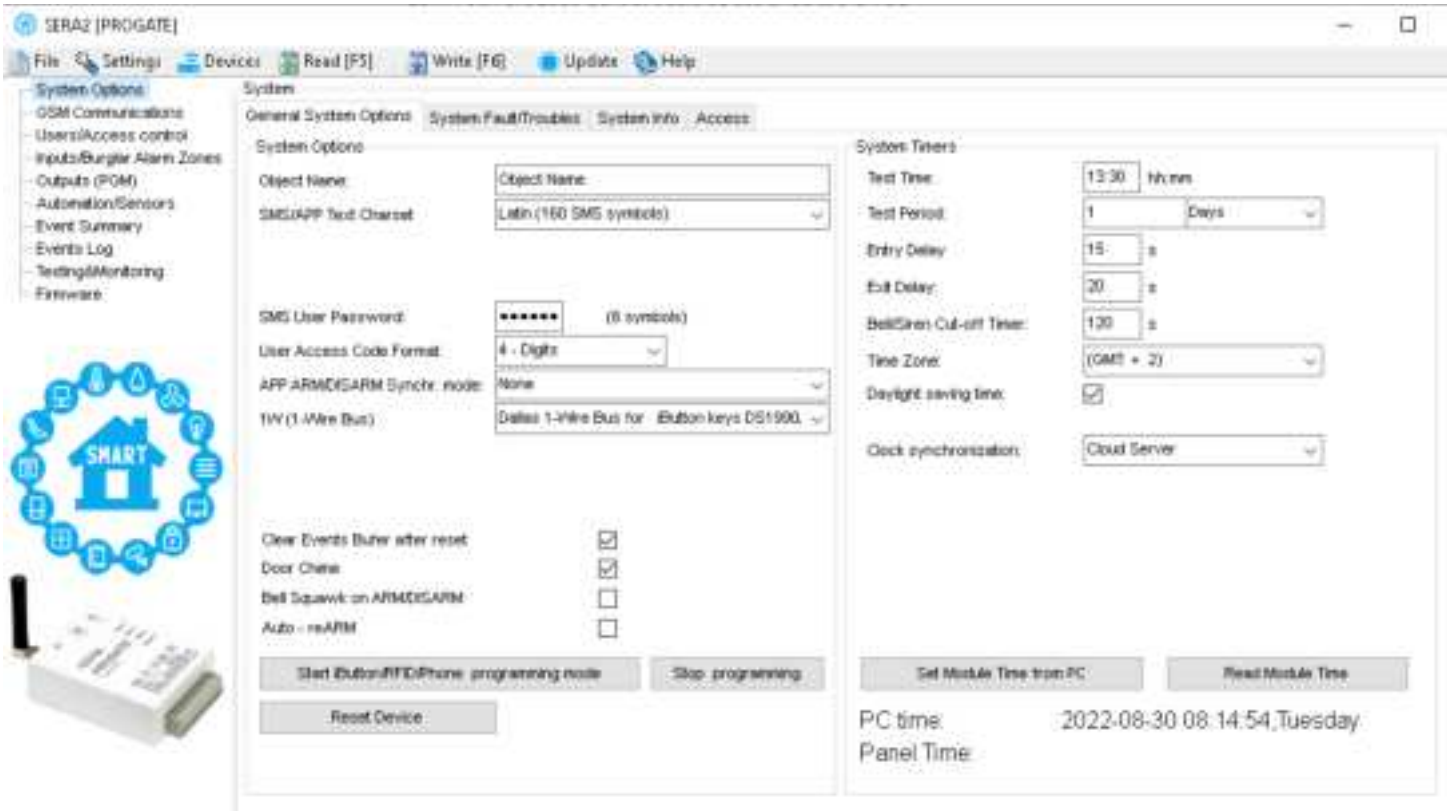
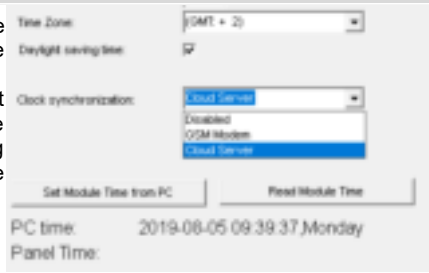


Figure 32The example of System Options > General system Options window.

1	**Object Name**	
2	**SIM Card PIN**	SIM card PIN code. Default 1234
3	**Installer Password**	The default installer password is **000000**. This password allows you to enter programming mode, where you can program all features, options, and commands of the module.
4	**SMS User Password**	The default SMS User Password is **123456**. This code allows you to utilize arming method, as well as program user codes.
5	**User Access Code Format**	A 4-digit or 6-digit user access code format can be selected.
6	**I/O1 Settings**	2-Wire Smoke detector (Fire current loop) **or** 0-10V Analog Input (Zone or Sensor) **or** Output **or** – 0-20mA, 4-20mA Current Loop Sensor could be assigned to the I/O1
7	**I/O2 Settings**	2-Wire Smoke detector (Fire current loop) **or** 0-10V Analog Input (Zone or Sensor) **or** Output **or** – 0-20mA, 4-20mA Current Loop Sensor could be assigned to the I/O2
15	**0-10V Analog Input (Zone or Sensor)**	0-10V Analog sensors will be connected to the input
16	**Output**	Input will be used as output
17	**2-Wire Smoke Detector (Fire current loop)**	2-Wire Smoke detectors will be connected t the input.
18	**0-10mA, 4-20mA Current Loop Sensor**	0-20mA, 4-20mA Current Loop Sensors will be connected to the input.
8	**Clear Event Buffer After Reset**	When the cell is checked, the memory of unsent reports will be deleted after the module resetting
9	**Door Chime**	When this box is checked, violations of set Delay zones at the alarm turned off will be accompanied by keyboard audible (Buzzer) signal
10	**Bell squawk on ARM/ DISARM**	The module can activate the bell output briefly causing the squawk to alert users that the module is being armed, disarmed or that an Entry or Exit Delay was triggered. Enable or disable the desired option.
11	**Auto re-ARM**	The module can be programmed to arm the module if there is no activity in the area after the system disarming.
12	**Start iButton/RFID programming**	All added iButton keys or RFID cards will be registered in the order of sequence by clicking Start programming
13	**STOP iButton/RFID programming**	To finish entering iButton keys or RFID cards, click Stop programming button
19	**Test Time**	Auto Test report time of day
20	**Test Period**	Auto Test report period
21	**Entry Delay**	This delay gives you time to enter the armed premises and enter your code to disarm your system before the alarm is triggered.
22	**Exit Delay**	The system will trigger the Exit Delay Timer to provide you with enough time to exit the protected area before the system is armed.
23	**Bell/ Sirel Cut – off Timer**	Duration of audible signal (sirens, Bell) after the alarm system activated. Time shall be written in seconds, duration from 0 to 9999.
24	**Time Zone**	
25	**Daylight saving time**	
26	**Set module time from PC**	To set the clock click Set time from PC button and the clock will be set using computer's clock.
27	**Read module time**	To read the clock of panel.
28	**PC Time**	
29	**Panel Time**	
14	**Reset Device**	Reset module command

Figure 33Explanation of every field in "General System Options" window

7.2 How to set clock synchronization?



The system comes equipped with internal real-time clock (RTC) that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly.

SERA2 software provides the ability to select the Time Zone and The user may also choose Set module time from PC, which instantly provides the exact PC time. When the system is connected to the monitoring station via IP connection the date and time will be automatically synchronized with the monitoring station. It is possible to select automatically time synchronization with: GSM Modem, Cloud Server or disable it.

If the module has been connected first time to the power supply, or power supply has been disconnected for a long time, the time of the module should be set again by auto synchronization or manually.

System clock can be synchronized in following ways:

1. **Cloud Server**. Synchronize by [SERA Cloud Service]. SIM card must have mobile data and [SERA Cloud Service] must be enabled.
2. **GSM Network (Local time).** Select this if cellular network provides local time format.
3. **GSM Network (GMT).** Select this if cellular network provides GMT time format.
4. **Disabled**. If you want to set time manually.

If the date and time of events and SMS messages received are incorrect, you need to set correct way of the clock synchronization.

Clock synchronization via GSM modem

- Go to SERA2> System Options> General System Options
- Set Clock synchronization via GSM modem
- Press “Write” in the command line

Figure 35 SERA2> GSM Communication> SERA Cloud Service

- Go to SERA2> System Options> General System Options
- Set Clock synchronization via Cloud Server
- Press “Write” in the command line

Figure 34SERA2> System Options> General System Options

Clock synchronization via Cloud server

- Go to SERA2> GSM Communication> SERA Cloud Service
- Enable SERA Cloud Service

Figure 36 SERA2> System Options> General System Options

7.3 System Fault/ Troubles Programming

System Options > System Fault/ Troubles	The System Fault/ Troubles settings let you set the communication options if the trouble occurs and let you set system voltage loss and restore options.

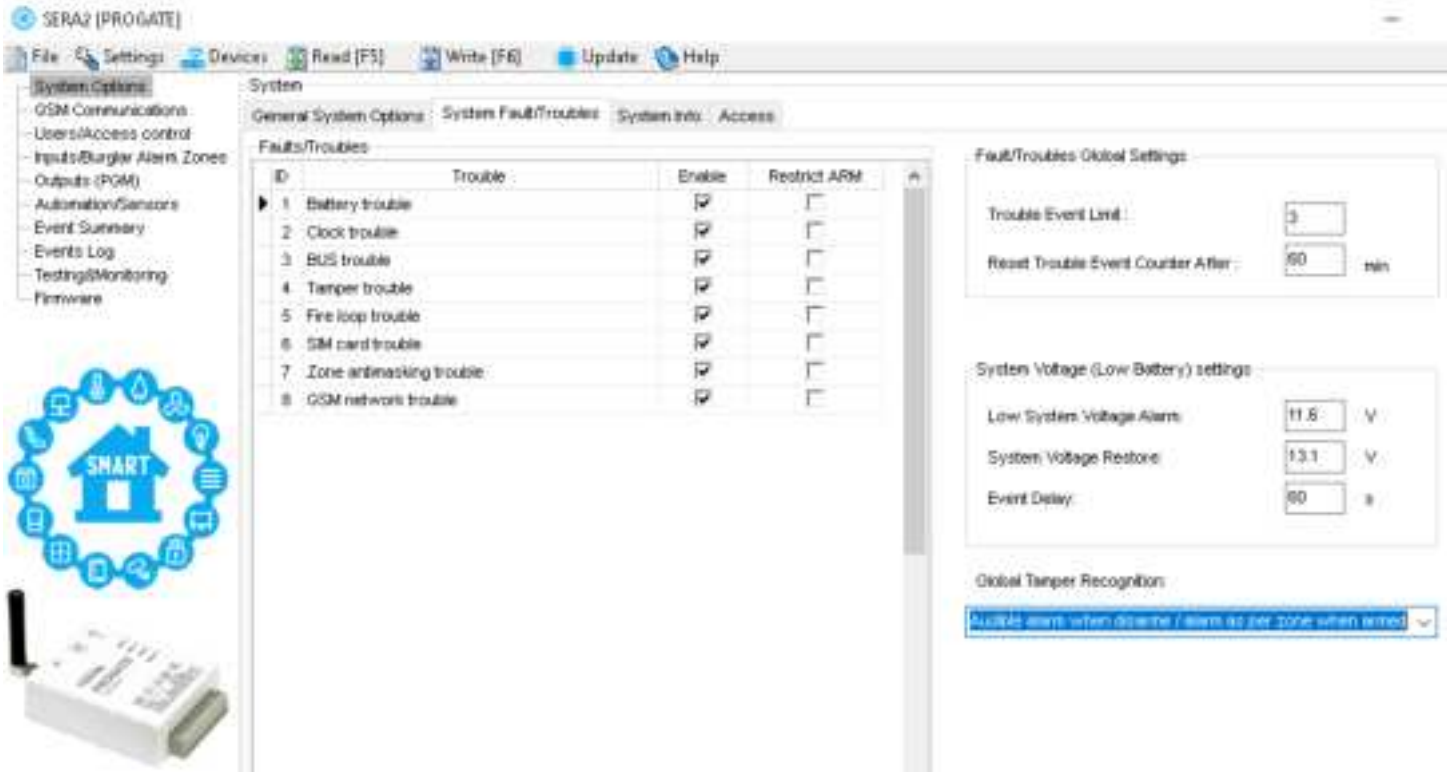


Figure 37 System Options> System Fault/ Troubles window

1	**Trouble**	This column lists potential system troubles
10	**Enable**	The system will detect a marked trouble
11	**Restrict ARM**	In case of such trouble, the arming activation will be restricted.
2	**Battery trouble**	Low system voltage. Power supply or backup battery voltage is low, needs to be recharged, or replaced.
3	**Clock trouble**	The time and date has not been set.
4	**BUS trouble**	The expansion device is no longer communicating with the module.
5	**Tamper trouble**	The zone(s) that was tampered
6	**Fire loop trouble**	The trouble is occurring with your smoke detectors.
7	**SIM card trouble**	Not available or impossible to read SIM card.
8	**Zone ant masking trouble**	Do not available in this module
9	**GSM network trouble**	SIM card is not registered with the GSM network provider
12	**Low System Voltage Alarm**	The module has detected a low voltage. This means that your system is running on the backup battery and voltage is dropped below allowed value.
13	**System Voltage Restore**	The module has detected that the system voltage has been restored.
14	**Event Delay**	System low voltage trouble event report delay.
15	**Trouble Shutdown**	Setting of the allowable number of the same trouble event, where in case of excess of such number the trouble reporting will be off. The number of such events is counted until the arming mode is changed (On/Off).
16	**Global Tamper Recognition**	How the control panel will operate after tamper recognition 18 **Tamper Disable** The module will not generate an alarm or trouble. 19 **Trouble when disarmed / alarm as per zone when armed** When disarmed: Generates Trouble Only The module transmits the defined report code. When armed: Follows Zone Alarm Type 20 **Trouble always** Generates Trouble Only (when armed or disarmed) 21 **Audible alarm when disarmed / alarm as per zone when armed** When disarmed: Generates Audible Alarm The module transmits the defined report code and generates an audible alarm. When armed: Follows Zone Alarm Type The module follows the zone's alarm type.

Figure 38Explanation of every field in "System Fault/Troubles" window

The module can send a system voltage alarm and restore events. It is possible to enable or disable the zone tamper tracking and to set how the module will operate after tamper recognition.

7.4 Zones programming

Detection devices such as motion detectors and door contacts could be connected to the module's zone terminals. Once connected, the associated zone's parameters must be configured.

PROGATE comes equipped with 2 on-board wired zones and 2 programmable I/O inputs.

Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored.

Stay mode allows the user to arm and disarm the alarm system without leaving the secured area. If the zones with Stay attribute enabled are violated when the system is STAY-armed, no alarm will be caused. Typically, this feature is used when arming the system at home before going to bed.

The system can be STAY-armed under the following conditions: If a Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exists, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay.

The difference between stay and sleep zone types: "stay" zone type has delay zone timeout, in "sleep" zone type delay zone becomes instant

The system will NOT activate siren and keypad buzzer only when Instant, Silent zone types is violated.

Any Delay type zone will operate as Instant type zone when the system is armed in the Stay mode. When the system is fully armed, the Delay type zone will operate normally.

If the zone is not used, it must be disabled.

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren/bell and the keypad buzzer and send the SMS text message to the listed user phone number. The system will cause tamper alarm under the following conditions: If the enclosure of a detection device, siren/bell, metal cabinet or keypad is opened, the physical tamper switch will be triggered. If needed to get tamper alarms, the field near "Tamper Enabled", should be marked. In that case, all tampers and tamper alarm notification by SMS text message is enabled.

The system will NOT cause any tamper alarm regarding the physical tamper violation if the associated zone is disabled.

The figure below shows an example of zone operation with a 3-time alarm event limit:

- Zone alarm is generated 3 times.
- After 3 alarm events the zone is blocked (bypassed) till *Event Repeat Timeout* will end.
- After *Event Repeat Timeout* zone will activated again.

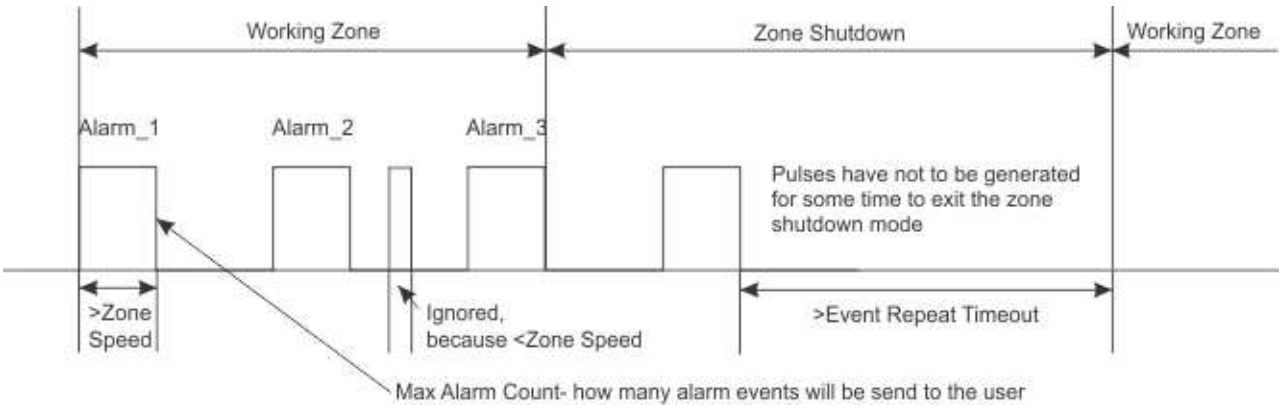


Figure 39the explanation of Zone Speed, Max Alarm Count, and Event Repeat Timeout

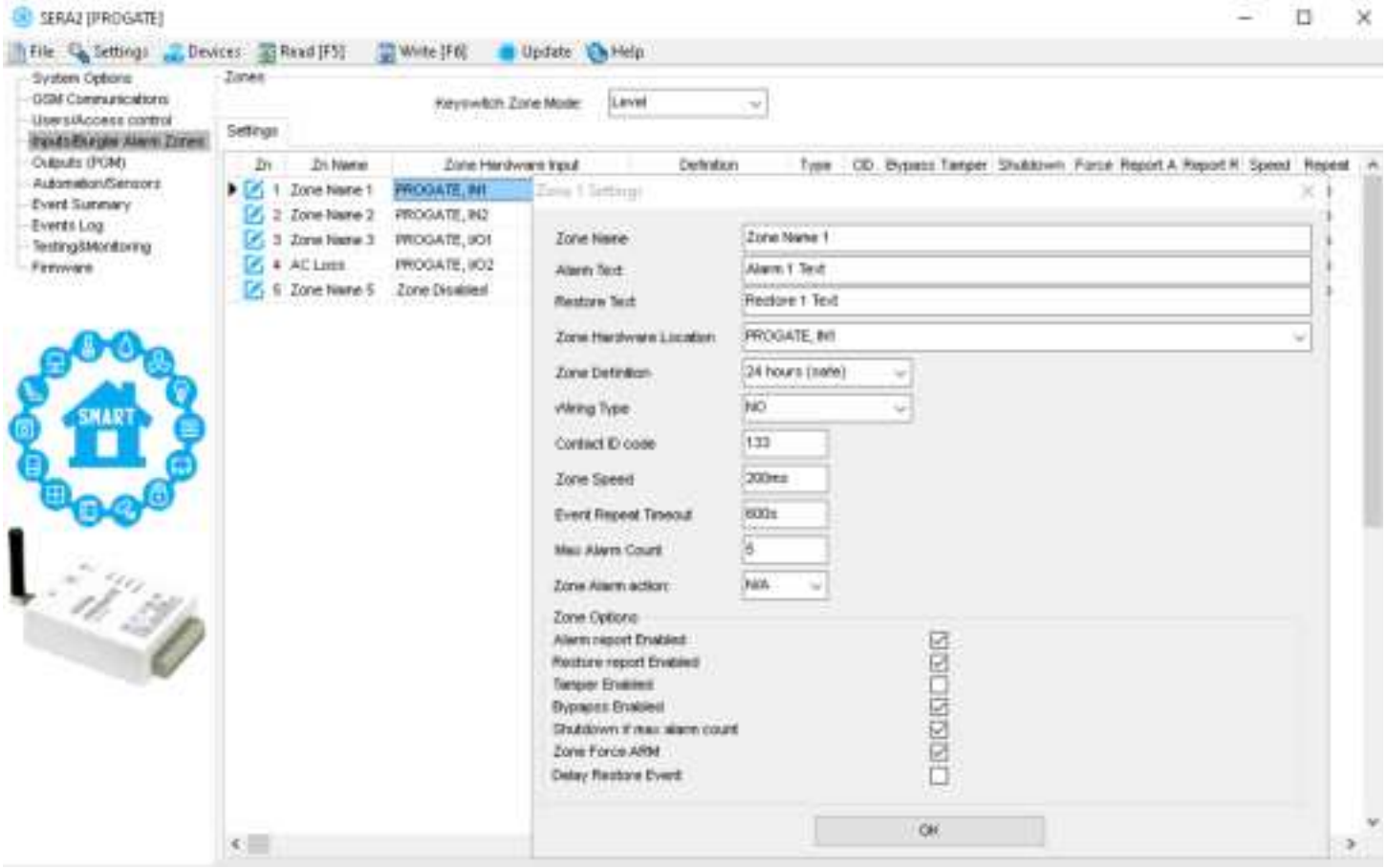


Figure 40the example of Double click on the required zone window

3	**Zone Name**	Zone name should be entered.
4	**Assign Module=** **Zone Hardware Input**	Select the zone hardware input **Zone Disabled** — Disables the corresponding zone. **, IN1…IN4** — The zone hardware input 1… input 4 assigned **, I/O1… I/O2** — The zone hardware optional Input/ Output 1… Input/ Output 2 assigned
5	**Zone Definition=** **Definition**	**Delay** — When armed, provides entry delay when violated. Recommended for door sensors. **Interior** — When armed, instant alarm will sound first if the zone is violated; instant alarm will follow the entry delay if entry delay is active. Recommended for motion sensor in front of the door. **Instant** — When armed, instant alarm when violated. **24 hours** — Instant alarm when violated, audible alarm at default not depending from ARM, DISARM modes. Recommended for safes, storehouses, tampers. **Silent** — Always active, not depending from ARM, DISARM modes. The sms will be send, but the siren will not be activated. Recommended for voltage, temperature control, AC mains failure control and for alarm of silent panic. **Fire** — Instant alarm and communication when violated not depending from ARM, DISARM modes. Siren signal with interruptions will be generated. Recommended for smoke, fire detectors. **ON/OFF** **Interior STAY** — Similar to 'Instant' except the module will auto bypass the zone if Armed in the Stay mode **Instant STAY** — Similar to 'Instant' except the module will auto -bypass the zone if Armed in the Stay mode
6	**Wiring Type= Type**	**EOL** — End of line resistor. Input type with resistor. **NC** — Normal Close. The alarm will be send when the circuit between input and ground (-V) will be broken. **NO** — Normal Open. The alarm will be send when the input will be connected with ground (-V)
7	**Contact ID code= CID**	The module supports Contact ID reporting. If any other data is programmed the module will automatically generate the reporting event when transmitting to the central station.
14	**Zone Speed= Speed**	The Input Speed defines how quickly the module responds to an open zone detected on any hardwired input terminal (does not apply to addressable motion detectors and door contacts).
15	**Event Repeat Timeout=** **Repeat**	Insensitive time to recurrent zone events
18	**Max Alarm Count=** **Alarm Limit**	When the particular number of zone events set has occurred, the other events of the same zone will not be responded for the time set in Event Repeat Timeout. After this time expired (or when disarmed), a new count of the number of zone events will be started.
12	**Alarm Report Enabled=** **Report A**	The system will report alarm event and log it to the event buffer
13	**Restore Report Enabled=**	The system will report restore event and log it to the event buffer

	Report R	
9	**Tamper Enabled= Tamper**	The system will detect a *tamper* condition with one or more sensors on the system
8	**Bypass Enabled= Bypass**	The system will allow zones to be Manually Bypassed.
10	**Shutdown if max alarm count= Shutdown**	The system will stop generating alarms once the **max alarm count** Limit is reached. It resets every time the system will be armed.
11	**Zone Force ARM= Force**	Only **force** zones can be bypassed when the module is Force armed. Fire Zones cannot be Force Zones.
19	**Zone Alarm Action= OUT**	determines which output will be activated

Figure 41Explanation of every field in "Zones" window

7.5 Outputs. Bell & PGM programming

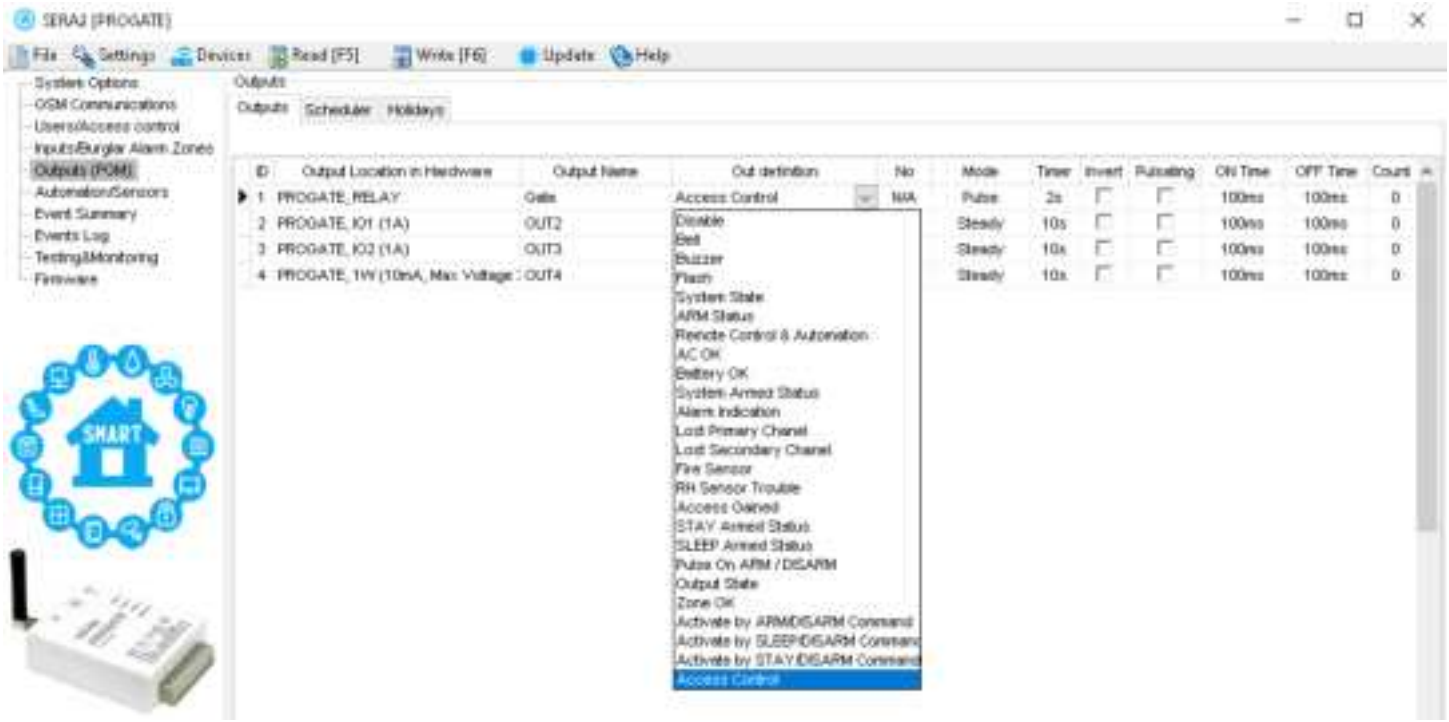
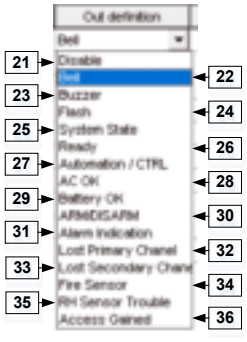


Figure 42The example of Outputs (PGM) window

1	**ID**	Output sequence number.
2	**Output Location in Hardware**	The outputs hardware location.
3	**Output Label**	Output name
4	**Out definition**	Selection of output operation mode.



21	Disable	Output disabled
22	Bell	Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.
23	Buzzer	Output for buzzer connection. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.
24	Flash	Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.
25	System State	Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.
26	Ready	Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.
27	Remote Control	Remote control by call mode is enabled. Output designed for connection of electrical devices which will be controlled by SMS message or phone call
28	AC OK	Output for connection of indicator about control panel supply from alternating current.
29	Battery OK	Output for connection of indicator about control panel supply from battery.
30	ARM/ DISARM	Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.
31	Alarm Indication	Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.
32	Lost Primary channel	Output where a continuous signal is generated when communication with primary channel was lost.
33	Lost secondary channel	Output where a continuous signal is generated when communication with secondary channel was lost.

		34 Fire Sensor Reset	Output for reset of fire sensor operation. Its status changes 5 sec. and returns to the initial one.
		35 RH Sensor Trouble	Output for RH Sensor trouble operation. In this mode output can automatically reset Humidity sensor if trouble occurs.
5	**Mode**	Output control mode. 36 Steady 37 Timer	Steady ON/OFF mode Output ON pulse mode
6	**Out Timer**	Pulse time duration can be from 1 to 999999 sec.	
7	**Invert**	Inversion is activated	
8	**Pulsating**	Pulsating mode is activated. Then output is activated it will pulsate according pulse ON/OFF time.	
9	**Pulse ON Time**	Pulsating mode pulse ON duration.	
10	**Pulse OFF Time**	Pulsating mode pulse OFF duration.	

Figure 43Explanation of every field in "Outputs" window

7.6 Users & Access Control programming details.

Users/ Access Control > Remote Control Users Table

The Users/ Access Control Table window let you set remote control options.

The system supports up to 800 user phone numbers for remote control purpose. When the phone number is set, the user will be able to arm/disarm the system and control outputs via SMS text messages and free of charge phone calls as well as to configure the system by SMS text messages. By default, the system accepts incoming calls and SMS text messages from any phone number. Once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number.

The module can be controlled only by these users, whose phone numbers entered in the memory of the module

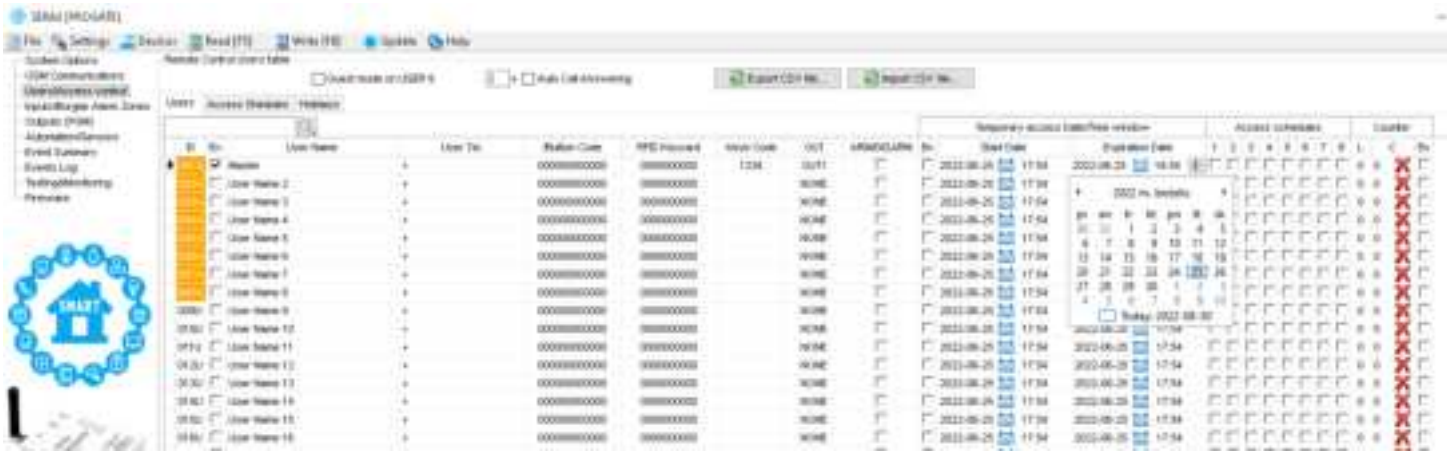


Figure 44 Users/ Access control window

1	**ID**	
2	**User Name**	The name of users who will be able to control the module should be entered in this column.
3	**User Tel.**	Telephone numbers of users who will be able to control the module by dialing should be entered in this column. User number should be entered with international code.
4	**iButton Code**	iButton Maxim iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000
5	**RFID Keycard**	RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
6	**Keyb Code**	Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
7	**OUT**	The selected input will be switched, if a user will call from this number. Preferred input may be assigned to each user's number. Thus different users are able to control different objects.
8	**ARM/DISARM**	If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
9	**MIC**	If checked, by calling from the specified phone, the controller responds and you can hear what's going on in the premises

Figure 45Explanation of every field in "Users & Remote Control" window

The PROGATE controls access by using schedules. Inputs, outputs, readers and cards through access levels are all configured with schedules by which they will be energized or de-energized, enabled or disabled. For example, you might assign an output to be energized from 12:00 a.m. to 6:00 a.m. every day. The 12:00 a.m. to 6:00 a.m., Monday through Sunday, time period is called a schedule. The "Access Schedules" tab enables you to create the schedule you will use to configure your PROGATE module. Click "Access Schedules" tab to display the Schedules screen:

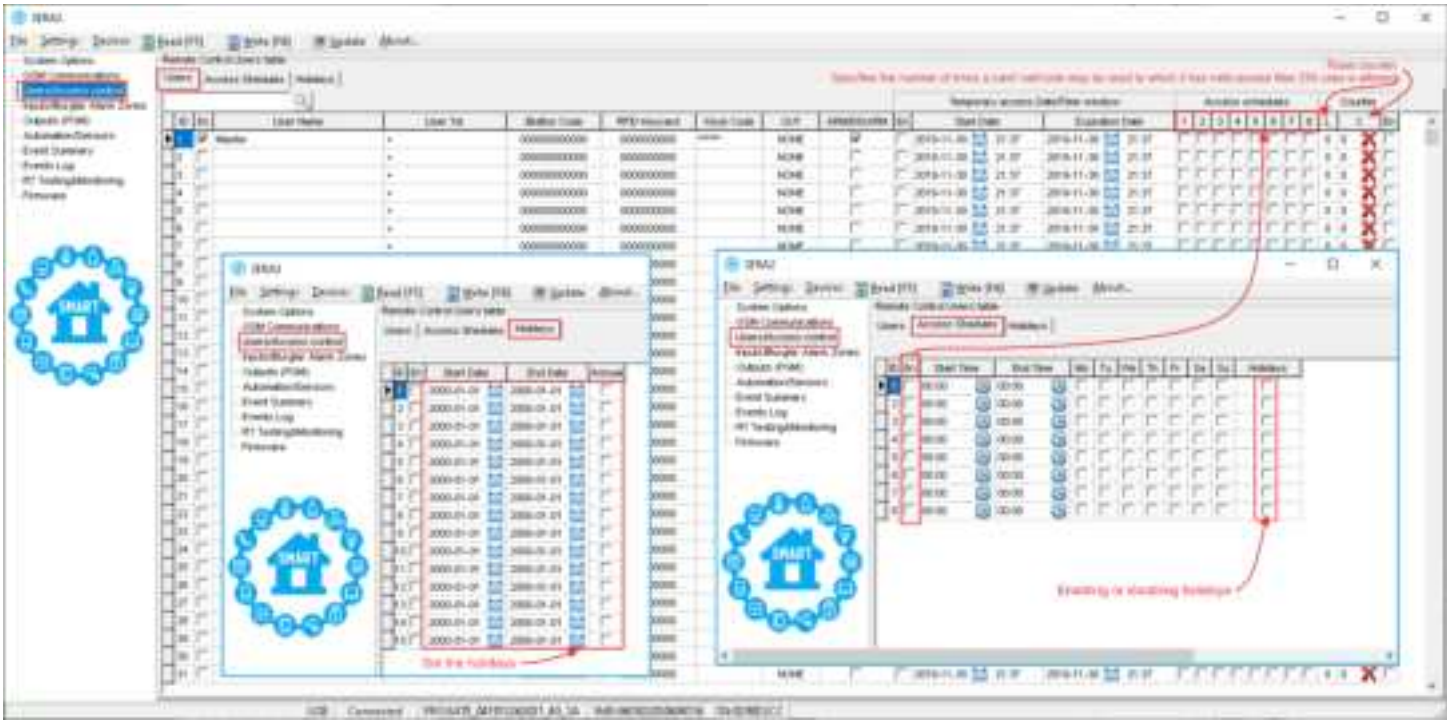


Figure 46 Users/ Access Control > Users, Users Access Control> Access Shedules and Users/ Access Control> Holidays window

Go to SERA2> System Options> General system Options
Set 1W (1-Wire Bus) to Dallas 1-Wire Bus
Set time zone
Set clock synchronization
Press “Write”

Go to SERA2> System Options> General system Options.
Press "Start iButton/ RFID/ Phone programming mode.
Go to SERA2> Users/ Access control window.
Touch RFID keycards, iButton keys to the reader.
Call to the module from your mobile
RFID keycard, iButtons code, phone number will appear in the list.
Go to System Options> General system Options and
Press "Stop programming" or wait until it will stop automatically.
Edit setting in the Users/ Access control window.
Press "Write"

Periodic, recurring at intervals of time access: access schedules, holidays

Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday.

Temporary access, that self-destructed after a certain time elapses

Suppose you must create a Cleaning Crew schedule. The schedules are to be set up as follows: Monday-Friday 5 p.m.-1 a.m., Saturday and Sunday 8 a.m.-1 p.m., no holidays. This becomes three separate schedules, as follows.
2 Monday-Friday, 5 p.m.-11:59 p.m. (Remember, the time range cannot cross midnight, so 11:59 p.m. is the limit.)
3 Tuesday-Saturday, 12:00 a.m.-1:00 a.m.
4 Saturday-Sunday, 8:00 a.m.-1:00 p.m.
Note: Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, schedules that contain that specific Holiday type will work. The Holiday allows users to further customize how the panel works. For example, the user can block access to a building on that day, or grant special access during that day. Each Holiday added is considered a full day, extending from midnight to midnight.

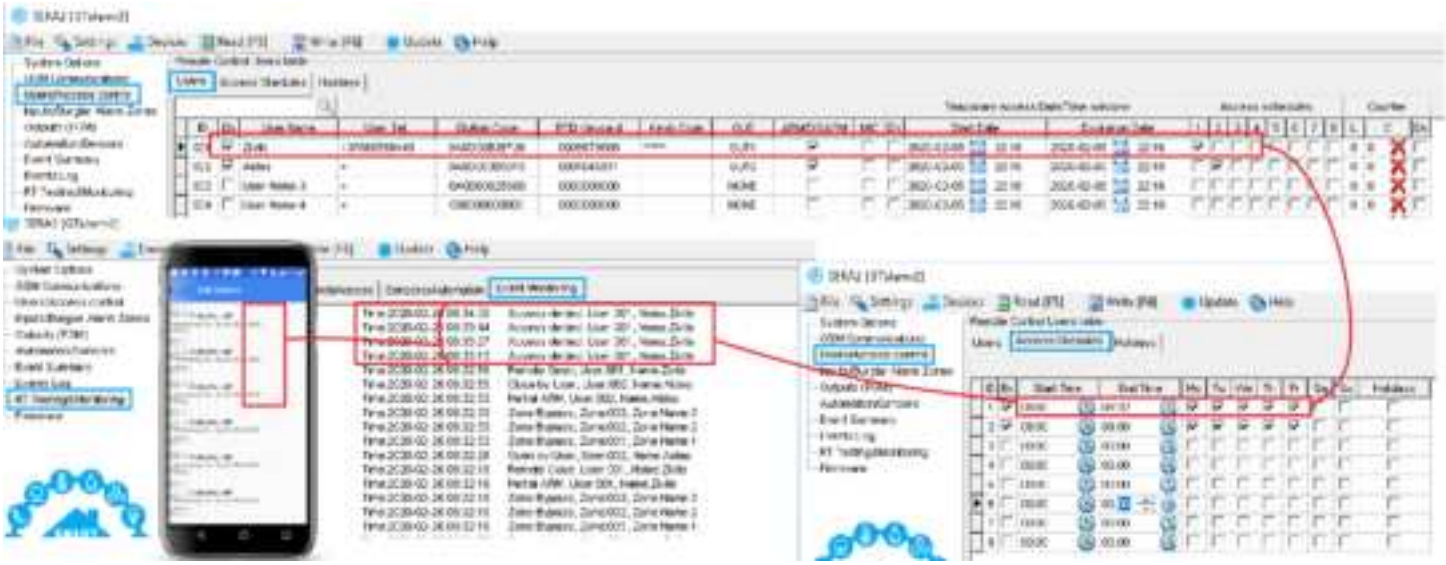


Figure 47 The example of schedule

The module can be controlled only by these users, whose phone numbers entered in the memory of the module

7.7 SMS&DIAL notifications of alarm events

The system supports up to 8 user phone numbers identified as User 1 through 8 for monitoring purpose: receive alarm phone calls via GSM connection and SMS text messages from the system. When the system is armed or disarmed by free of charge phone call or SMS text message, the system sends a confirmation by SMS text message to user phone number that the system arming/disarming.

The system supports up to 8 user receive SMS text messages and alarm phone calls.

7.7.1 Reporting to the user‘s mobile phone

GSM Communications > SMS DIAL Reporting

The SMS DIAL Reporting settings let you enter user’s phone numbers and set events that will be reported to the user

When a zone or tamper is violated, depending on zone, the system will cause an alarm. During the alarm, the system will follow this pattern:

1. The system activates the siren/bell. The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.

2. The system attempts to send an SMS text message (if programmed), containing the violated name. The system will send SMS text messages regarding each violated zone separately.

a) If the user phone number is unavailable, it will attempt to send the SMS text message to the next listed user phone number, assigned to the same zone as the previous one. The user phone number may be unavailable due to the following reasons: mobile phone was switched off or was out of GSM signal coverage.

b) By default, the system will continue sending the SMS text message to the next listed user phone numbers in the priority order. The system try to send the SMS text message as many times as programmed.

3. If programmed, the system attempts to ring the first user phone number via GSM. The system will dial regarding each violated zone separately. The system will dial the next listed user phone number, assigned to the same zone. The user can be unavailable due to the following reasons: Mobile phone was switched off, mobile phone was out of GSM signal coverage or provided “busy” signal.

d) The system will continue dialing the next listed user phone numbers in the priority order. The system will dial again as many times as programmed and the same order as phone numbers listed in the memory if it end up with all unsuccessful attempts to dial to the user.

The module could be controlled and monitored only by these users, whose phone numbers entered in the memory of the module

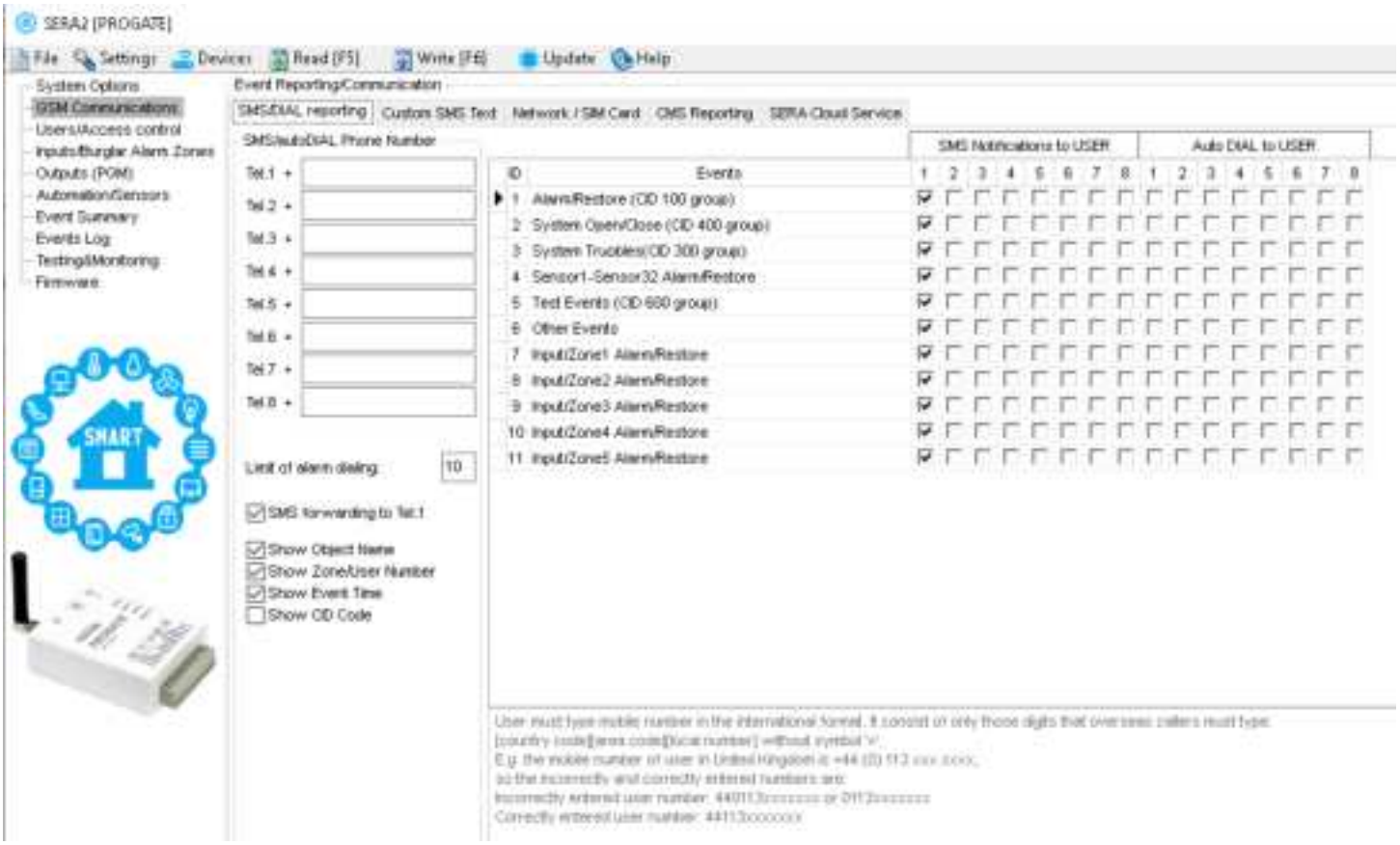


Figure 48 GSM Communication> SMS/ DIAL reporting

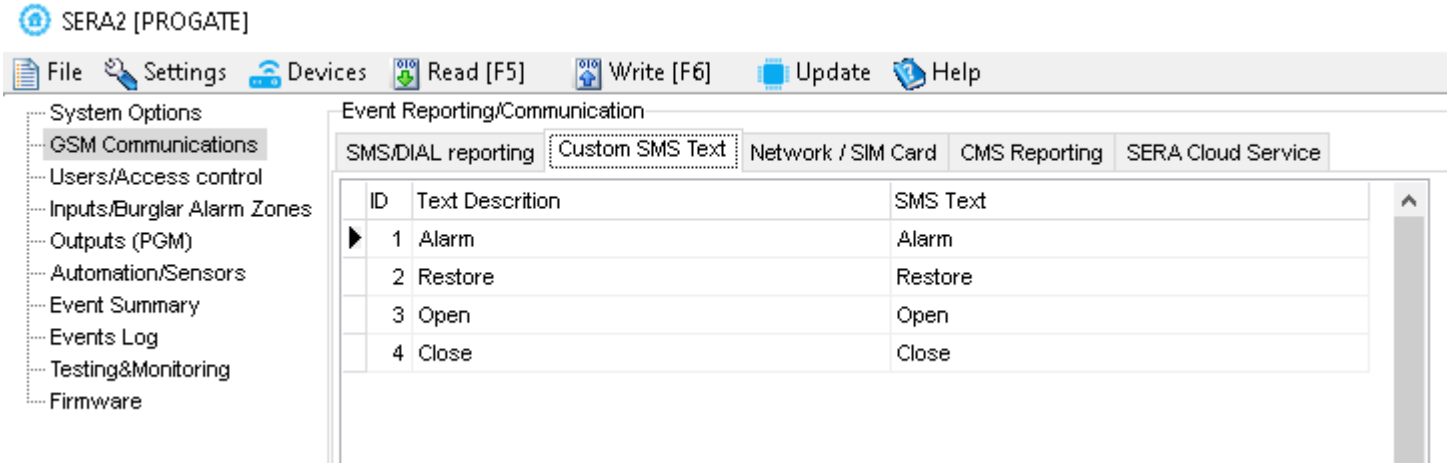
1	**The SMS/auto DIAL Phone Numbers**	**The SMS/auto DIAL Phone Numbers** whom SMS messages will be send and calls will be made should be entered. User number up to 8. User numbers should be entered with international code. Near the telephone number of each user, check boxes which events will be sent to that user. User must type mobile number in the international format (it consist of only those digits that overseas callers must type: **[country code][area code][local number])** Without symbol '+'. E.g. the mobile number of user in United Kingdom is +44 (0) 113 xxx xxxx, so Correctly entered user number: 44113xxxxxxx Incorrectly entered user number: 440113xxxxxxx or 0113xxxxxxx
2	**SMS Character Set**	SMS character set selection.
3	**Limit of Dialing**	Indicate maximum number of unsuccessful calls
4	**Show Object Name**	Object name will be displayed in the SMS message
5	**Show Zone Number**	Zone number will be displayed in the SMS message
6	**Show Event Time**	Event time will be displayed in the SMS message
7	**Show CID Code**	Report Contact ID code
8	**Zone1- Zone32 Alarm/ Restore**	Zone1- Zone32 alarm and restore events reporting is enabled.
9	**System Open/ Close (CID 400 group)**	System ARM/DISARM/STAY reporting is enabled.
10	**System Troubles (CID 300 group)**	System trouble reporting is enabled.
11	**Sensor1- Sensor32 Alarm/ Restore**	Sensor 1 – Sensor32 alarm and restore events reporting is enabled.
12	**Test Events (CID 600 group)**	Communication test reporting is enabled.
13	**Other Events**	Other events reporting is enabled.
14	**Send SMS to USER**	SMS reporting to selected index of telephone number is enabled.
15	**1…8**	To which from the specified phone numbers will be send SMS messages if the specified event will occur in the system
16	**Auto DIAL to USER**	Auto DIAL to selected index of telephone number is enabled.
15	**1…8**	To which from the specified phone numbers will be dial if the specified event will occur in the system

Figure 49Explanation of every field in "SMS DIAL Reporting" window

7.7.2 Custom SMS Text

GSM Communication > Custom SMS Text

The Custom SMS Text options let you enter the text that will be send to the user in case if the alarm event occur.



1	**Text Description**	Event type text
2	**SMS Text**	Text which will be visible in SMS message is entered.
3	**Alarm**	SMS message text of alarm report can be entered.
4	**Restore**	SMS message text of restore report can be entered.
5	**Open**	SMS message text of open report can be entered.
6	**Close**	SMS message text of close report can be entered.

Figure 50Explanation of every field in "Custom SMS Text" window

7.8 Event Summary (Events)

Event Summary (Events)

The Event Summary (Events) window illustrates Contact ID codes of the events and enable user to change the text that will be reported in case if the event occur.

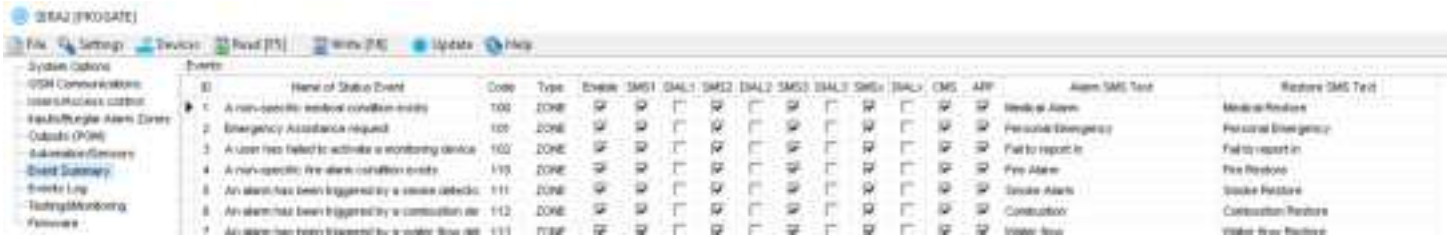


Figure 51 Event Summary window

2	**ID**	Report sequence number
3	**Name of Status Event**	Event (report) name
4	**Code**	Report Contact ID code.
5	**Enable**	The indicated report will be sent when it is checked.
6	**Alarm SMS Text**	Alarm text which will be visible in SMS message is entered.
7	**Restore SMS Text**	Restore text which will be visible in SMS message is entered.

8	**Type**	9	None
		10	USER — Refer to USER Report Options
		11	ZONE — Refer to Zone Report Options
		12	NUM — Refer to Numerical Report Options

Figure 52 Explanation of every field in "Event Summary" window

7.9 RT Testing & Monitoring. Hardware.

RT Testing & Monitoring > Hardware

The Hardware monitoring window let you see real time input, output actions and GSM information. Thus it would be easier to evaluate whether the input, output actions, registration to the network operates as appropriate.

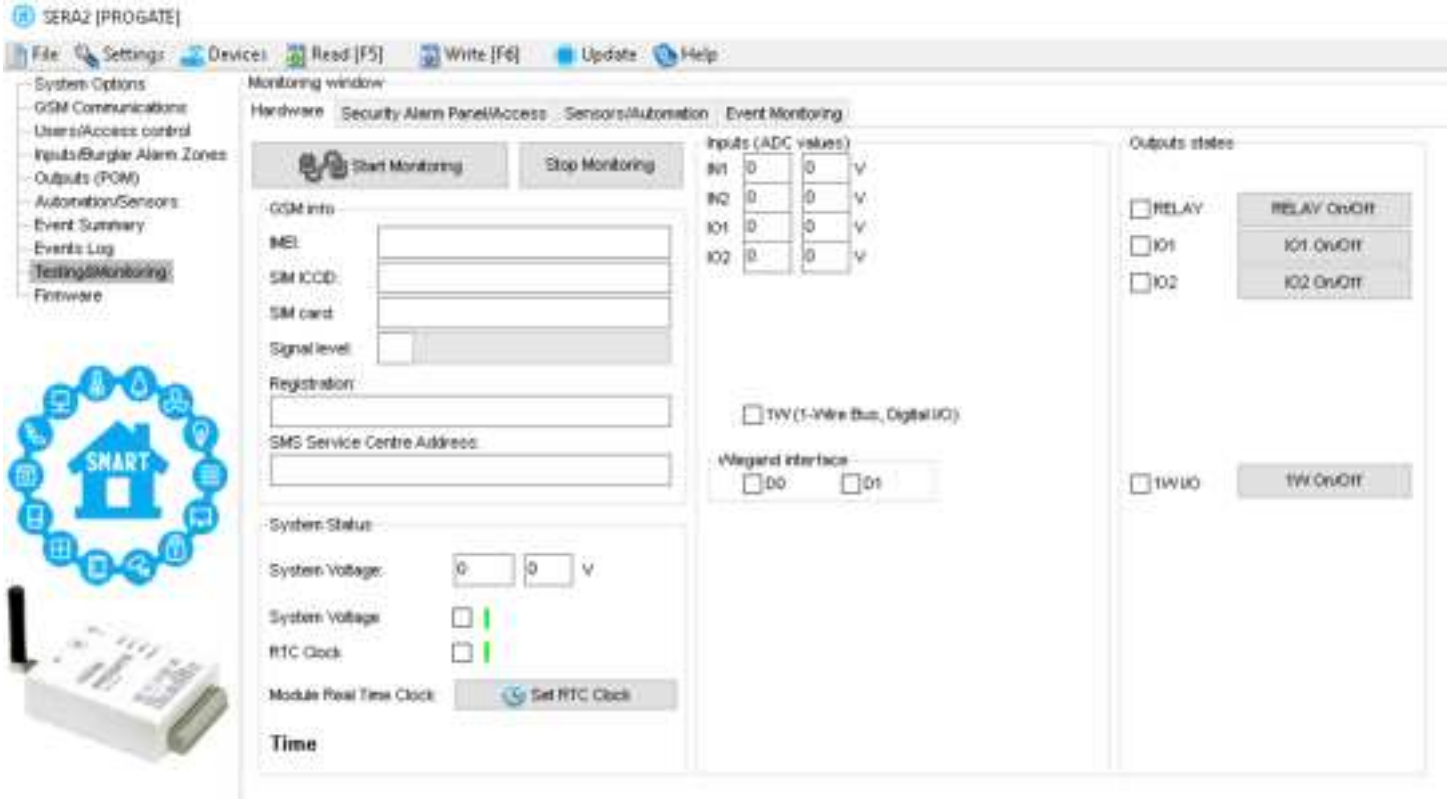


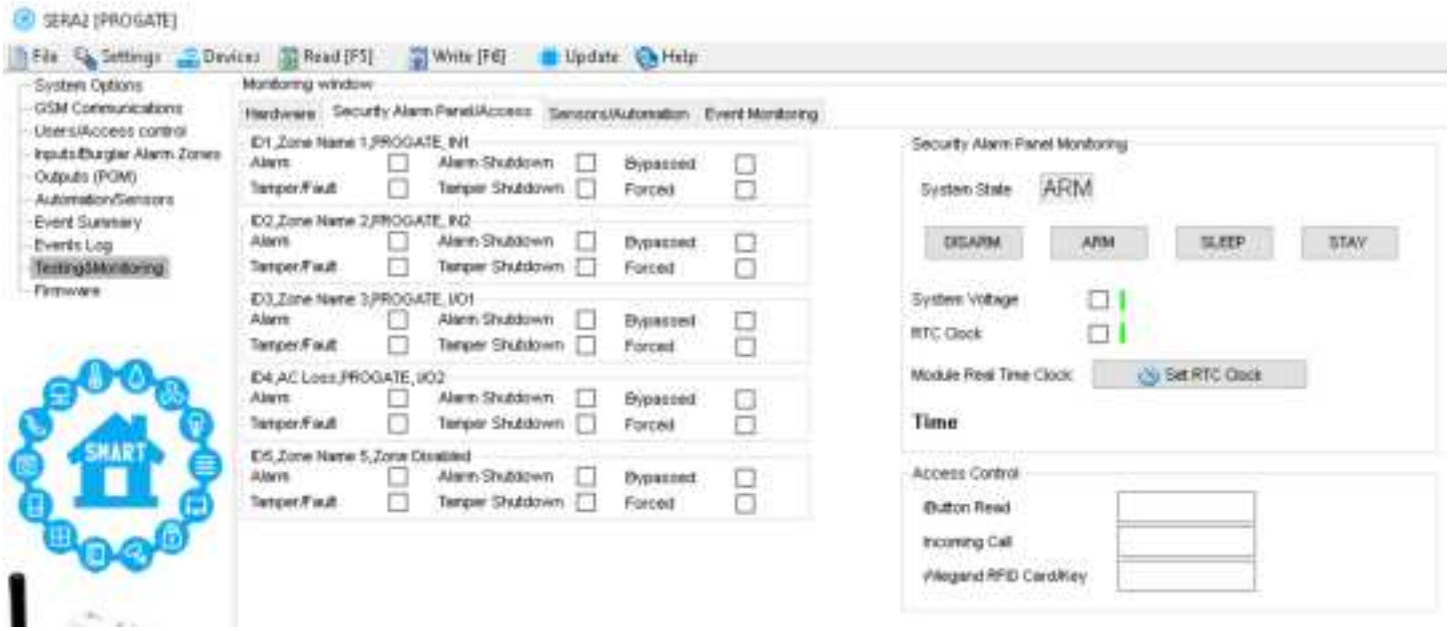
Figure 53 RT Testing Monitoring> Hardware window

1	Start Monitoring	Pressing Start Monitoring button starts the monitoring of the module.
2	Stop Monitoring	Pressing Stop Monitoring button stops the monitoring of the module.
3	IMEI	IMEI number of GSM modem available in the module
4	SIM ICCID	ICCID (Integrated Circuit Card Identifier) - A SIM card contains its unique serial number (ICCID). ICCIDs are stored in the SIM cards and are also printed on the SIM card.
5	SIM Card	If note READY is visible, it means that SIM card is fully functioning. Otherwise, check whether PIN code request is off or replace SIM card.
6	Signal level	Signal strength of GSM communication
7	Registration	State of GSM modem registration to GSM network.
8	SMS Service Centre Address	SMS center number. This number should be checked if it is correct. If this number is incorrect. SMS messaging may be impossible. This number may be changed after inserting SIM card into any mobile phone.
9	System Voltage	Power supply voltage. Nearby number is value of ADC voltage. When multiplying this number by the coefficient Fig. 32, voltage value (V) will be achieved.
10	System Voltage	System voltage OK/Trouble
11	RTC Clock	Real time clock OK/Trouble
12	Module Real Time Clock	Indicates the time of the module RTC
13	Set RTC Clock	By pressing this button real time clock of the module will be set.
14-17	Inputs In1…In4	In1…In4 is the indicated input ADC and voltage value V.
18-19	I/O1…I/O2	I/O1…I/O2 is the indicated voltage ADC value and current ADC value mA.
20-22	D1…D3 (I/O)	Check box nearby the digital inputs D1…D3 (I/O) means that the input has ‘0’ or ‘1’ state.
23	BUS (I/O)	Check box nearby the zone expansion module BUS (I/O) means that the input has ‘0’ or ‘1’ state.
24-27	Out1…Out4 On/Off	Checked box nearby the appropriate output Out1…Out4 means that this output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button
28-29	I/O1…I/O2 On/Off	Checked box nearby the appropriate input/output I/O1…I/O2 means that this input/output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button
30-32	D1…D3 (I/O) On/Off	Checked check box nearby the digital outputs D1…D3 (I/O) means that the output currently has ‘0’ or ‘1’ state.
33	BUS (I/O) On/Off	Checked check box BUS (I/O) means that the output currently has ‘0’ or ‘1’ state.

7.10 RT Testing & Monitoring Security Alarm Panel/ Access

RT Testing & Monitoring > Security Alarm Panel/ Access

The Security Alarm Panel/ Access window let you see real time zones states: is zone alarmed, bypassed, forced etc. This window it let you change system state: disarm, arm, sleep, and stay. This window let you look to access control area also.



1	**Zone1…Zone32**	Zone number
2	**Alarm**	If checked and the color is red the zone is alarmed
4	**Alarm Shutdown**	If checked and the color is red alarm shutdown for the zone is activated. Allowable number of the same alarm events is reached and the same events will not be reported.
6	**Bypassed**	If checked and the color is red, the zone is bypassed.
7	**Forced**	If checked and the color is red, the zone is forced
3	**Tamper/Fault**	If checked and the color is red, the zone is tampered.
5	**Tamper Shutdown**	If checked and the color is red tamper shutdown for the zone is activated. Allowable number of the same tamper shutdown events is reached and the same events will not be reported.
8	**System State**	Indication that at the moment the module is in waiting ARM, ARM, DISARM, SLEEP or STAY mode
9	**DISARM**	After pressing the button DISARM, disarm mode should be entered
10	**ARM**	After pressing the button ARM, arm mode should be entered
11	**SLEEP**	After pressing the button SLEEP, sleep mode should be entered
12	**STAY**	After pressing the button STAY, arm mode should be entered
13	**System Voltage**	If the checkbox is checked and the color is red the trouble with system voltage is indicating. If color is green, there is no trouble with system voltage.
14	**RTC Clock**	If the checkbox is checked and the color is red RTC clock is not set. If color is green, RTC clock is set.
15	**Module Real Time Clock**	Real time and date is indicating.
17	**iButton Read**	The number of iButton Maxim iButton key DS1990A - 64 Bit ID code that is arming the system.
18	**Incoming call**	The number of users phone that is calling to the module's SIM.
19	**Wiegand RFID Card Key**	The number of Wiegand RFID Key Card that is arming the system.

Figure 54 Explanation of every field in "Security Alarm Panel/ Access" window

GPRS/ IP/ TCP/ UDP details must be configured before TCP/IP Remote control will be set

It was discussed in *Error: Reference source not found*

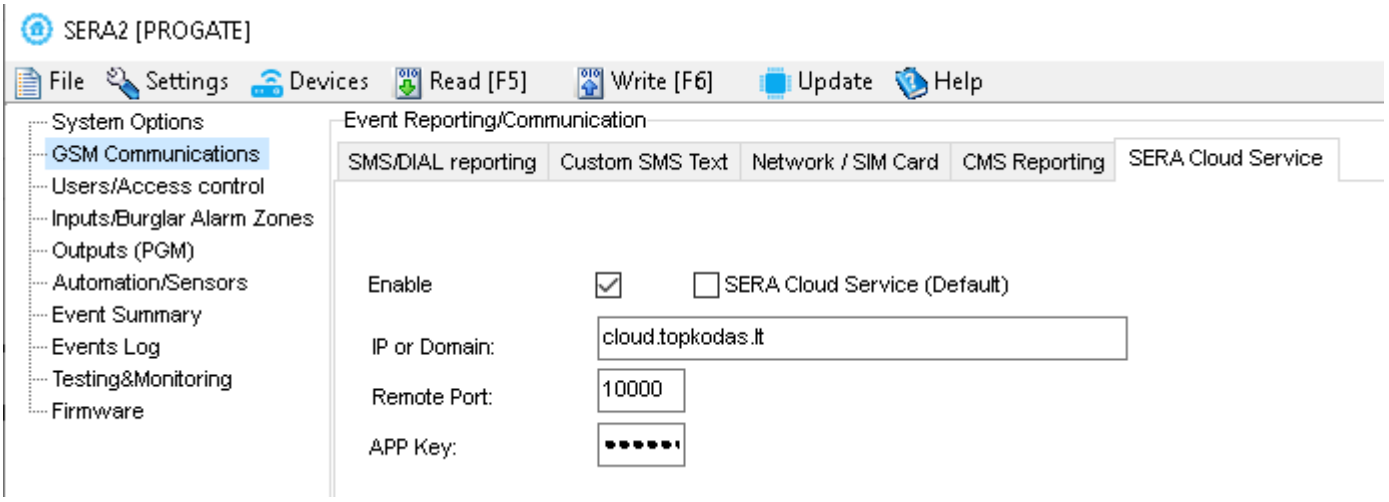
7.10.1 TCP/ IP Remote Control

GSM Communication > SERA Cloud Service

The TCP/ IP Remote Control window let you set basic TCP IP remote control settings and enable or disable remote communication.

1		**Enable**	Check the particular checkbox to enable remote control/configure module over internet.
2		**IP or Domain**	IP address xxx.xxx.xxx or domain name of remote control server.
3		**Remote Port**	Remote server port.
4		**Ping Time**	Period of communication test signal PING sending via GPRS channel.
5		**Encryption Key**	Server encryption key .

Figure 55Explanation of every field in "TCP/ IP Remote Control" window



7.11 Events Log

Events Log The Event Log window show real time information of the events that has been occurred

The event log allows to chronologically register up to 2048 time stamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Temperature deviation by MIN and MAX boundaries.
- System faults.
- Configuration via USB.
- User phone number that initiated the remote configuration.

Communication with monitoring station status.

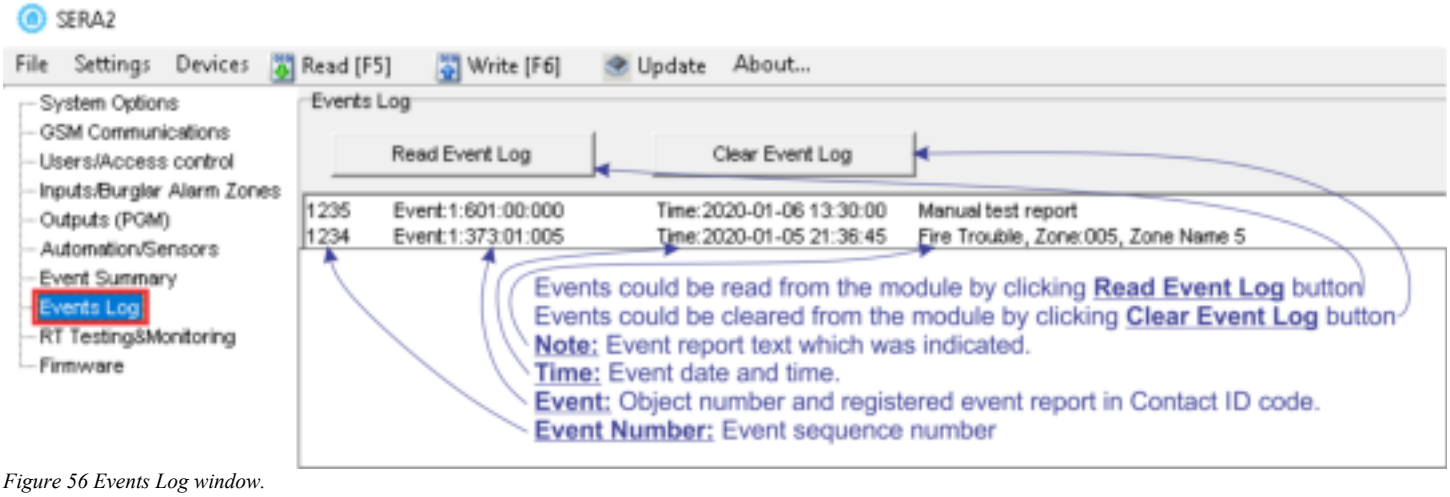


Figure 56 Events Log window.

1	**Read Event Log**	Events could be read from the module by clicking **Read Event Log** button
2	**Clear Event Log**	Events could be cleared from the module by clicking **Clear Event Log** button
3	**Event Number**	Event sequence number
4	**Event**	Object number and registered event report in Contact ID code.
5	**Time**	Event date and time.
6	**Note**	Event report text which was indicated.

7.12 Remote Monitoring, Control, Configuration, FW update over the internet

What can be done remotely connecting to a module over the internet?

- The system parameters may be changed
- Monitoring system status, temperature sensors may be observed.
- Firmware update of the module

How does it works?

Remote connection is established via GPRS using TCP/IP protocol;
The GSM module connects to the internet via a GPRS to SERA cloud server [cloud.topkodas.lt].
The connection is established by the SERA2 configuration tool using unique ID of the module UID IMEI.

PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→SERA2

Or

PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→Standard web browser. Firefox, Chrome etc.

Sera Cloud Server opens tunnel between module PROGATE and SERA2 or APP and lets them communicate to each other via TCP protocol.

GPRS service should be activated for the SIM card of the GSM module. Usually GPRS service is activated automatically otherwise need contact GSM service provider to inquire about activation of the GPRS service.

Steps to activate Remote control over internet:

1. Install SERA2 software
2. Go to “GSM Communication” window, “GPRS/IP/TCP/UDP” tab.
3. Set APN, Login, Password (default 123456).
4. Go to “GSM Communication” window, “Sera Cloud Service” tab. Set Sera Cloud Service to Default parameters.
5. Write the configuration into the module by pressing “Write” icon

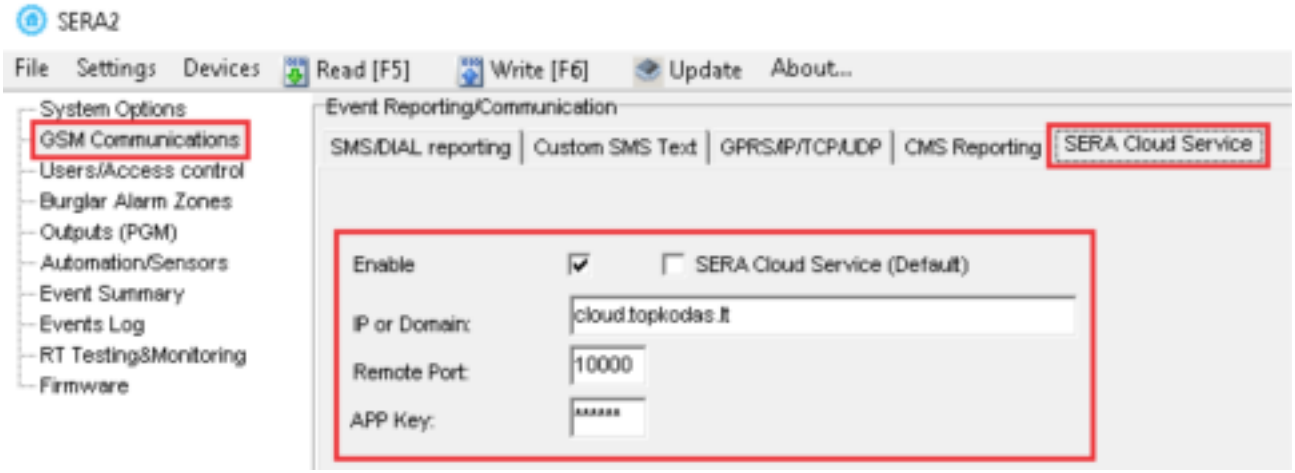


Figure 57 GSM Communication> Sera Cloud Service window

6. Go to SERA2> GSM Communication> CMS Reporting

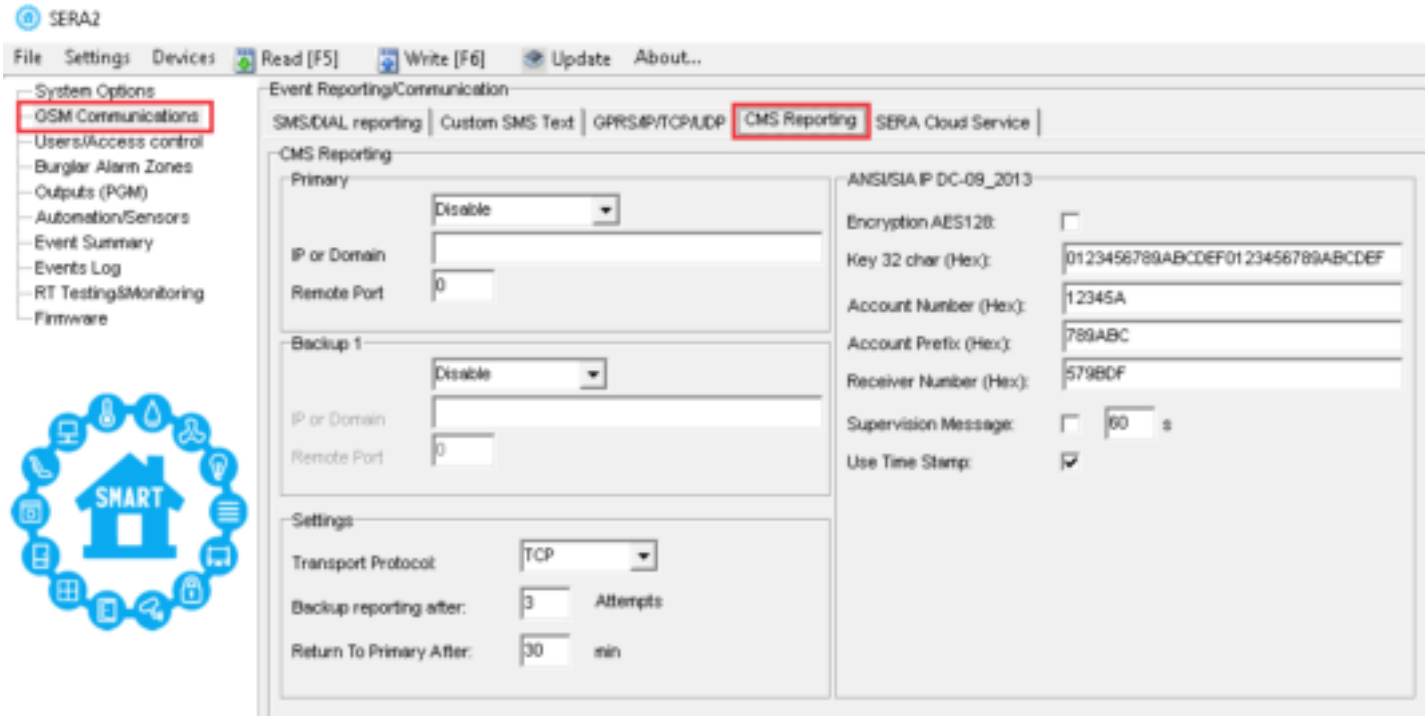


Figure 58GSM Communication> CMS Reporting window

6. Public IP or domain must be entered. Enter remote port, ping time, encryption key and enable the communication.
7. If needed, APN/Password/Login/IP/Domain/ Port /PING time /KEY can be set by SMS commands

GPRS network settings	**Remote control of the module over the Internet.**
INST000000␣008␣APN#LOGIN#PSW#	INST000000␣009␣ADDR#PORT#PING#KEY#
008= command code (GPRS network settings) APN=31 symbols LOGIN=31 symbols PSW=31 symbols	009= command code (Remote control of the module over the Internet) ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain text length of up to 47 characters) PORT= TCP port number from 1 to 65535 PING= communication control ping time from 30 to 9999s KEY= encryption key. Encryption key should be the same as server key. Default 123456

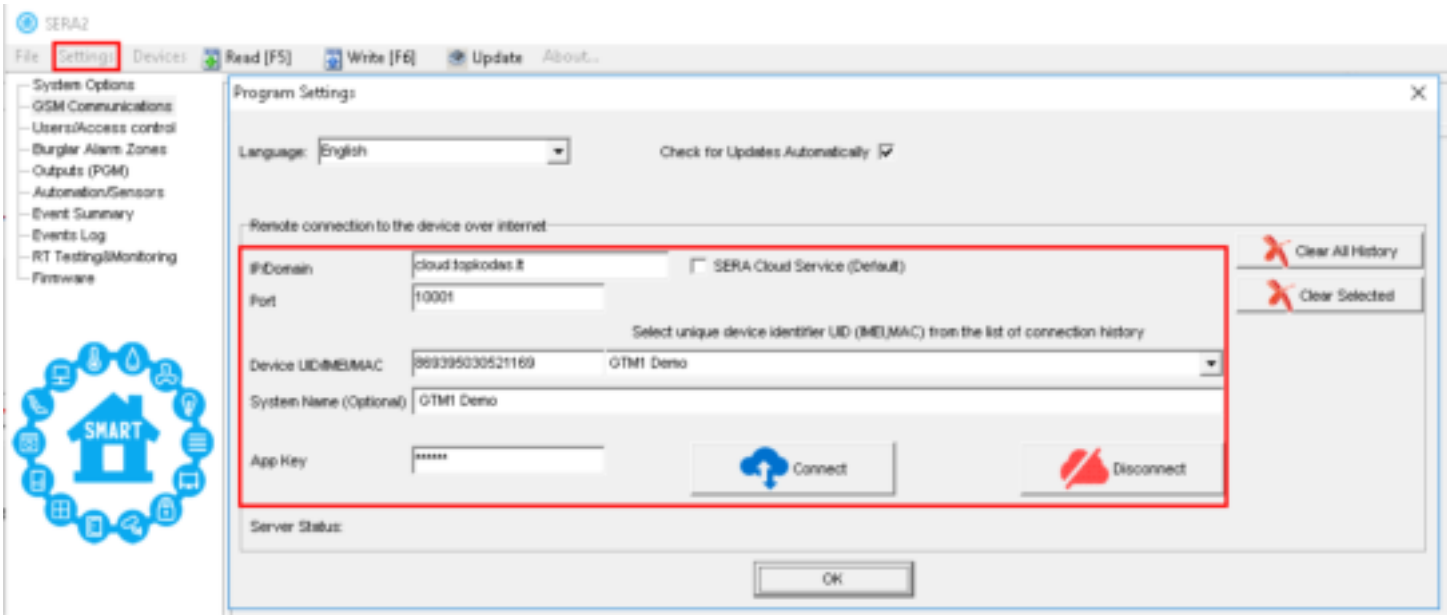


Figure 59 Command line> Settings window

8. SERA2> Settings Check “SERA Cloud Service (default)” checkbox.
9. Enter Device UID/IMEI. Press *Connect* button and wait till connection will be established. In the bottom in the task bar appears TCP connected notification.

SERA2 software can remember all IMEI that was entered in the past. If needed to clean the list UID/IMEI, press “Clear History”.

8 SMS Commands for remote control and configuration

List of user SMS commands:	**List of installer SMS commands**:
• Set the system mode: Arm/Disarm/Stay/Sleep • Bypass zones • Set the time of the module • Request zone test and system state • Forward messages to other number	• Add/Edit/Delete user phone numbers • Control outputs • Arm/disarm the system or select stay, sleep mode • Bypass zones • Set the time of the module • Request zone test and system state • Forward messages to other number • Set periodical test, • Set GPRS network settings • Remote control via Internet • Activate/ deactivate connection to the remote control server. • Enter/ deleting iButton keys • Change sensor's values • Request module configuration information • Change user, installer password

Installer code – 6-digit password used for system configuration, control and request for information.
By default, installer code is 000000, which is highly recommended to change.
User code for SMS commands – 6-digit password used for system control and request for information.
By default, user code is 123456, which is highly recommended to change.

The module could be controlled only by these users, whose phone numbers entered in the memory of the module

- INST- Installer identification
- Installer's or user's password.
- space character
- Command code.
- space character
- First configuration array
- space character
- Second configuration array
- - etc.

- USER - User identification
- User's password.
- space character
- Command code.
- space character
- First configuration array
- space character
- Second configuration array
- - etc.

Example of how to add a User1 SMS and an autodialer notifications. For more information see the command table

INST000000␣001␣1#37066666666#11111111#10000000#

Please note: Symbol ␣ = **Space character** in SMS.

␣ Symbol in examples is used only to make the visual easier to understand.

8.1 The table of installers SMS commands

SMS commands with **correct INST password** can be send from any phone number. Keep INST password in secret!

SMS configuration is allowed only with Latin characters. Unicode is not allowed.

Please note: Symbol ␣ = **Space character** in SMS. ␣ Symbol in examples is used only to make the visual easier to understand.

Table 6 the table of installers commands

INST000000␣001␣N#TEL#SMS#DIAL# e.g. INST000000␣001␣1#37066666666#11111111#10000000#	**Add users telephone numbers to send SMS and to make a call if the event occur:** 001= programming user's tel. numbers for SMS and DIAL N = user ID number 1-8 TEL = user's telephone number (max 16 digits) without (+) country code, operator's code and user's telephone number included. The end symbol #; SMS = notifications event filter. 1- Send event, 0- don't send event. Sequence of the events 1.2.3...n For example: 001000 DIAL = event filter for DIAL. 1-DIAL if the event occur, 0-don't DIAL Sequence of the events 1.2.3...n For example: 101000 #= delimiter **e.g.: INST000000 001 1#37066666666#0001000000#0000011111#** Event filter from left to right 0-disabled;1-enabled: 1. Alarm/Restore (CID 100 group) 2. System Open/Close (CID 400 group) 3. System Troubles(CID 300 group) 4. Sensor1-Sensor32 Alarm/Restore 5. Test Events (CID 600 group) 6. Other Events 7. Input/Zone1 Alarm/Restore 8. Input/Zone2 Alarm/Restore etc…….
INST000000␣002␣ID	**Delete user's phone number according the** user ID number**. Phone number used for receive user's information.** 002 = command code (deleting user's numbers according the user ID number) ID = user ID number from 1 to 8
INST00000 0␣004␣ID#TEL#OUT#OPT#NAME# e.g. INST000000␣004␣1#37066666666#1#10#Jon#	**To enter user's telephone number for remote control via short call** **USER NAME-only Latin characters is allowed inside SMS** 004= command code (enter user's telephone number for remote control via short call) ID = user ID number 001-800 TEL = user's telephone number (max 16 digits) without (+) comprised of country code, operator's code and user's telephone number. the end symbol #; OUT= output number, that will be controlled, 1-32. 0-Disabled OPT = 0 – disabled 1 – enabled, Sequence from the left to the right 1. User Enabled 2. Enable Arm/Disarm system by call NAME = User Name
INST000000␣005␣TEL#	**To delete user's phone number for remote control, according phone number** *005= command code (delete user's phone number for remote control, according phone number)* TEL = user's phone number (max 16 digits) without (+) comprised of country code, operator's code and user's telephone number. User's phone number must be the same as in the memory of the module.
INST000000␣006␣ID	**Delete user's all data by index ID** 006= command code (Delete user's phone number by index) ID = user's index number from 001 to 800.
INST000000␣007␣P#PER#HH:mm# e.g. INST000000␣007␣1#7#18:30#	**Automatic periodical test settings** 007= command code (Automatic periodical test) P= 0-test disabled, 1- test period by 24 hours, 2- period by hours PER= automatic test sending period from 1 to 99999 days or hours HH-hours 0-23 , mm- minutes 0-59 e.g. INST000000 007 2#1#14:50# The test will be send every 1 hour
INST000000␣008␣APN#LOGIN#PSW# e.g. INST000000␣008␣internet### Apn="internet and no login and password.	**DATA/GPRS/LTE network settings** 008= command code (network settings) APN=31 symbols LOGIN=31 symbols PSW=31 symbols

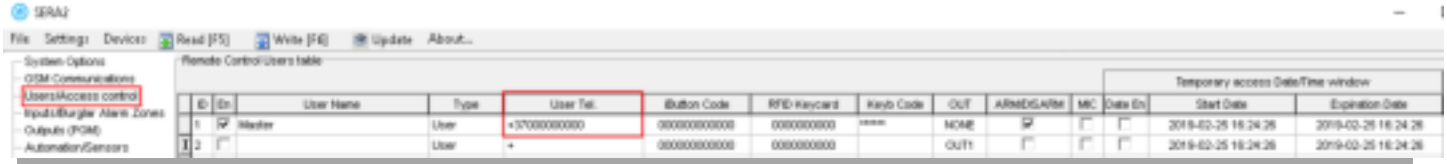
INST000000␣009␣ADDR#PORT#PING#KEY# e.g. INST000000 009 cloud.topkodas.lt#1000#600#123456#	**SERA cloud Service Parameters** 009= command code (Remote control of the module over the Internet) ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain text length of up to 47 characters) PORT= TCP port number .Default:10000 PING= 600 default. KEY= App Key. App and remote service key. Default:"123456" Default parameters is in the picture bellow. We recommend do not change these parameters. 
INST000000␣010␣E	**Activate/Deactivate SERA Cloud service. APP and remote connection to device.** 010= command code (To activate the connection to the remote control server) E= 1-enabled, 0-disabled
INST000000␣011␣E e.g. INST000000␣011␣1 - Enable GUEST mode e.g. INST000000␣011␣0 - Disable GUEST mode e.g. Dual command 011 and 004 set USER9 INST000000␣011␣1␣004␣9##1#10#Unauthorized# Enable Guest mode on USER9, set control OUT1, UserName:'Unauthorized'	**Enable/Disable GUEST (unauthorized call) mode on USER 9. APP and remote connection to device.** 011= command code (activate GUEST mode on USER 9). Enable incoming call guest mode on USER 9 settings. Module will accept all unauthorized calls and do selected action(e.g to control an output, gate) on USER 9. E= 1-enabled, 0-disabled
INST000000␣012␣TEL#OUT#OPT#NAME# e.g. INST000000␣012␣37066666666#1#10#Jon#	**To enter user's telephone number for remote control via short call without index** **USER NAME-only Latin characters is allowed inside SMS** 012= command code (enter user's telephone number in free space for remote control via short call) TEL = user's telephone number (max 16 digits) without (+) comprised of country code, operator's code and user's telephone number. the end symbol #; OUT= output number, that will be controlled, 1-32. 0-Disabled OPT = 0 – disabled 1 – enabled, Sequence from the left to the right 1. User Enabled 2. Enable Arm/Disarm system by call NAME = User Name
INST000000␣019␣N#P e.g. INST000000␣019␣1#24 Set OUT1 as [Access Control]	**To change the operation algorithm of the output** 019= command code (To change the operation algorithm of the output) N = output number from 1 to 32 P = output operation algorithm. Set 0 to 24 0. Disable 1. Bell 2. Buzzer 3. Flash 4. System State 5. ARM Status 6. Remote Control & Automation 7. AC OK 8. Battery OK 9. System Armed Status 10. Alarm Indication 11. Lost Primary Chanel 12. Lost Secondary Chanel 13. Fire Sensor 14. RH Sensor Trouble 15. Access Gained 16. STAY Armed Status 17. SLEEP Armed Status 18. Pulse On ARM / DISARM 19. Output State 20. Zone OK 21. Activate by ARM/DISARM Command 22. Activate by SLEEP/DISARM Command 23. Activate by STAY/DISARM Command 24. Access Control
INST000000␣020␣N	**Invert output state** 020= command code (outputs inversion) N = output number from 1 to 32.
INST000000␣021␣N#ST	**Output activation or deactivation** 021= command code (Output activation or deactivation) N = output number 1-32 ST = output mode 0 – OFF, 1- ON
INST000000␣022␣N#TIME#	**Output activation for the time interval** 022= command code (Output activation for the time interval) N = output number 1-32 TIME = 0-999999 Time interval in seconds for the output activation.
INST000000␣030␣ST	**Change security system's mode (ARM/DISARM/STAY/SLEEP)** 030= command code (Change security system's mode) ST = 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP
INST000000␣031␣ZN#BYP	**Zone bypassing by sms command** 031= command code (Zone bypassing) ZN = zone number from 1 to 32 BYP= 1 – zone bypass 0- zone active.
INST000000␣063␣S	**iButton keys learning/deleting mode** 063= command code (iButton keys learning/deleting mode) S=iButton keys entering/deletion mode.

	0-Disable iButton/RFID keys learning mode 1-Enable iButton/RFID keys learning mode 2-iButton/RFID keys deleting mode. To delete these keys from memory, which will be touched to the reader
INST000000␣070␣N#VALUE # e.g. INST000000␣070␣1#23.5#	**Programming of max sensors value upon reaching, the SMS message with „High Alarm“ text will be sent** 070= command code (max sensors value upon reaching which, the SMS message with „High Alarm“ text will be sent) N = sensor number VALUE= Format 0000.00 High Alarm Value
INST000000␣071␣N#VALUE #	**Programming of minimal sensors value upon reaching the SMS message with „Low Alarm“ text will be sent** 071= command code (min sensors value upon reaching which, the SMS message with „Low Alarm“ text will be sent) N = sensor number VALUE = Format 0000.00 Low Alarm Value
INST000000␣072␣N#VALUE#	**Programming of sensor max value upon reaching the selected output will be activated.** For example cooling equipment 072= command code (sensor max value upon reaching the selected output will be activated.) N = sensor number VALUE= Format 0000.00 sensor max value upon reaching, the selected output will be activated.
INST000000␣073␣N#VALUE#	**Programming of sensor min value upon reaching the selected output will be activated.** For example heating equipment 073= command code (sensor min value upon reaching the selected output will be activated.) N = sensor number VALUE= Format 0000.00 Sensor min value upon reaching which, the output will be activated.
INST000000␣090␣NewInstPsw	**Change installer‘s password** (Installers password should be changed before exploitation of the module) 090= command code (Change of installer‘s password) NewInstPsw = New Installer‘s password.
INST000000␣091␣NewUserPsw e.g. INST000000␣091␣654321	**Change user‘s password** (User‘s password should be changed before exploitation of the module) 091= command code (Change user‘s password) NewUserPsw = New user‘s password.
INST000000␣092	**Remote reset of the module via SMS messages** 092= command code (Remote reset of the module via SMS messages)
INST000000␣093␣yyyy/MM/dd#HH:mm#	**Time of the module setting via SMS message.** The time is usually synchronized via a server or mobile network. However, if synchronization is disabled, it can be set manually via SMS. 093= command code (Time of the module setting via SMS message) Time format of the module: yyyy/MM/dd#HH:mm# yyyy -year MM-month 1-12 dd - day of the month 1-31 HH-hours 0-23 mm- minutes 0-59
INST000000␣094␣TEL#SMS e.g. INST000000␣094␣+370616111111#Hello	**SMS from the module forwarding to the other phone number** 094= command code (SMS from the module resending to the other phone number) TEL = phone number to which will be forwarded sms text SMS = sms text that will be send to the referred number. TEL=861611111111 local number or international format e.g. +370616111111 **SMS text =Latin Charset** After this commands could not be other commands like: 094 SMS 030 1 because all messages will be forwarded to other numer "SMS 030 1"
INST 000000␣095␣E	**Zone Walk Test request** 095= command code (Zone Test request) E = 1- test request activated, 0- test request deactivated When zone is activated, the bell generates the sound, ARM/DISARM system automatically turn off this function
INST 000000␣096	**Fire sensors reset.**

INST000000␣100␣N	**System state request:** 100= command code (System state request) N = System state request type 1- System test request, Request information about the module (: IMEI, FW, LEVEL etc.) 2- the values of active sensors request 3 -Request about active zone states 4 -Request about output states 5 - System state request. The module will send information on input/output states and system state (ARM/DISARM/STAY).

8.2 The table of users SMS commands

If USER123456 commands are used, the phone number must be in the list of users **SERA2> Users/ Access control**; if the phone number is not in the list, SMS commands from this phone number will be blocked.



SMS configuration is allowed only with Latin characters. Unicode is not allowed.

Table 7 the table of user's commands

USER123456␣020␣N	**Change state of selected OUT output to the inverted state.** Output state changes every time after sending command code. 020= command code (Change state of selected OUT output to the inverted state.) N = output number from 1 to 10.
USER123456␣021␣N#ST	**Activate or deactivate selected output N.** 021= command code (Activate or deactivate selected output N) N = output number from 1 to 10. ST= output mode: 0 – deactivated output, 1- activated output
USER123456␣022␣N#TIME#	**Output activation for the time interval** 022= command code (Output activation for the time interval) N = output number 1-10 TIME = 0-999999 Time interval in seconds for the output activation.
USER123456␣030␣ST	**Change security system's mode (ARM/DISARM/STAY/SLEEP)** 030= command code (Change security system's mode (ARM/DISARM/STAY/SLEEP) ST = Security system mode 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP Enter user phone number in **the SERA2> Users/ Access control** list
USER123456␣031␣ZN#BYP	**Zone bypassing by sms command** 031= command code (Zone bypassing) ZN = zone number from 1 to 32 BYP= 1 – zone bypass 0- zone active.
USER123456␣094␣TEL#SMS	**SMS from the module forwarding to the other phone number** 094= command code (SMS from the module resending to the other phone number) TEL = phone number to which will be forwarded sms text SMS = sms text that will be send to the referred phone number
USER123456␣100 ␣N	**System state request:** 100= command code (System state request) N = System state request type 1- System test request, Request information about the module (: IMEI, FW, LEVEL etc.) 2- the values of active sensors request 3 -Request about active zone states 4 -Request about output states 5 - System state request. The module will send information on input/output states and system state (ARM/DISARM/STAY).

9 Info: Hardware, Firmware, Bootloader, Serial No & Updates

System Options > System Info

The System Info window let you take a look to the main hardware, boot loader, firmware, serial no, IMEI, GSM Modem information.

Figure 60 System Options > System Info window.

1	**Hardware**	Control panel type.
2	**Bootloader**	Bootloader version
3	**Firmware**	Configuration software
4	**Serial No**	Module registration number
5	**IMEI**	GSM modem IMEI address.

Figure 61Explanation of every field in "System Info" window

9.1 Firmware Update

Firmware

This window let you update the firmware of the module.

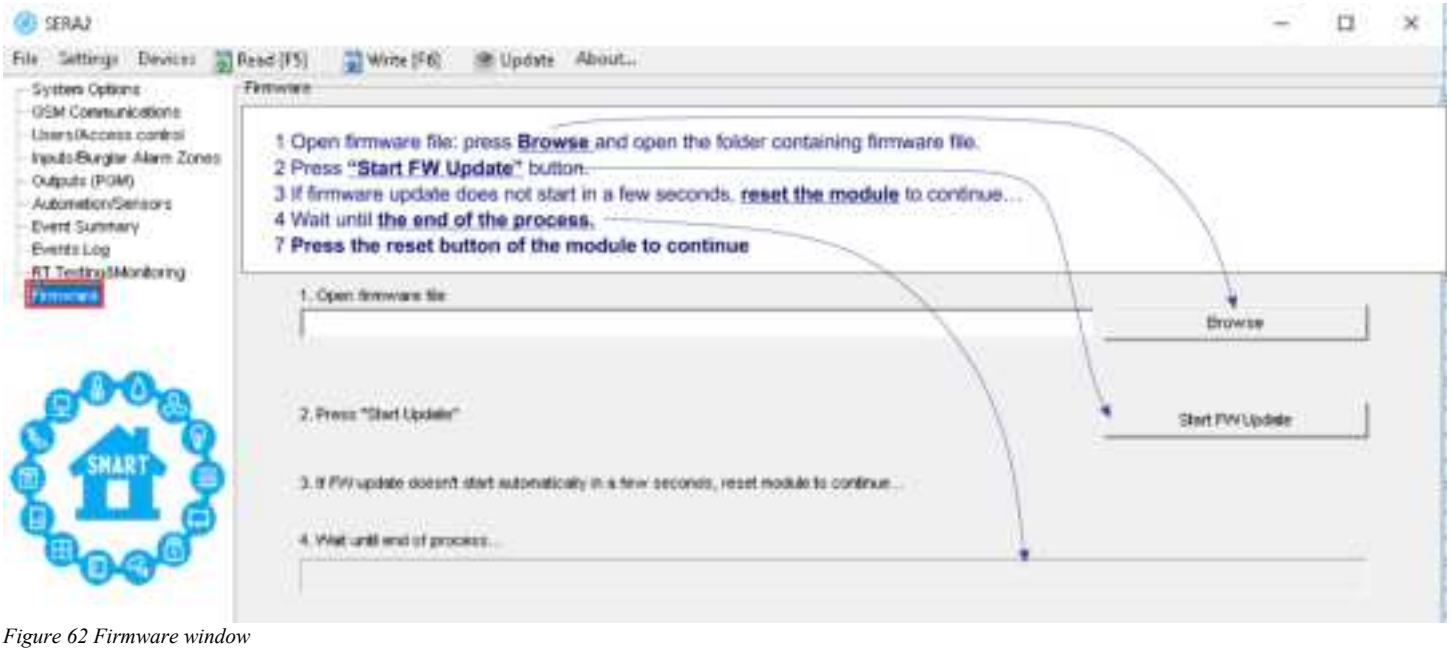


Figure 62 Firmware window

1 Open firmware file: press Browse 2 and open the folder containing firmware file. 3 Press “Start Update” 4 button. 5 If firmware update does not start in a few seconds, reset the module to continue… 6 Wait until the end of the process. 7 Press the reset button to continue…

10 Warranty Terms and Conditions

SAFETY INSTRUCTIONS FOR SERVICE PERSONS
Use the following list as a guide to find a suitable place for PROGATE module:
• Locate the module near a power outlet.
• Select a place that is free from vibration and shock.
• Place the module on a flat, stable surface and follow the installation instructions:
Do NOT locate the module where persons can walk on the secondary circuit cable(s).
Do NOT connect the module to electrical outlets on the same circuit as large appliances.
Do NOT select a place that exposes the module to direct sunlight, excessive heat, moisture, vapors, chemicals or dust.
Do NOT install the module near water (e.g., bathtub, wash bowl, kitchen/laundry sink, wet basement, or near a swimming pool).
Do NOT install the module and its accessories in areas where there is a risk of explosion.
Do NOT connect the module to electrical outlets controlled by wall switches or automatic timers.
AVOID sources of radio interference.
AVOID setting up the equipment near heaters, air conditioners, ventilators, and/or refrigerators.
AVOID locating module close to or on top of large metal objects (e.g., metal wall studs).
Safety Precautions Required During Installation
• NEVER install the module during a lightning storm.
• Ensure that cables are positioned so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain.
• The power supply must be Class II, FAIL SAFE with double or reinforced insulation between the PRIMARY and SECONDARY circuit/ENCLOSURE and be an approved type acceptable to the local authorities. All national wiring rules shall be observed.

Limited Warranty
UAB “Topkodas” warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, UAB “Topkodas” shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labor and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original purchaser must promptly notify UAB “Topkodas” in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period. There is absolutely no warranty on software and all software products are sold as a user license under the terms of the software license agreement included with the product. The Customer assumes all responsibility for the proper selection, installation, operation and maintenance of any products purchased from UAB “Topkodas”. In such cases, UAB “Topkodas” can replace or credit at its option.

International Warranty
UAB “Topkodas” shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure
To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to UAB “Topkodas” must first obtain an authorization number. UAB “Topkodas” will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty
This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:
• Damage incurred in shipping or handling;
• Damage caused by disaster such as fire, flood, wind, earthquake or lightning;
• Damage due to causes beyond the control of UAB “Topkodas” such as excessive voltage, mechanical shock or water damage;
• Damage caused by unauthorized attachment, alterations, modifications or foreign objects;
• Damage caused by peripherals (unless such peripherals were supplied by UAB “Topkodas”.);
• Defects caused by failure to provide a suitable installation environment for the products;
• Damage caused by use of the products for purposes other than those for which it was designed;
• Damage from improper maintenance;
• Damage arising out of any other abuse, mishandling or improper application of the products.

Items Not Covered by Warranty

(i) Freight cost to the repair center;
(ii) Products which are not identified with UAB “Topkodas” product label and lot number or serial number;

Poducts disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection or testing to verify any warranty claim.

Under no circumstances shall UAB “Topkodas” be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser’s time, the claims of third parties, including customers, and injury to property. The laws of some jurisdictions limit or do not allow the disclaimer of consequential damages. If the laws of such a jurisdiction apply to any claim by or against UAB “Topkodas”, the limitations and disclaimers contained here shall be to the greatest extent permitted by law. Some states do not allow the exclusion or limitation of incidental or consequential damages, so that the above may not apply to you.

Disclaimer of Warranties

UAB “Topkodas” neither assumes responsibility for, nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

WARNING:
UAB “Topkodas” recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs
UAB “Topkodas” will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to UAB “Topkodas” must first obtain an authorization number. UAB “Topkodas” will not accept any shipment whatsoever for which prior authorization has not been obtained. Products which UAB “Topkodas” determines to be repairable will be repaired and returned. A set fee which UAB “Topkodas” has predetermined and which may be revised from time to time, will be charged for each unit repaired. Products which UAB “Topkodas” determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

WARNING - READ CAREFULLY

Note to Installers
This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the users of this system.

System Failures

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some but not all of these reasons may be:

• Inadequate Installation

The module must be installed properly in order to provide adequate protection.

• Criminal Knowledge

This system contains security features which were known to be effective at the time of manufacture. It is possible for persons

With criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

• Access by Intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.

• Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

• Failure of Replaceable Batteries

Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

• Compromise of GSM network

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent signal interference.

• System Users

A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the module and that they know how to respond when the system indicates an alarm

• Smoke Detectors

Smoke detectors may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fire is equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, and improper storage of flammable materials, overloaded electrical circuits, and children playing with matches or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

• Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

• Warning Devices

Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

• GSM network

If GSM network are used to transmit alarms, it may be out of service for certain periods of time.

• Insufficient Time

There may be circumstances when the system will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.

• Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

• Inadequate Testing

Most problems that would prevent the module from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an accident, or any kind of construction activity inside or outside the premises.

•Security and Insurance

Regardless of its capabilities, the module PROGATE is not a substitute for property or life insurance. The module PROGATE also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation.