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 a versatile gate controller with a relay output and programmable inputs or outputs, supporting up to 800 remote users. It enables remote control of automatic gates and other equipment, providing high-level security and automation for residential homes and other secure areas.

Users can operate devices via the SERANOVA app, phone calls, or SMS. The controller recognizes up to 800 user phone numbers and can send customizable SMS alerts to up to 8 administrators about input and output status changes. It can also send event messages to a security company receiver.

PROGATE is user-friendly and can be programmed remotely via Internet Cloud Service or USB using the SERA2 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 °C / -40 to 185 °F
- Operational temperature range from -30 to +75 °C / from -22 to 167 °F
- Max relative humidity under +40 °C / 104 °F 95%

Package weight 90g

Module weight: 70g

Overall dimensions of the module:

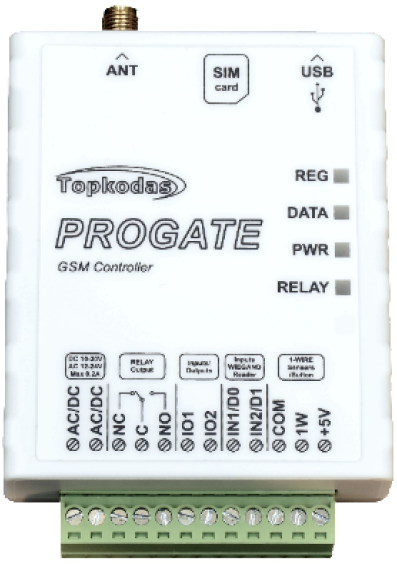
73x62x26mm

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

Din Rail mounting adapter

Digital Temperature/Humidity Sensor Am2305

Waterproof Digital Thermal Probe or Sensor DS18B20

4G LTE Antena 5dBi 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

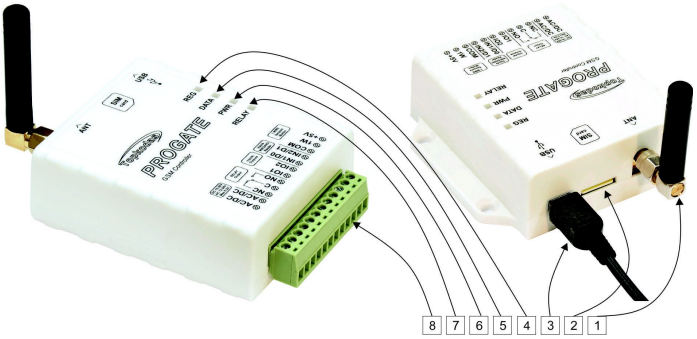


Figure 1 General view of the module PROGATE

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

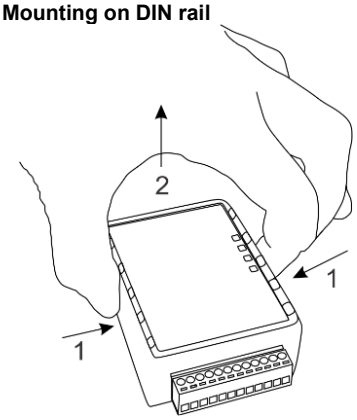


Figure 2 remove the top lid

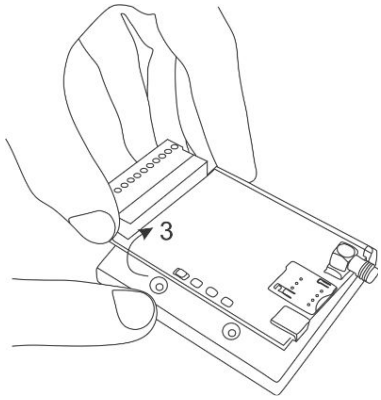


Figure 3 Remove the PCB board

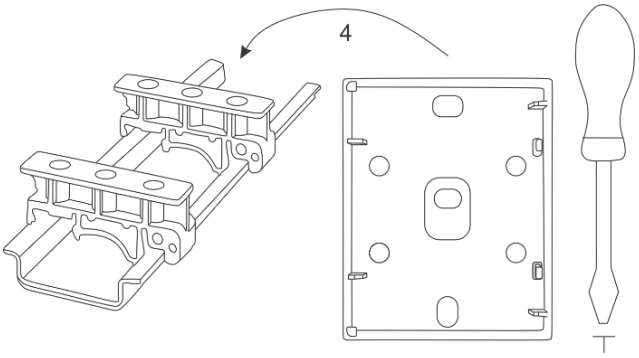


Figure 4 Fasten DIN rail adapters to the base of the case

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

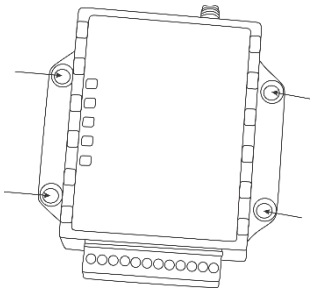
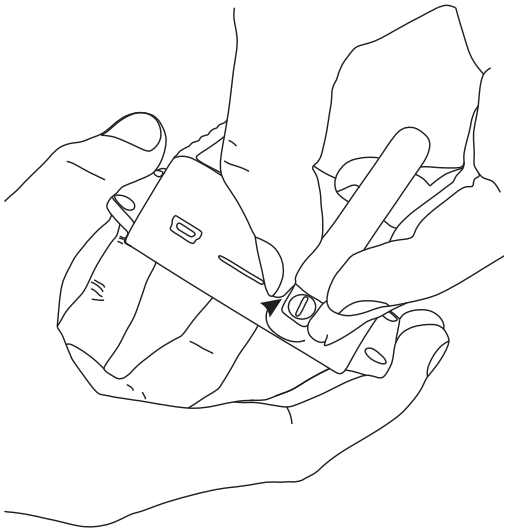
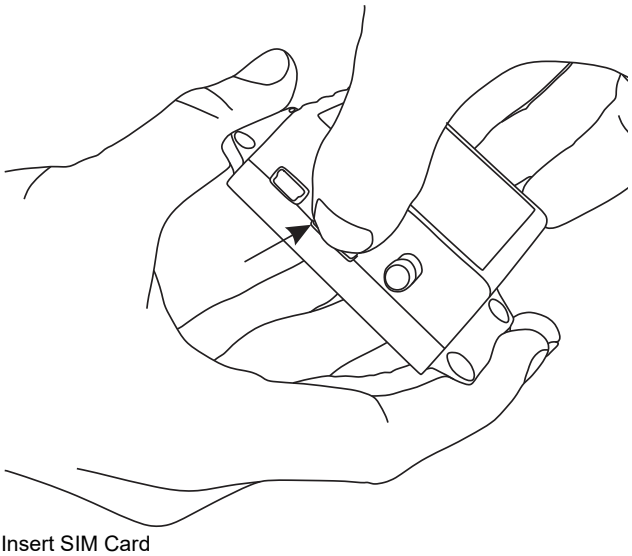


Figure 5Fasten the base of the case

2.2 Preparation



Screw the GSM antenna



Insert SIM Card

2.3 Wiring PROGATE to the gate control unit

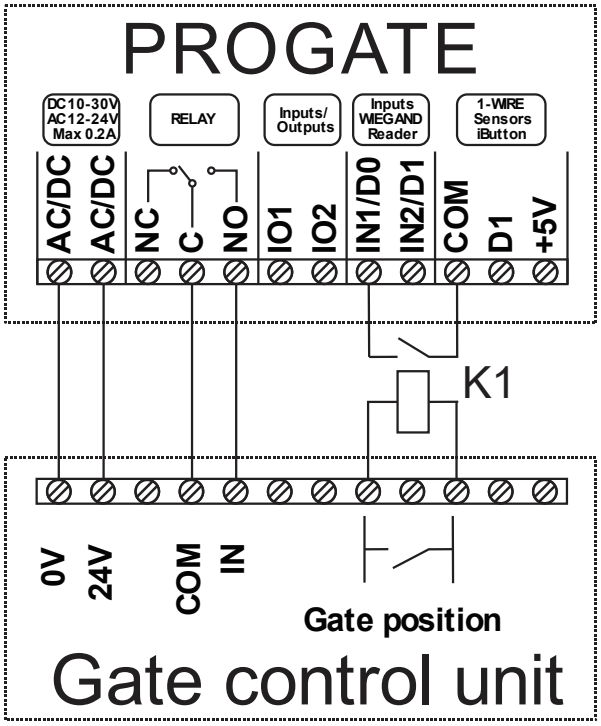


Diagram 1General connection

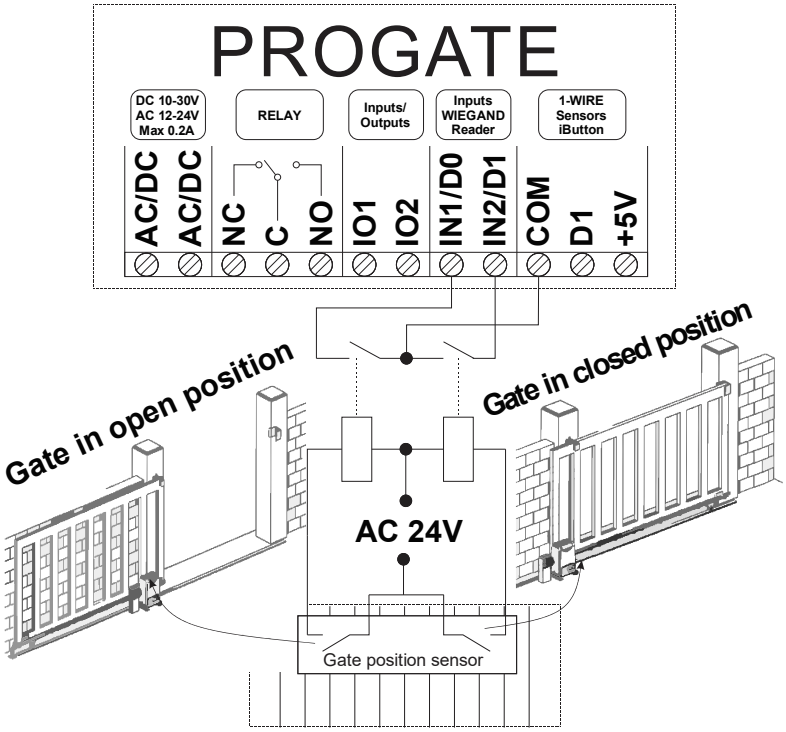


Diagram 2Connection with dual gate position sensor to detect fully open and fully closed gate status

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 come with a control input for connecting the PROGATE relay, enabling operation through pulse or latch signals. They also have a position sensor output for gate status indication. As shown in the diagram, relay K1 links to the gate's voltage output. When the gate opens, K1 activates PROGATE's IN1 input, providing gate status visible 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

2.3.1 Connecting PROGATE to Automatic Gate with Magnetic Sensor

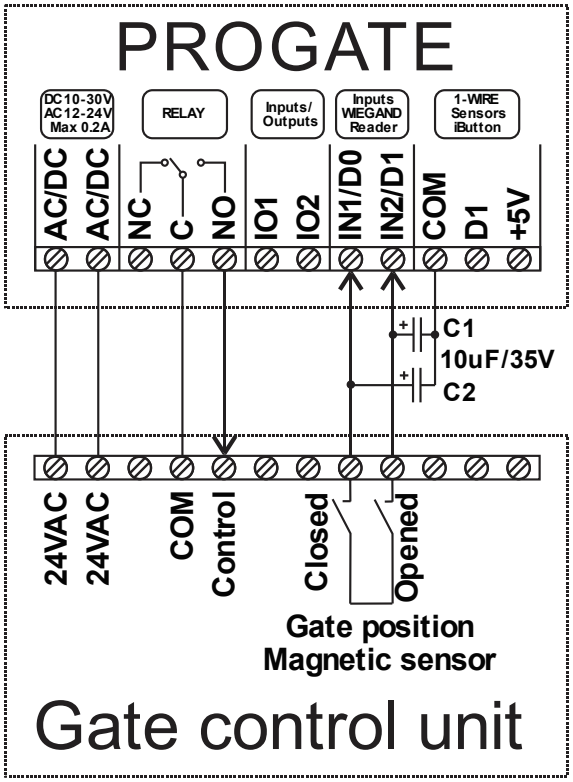
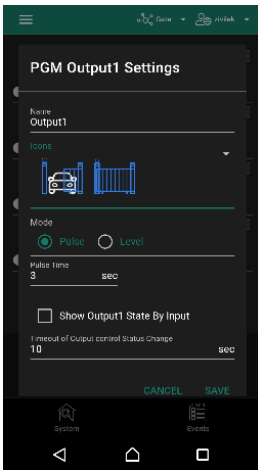
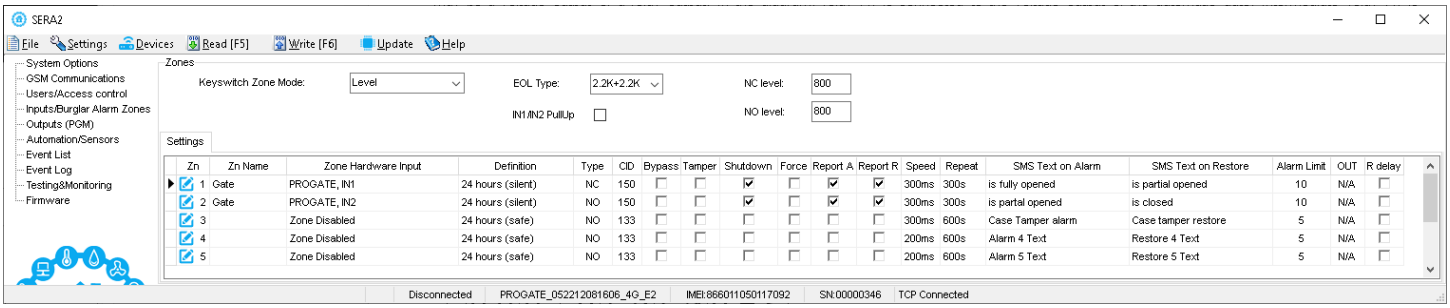


Diagram 3

This wiring diagram and settings have been tested with the **BFT DEIMOS BT** series sliding gate automation with magnetic position sensor.

- Connect the PROGATE relay contact and power supply to the control unit according to the wiring diagram.
- Connect the Closed/Open terminals of the gate position magnetic sensor to IN1/IN2 of PROGATE as shown in the diagram. If necessary, add external capacitors C1/C2 of 4,7-10uF to eliminate pulsations on the inputs.
- SERA2>Inputs set IN1/IN2 internal pull-up resistors off.
- SERA2>Inputs set NC/NO input level ADC trigger to 500-800. The ADC value may be differ depending of magnetic sensor model. Run SERA2>Testing&Monitoring to check real ADC valued during gate position sensor is opened/closed. The ADC trigger value is proportional to the system voltage of 12 V.
  This means that if you need to activate an input with an ADC value of 2000 and the system voltage is 24 V.
  ADC=2000/(24/12)=1000. You need to enter value 1000.
- Set input names and alarm/restore text if needed. It will be used for SMS and event log.
- In SERANOVA output settings set:
  - Name, Icon.
  - Mode [Pulse]
  - Pulse time 2s
  - Reflect output state by Input1





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.*

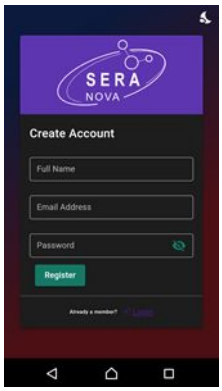
SMS command to set APN DATA/GPRS/LTE network settings. Some networks require exact APN name to be entered, otherwise data connection will not work. Network APN can be configured using SERA2 via USB or following SMS command:
INST000000␣008␣APN#LOGIN#PSW# where: APN=the name of network APN default=”internet”, 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/

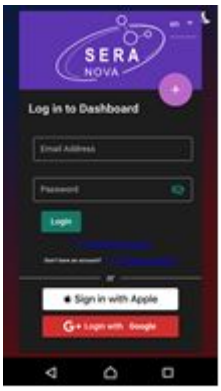
SERANOVA app for iPhone iOS: https://apps.apple.com/app/SERANOVA-smart-home/id1596644632?platform=iphone
Android SERANOVA app: https://play.google.com/store/apps/details?id=com.SERANOVA.cloud&hl=en&gl=US

2. **Register** or sign in to your account.
3. To add a system, the device's IMEI is required. Obtain the IMEI by:
   - Making the initial call to the device. The first caller becomes the owner and administrator and receives an SMS with the IMEI from PROGATE. Copy the IMEI, which serves as the module's UID and allows connection to the free SERANOVA app.
   - Sending an IMEI request SMS command INST000000␣100␣1 to the controller's SIM card number. The sender will receive an SMS response with complete device information, including the IMEI.
   - Reading the IMEI via USB using the SERA2 configuration program from *System Options* > *System Info*
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 the **User Access Code** (default: 123456). Without a user access code, the system cannot operate. This code serves as both the user ID and password within the system. Each user must have a unique code, which is located in the user table. The system administrator creates and provides these codes to each user.
   - 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

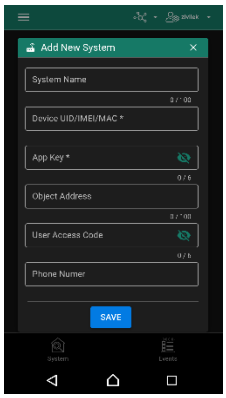
Enter a valid email address of a user who already has a SERANOVA account. The system will be automatically added to the user's account. If the user is added without a valid SERANOVA account email. The user can create a SERANOVA account later and add the system manually.



1.Install SERANOVA app
2.Create account

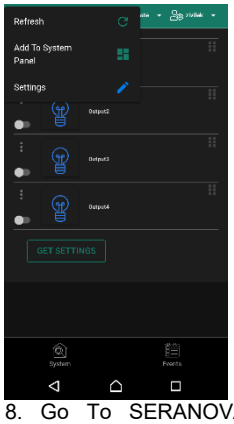


3.Log In
4. The first person to call the PROGATE SIM card number becomes the owner and administrator.

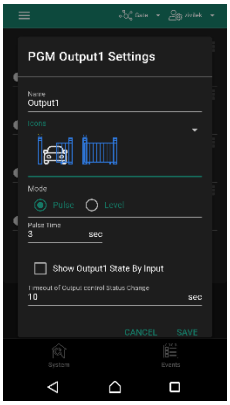


5. PROGATE sends a message with the IMEI
6. Enter the IMEI and App Key (Default 123456), **Enter User access code (Default 123456)**

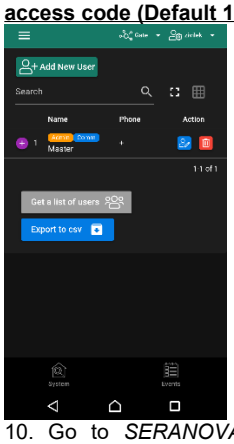
7. The system is now manageable



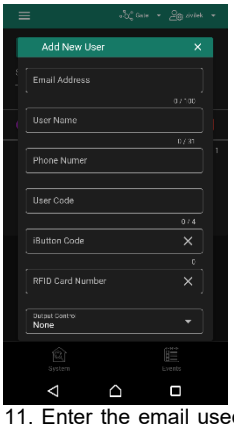
8. Go To SERANOVA> Menu> Outputs. Edit settings



9. Select pulse or level



10. Go to *SERANOVA> Menu> Users:* Press *[Add New User]* Owner or administrator can add other users or administrators



11. Enter the email used to create the SERANOVA account, along with your unique user code. Please note, system control is not possible without this user code.

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:

YouTube LT QUICK START SERANOVA app *https://youtu.be/Benf6xKcnjM*

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: *10 SMS Commands for remote control and configuration*

SERA2 software

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

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.

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.

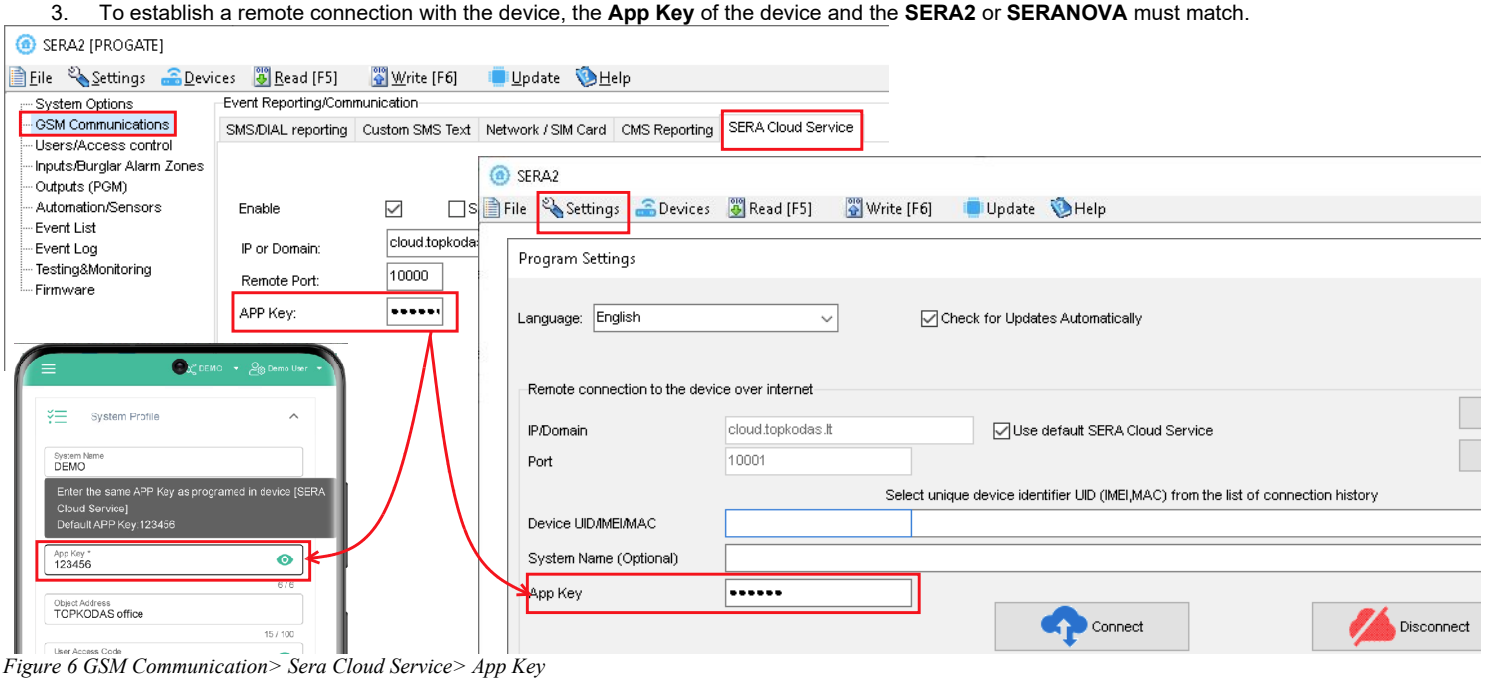


Figure 6 GSM Communication> Sera Cloud Service> App Key

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]

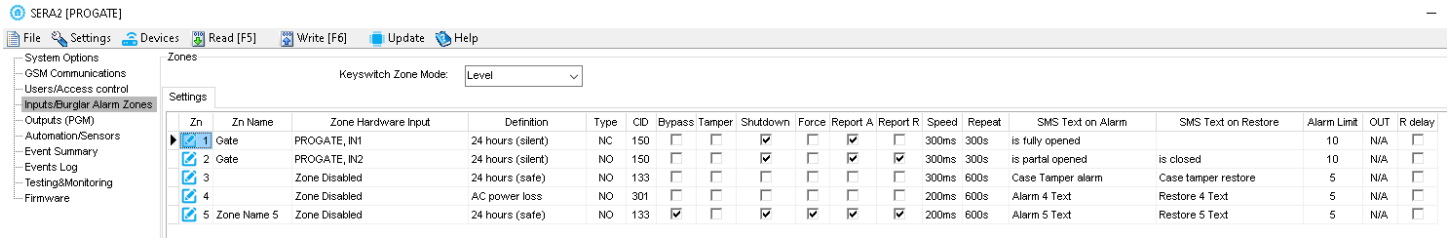


Figure 7SERA2> Inputs/ Burglar Alarm Zones

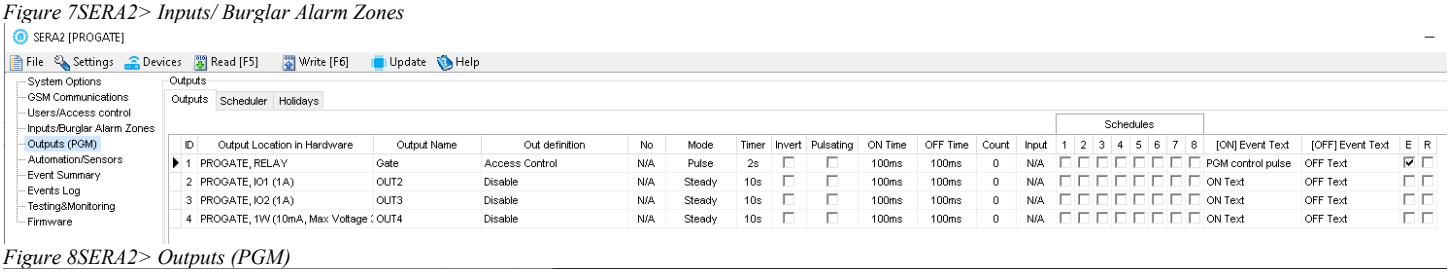


Figure 8SERA2> Outputs (PGM)

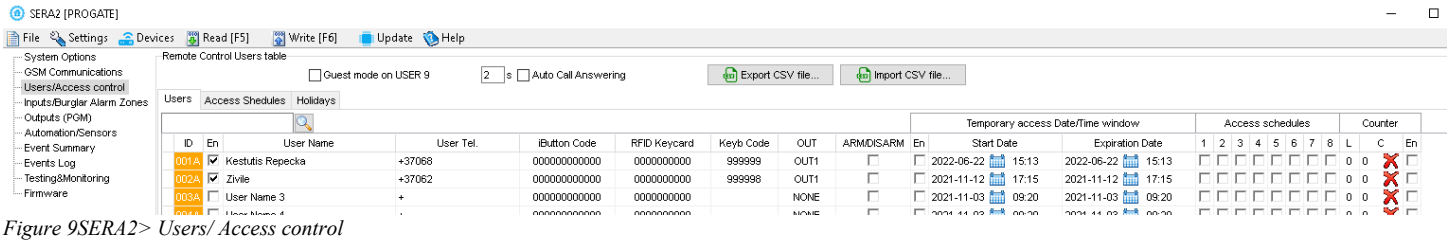


Figure 9SERA2> Users/ Access control

4 System Access: Codes, Passwords, and Permissions

4.1 Default Codes/Passwords and Explanations

Table 5 Default passwords and explanations

Password	Default	Location in SERA2	Explanation
Administrator password	123456	SERA2> System Options> Access	The **'Administrator password'** allows full module configuration access. The system administrator can adjust device settings, update firmware, and set permissions for the **Installer**, specifying which parameters they can modify. This ensures protection of sensitive data such as IP addresses, phone numbers, and other confidential information.
Installer Password	000000	SERA2> System Options> Access	The 'Installer password' allows sending SMS commands with INST identification and provides access to SERA2's programming mode. However, the Installer can only modify or see those module settings in SERA2 that the system administrator has granted permission for. Refer to section *10.1* for more details.
SMS User Password	123456	SERA2> System Options> Access	The '**SMS User Password**' permits sending SMS commands with **USER** identification. The user phone number must also be authorized for remote or SMS control. The default SMS user password is 123456, used for module control with USER commands. Refer to section *10.2* for more details.
App Key	123456	SERA2> GSM Communications> Sera Cloud Service	The **'APP Key'** links to the **'SERA Cloud service'**, allowing remote access through the **SERA2** or **SERANOVA** app. For a successful connection, the code must match on both the device and app. ! For users with multiple systems, use the same '**App Key**' across all systems. Different App Keys on the same SERANOVA account can cause functionality issues.
User Code (APP/Keyboard)	123456	SERA2> Users/Access> Users Table[Code] column	The **'User Code'** is a unique identifier for controlling the system via the **SERANOVA** app or **Wiegand keypad**. The default Master Code is 1234 or 123456, based on the format. ! This code must match on the device and in the **SERANOVA** app under *Settings > System Profile > User Access Code*. Without the correct code, users cannot control the system.
SIM card PIN	1234	SERA2> GSM Communications> Network/SIM Card	It is automatically ignored if pin request in SIM card is disabled

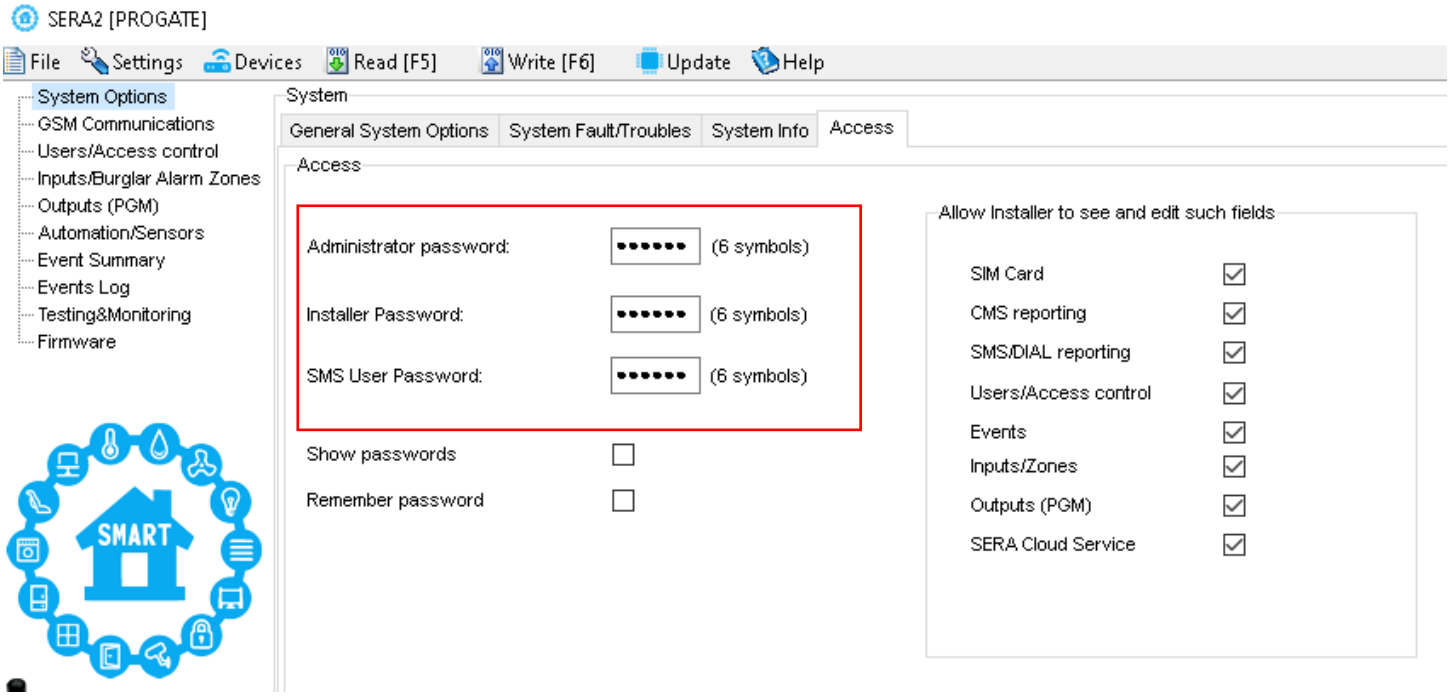


Figure 10System Options> General System Options

4.2 User codes for access control via keypad and SERANOVA app

Each user requires a unique code for system control via the SERANOVA app or Wiegand keypad. The default Master Code is either 1234 or 123456, depending on the code format. To set this up:

- Choose a 6 or 4 digit user access code format in *SERA2> System Options> General System Options > [User Access Code Format].*
- The system administrator or installer assigns a unique code for each user in *SERA2> Users/ Access control in* user table [Code].
- To open the gate, control outputs, or ARM/DISARM the security system via the SERANOVA app, enter your unique code provided by the system administrator in SERANOVA > Settings > System Profile > User Access Code. Each user must have a distinct code.

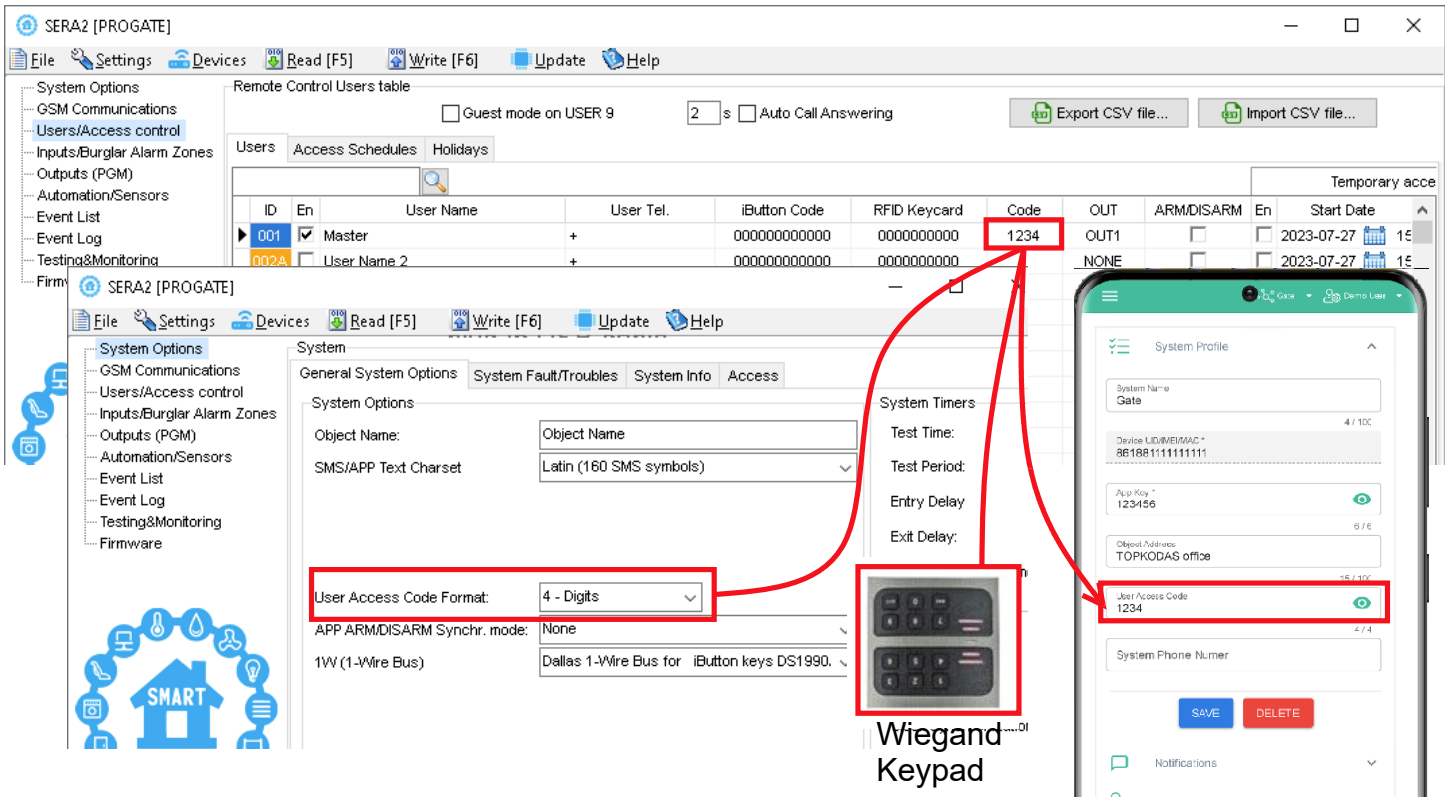


Figure 11User/ Access control and System Options> General System Options

5 Wiring of Wiegand Keypad, RFID Card Reader, and iButton Probe

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

The 1-Wire interface (1W) by Maxim-Dallas is used for iButton DS1990A keys (with unique 64-bit IDs) and temperature sensors. The system can accommodate up to 800 keys. The first key, automatically registered upon contact with the reader and confirmed by two beeps, is the MASTER key with assigned control functions. The 1-Wire bus length can be up to 100 meters, depending on cable quality and environmental noise.

Figure 12 Wiegand keypad wiring

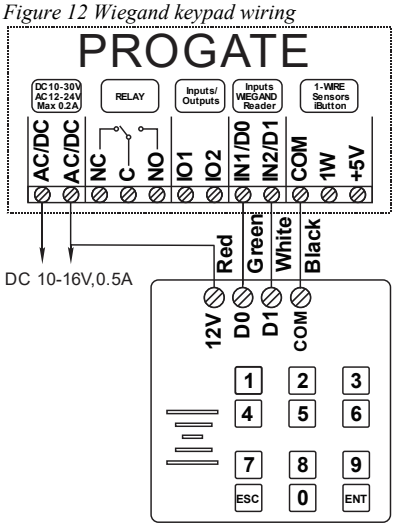


Figure 13iButton connecting diagram

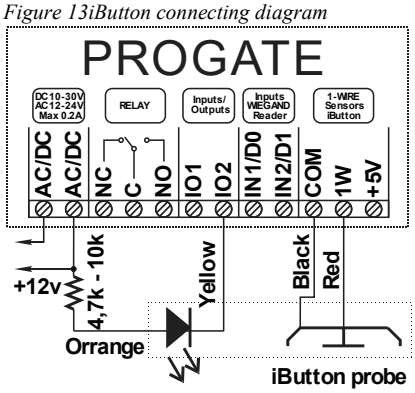
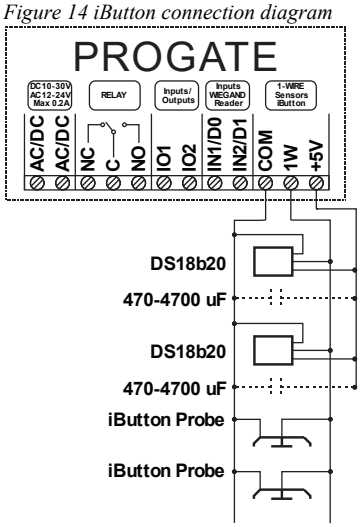


Figure 14 iButton connection diagram



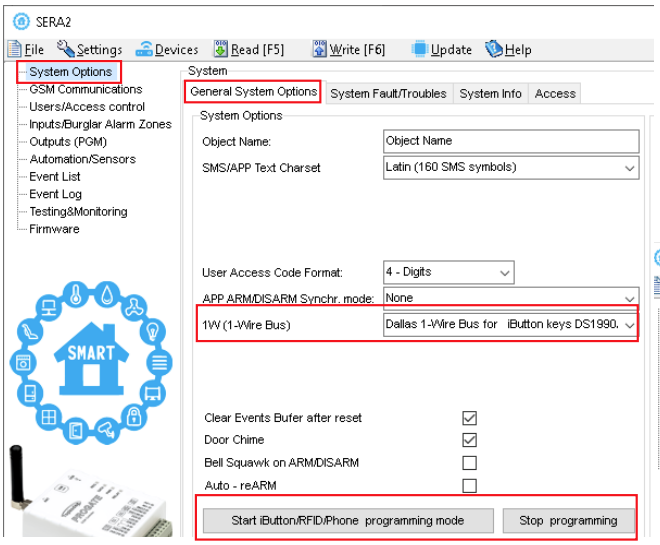
5.1.1 Adding iButton, RFID, and Phone Numbers to the Module's Memory

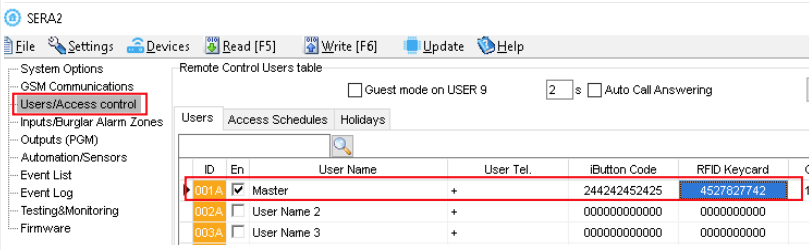
First steps:
- Connect iButtons or RFID reader to the module.
- Insert SIM card;
- Screw GSM antenna;
- Connect power supply;
- Connect the module to the computer.

Configuration methods:
- Start automatic learning mode via mini USB cable (SERA2 software).
- Start automatic learning mode via SMS command INST000000_063_1
- Enter Keycard numbers manually via mini USB cable (SERA2 software).
- Start automatic learning mode remotely via SERA2 software.

If you want to edit existing configuration,
- Press [**Read**] to view the current configuration.
- Make the necessary edits.
- Press [**Write**] to save the changes.

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





- Navigate to *SERA2* > *System Options* > *General System Options.*
- Select the 'Dallas 1-Wire Bus' option (for iButton keys).
- Click on [**Write**].
- Click on [**Start iButton/RFID/Phone Programming Mode**].
- Navigate to *SERA2* > *Users/Access Control*.
- Touch the RFID keycards or iButton keys to the reader. The key numbers will appear in the list.
- To finish, go back to *System Options* > *General System Options* and click on [**Stop Programming**].

- You can edit additional settings in the Users/Access Control window. Remember to click [**Write**] after making changes.
- Navigate to *RT Testing & Monitoring* > *Hardware* and click on [Start Monitoring].
- Finally, go to *RT Testing & Monitoring* > *Security Alarm Panel/Access*

Start the automatic key programming mode by SMS command

> **!** Before starting programming iButton keys using SMS command, ensure 'Dallas 1-Wire Bus for iButton keys DS1990A' is selected in SERA2>System Options > General System Options> 1W(1-Wire Bus) list box.

- 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.

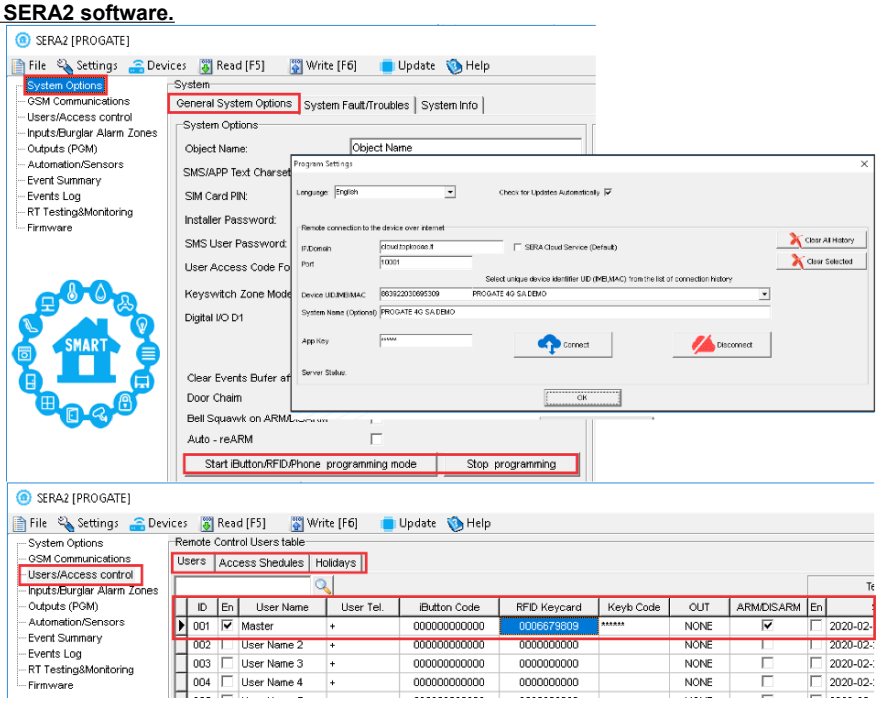
0- Disable iButton keys learning mode,
1- Enable iButton keys learning mode,
2- IButton keys deleting mode. Delete these keys from memory, which will be touched to the reader.

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 tab [**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 parameters: IMEI/UID and App Key
- 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.

6 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
- Outputs can be controlled via short call, SMS, RFID, iButton, or the SERANOVA app. This is particularly useful such as gate opening.
- The system supports automatic scheduling, including holidays.
- Programmable algorithms for outputs operation: Access Control /CTRL/SMS/DIAL, SIREN, BUZZER, ARM state, Zones OK, Light Flash, inverting, pulse mode

The output responds to specific system events or remote control via App, SMS, Caller phone number, iButton, or RFID. It's versatile for tasks such as operating garage doors, activating lights, controlling heating, managing watering, and more.

! If an output is not in use, it should be disabled. A disabled output cannot be toggled ON or OFF until it is re-enabled.

6.1.1 Bell, Relay, and 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.

Connect devices to the designated outputs as illustrated below. For sound signaling, a DC 12V siren up to 1500mA is recommended. Use a 2 x 0.75 sq. mm double insulation cable for siren connection. Install an auxiliary buzzer indoors near the entrance. This buzzer works in tandem with the main siren during exit/entry delay periods. A piezoelectric 12V DC, 150mA max buzzer, like the PB12N23P12Q model or similar, can be used.

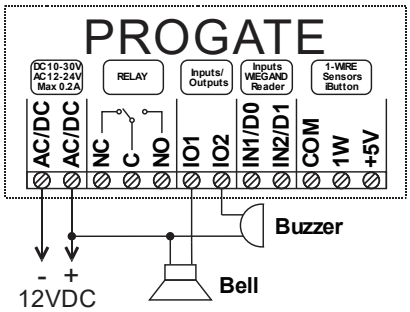


Figure 15 Bell, buzzer connection to I/O1, I/O2

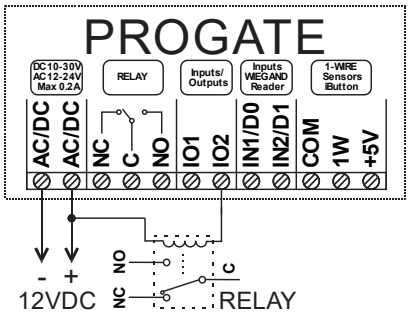


Figure 16 Relay connection to , I/O1, I/O2

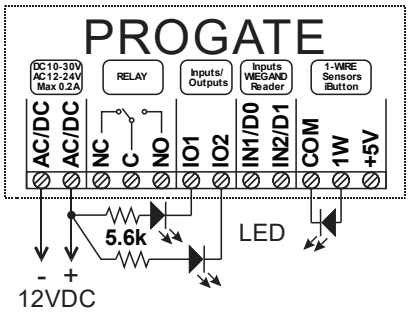


Figure 17 LED connection toI/O1, I/O2

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.

Users can customize the SMS text message that is sent when an automatic PGM output action occurs.
To set output parameters:

- Go to *SERA2 > Device > PROGATE > Outputs.*
- Input the necessary parameters.
- Disable any unused outputs.
- Click the [**Write**] to save changes.

To modify an existing configuration:

- Click [**Read**] to load the current configuration.
- Edit settings
- Click [**Write**] to save the updated configuration.

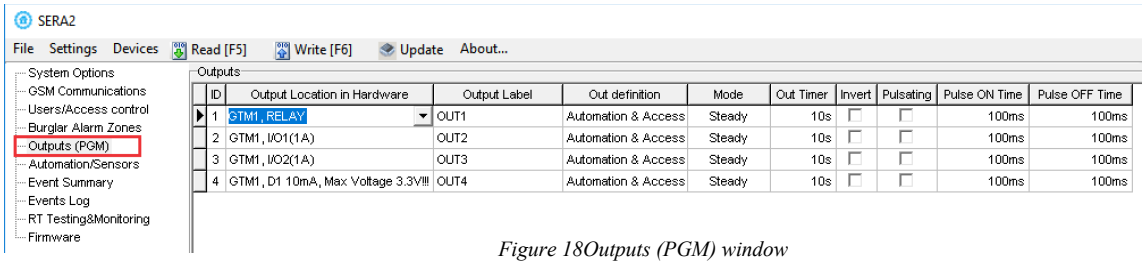
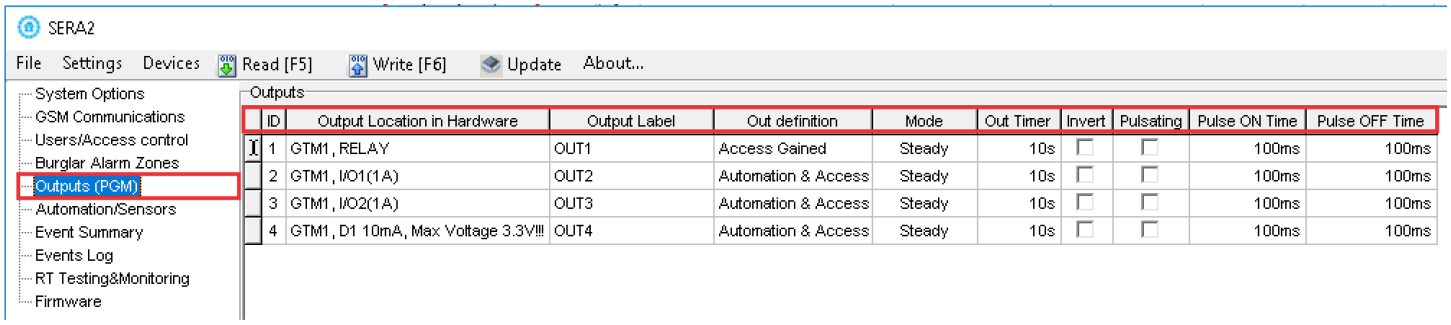


Figure 18Outputs (PGM) window

6.1.2 Output Programming

Quick start outputs

- Install SERA2 software (refer to section at *3.5.2*).
- Connect the module to your computer via a mini USB cable.
- Open the 'Outputs (PGM)' window in SERA2.
- Set parameters for the chosen output: Set definition (options include disable, bell, buzzer, flash, system state, etc.)
- Mode (pulse, steady(latch), Pulse Count
- Invert operation if required.
- Click [**Write**] to save your settings.



ID	Output Location in Hardware	Output Label	Out definition	Mode	Out Timer	Invert	Pulsating	Pulse ON Time	Pulse OFF Time
1	GTM1, RELAY	OUT1	Access Gained	Steady	10s	☐	☐	100ms	100ms
2	GTM1, I/O1(1A)	OUT2	Automation & Access	Steady	10s	☐	☐	100ms	100ms
3	GTM1, I/O2(1A)	OUT3	Automation & Access	Steady	10s	☐	☐	100ms	100ms
4	GTM1, D1 10mA, Max Voltage 3.3V!!!	OUT4	Automation & Access	Steady	10s	☐	☐	100ms	100ms

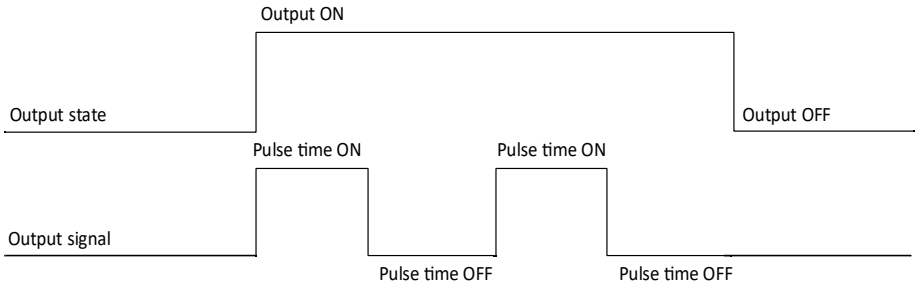
Figure 19 Outputs (PGM) window

To modify an existing configuration:

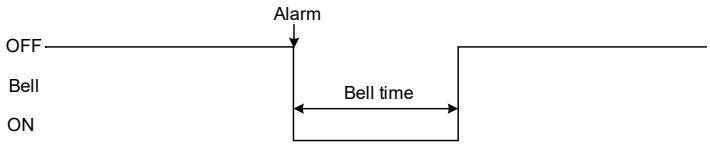
- Click on [**Read**] to load the current settings.
- Make the necessary changes.
- Click on [**Write**] to save the updated configuration.
- Write edited configuration press [Write]

In pulsating mode (timer), the output behaves as follows:

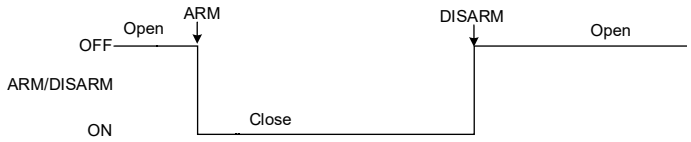
- Upon activation, the output operates for a specified "Out Timer" interval or steady pulsating.
- The relay contact alternates between ON (for "Pulse time ON") and OFF (for "Pulse time OFF").
- This ON-OFF cycle continues until the output is deactivated.



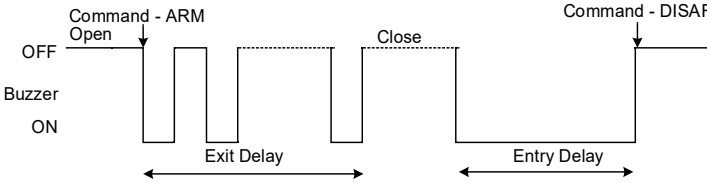
Bell: Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.



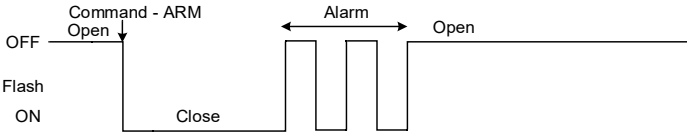
ARM/DISARM: Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.



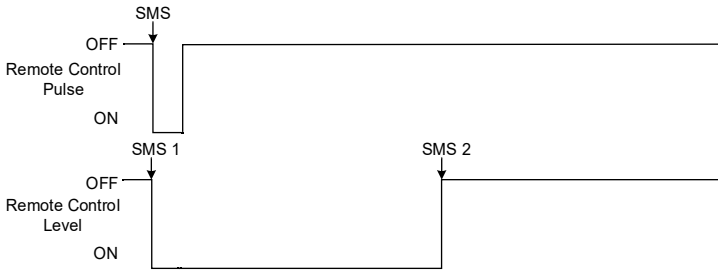
Buzzer: Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.



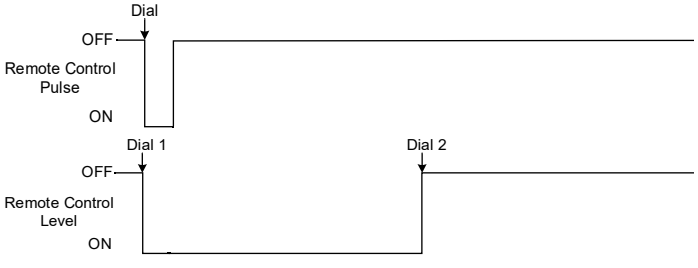
Flash: Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



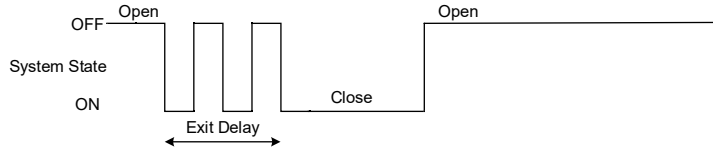
Remote Control: Output designed for connection of electrical devices which will be controlled by SMS message or phone call a) control by SMS message



Remote Control b) control by phone call

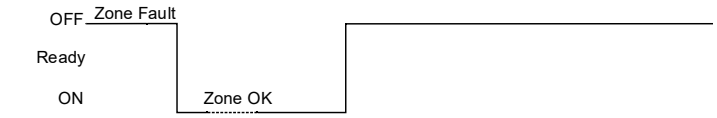


System State: Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.

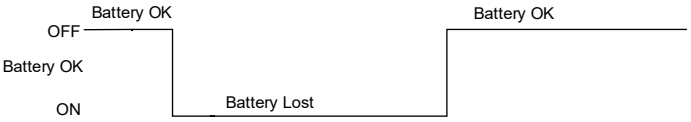


AC OK: Output for connection of indicator about control panel supply from alternating current

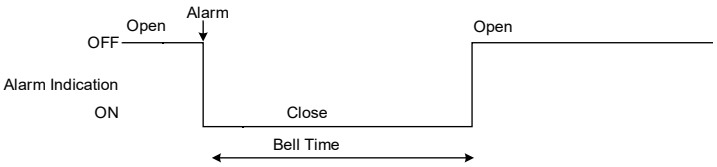
Ready: Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.



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

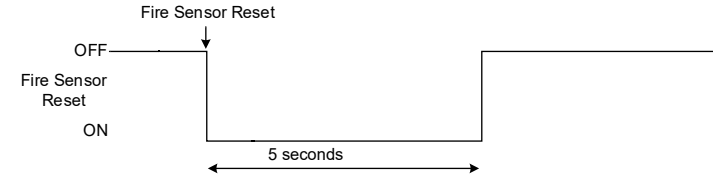


Alarm indication: Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.

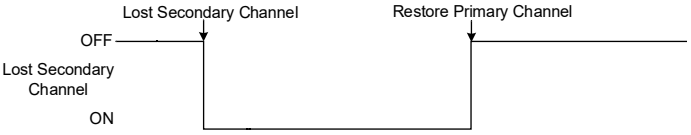


Lost Primary Channel: Output where a continuous signal is generated when communication with primary channel was lost.

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.



6.1.3 Output Control with User Access

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

The [**Access Control**] output definition algorithm functions as follows:

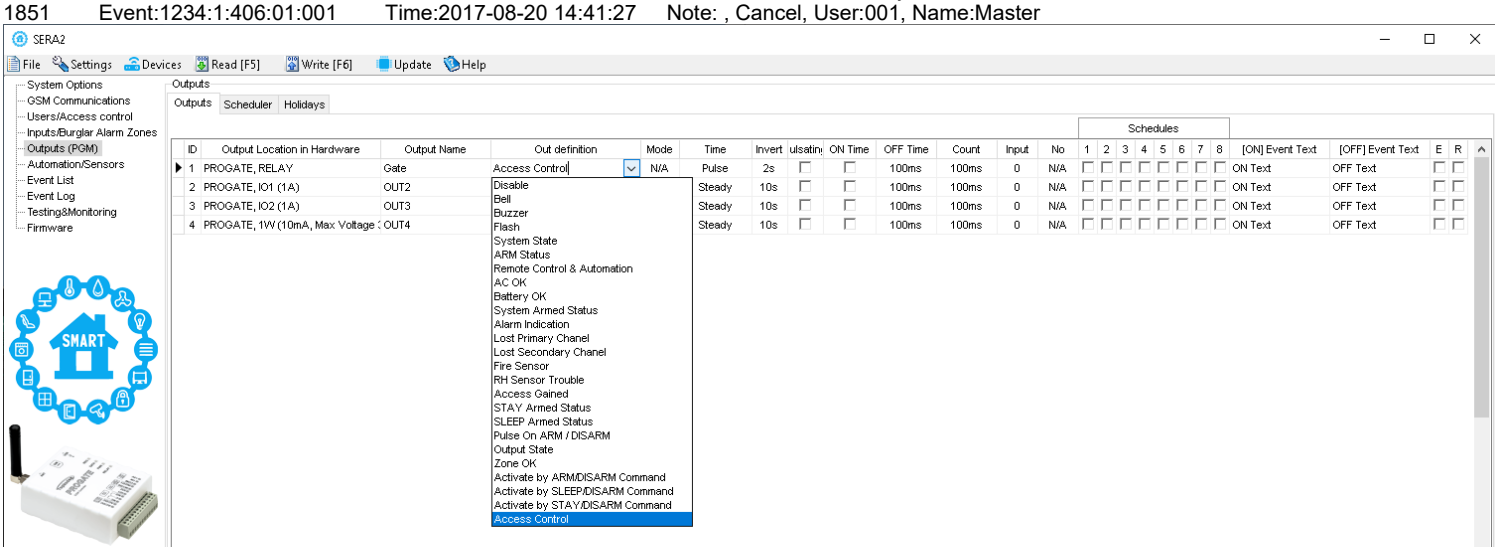
- User activates the output (e.g., connected to a Gate) through the SERANOVA app, Call, SMS, iButton key, or Wiegand reader, the system logs a '422' CID 'Access Gained' event.
- Additionally, if output ON/OFF events are enabled, the system can log a '780' CID event, indicating 'The output state has been changed by the user'.

The **[Access Gained]** output definition (algorithm) operates as follows:

- Users with the right to ARM/DISARM the system always have access to control this output.
- Users without the right to ARM/DISARM the system (indicated by an unmarked field near ARM/DISARM in window *SERA2> User/ Access control*) can only access this output when the system is disarmed.
- When a user is granted access, the event 'Access granted' (CID code 421) is logged. If access is denied, the event 'Access denied' (CID code 422) is logged (see *SERA2> Events Log*).
- If the output is defined as [Automation / CTRL], it can be controlled by the user in any manner, but it will not generate events CID codes 421 and 422.

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



7 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,

7.1 Input / zones wiring NC/NO/EOL/Tamper

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

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.

All inputs has pull up resistors 10k (IN1,IN2 is configurable)

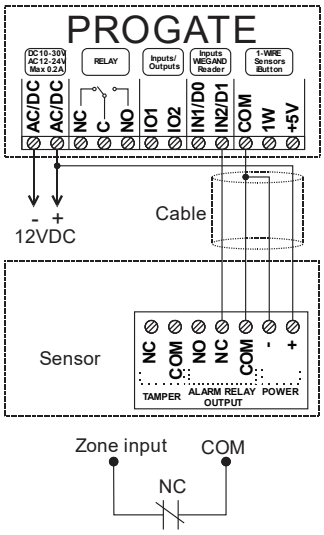


Figure 20NC Contacts, No EOL

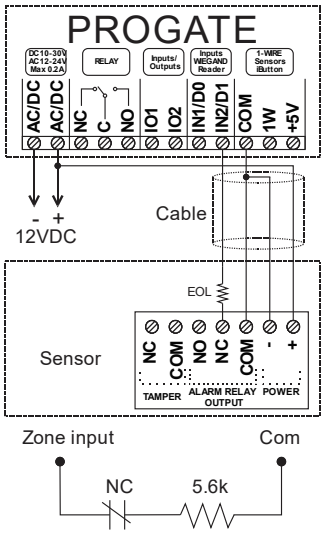


Figure 21 NC, With EOL

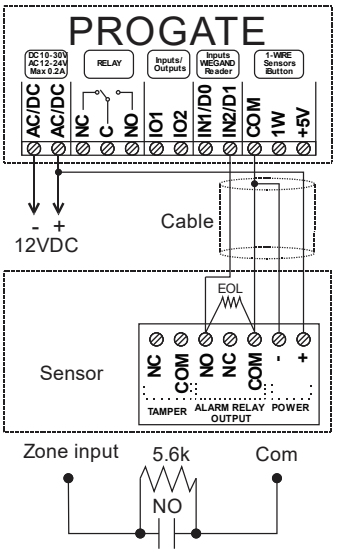


Figure 22 NO, With EOL

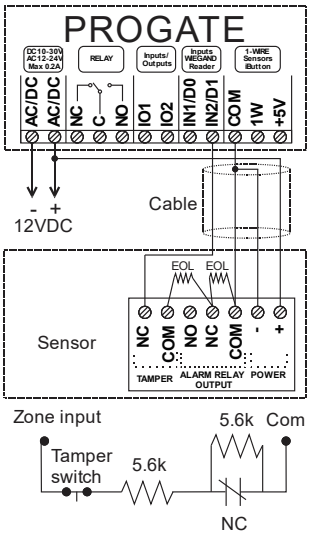


Figure 23NC With EOL Wire Fault Recognition

Refer to: Zones programming

8 SERA2 configuration software

The SERA2 software is a configuration tool for the PROGATE module, allowing local configuration via USB or remote configuration via the GPRS/LTE network. It simplifies the system configuration process by enabling use of a personal computer. We recommend programming the PROGATE module with SERA2 software. Here's how to install and start it:

- Open the folder containing the SERA2 software installation and click on the "SERA2 setup.exe" file.
- If the software installation directory is correct, click [Next]. If you want to install the software in a different directory, click [Change], specify the new installation directory, and then click [Next].
- Verify the entered data and click [Install].
- After successful installation of the SERA2 software, click [Finish].
- To start the SERA2 software, go to Start > All programs > SERA2, or navigate to the installation directory and click on "SERA2.exe".

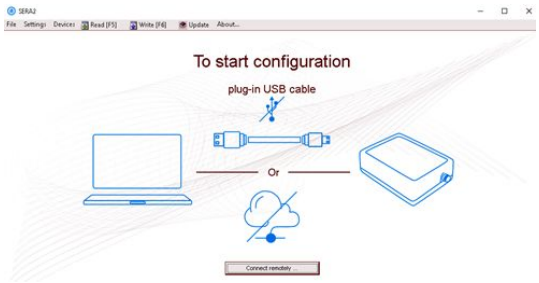


Figure 24Sera2 software

Connection of the module to PC

The module requires a power supply of DC 10-33V or AC 12-24V, with a maximum of 0.2A. Ensure that the module has a SIM card inserted (with a topped-up account and PIN code request removed). The module should be connected to the PC via a 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

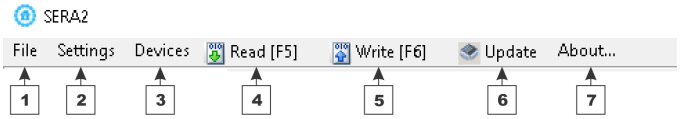


Figure 25 Command line

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

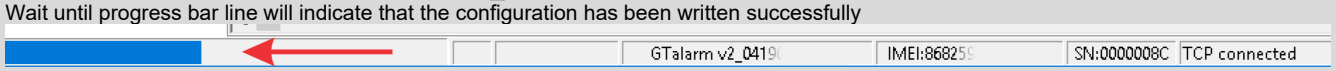


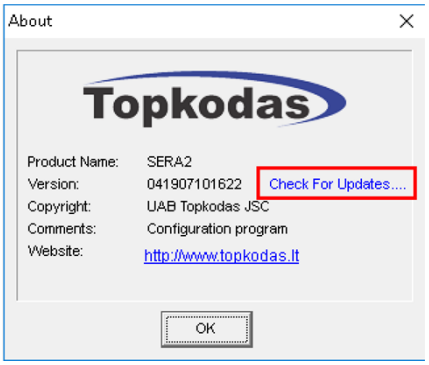
Figure 26 Progress bar

After configuring the module, you can save all settings to your PC. This saves time when using the same configuration in the future, as you won't need to set the same parameters again. To save the current module configuration:

- Press the [**Read**] to load the current module configuration.
- **Edit** the configuration
- Go to File, then select "**Save As**" or "**Save**".
- To load a saved configuration, go to File > **Open**. This allows you to copy the same programmed content into as many modules as required.

To receive software updates:

- Go to **Settings** and select "**Check for Updates Automatically**". The program will notify you when a new update is available.
- Start the update process when prompted.
- Connect the module to your computer using a mini USB cable.
- Write the update to the PROGATE module by pressing the [Update] button in the SERA2 software.
- If you want to update the module manually, press [Update]



For support with configuration software or device-related questions, follow these steps:

- Press the [Read] to read the configuration from the module.
- Go to "*File* > *Save As*" and save the configuration.
- Save the Events Log file.
- Send these files along with your question to the seller. These steps will let better understand the problem and will reduce the time to find the solution.

Remote configuration or firmware updates via an internet cloud service may be slower than USB connections. The solution is that multiple modules can be configured on the same computer concurrently. The speed of reading and writing configurations remains unaffected as these processes run in parallel. Multiple instances of the SERA2 program can be operational simultaneously.

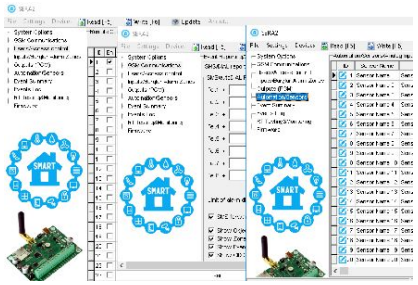


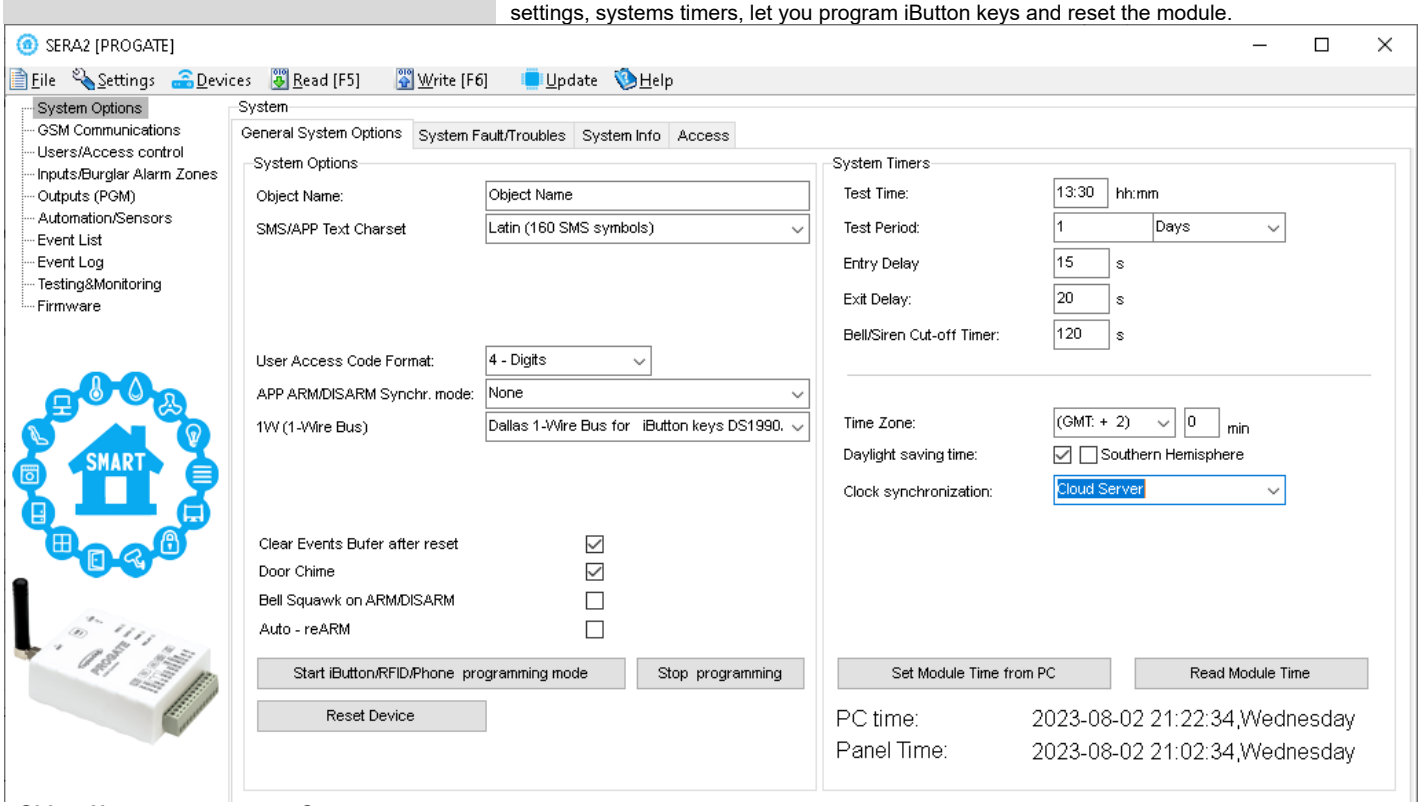
Figure 27configuration at the same time. Unlimited number of modules

8.1 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.

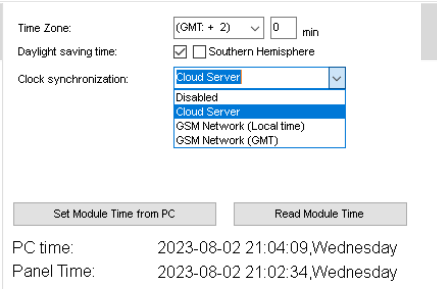
System Options > General system Options

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



Object Name	System name
SIM Card PIN	SIM card PIN code. Default 1234
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.
SMS User Password	The default SMS User Password is **123456**. This code allows you to utilize arming method, as well as program user codes.
User Access Code Format	A 4-digit or 6-digit user access code format can be selected.
1W (1-Wire Bus)	1W Digital I/O Mode. 1-Wire bus / Digital Input / Digital Output
Clear Event Buffer After Reset	When the cell is checked, the memory of unsent reports will be deleted after the module resetting
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
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.
Auto re-ARM	The module can be programmed to arm the module if there is no activity in the area after the system disarming.
Start iButton/RFID programming	All added iButton keys or RFID cards will be registered in the order of sequence by clicking Start programming
STOP iButton/RFID programming	To finish entering iButton keys or RFID cards, click Stop programming button
Test Time	Auto Test report time of day
Test Period	Auto Test report period
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.
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.
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.
Time Zone	System time zone.
Daylight saving time	
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.
Read module time	To read the clock of module.

8.2 Real-time clock Time Zone and Synchronization



The SERA2 software allows setting the PROGATE real time clock 'Time Zone' and automatic 'Daylight Saving'. Correct settings are crucial for modules using automatic schedules, as incorrect time zones can lead to erroneous schedule activation times.

Users can opt to set the module time from their PC for immediate synchronization.

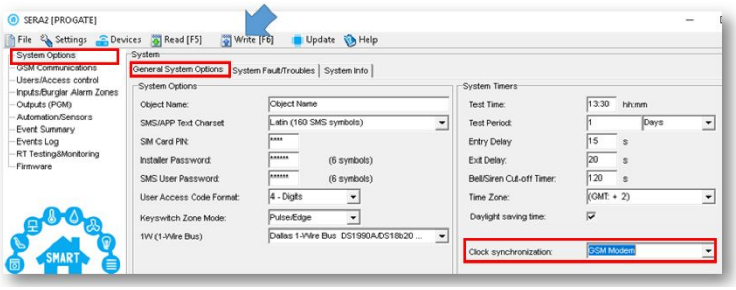
When connected to a monitoring station via an IP connection, the system's date and time will automatically synchronize with the monitoring station.

Time synchronization options include: GSM Modem, Cloud Server, or disabling it.

! If the module has been connected first time to the power supply, or power supply has been disconnected, 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

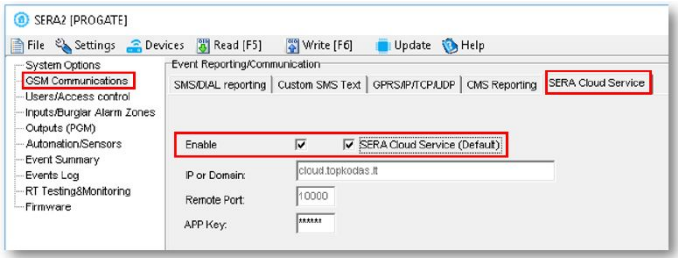


Figure 29 SERA2> GSM Communication> SERA Cloud Service

- Go to *SERA2> System Options> General System Options*
- Set Clock synchronization via Cloud Server
- Press [**Write**]

Clock synchronization via Cloud server

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

Figure 28SERA2> System Options> General System Options

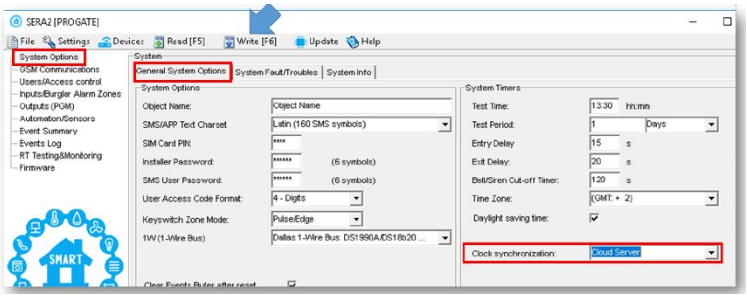


Figure 30 SERA2> System Options> General System Options

8.3 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.

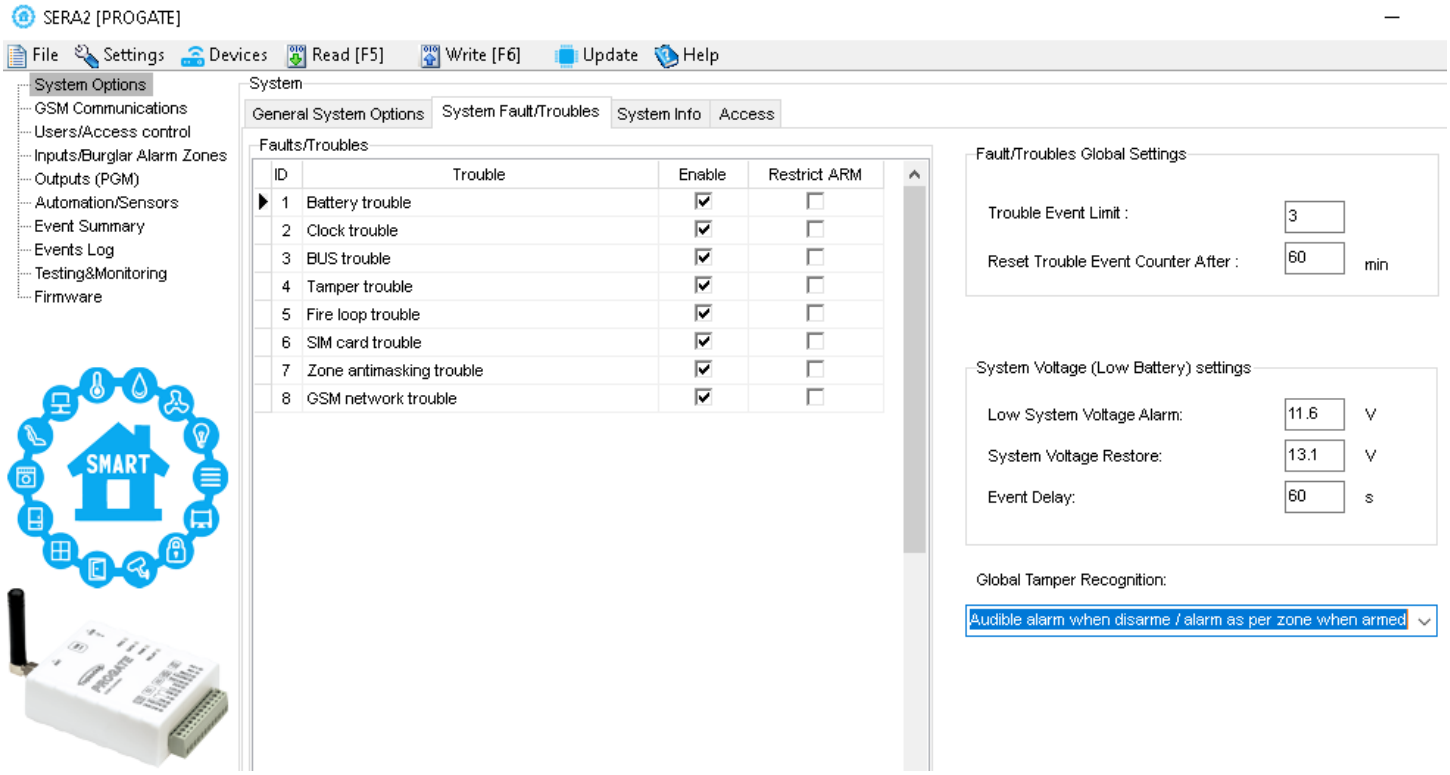


Figure 31 System Options> System Fault/ Troubles window

Trouble	This column lists potential system troubles
Enable	The system will detect a marked trouble
Restrict ARM	In case of such trouble, the arming activation will be restricted.
Battery trouble	Low system voltage. Power supply or backup battery voltage is low, needs to be recharged, or replaced.
Clock trouble	The time and date has not been set.
BUS trouble	The expansion device is no longer communicating with the module.
Tamper trouble	The zone(s) that was tampered
Fire loop trouble	The trouble is occurring with your smoke detectors.
SIM card trouble	Not available or impossible to read SIM card.
~~Zone ant masking trouble~~	Do not available in this module
GSM network trouble	SIM card is not registered with the GSM network provider
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.
System Voltage Restore	The module has detected that the system voltage has been restored.
Event Delay	System low voltage trouble event report delay.
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).
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.

- 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.

8.4 Zones programming

- PROGATE includes 2 wired zones and 2 programmable I/O inputs.
- Detection devices can be connected to the module's zone terminals, with each zone's parameters configured accordingly.
- Zone bypassing allows for system arming without restoring a violated zone, which will be ignored if violated or restored during exit/entry delay or when armed.
- Stay mode enables system arming and disarming without leaving the secured area, preventing alarms from zones with the Stay attribute when STAY-armed.
- The system enters Stay mode if a Delay-type zone isn't violated during exit delay and a zone with the Stay attribute exists. An arming method providing exit delay must be used in this case.

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.

In Stay mode, all Delay-type zones function as Instant-type zones.
However, when the system is fully armed, Delay-type zones resume normal operation.

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

The tamper circuit, independent of the system's status, triggers an alarm upon any disruption. Tamper alarm activates the siren/bell, keypad buzzer, and dispatches an SMS to the user. Tamper alarms are initiated by opening the enclosure of any detection device, siren/bell, metal cabinet, or keypad. Enable these alarms by selecting “Tamper Enabled”. If the associated zone is disabled, tamper alarms are suppressed.

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.

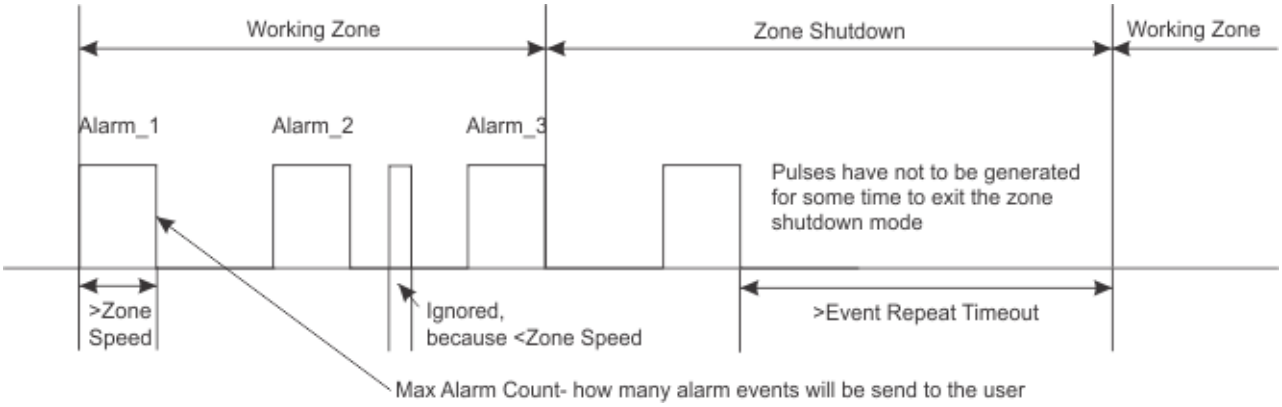
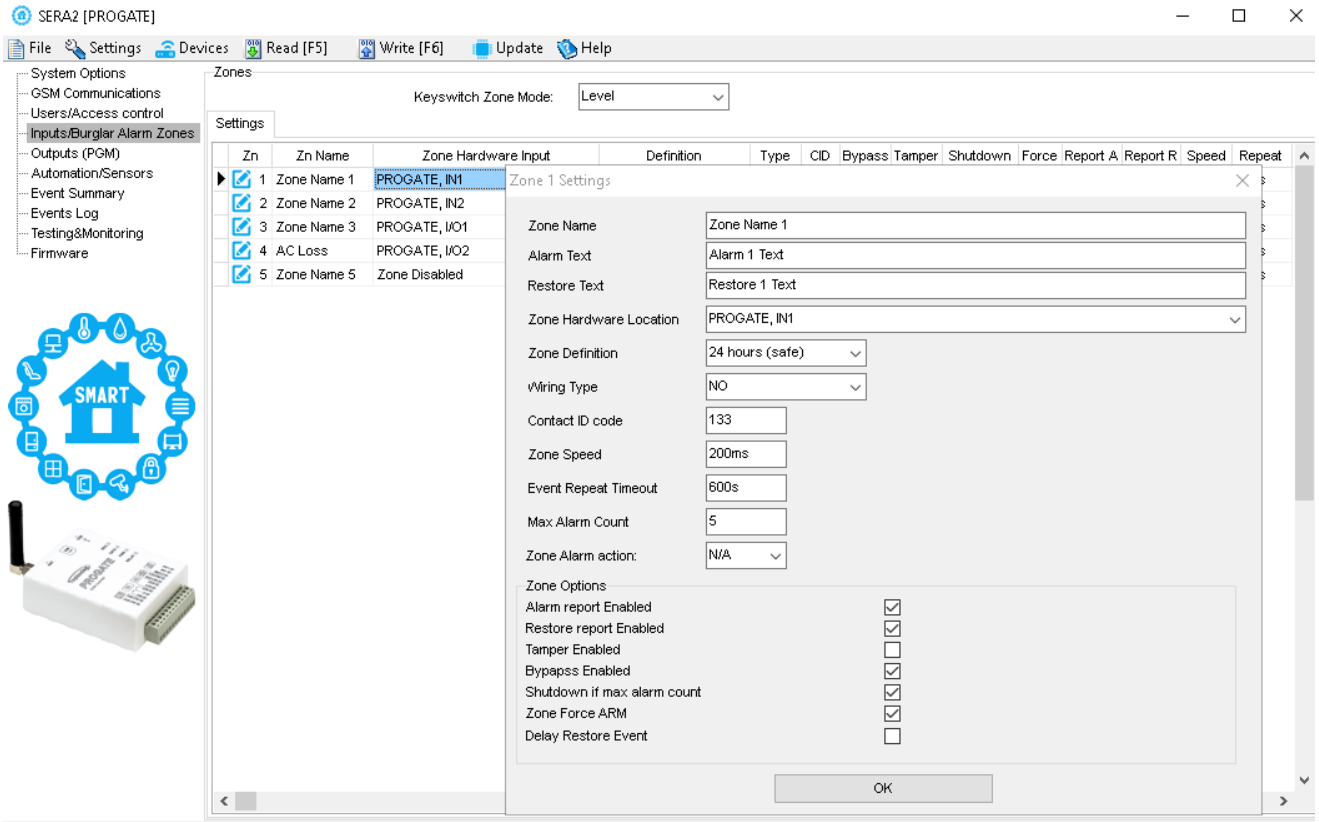
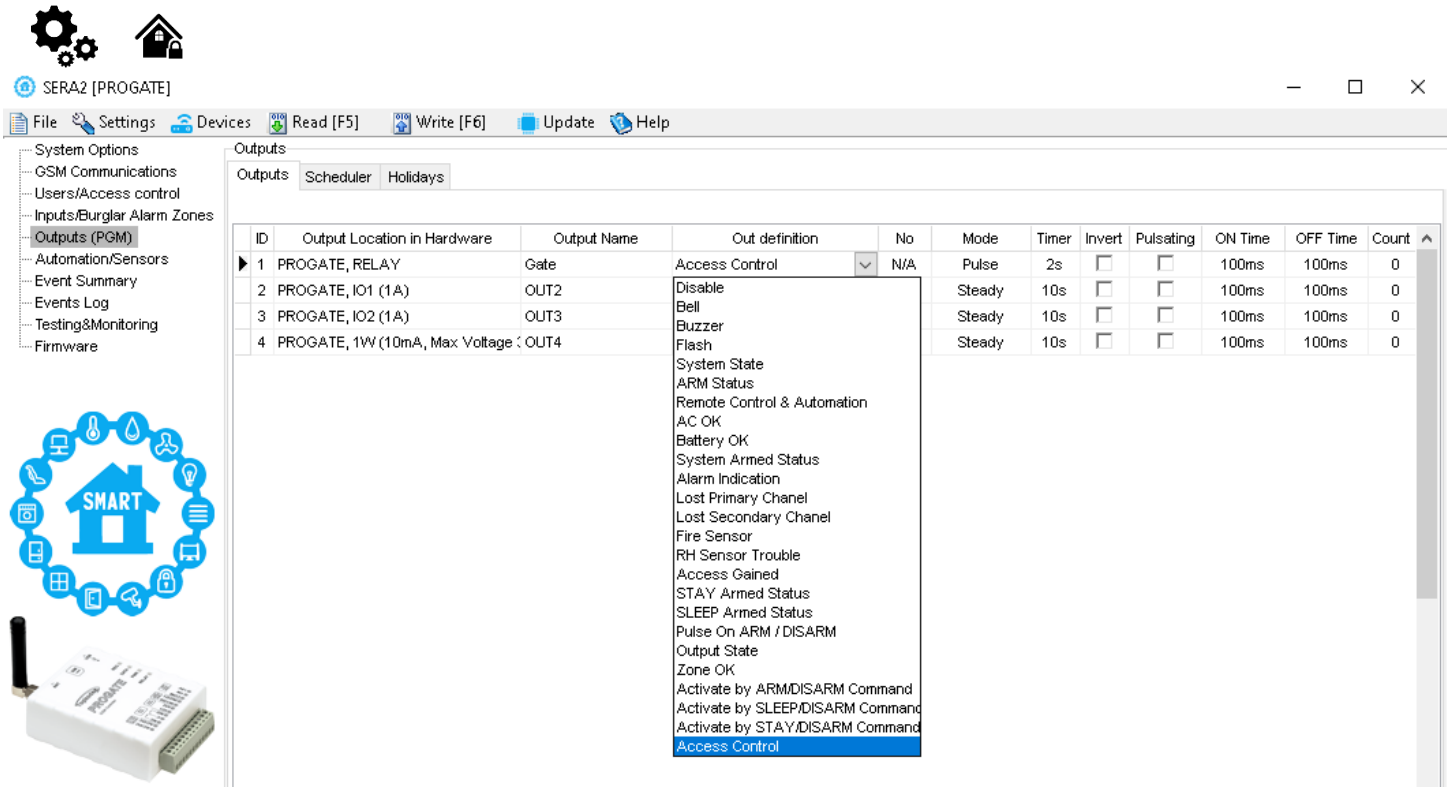


Figure 32the explanation of Zone Speed, Max Alarm Count, and Event Repeat Timeout

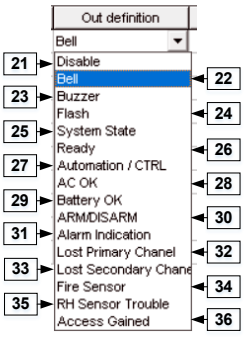


Zone Name	Zone name should be entered.
Assign Module= **Zone Hardware Input**	Select the zone hardware input **Zone Disabled** — Disables the corresponding zone. **, IN1…IN4** — The zone hardware input 1… input 4 assigned **, I/O1… I/O2** — The zone hardware optional Input/ Output 1… Input/ Output 2 assigned
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
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)
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.
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).
Event Repeat Timeout= **Repeat**	Insensitive time to recurrent zone events
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.
Alarm Report Enabled= **Report A**	The system will report alarm event and log it to the event buffer
Restore Report Enabled= **Report R**	The system will report restore event and log it to the event buffer
Tamper Enabled= Tamper	The system will detect a *tamper* condition with one or more sensors on the system
Bypass Enabled= Bypass	The system will allow zones to be Manually Bypassed.
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.
Zone Force ARM= Force	Only **force** zones can be bypassed when the module is Force armed. Fire Zones cannot be Force Zones.
Zone Alarm Action= OUT	determines which output will be activated

8.5 Outputs. Bell & PGM programming



ID	Output sequence number.
Output Location in Hardware	The outputs hardware location.
Output Label	Output name
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	When the alarm system is activated, it generates a pulse signal during the Exit Delay time and a continuous signal during the Entry Delay time or when the system is disturbed. When the alarm system is turned off, it functions like a keyboard buzzer.
24 Flash	This output connects to a light indicator that displays the alarm system's status. It generates a pulsating signal during the Exit Delay time and a continuous signal when the alarm system is activated. The signal stops when the alarm system is turned off.
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.

Mode	Output control mode.	
	36 Steady	Steady ON/OFF mode
	37 Timer	Output ON pulse mode
Out Timer	Pulse time duration can be from 1 to 999999 sec.	
Invert	Inversion is activated	
Pulsating	Pulsating mode is activated. Then output is activated it will pulsate according pulse ON/OFF time.	
Pulse ON Time	Pulsating mode pulse ON duration.	
Pulse OFF Time	Pulsating mode pulse OFF duration.	

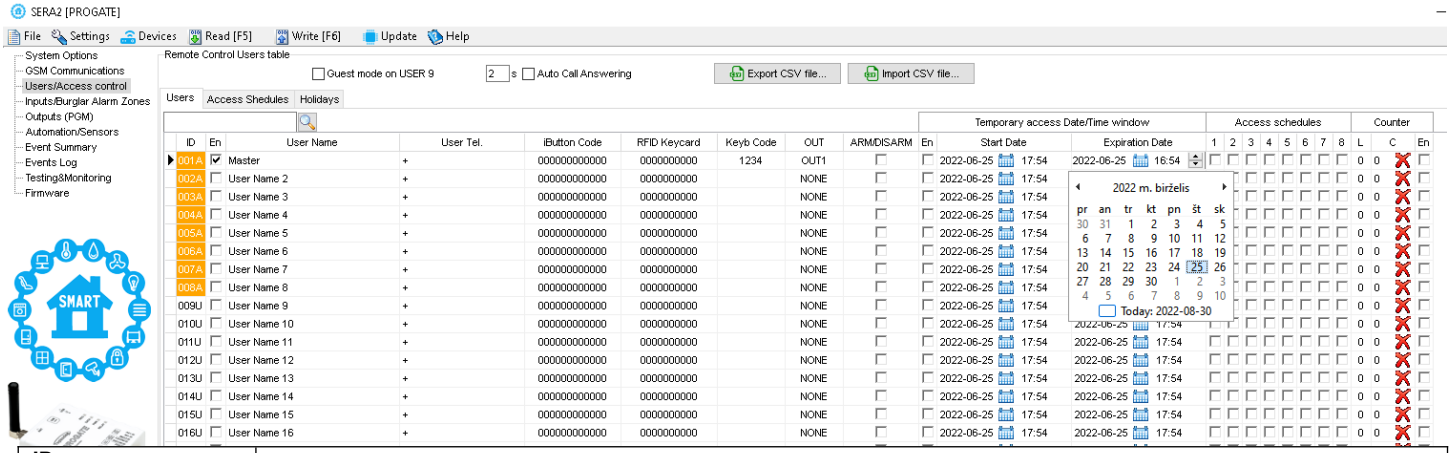
8.6 Users & Access Control programming details.

Users/ Access Control > Remote Control Users Table

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

The system can register up to 800 phone numbers for remote control. Registered users can operate the gate, arm/disarm the system, control outputs via SMS or free calls, and adjust system settings via SMS. Initially, the system accepts calls and SMS from all numbers. However, once a number is registered, the system only responds to listed numbers and ignores unlisted ones. It also rejects SMS from registered numbers if the SMS password is incorrect. The system accepts SMS commands with the 'INST' identifier and installer password from any phone.

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



ID	
User Name	The name of users who will be able to control the module should be entered in this column.
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.
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
RFID Keycard	RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
Keyb Code	Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
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.
ARM/DISARM	If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
MIC	If checked, by calling from the specified phone, the controller responds and you can hear what's going on in the premises

The PROGATE module has User Access Schedules for controlling access. Inputs, outputs, readers, and cards are all set up with schedules that dictate their activation or deactivation times. For example, a user could be granted access to control a specific output from 12:00 a.m. to 6:00 a.m. daily. This time frame, from 12:00 a.m. to 6:00 a.m., Monday through Sunday, is defined as a schedule during which the user can open the Gate. These schedules can be configured under the Users> Access Schedules tab To view User Schedules , click on the "Access Schedules" tab.

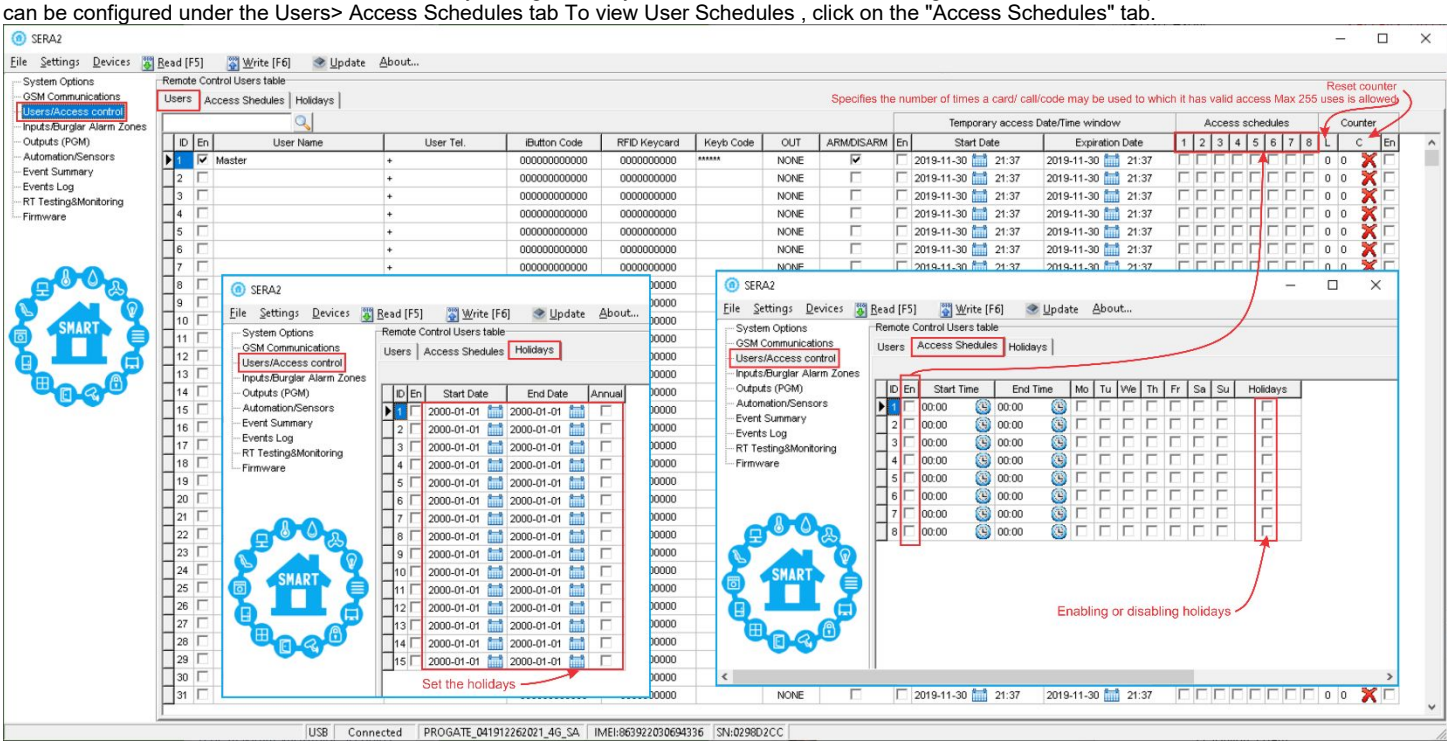


Figure 33 Users/ Access Control > Users, Users Access Control> Access Shedules and Users/ Access Control> Holidays window

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

Lets say need to create create a Cleaning Crew schedule as follows: Monday-Friday from 5 p.m. to 1 a.m., and Saturday-Sunday from 8 a.m. to 1 p.m., excluding holidays. This results in three schedules:

- Monday-Friday, 5 p.m.-11:59 p.m.
- Tuesday-Saturday, 12:00 a.m.-1:00 a.m.
- Saturday-Sunday, 8:00 a.m.-1:00 p.m.

Holidays are treated as special days, superseding regular weekdays. If a Holiday is set, the controller bypasses the schedule, preventing user access during that period. Each Holiday spans a full day, from midnight to midnight.

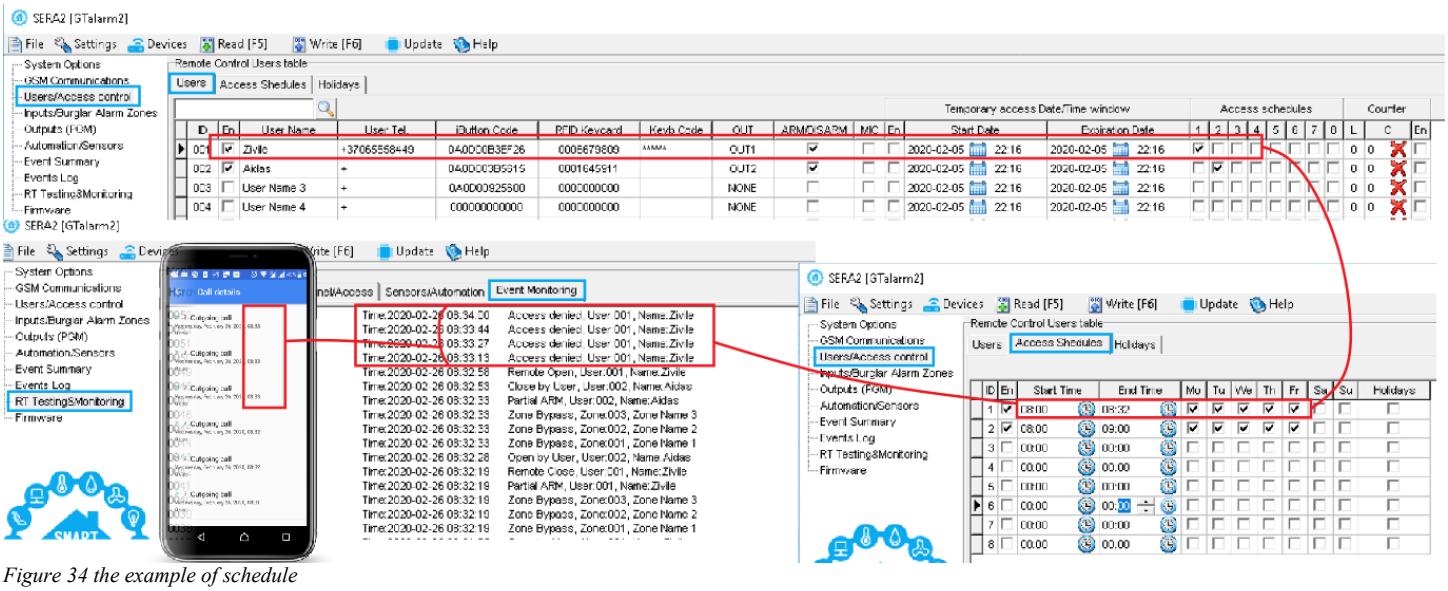


Figure 34 the example of schedule

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

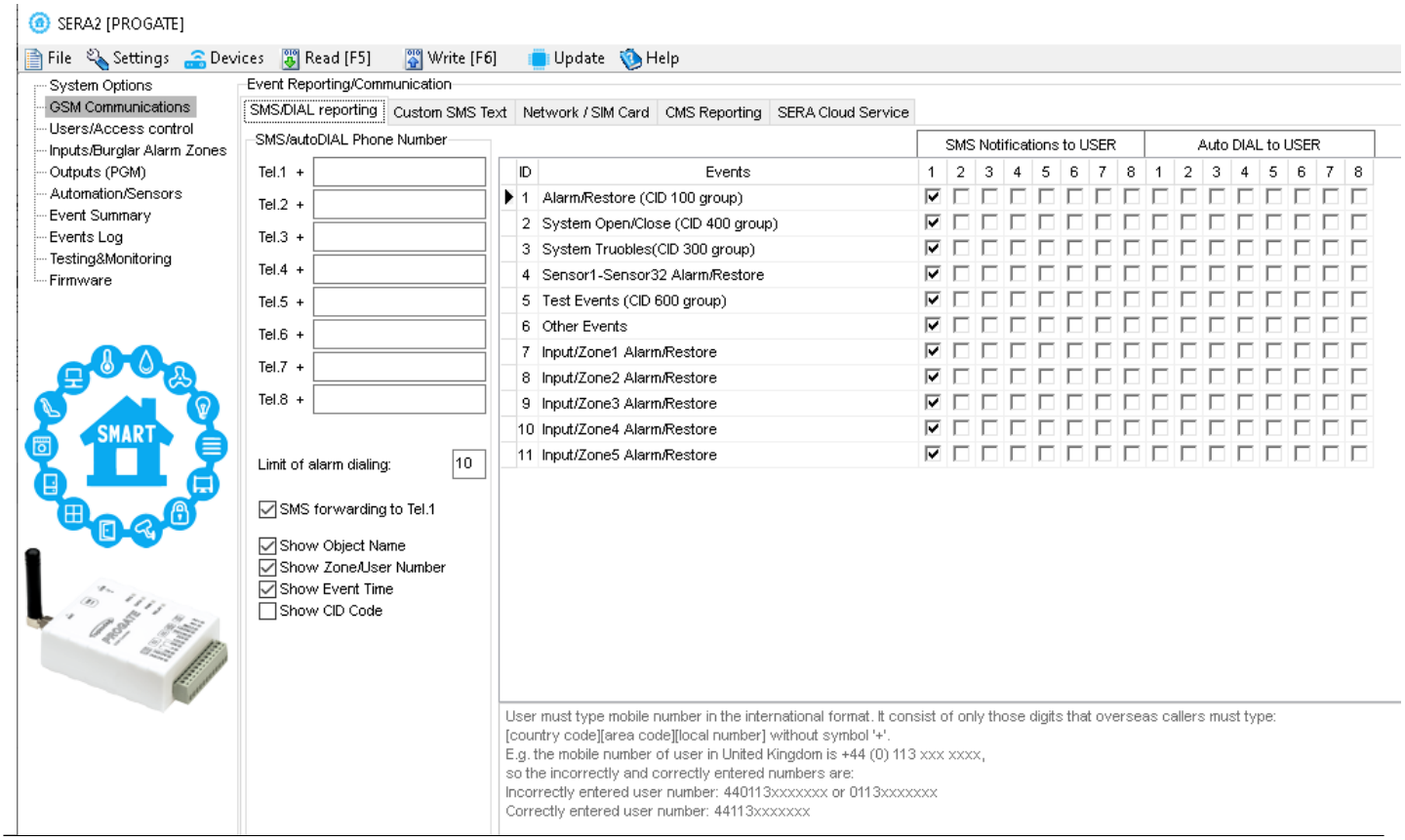
8.7 Event Notifications via SMS & DIAL

GSM Communications > SMS DIAL Reporting

Up to 8 admin users can be set to receive SMS or DIAL notifications. These users can receive alarm phone calls and SMS text messages from the system via a GSM connection. When the gate is opened or the system is armed/disarmed, an SMS notification is sent to the user's phone number. In the SMS and DIAL Reporting settings under GSM Communications, users can input their phone numbers and select the events they wish to be notified about.

When a zone or tamper is violated, the system triggers an alarm. The alarm sequence is as follows:

- The siren/bell is activated. If the violated zone is of Fire type, the siren/bell emits a pulsating sound. Otherwise, the sound is steady.
- The system attempts to send an SMS text message, containing the violated zone's name. Each violated zone triggers a separate SMS. If the user's phone number is unavailable, the system tries the next listed number assigned to the same zone. Unavailability can be due to the mobile phone being switched off or out of GSM signal coverage. By default, the system continues to send the SMS to the next listed numbers in priority order, repeating as many times as programmed.
- If programmed, the system attempts to call the first user phone number via GSM, with each violated zone triggering a separate call. If the user is unavailable, the system dials the next listed number assigned to the same zone. Unavailability can be due to the mobile phone being switched off, out of GSM signal coverage, or busy.

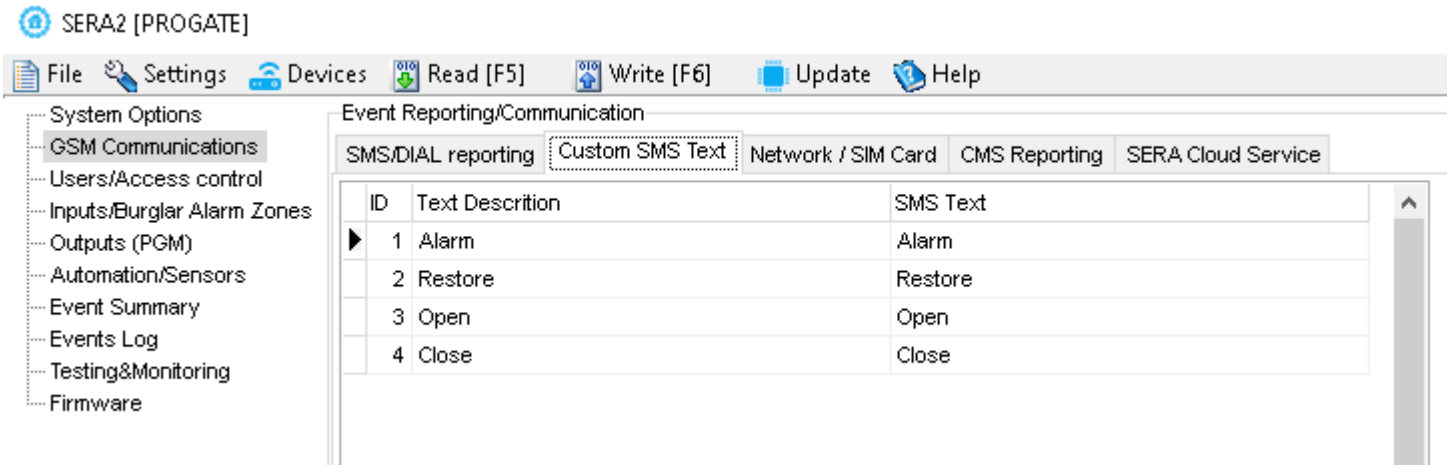


The SMS/auto DIAL Phone Numbers	Enter up to 8 user phone numbers for SMS and auto-dialing, using the international format **[Country code][Area code][Local number]** without the '+' symbol. For example, a UK number +44 (0) 113 xxx xxxx should be entered as 44113xxxxxxx. Incorrect formats would be 440113xxxxxxx or 0113xxxxxxx. Next to each user's phone number, select the checkboxes for the events that will trigger an SMS or auto-dial to that user.
SMS Character Set	SMS character set selection.
Limit of Dialing	Indicate maximum number of unsuccessful calls
Show Object Name	Object name will be displayed in the SMS message
Show Zone Number	Zone number will be displayed in the SMS message
Show Event Time	Event time will be displayed in the SMS message
Show CID Code	Report Contact ID code
Zone1- Zone32 Alarm/ Restore	Zone1- Zone32 alarm and restore events reporting is enabled.
System Open/ Close (CID 400 group)	System ARM/DISARM/STAY reporting is enabled.
System Troubles (CID 300 group)	System trouble reporting is enabled.
Sensor1- Sensor32 Alarm/ Restore	Sensor 1 – Sensor32 alarm and restore events reporting is enabled.
Test Events (CID 600 group)	Communication test reporting is enabled.
Other Events	Other events reporting is enabled.
Send SMS to USER	The system allows for SMS reporting to selected phone numbers (1-8). If a specific event occurs in the system, an SMS message will be sent to the enabled phone numbers.
Auto DIAL to USER	The system supports automatic dialing to selected phone numbers (1-8). If a specific event occurs, the system will automatically dial the enabled phone numbers.

8.7.1 Custom SMS/APP 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 35Explanation of every field in "Custom SMS Text" window

8.8 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.

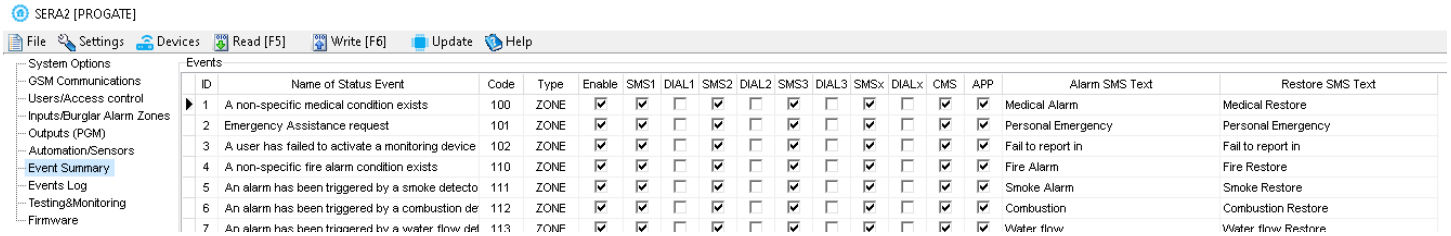


Figure 36 Event Summary window

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 37 Explanation of every field in "Event Summary" window

8.9 Real-Time Testing & Monitoring of Hardware

RT Testing & Monitoring > Hardware

The Hardware Monitoring window provides real-time visibility into the states of inputs and outputs, as well as GSM information. This facilitates the evaluation of whether the inputs, outputs, and network registration are functioning correctly.

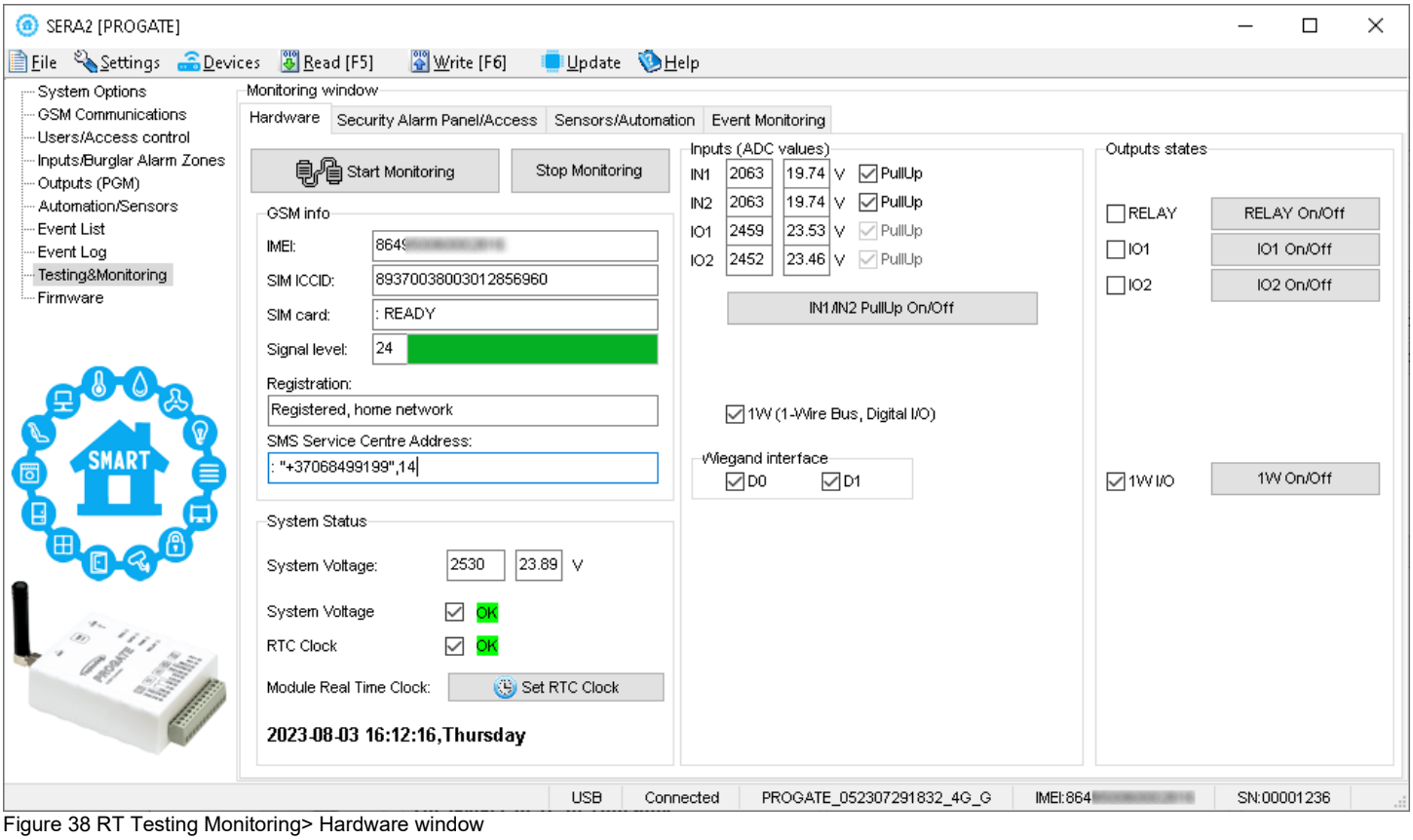


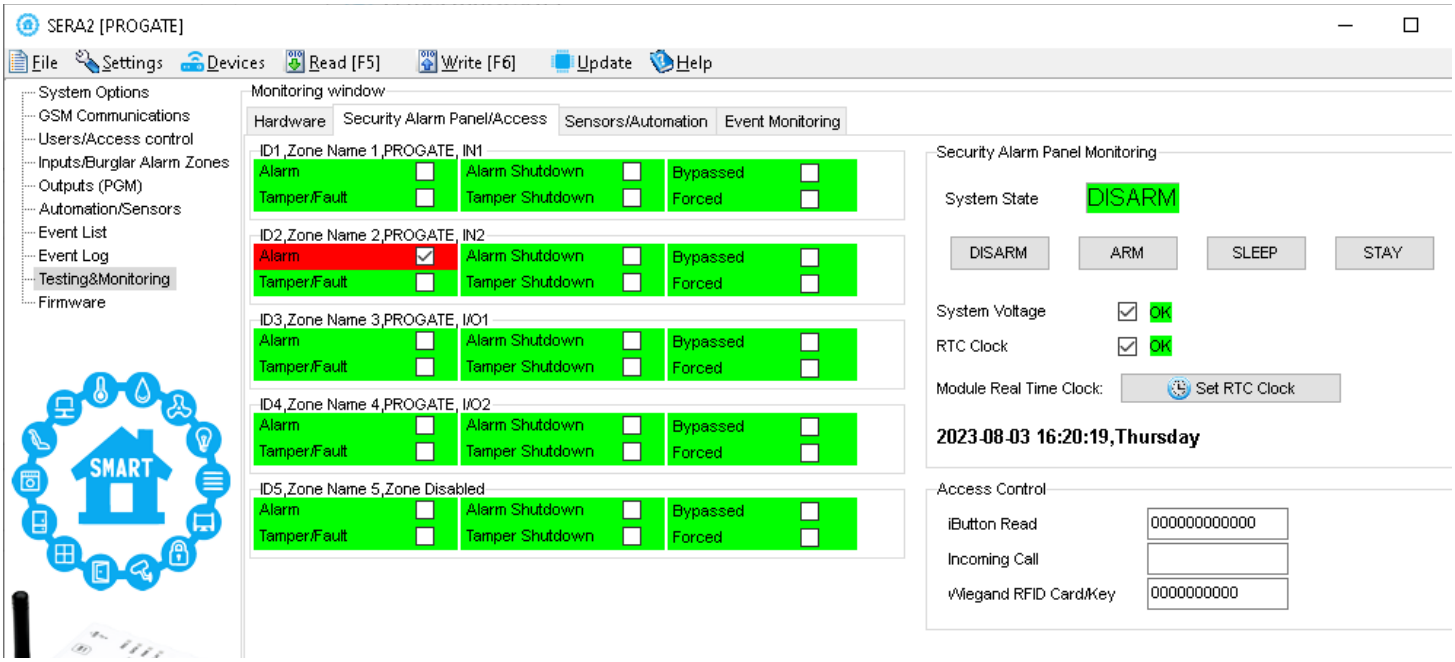
Figure 38 RT Testing Monitoring> Hardware window

Start Monitoring	Pressing Start Monitoring button starts the monitoring of the module.
Stop Monitoring	Pressing Stop Monitoring button stops the monitoring of the module.
IMEI	IMEI number of GSM modem available in the module
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.
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.
Signal level	Signal strength of GSM communication
Registration	State of GSM modem registration to GSM network.
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.
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.
System Voltage	System voltage OK/Trouble
RTC Clock	Real time clock OK/Trouble
Module Real Time Clock	Indicates the time of the module RTC
Set RTC Clock	By pressing this button real time clock of the module will be set.
Inputs In1…In4	In1…In4 is the indicated input ADC and voltage value V.
I/O1…I/O2	I/O1…I/O2 is the indicated voltage ADC value and current ADC value mA.
D1…D3 (I/O)	Check box nearby the digital inputs D1…D3 (I/O) means that the input has ‘0’ or ‘1’ state.
BUS (I/O)	Check box nearby the zone expansion module BUS (I/O) means that the input has ‘0’ or ‘1’ state.
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
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
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.
BUS (I/O) On/Off	Checked check box BUS (I/O) means that the output currently has ‘0’ or ‘1’ state.

8.10 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.



Zone1…Zone32	Zone number
Alarm	If checked and the color is red the zone is alarmed
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.
Bypassed	If checked and the color is red, the zone is bypassed.
Forced	If checked and the color is red, the zone is forced
Tamper/Fault	If checked and the color is red, the zone is tampered.
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.
System State	Indication that at the moment the module is in waiting ARM, ARM, DISARM, SLEEP or STAY mode
DISARM	After pressing the button DISARM, disarm mode should be entered
ARM	After pressing the button ARM, arm mode should be entered
SLEEP	After pressing the button SLEEP, sleep mode should be entered
STAY	After pressing the button STAY, arm mode should be entered
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.
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.
Module Real Time Clock	Real time and date is indicating.
iButton Read	The number of iButton Maxim iButton key DS1990A - 64 Bit ID code that is arming the system.
Incoming call	The number of users phone that is calling to the module's SIM.
Wiegand RFID Card Key	The number of Wiegand RFID Key Card that is arming the system.

8.11 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 3072 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.

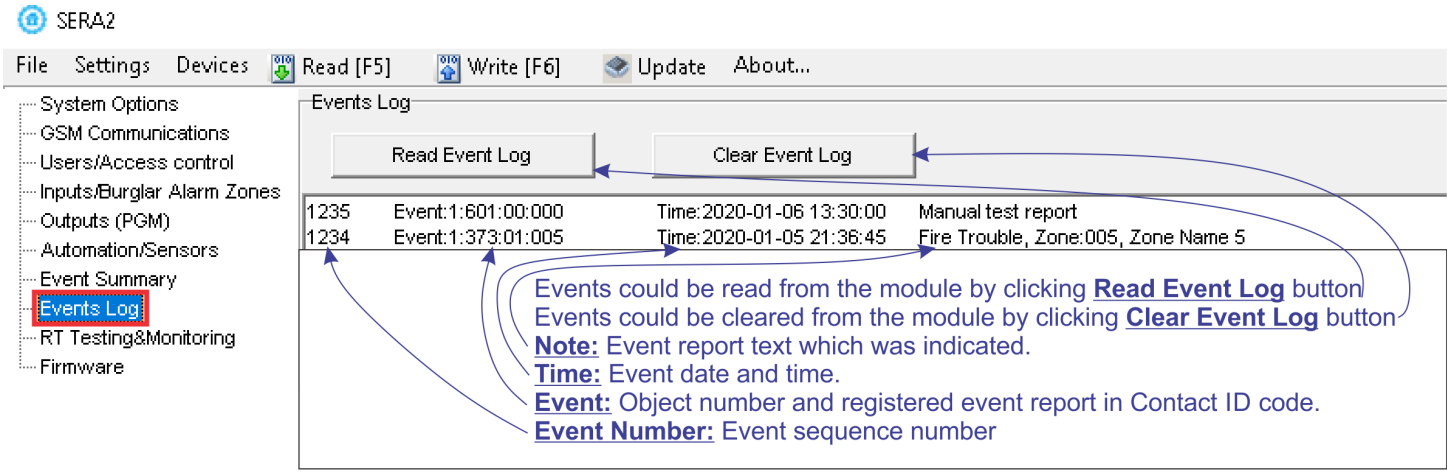


Figure 39 Events Log window.

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.

9 Remote Device Management: Configuration, Firmware Updates, Monitoring, and Logging

What actions can be performed remotely when connected to a module over the internet?

- System configuration parameters can be changed.
- Read/Clear event log
- System status and temperature sensors can be monitored.
- Firmware updates for the module can be implemented.

How does remote connection work?

- The remote connection is established via GPRS/LTE using the TCP/IP protocol.
- The GSM module connects to the internet through GPRS, linking to the SERA cloud server [cloud.topkodas.lt].
- The SERA2 configuration tool establishes the connection using the unique ID (IMEI) of the module.

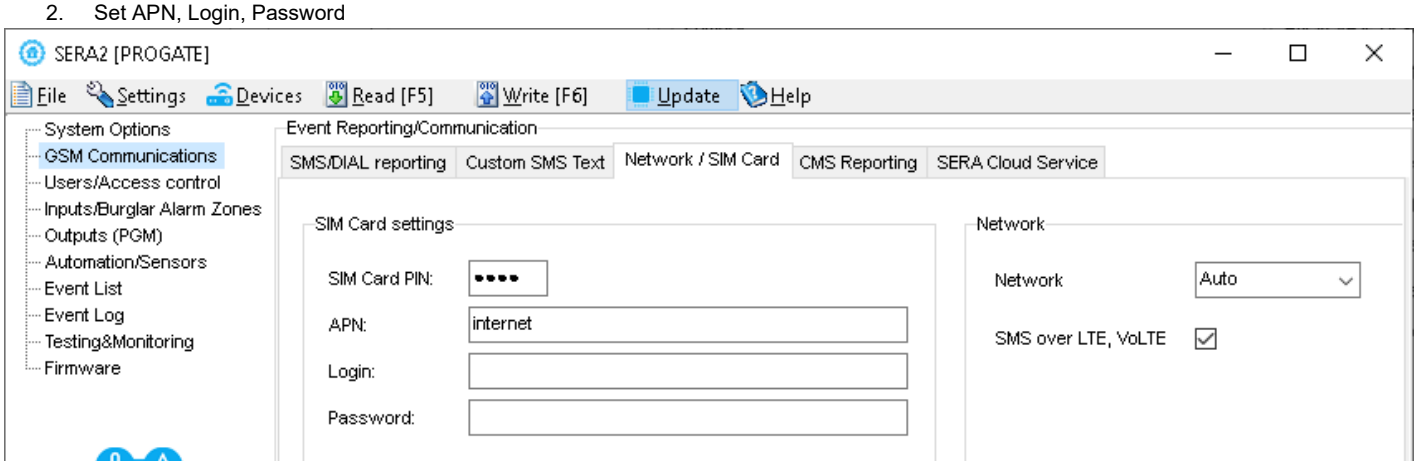
PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→SERA2 Configuration software (Windows)
Or
PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→SERANOVA app (Web,Android,IOS)

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

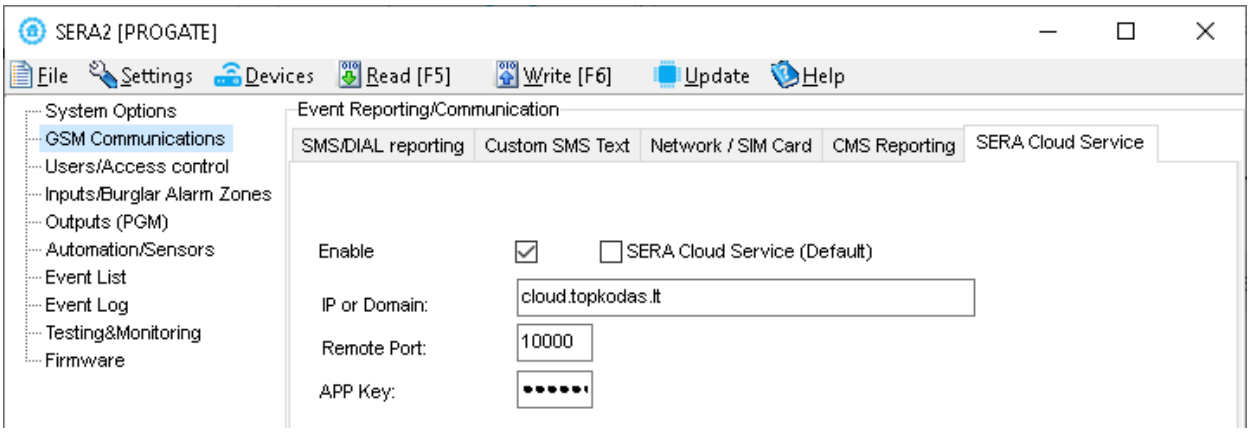
Ensure the SIM card has GPRS/LTE mobile data service activated by the network provider. Usually, this service is enabled by default. If not, reach out to the GSM service provider for activation.

Steps to activate Remote control over internet:

1. Go to *SERA2 > GSM Communication > Network/ SIM* card tab
2. Set APN, Login, Password

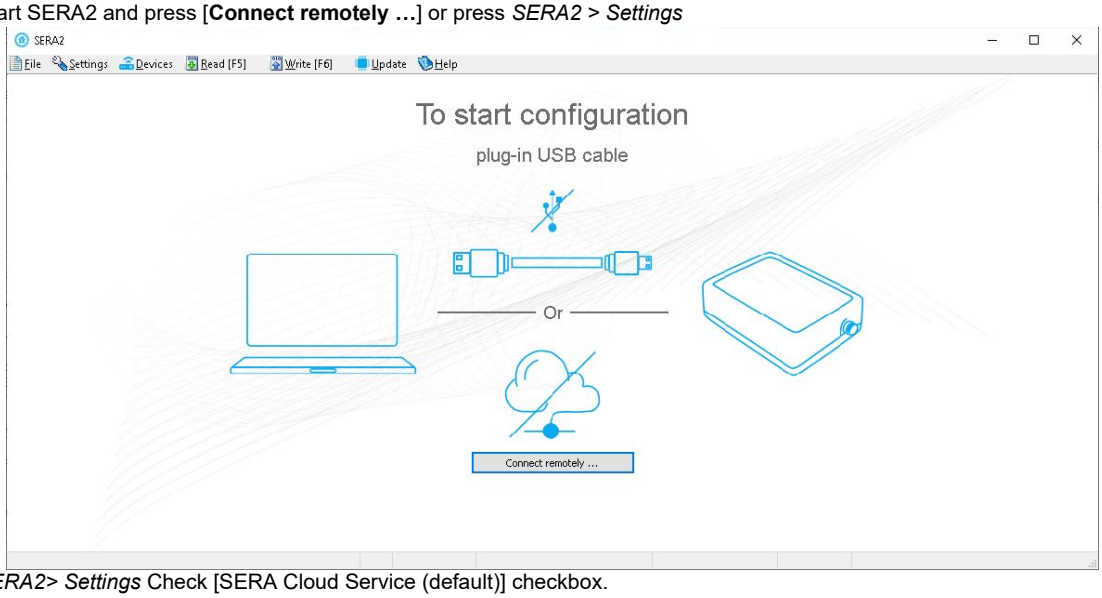


3. If needed, APN/Password/Login/IP/Domain/ Port /PING time /KEY can be set by SMS commands
   INST000000␣008␣APN#LOGIN#PSW#
   008= command code (GPRS network settings); APN=31 symbols; LOGIN=31 symbols; PSW=31 symbols
   e.g.
   INST000000␣008␣internet### - Apn="internet and no login and password.
4. Go to *SERA2 > GSM Communication window> Sera Cloud* Service tab. Set 'Sera Cloud Service' (default) checkbox.

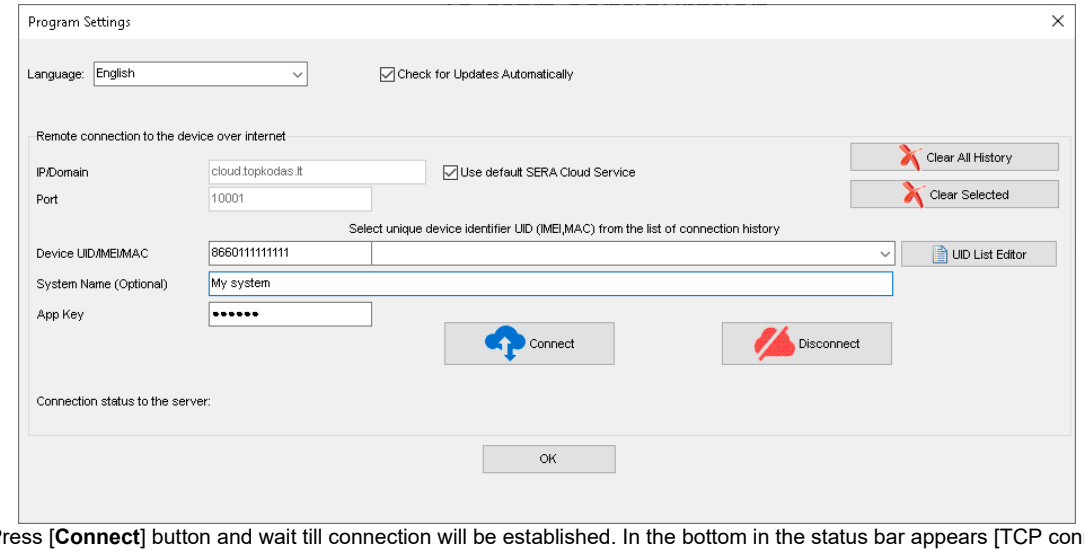


5. Write the configuration into the module by pressing [**Write**] icon
6. Ready the module by inserting the SIM card, attaching the antenna, and connecting the 12V/1A VDC power supply.
7. Wait for the module to register to the network and connect to the '*SERA Cloud service*'

8. Start SERA2 and press [**Connect remotely …**] or press *SERA2* > *Settings*



9. *SERA2*> *Settings* Check [SERA Cloud Service (default)] checkbox.
10. Enter module IMEI, App key (default: 123456), system name (optional)



11. Press [**Connect**] button and wait till connection will be established. In the bottom in the status bar appears [TCP connected] notification.

The SERA2 software maintains a connection history for convenience, remembering all previously entered IMEI numbers. If there's a need to clear the list of UID/IMEI, simply press [Clear History] or press [UID List Editor] to edit the connection history list.

10 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.

USER commands are exclusively accessible to individuals whose phone numbers have been registered in the module's system. Conversely, INST commands can be transmitted from any phone number, provided the correct installer password is used.

- 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#

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

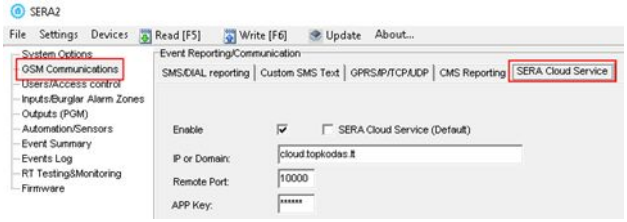
In this guide, we use the symbol "␣" to represent a single space. Each "␣" you see should be replaced with one space in your actual SMS text. Please avoid any extra spaces or characters before and after your message. Remember: For SMS, "␣" = Space. We use "␣" in examples for better clarity.

10.1 The table of installers SMS commands

SMS commands can be sent from any phone number as long as the correct installer (INST) password is used. Please safeguard your INST password diligently! The default password is set to '000000'

Table 6 the table of installers commands

INST000000␣001␣ID#TEL#SMS#DIAL# e.g. INST000000␣001␣1#37066666666#11111111#10000000#	**To add admin user phone numbers for SMS and Call notifications upon an event, use the following format:** 001 = Code for adding admin user's phone numbers ID = User index (1-8) TEL = User's phone number (max 16 digits), without (+), including country and operator's code. End with '#' SMS = Notification event filter. 1 sends the event, 0 doesn't. Events are ordered (1.2.3...n), e.g., 001000 DIAL = Dial event filter. 1 dials if the event occurs, 0 doesn't. Events are ordered (1.2.3...n), e.g., 101000 #= delimiter **Example: INST000000 001 1#37066666666#0001000000#0000011111#** The event filter order is as follows, with 0 indicating disabled and 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 9. And so on.
INST000000␣002␣ID e.g. Delete admin User1 at index 1 INST000000␣002␣1	**To delete an admin user's phone number (used for SMS notifications), use the command '002' followed by the user ID index (1-8)**. 002 = Command code for deletion ID = User index (1 to 8)
INST000000␣003	**Delete all users in database.** 003 = Command code
INST00000 0␣004␣ID#TEL#OUT#OPT#NAME# e.g. Add user at index 1 , phone-37066666666, out1 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, 1=OUT1=RELAY,2-OUT2,… 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 up to 31 characters.
INST000000␣005␣TEL# e.g. delete user associated with phone 37061611111 INST000000␣005␣37061611111	**To delete a user's remote control access according phone number, use:** 005 = Command code for deletion. TEL = User's phone number (16 digits max, without '+'), including country and operator codes. The number must match the one in the module's memory."
INST000000␣006␣ID e.g. delete user at index 200 INST000000␣006␣200	**Delete user's phone number by index.** 006= command code ID = Enter the user's index number from 001 to 800 to delete all data associated with the user.
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

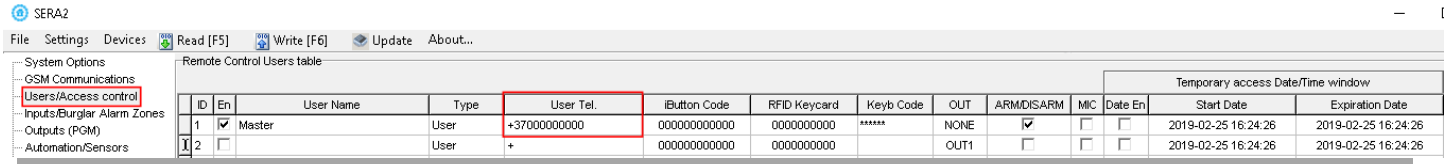
INST000000␣009␣ADDR#PORT#PING#KEY# e.g. INST000000 009 cloud.topkodas.lt#1000#600#123456#	**SERA cloud Service Parameters** 009= command code (Remote control of the module over the Internet) ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain 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 e.g. deactivate cloud service INST000000␣010␣0 e.g. activate cloud service INST000000␣010␣1	**Enable or disable the 'SERA Cloud service' for APP and remote device connection.** 010= command code (To activate the connection to the remote control server). E= 1- (enabled) or 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: 'Guest'	**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#	**Enter the user's telephone number for remote control via a short call without an index.** **USER NAME-only Latin characters is allowed inside SMS** 012= Command code (enter the user's telephone number in the free space for remote control via a short call) TEL = The user's telephone number (max 16 digits) without the (+) sign, consisting of the country code, operator's code, and the user's telephone number. Use the end symbol #. OUT = Output number for remote control that will be controlled value= (0-32). 0 = Disabled, 1=OUT1(RELAY), 2=OUT2… and so on. OPT = 0 – Disabled, 1 – Enabled (Sequence from left to right): 1. User Enabled 2. Enable Arm/Disarm alarm system by call NAME = User Name up to 31 characters.
INST000000␣013␣TEL # NAME# e.g. INST000000␣013␣37066666666#Jon#	**Add the user's telephone number for remote control via a short call to the free space of memory. Enable the user and assign control of RELAY (OUT1).** **i** Note: To assign a user to a specific index or enable user control for other outputs, utilize the commands 004 or 012. 013= Command code TEL = The user's telephone number (max 16 digits) without the (+) sign, consisting of the country code, operator's code, and the user's telephone number. Use the end symbol #. NAME: User Name (optional, up to 31 characters).
INST000000␣018	**View user phone numbers from the user database using:** 018= Command code The response SMS will appear as: **[Enabled],[ID],[Phone],[Output]** Where: User Enabled (0 for disabled, 1 for enabled) ID= User index Phone= User phone number Output= Chosen output number for remote control.
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).

10.2 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.

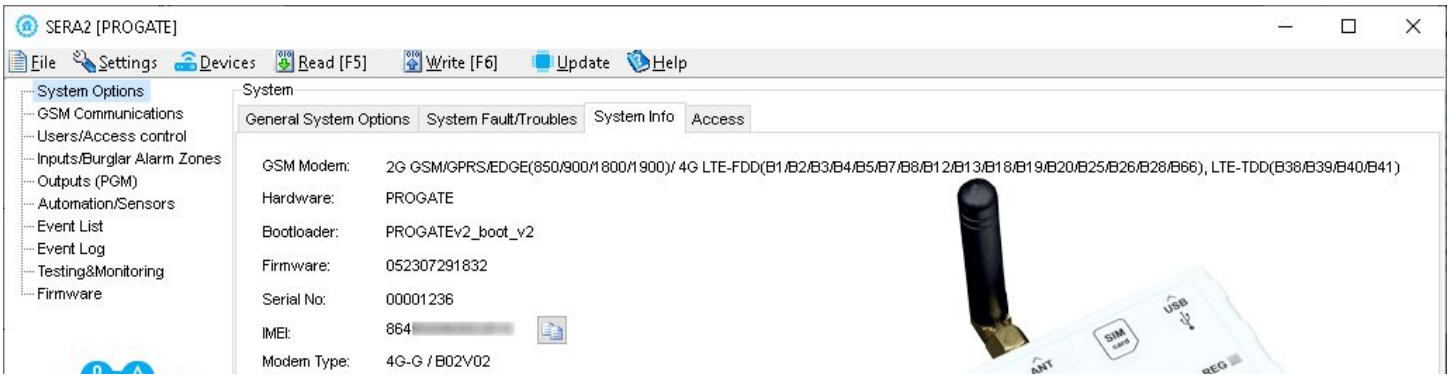
Table 7 the table of user's commands

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).

11 System Info of device and Firmware 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.

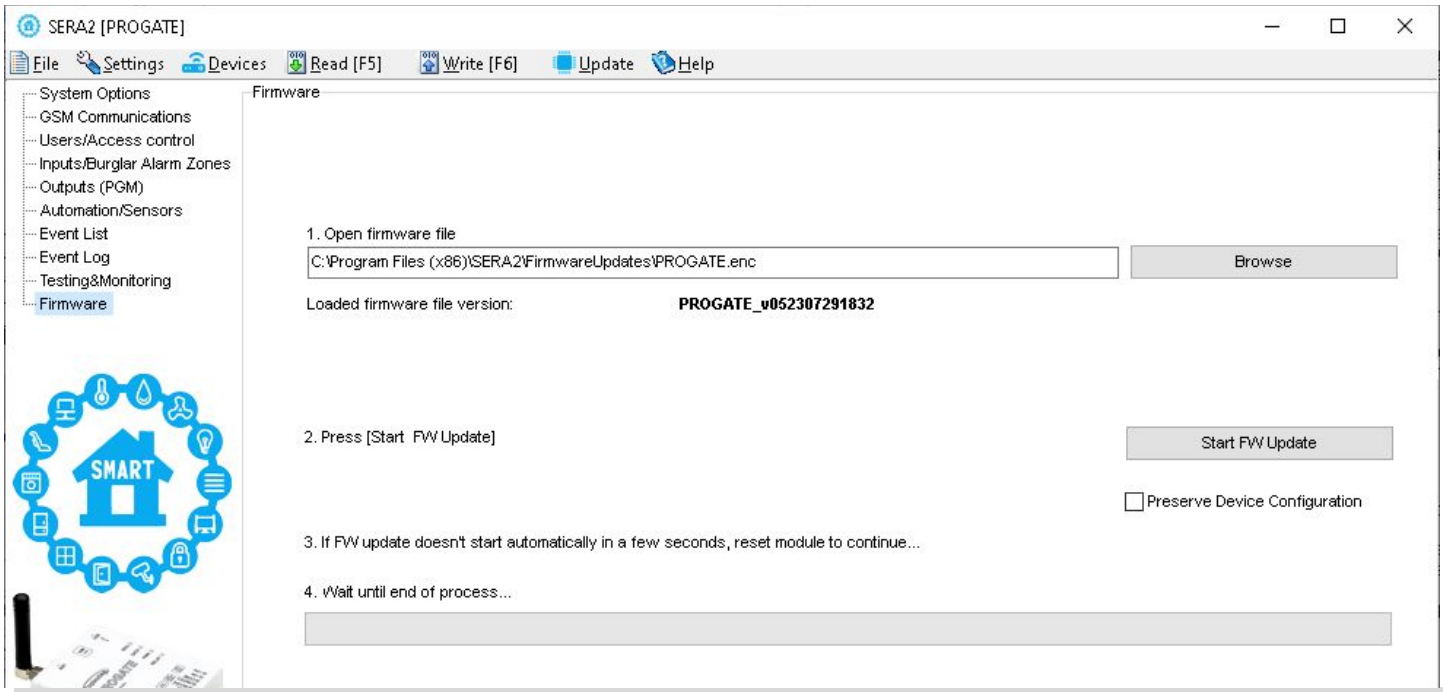


GSM Modem	Modem type and supported bands
Hardware	Device type
Bootloader	Bootloader version
Firmware	Configuration software
Serial No	Module registration number
IMEI	GSM modem IMEI address.

11.1 Firmware Update

SERA2 > Firmware

This window let you update the firmware of the module.



The device's firmware can be updated either through a USB connection or remotely over the internet using the 'SERA Cloud Service'.

Firmware Update Steps:

- Always keep SERA2 software updated. Each SERA2 software version includes the latest firmware update files.
- (Optional) To change the default firmware file, click [**Browse**] and open the folder containing the new firmware file.

To retain the device's current configuration after the update, check the [**Preserve Device Configuration**] box. If unchecked, the configuration will reset to default after the update.

- Click [**Start Update**].
- If the update doesn't start within a few seconds, reset the module.
- Wait for the process to complete.
- Reset module to continue.

12 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.