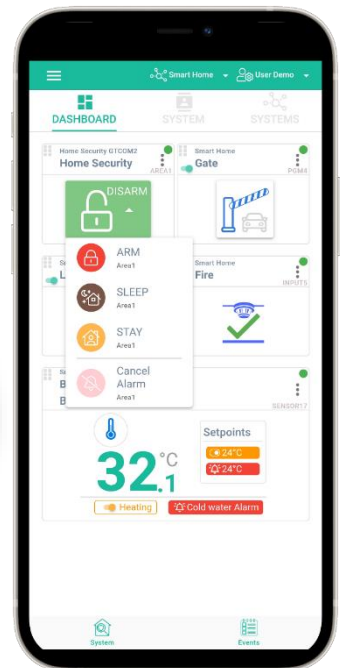


# PROGATE

## 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.



The module Progate is a **security, automation and access control system** with **programmable selectable inputs or outputs, 1wire bus for temperature, humidity sensors DHT22**. It is possible to connect **up to 32 sensors. Output for relay connection**,

The module Progate features up to 800 users for remote control purpose.

The module Progate provides the high level of protection residential homes and any place where high security and automation is essential. These systems are designed to be easy to use, and the modular concept of these systems provides installers with labor-saving features that make expanding, installing and servicing these systems quick and convenient.

Once installed, module can be programmed remotely via GPRS connection or via USB using SERA2 upload/download software.

The module Progate is a logical solution to every installer's security, access control and home automation installation needs.

## Features of the module Progate

- Communication via SIA IP DC09 protocol
- 2G Quad-band (850/900/1800/1900 MHz) or 4G LTE modem
- **Inputs:**
  - IN1, IN2 0-30V
  - I/O1, I/O2 0-30V
  - 1W :
  - Dallas 1wire bus,
  - Aosong 1 wire bus,
  - Digital input max 3.3V
- **Outputs**
  - RELAY
  - I/O1, I/O2 (1A)
  - 1W, 10mA, Max Voltage 3.3V!
- Up to 32 sensors, temperature, humidity etc.
- Built-in access control features
- In-field firmware upgradeable via USB and SERA2 software GPRS
- Events log buffer. 3072 events
- Program remote controls using the master or installer codes
- Up to 800 users remote controls with mobile, web app.
- Up to 800 users remote controls with iButton or RFID keycard
- Up to 800 user code. To control with Wiegand keyboard.
- Unlimited control via SMS.
- Push button software reset

### The meaning of icons in the manual:



Automation part



Security system's part



Very important



Important



About the manual

# Contents

1	General information about the module Progate	4
1.1	Specifications	4
1.2	Used definitions and terms	4
1.3	Package content	5
1.4	General view of the module	6
1.5	Configuration methods	7
1.6	System Access codes	8
1.6.1	AppKey	8
1.6.2	Installer and User passwords	9
1.6.3	Master code for access control via keypad	9
2	<b>QUICK START</b> . First steps to prepare Progate module and SERA2 software	10
3	Fastening	11
4	Installation	11
4.1	Power supply, Battery Wiring	12
4.2	Access control. Arming/Disarming methods	13
4.2.1	Wiegand Keypad & RFID Card Reader, iButton Probe Wiring	14
4.2.2	Enter iButton, RFID, Phone numbers to the memory of the module	15
4.3	Outputs	17
4.3.1	Output PGM wiring. Bell, Relay, Led Wiring	17
4.3.2	Control Outputs via SMS	18
4.3.3	Control Outputs via short call, iButton, RFID	18
4.3.4	Control Outputs via app	18
4.3.5	Output programming	18
4.3.6	Access control output with logging	20
4.4	How to set clock synchronization?	21
4.5	Inputs	23
4.5.1	Humidity sensors AM2302/DHT22/AM2305/AM2306/AM2320/AM2321	23
4.5.2	Analog inputs 0-30V	25
4.5.3	Temperature sensors Dallas 1-wire DS18B20 installation & recommendations	26
4.5.3.1	Wiring Dallas 1-wire DS18B20	26
4.5.3.2	Temperature sensors Dallas 1-wire DS18B20 Configuration	27
4.5.3.3	How to change temperature scale from Celsius to Fahrenheit	28
4.5.4	Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?	29
4.5.5	How to edit alarm SMS text?	30
4.5.6	Burglar Alarm sensor zones wiring EOL NO NC	32
4.5.7	Fire alarm and Smoke sensors	33
4.5.7.1	Guidelines for Locating Smoke Detectors and CO Detectors	33
4.5.7.2	[4-Wire] Smoke detector Wiring	33
5	Programming	34
5.1	SERA2 Uploading/Downloading Software	34
5.2	General system options programming	35
5.3	System Fault/ Troubles Programming	37
5.4	Zones programming	38
5.5	Outputs. Bell & PGM programming	39
5.6	Users & Access Control programming details	40
5.7	DISARM /ARM/SLEEP/STAY the security system	42
5.8	Reporting SMS&Dial in Case of Alarm Events	44
5.8.1	Reporting to the user's mobile phone	44
5.8.2	Custom SMS Text	45
5.9	Reporting to the Central Monitoring Station	45
5.9.1	GPRS/ IP/ TCP/ UDP details programming	46
5.9.2	Central Monitoring Station details programming	46
5.10	Event Summary (Events)	47
1.1.	RT Testing & Monitoring. Hardware.	48
5.11	RT Testing & Monitoring Security Alarm Panel/ Access	49
5.12	Automation & Sensors Programming	50
1.1.	Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software	51
5.12.1	How does smart thermostat, alarm system works?	53
5.12.2	How to prevent the output from frequently changes according to minute temperature changes	53
5.12.3	The example of heating, cooling control with the module Progate	54
5.13	Data Transmitting to Server & Remote Control	54
5.13.1	TCP/ IP Remote Control	54
5.14	Events Log	55
5.15	Remote Monitoring, Control, Configuration, FW update over the internet	55
5.16	Testing & Monitoring Automation	57
5.16.1	Real-time Testing & Monitoring > Sensors/ Automation	57
5.16.2	Real-time Testing & Monitoring > Event Monitoring	58
6	Info: Hardware, Firmware, Bootloader, Serial No & Updates	58
6.1	Firmware Update	59
7	Recommendations for the user & installer	59
8	Remote control and configuration using SMS Commands	59
9	The table of installers commands	60
10	The table of users commands	63
11	APP configuration	64
12	Warranty Terms and Conditions	64

# 1 General information about the module Progate

## 1.1 Specifications



### Parameters of built-in GSM module:

- Quad-band (850/900/1800/1900 MHz)
- *Optional 3G, 4G LTE bands*
- Sending of SMS messages
- Receiving of calls and dialing
- Data download/upload via GPRS network

### Outputs:

#### RELAY

I/O1(1A), I/O2 (Programmable selectable input or output)

**D1 (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: CTRL/SMS/DIAL, SIREN, BUZER, ARM state, Zones OK, Light Flash, inverting, pulse mode

### Inputs:

Analog inputs In1, In2: 0-30V

Analog inputs I/O1, I/O2: 0-30V (Programmable selectable input or output)

Digital input 1W for 1 wire DHT22 temperature-humidity sensors (Programmable selectable input or output)

- SMS text for input alarm and restore
- Available to monitor up to 32 sensors
- Programmable enabling or disabling of inputs;
- 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

### Digital input/ output 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
- Wiegand interface DATA0/ DATA1, RFID reader, Keyboard.
- The total length of the bus up to 100m.

### Module control:

#### ARM/DISARM of the security system via:

- „Key switch” input level or pulse mode.
- 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
- Mobile, web app

#### 5V power source output for Dallas 1-Wire Bus, DS18B20, DS1990A, Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321

- Voltage 5V
- Current limit 100mA

#### Automatic periodical test:

- Test sending in a form of SMS message. Periodicity for communication control messages (tests) from 1 to 99 nights and days according to selected time. Or fixed periodical interval 1-99999 minutes.

#### Power supply voltage:

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

### 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



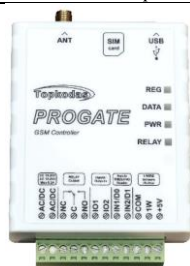
Term	Description
Alarm Log	Contains information about alarms that are currently active on the system or information about alarms that have been raised and then resolved on the system. This log can be useful in analyzing problems and trends in the system.
Arming/Disarming	A process of enabling/disabling 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!

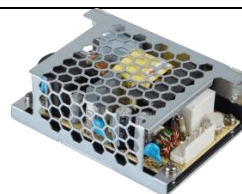
Table 2 Additional, under request package content



5.6 kOhm resistors - 4 pcs  
100 Ohm resistors – 2 pcs



Spaces for PCB installation - 4 pcs



TPS12 13.7V/1.8A AC/DC Mini  
Switching Power Supply with battery  
charging



Wiegand keypad & RFID reader



### 1.4 General view of the module

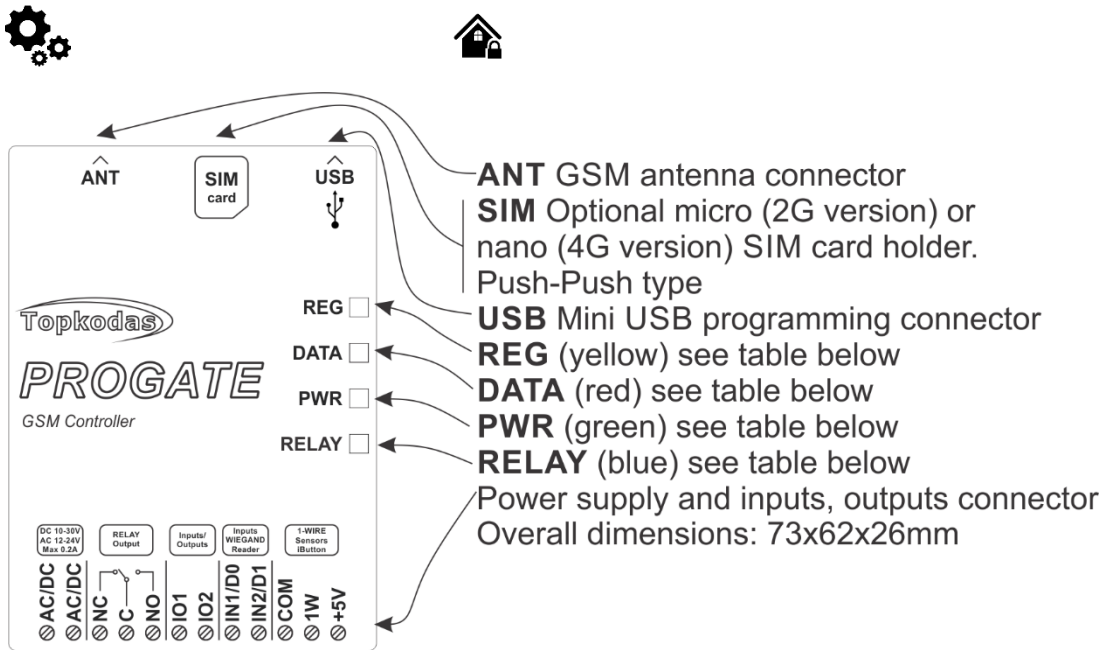


Figure 1 General view of the module Progate

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

## Meaning of LEDs and contacts



Table 3 Meaning of LEDs

Name	Indication variations	Meaning
PWR (green) built-in LED	Watchdog heart beat blinking, remains lit for 50ms, and turns off after 1000ms.	The module is functioning.
	Off	The module is out of order or no voltage
REG (yellow) built-in LED	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) built-in LED	Lights continuously	The memory of the module contains unsent reports to the user or to the server.
	Off	All reports has been send.
RELAY (blue) built-in LED	ON OFF	Relay switched ON Relay switched 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 10K resistor to the VD+ (Pull UP) Output 1A	
		Analog voltage input 0-30V	
	Max available voltage	30V	
IN1/D0 ... IN2/D1	Programmable functions	Input with 10K resistor to the VD+ (Pull UP) The zone for security system NC/NO/EOL/EOL+Tamper	
		Wiegand (1) interface, 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. DS18B20, DS1990A 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	

## 1.5 Configuration methods

### 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.

### Sera2 software

**!** Sera2 software is intended for PROGATE configuration locally via USB port or remotely via 2G/3G/4G network. This software simplifies system configuration process. Sera2 software is free, which you can download from our website: [topkodas.it](http://topkodas.it)

### Remote connection



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



Sera2 software provides remote system configuration ability using Topkodos Cloud server via GPRS.

## 1.6 System Access codes

Table 5 Default passwords and explanation

Password	Default	How to find and how to change	Explanation
SIM card PIN	1234	SERA2> System Options> General system options	It is automatically ignored if pin request in SIM card is disabled
Installer Password	000000	SERA2> System Options> General system options	This password allows you to enter programming mode, where you can program all features, options, and commands of the module.
SMS User Password	123456	SERA2> System Options> General system options	This code allows you to utilize arming method, as well as program user codes.
User password of GSM operator	123456	SERA2> GSM Communications> GPRS/IP/TCP/UDP	User password of GSM operator network where SIM card inserted in the module is operating.
App Key	123456	SERA2> GSM Communications> Sera Cloud Service	“APP Key” in module must be same as Remote connection password via [cloud app] also in [SERA remote] default: 123456
Installer code (for SMS control and configuration)	000000	INST000000_090_PSW 090= command code (Change of installer's code) PSW = New Installer's password.	6-digit password used for system configuration, control and request for information.
User code (for SMS control and configuration)	123456	INST000000_091_PSW Change user's code 091= command code (Change user's code) PSW = New user's password.	6-digit password used for system control and request for information.
Master password (Keybutton code)	1234 or 123456 (if selected 6 digit)	in user table SERA2> Users/ Access control 6 or 4 digit code selected: System Options> General system options> User Access Code Format	Control functions for all newly associated keys will be assigned according to MASTER key. For example: If MASTER key will control Out1, all newly associated keys will also control Out1.

### 1.6.1 AppKey

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

Enter App Key for the remote connection via Cloud service. Go to <https://cloud.topkodos.lt/index.php> > Settings

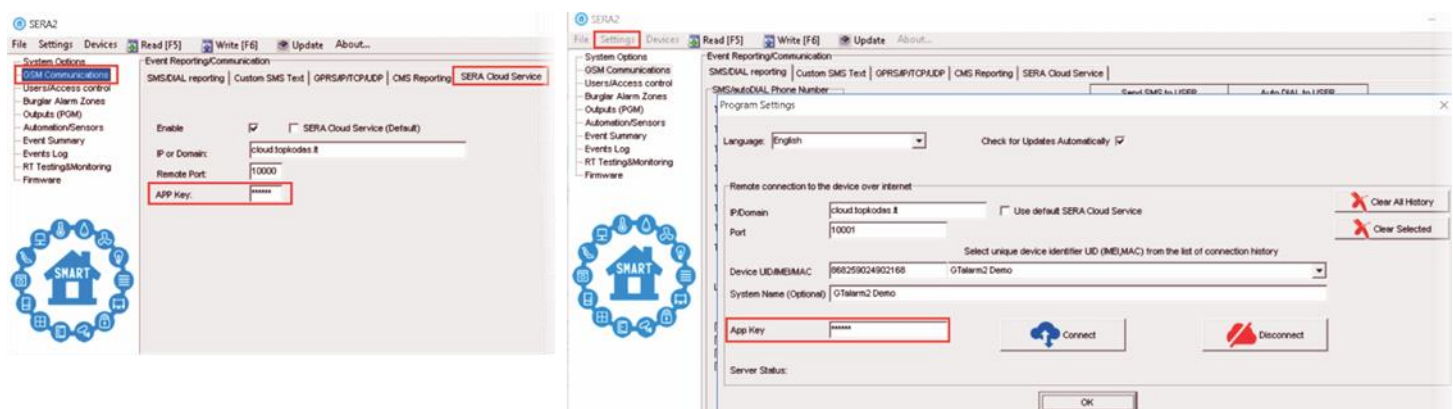


Figure 2 GSM Communication> Sera Cloud Service> App Key



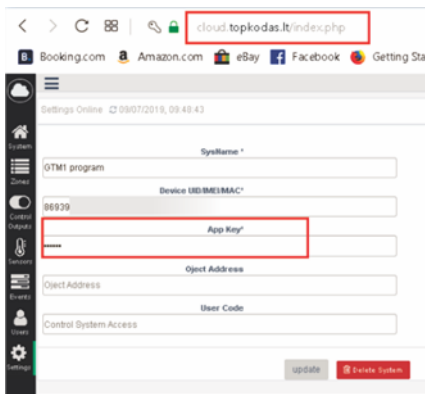


Figure 3 <https://cloud.topkodos.lt/index.php> > Settings > App Key

## 1.6.2 Installer and User passwords

### If you want to edit existing configuration,

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

**The password for remote and SMS configuration.** Installer Password (Default: 000000). This password used for remote configuration or for configuration via SMS messages with INST code

**The password for remote control or for control via SMS messages.** SMS user password: 123456. The password used for remote control of the module or control of the module via SMS messages with USER code

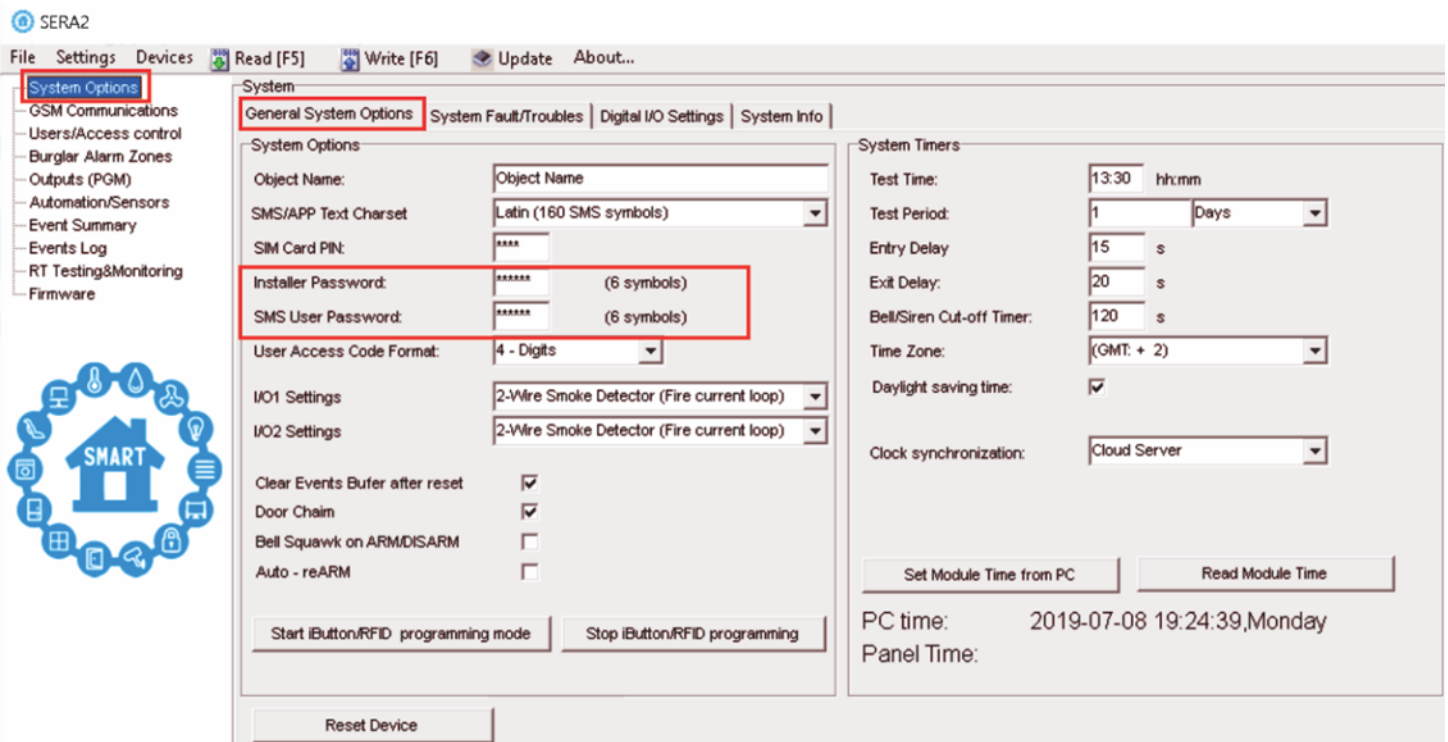


Figure 4 System Options > General System Options

## 1.6.3 Master code for access control via keypad

### If you want to edit existing configuration,

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

**Master Code for access control via keypad.** Default Master code: 1234 or 123456

1. Select 6 or 4 digits user access code format. Sera2> System Options> General System Options>User Access Code Format
2. Enter 6 or 4 digits codes in the Sera2> Users/ Access control > Keyb Code

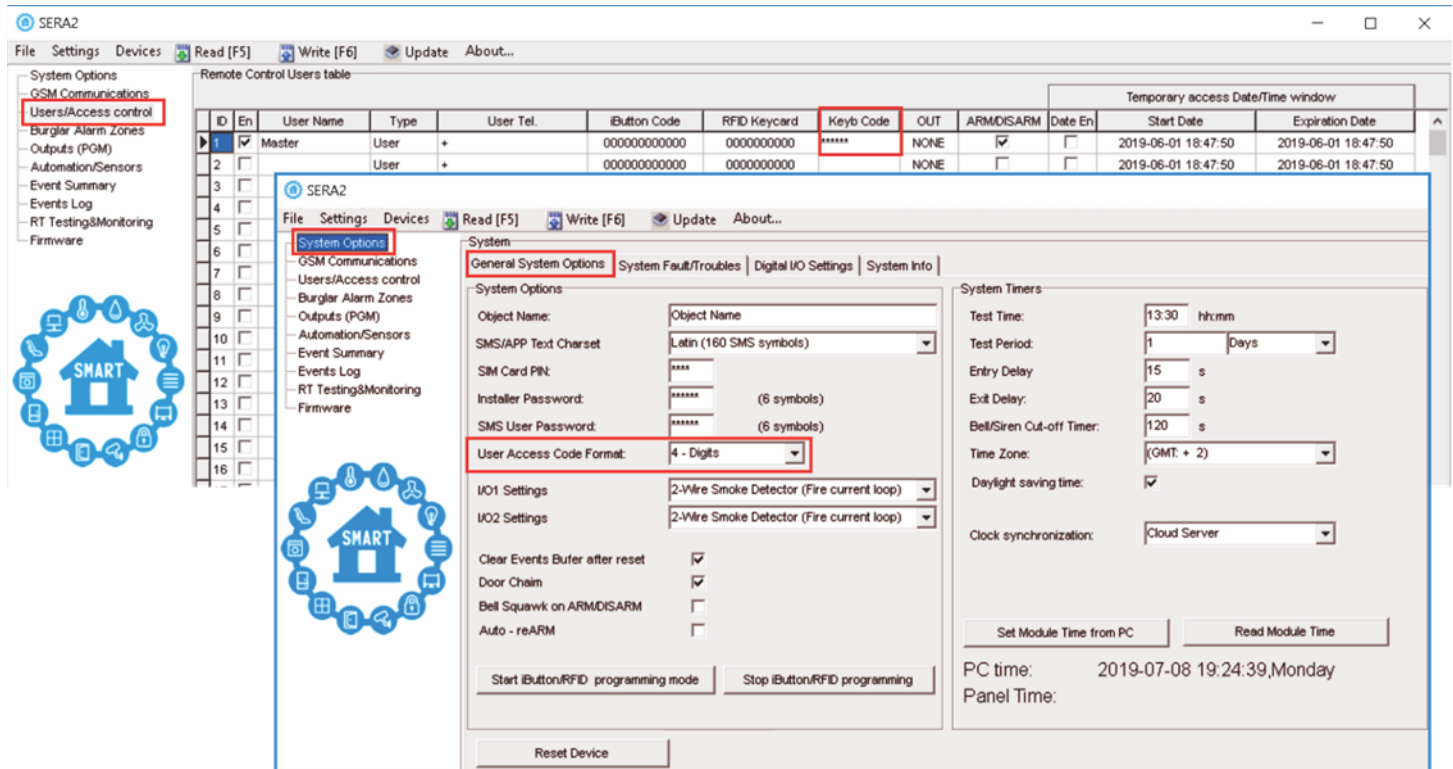


Figure 5 User/ Access control and System Options> General System Options

## 2 QUICK START. First steps to prepare Progate module and SERA2 software.

**QUICK START** <https://youtu.be/-XBAAWxpn3E>

### Preparation procedure of the module PROGATE.

- Connect the GSM antenna to the antenna connector.
- 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.
- Connect the module to the computer via mini USB cable.

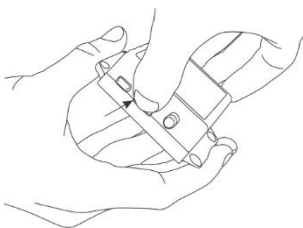


Figure 7 Insert SIM card

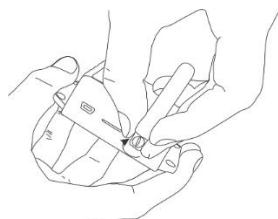


Figure 6 Screw GSM antenna

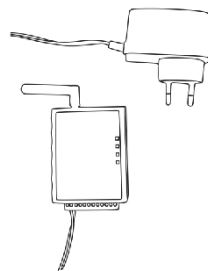


Figure 8 Connect power supply

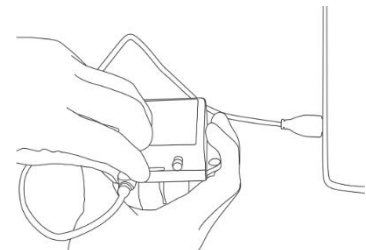


Figure 9 Connect the module to the computer

**i** CALL TO THE MODULE FROM YOUR MOBILE  
YOU WILL RECEIVE SMS FROM THE MODULE

When you call to the module PROGATE for the first time, your phone number will be stored in the module's memory automatically. This means you can control the first output of RELAY with a short, free call. You will also be able to receive SMS alarm messages. The settings can be changed with the free SERA2 program.

### Install configuration software SERA2.

Go to the <http://topkodas.lt/> website and download SERA2 software.

Open the folder containing installation of the software SERA2. Click the file „SERA2 setup.exe“

If installation directory of the software is OK, press [Next]. If you would like to install the software in the other directory press [Change], specify other installation directory and then press “next”.

- Check if the correct data are entered and press Install
- After successful installation of the software SERA2, press [Finish]



It is possible to select output mode in SERA2 software  
It is possible to select pulse mode or steady, pulsating mode in SERA2> Outputs (PGM) window.  
Don't forget to write edited configuration to the memory of the module (Press „Write“ icon in the command line)



There is RELAY already integrated in PROGATE. If you can't use it and

If you want to connect RELAY, you have to connect it to I/O (programmable selectable input or output) page **Output PGM wiring.**

### Bell, Relay, Led Wiring

I/O could be programmable selectable as input or output in SERA2. If you use I/O as output, you should programmable disable it as input in "inputs/ burglar alarm zones" window in SERA2.

## 3 Fastening

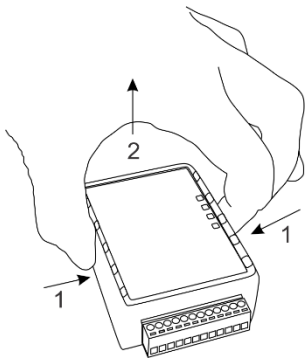


Figure 10 Remove the top lid

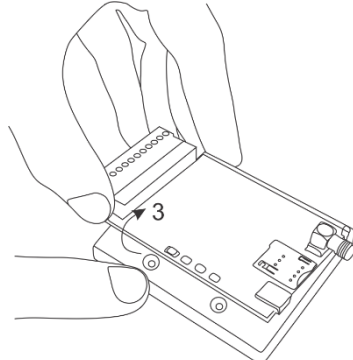


Figure 12 Remove the PCB board

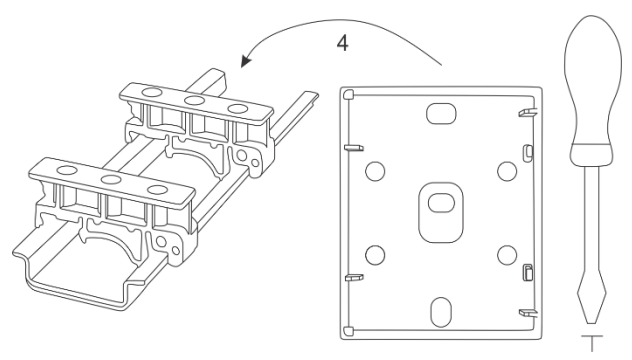


Figure 11 Fasten the base of the case

- 1.Remove the top lid.
- 2.Remove the PCB board.
- 3.Fasten the base of the case in the desired place using screws. DIN rail standard.

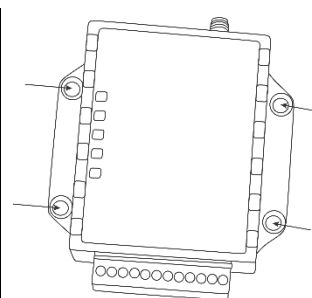
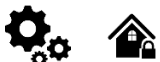


Figure 13 Fasten the base of the case

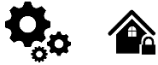
Fasten the base of the case in the desired place using screws.

## 4 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.

## 4.1 Power supply, Battery Wiring



Power supply DC 10-30V AC 12-24V Max 0.2A. It is necessary to calculate max current of power supply. The current of the alarm system is the current used by sensors, relays, siren and other devices. It is most convenient to use power supply source applied for power supply of security systems with the option to connect backup lead battery. It is recommended to mount remote control relays into sockets. Sockets may be easily fixed in metal box. It is necessary to select relays according to preferred voltage and current.

The example how to configure the module Progate for AC failure, restore function

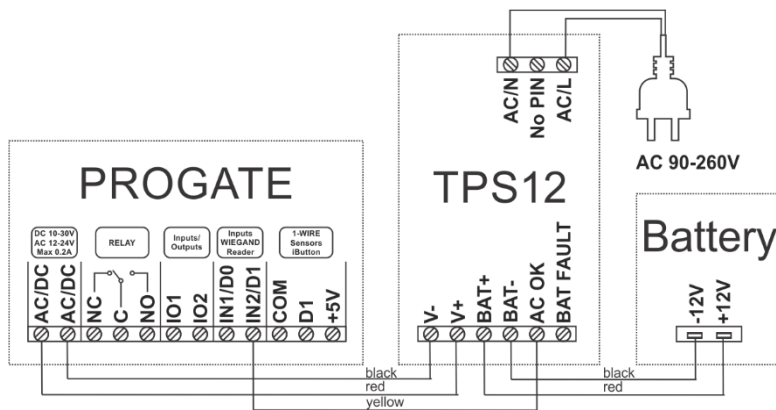


Figure 14 power supply, battery wiring

means only one AC loss event will be generated within 10 minutes.

If you want to edit existing configuration,

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

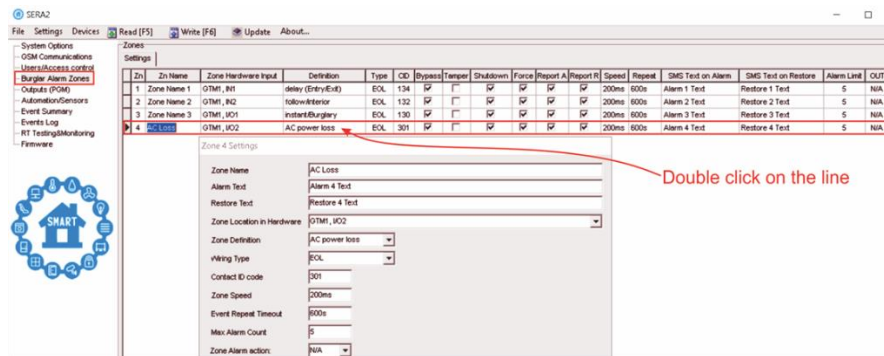


Figure 15 Burglar Alarm Zones

How to set Low system voltage trouble?

1. It is possible to edit low voltage alarm, restore texts. Go to Sera2> GSM Communication> Custom SMS Text and edit alarm and restore texts.
2. Go to Sera2> System Options> System Fault/ Troubles. Mark "Enable" near the Battery trouble field. , Set low system voltage alarm and restore values. When low battery level will be reached, the system will send alarm message. Setting of the allowable number of the same trouble event should be defined in the "Trouble Shutdown" field.

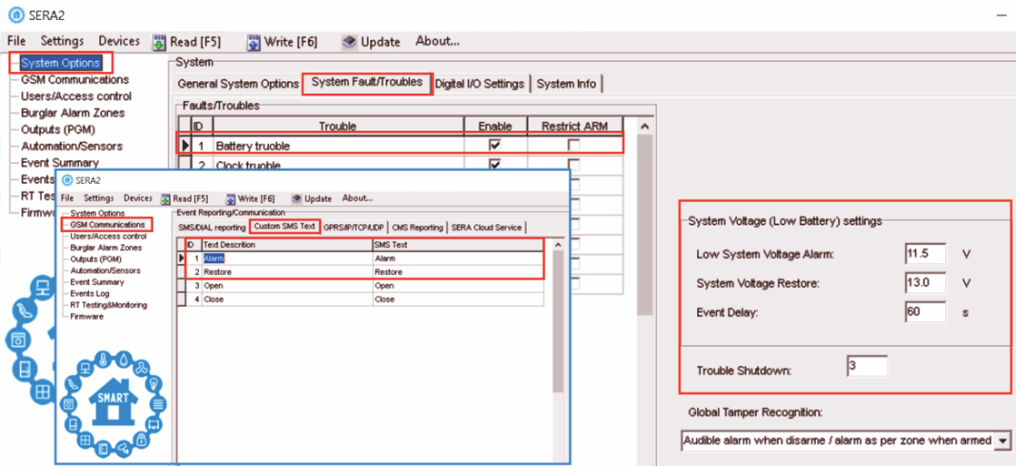


Figure 16 System Options> System Fault/ Troubles and GSM Communications> Custom SMS Text



Power supply TPS12 installation manual: [https://topkodas.lt/Downloads/TPS12\\_UM\\_EN.pdf](https://topkodas.lt/Downloads/TPS12_UM_EN.pdf)  
 Power supply TPS12 : [https://topkodas.lt/Downloads/GTalarm2\\_TPS12\\_AN\\_EN.pdf](https://topkodas.lt/Downloads/GTalarm2_TPS12_AN_EN.pdf)



AC equipment cannot be connected directly to the module. It is necessary to use a special relays or other methods, which are in compliance with electrical safety requirements.  
 When controlling devices from the AC network, it is necessary to follow all electrical safety requirements.

## 4.2 Access control. Arming/Disarming methods



### Arming process:

- **If ready** (no violated zone/tamper), **the system will arm.**
- **If unready** (violated zone/tamper is present), the system will not arm and **provide a list of violated zones/tampers** by SMS text message to user phone number. In such case the user **must restore all violated zones and tampers** before arming the system. Alternatively, the violated zones can be **bypassed, disabled or a Force** attribute enabled, and the tampers can be disabled when arming. The system initiates the exit delay countdown intended for the user to leave the secured area.



The alarm will be caused even if a tamper is violated while the system is disarmed



Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system.

### Access control methods is defined in Sera2> User/ Access control window

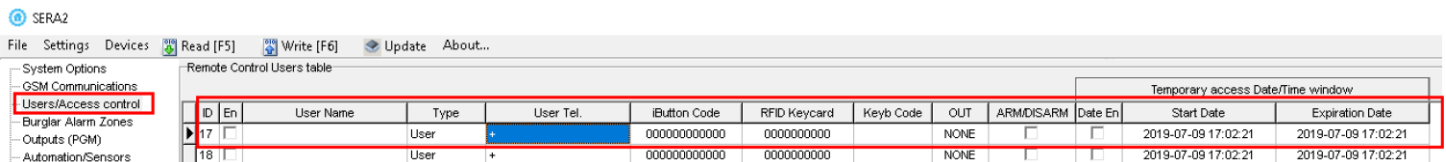
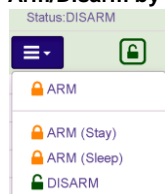


Figure 17Users/ Access control window

### Arm/Disarm by mobile, web app



Tap the ARM, ARM (Stay), ARM (Sleep), DISARM in the mobile, web app> System window



### Arm/Disarm by call

It is possible to arm, disarm the system and turn OFF the alarm by dialing the system's phone number from any of 800 available user phone numbers. The system **ignores any incoming calls from a non-listed phone number. The phone call is free of charge** as the system rejects it and carries out arming/disarming procedure afterwards. If there is more than one listed user dialing to the system at the same time, the system will accept the incoming call from the user who was the first to dial while other user (-s) will be ignored. To disable/enable arming or disarming for certain listed user phone numbers, please mark near ARM/DISARM in the "Users & Remote control" window

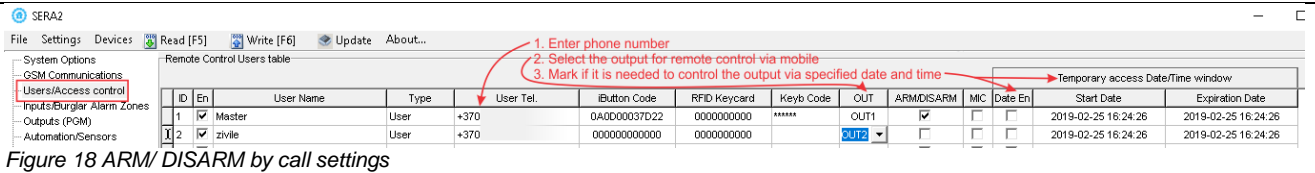


Figure 18 ARM/ DISARM by call settings

### Arm/Disarm via SMS



#### Enter user phone number in the Sera2> Users/ Access control list

The system **rejects the SMS text messages containing wrong SMS password** even from a listed user phone number. To arm the system by SMS text message, send the following text to the system's phone number **USER 123456\_030\_ST**

030= command code (Change security system's mode (ARM/DISARM/STAY/SLEEP)

ST = Security system mode 0-DISARM, 1-ARM ,2-STAY ,3-SLEEP

### Arm/Disarm by keypad

To arm/ disarm the system by Wiegand Keypad, enter User/Master Code

To cancel the arming process: Enter the user/master code again during exit delay countdown.

Disarming the System and Turning OFF the Alarm To disarm and turn OFF the alarm, enter any out of available user codes or master code using the number keys on the keypad.

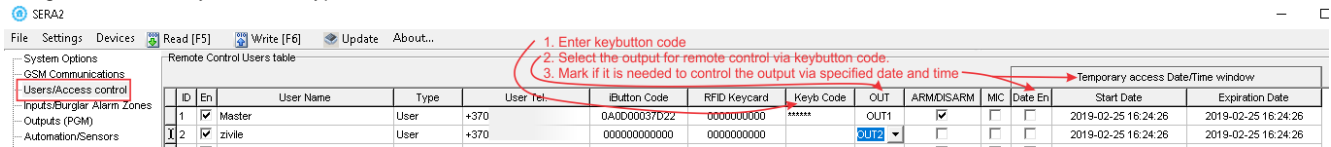


Figure 19 ARM/DISARM by keypad settings

### Arm/Disarm by iButton key

To arm or disarm the system and turn OFF the alarm, touch the iButton key reader by any of 800 available iButton keys. When the iButton is touched to the iButton key reader for arming/ disarming, the system will proceed arming/ disarming process.

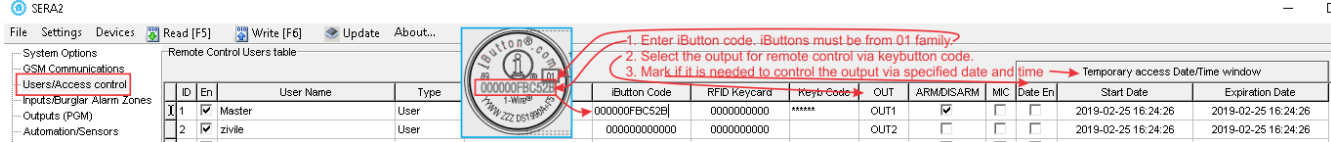


Figure 20 ARM/DISARM by iButton code settings



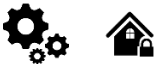
### Arm/Disarm by RFID key card, keyfob

To arm/ disarm the system with RFID keycard, touch 1 of 800 RFID keycard to the Wiegand keypad. When the RFID keycard is touched to the reader for arming/ disarming, the system will proceed arming/ disarming process.



Refer to: Users & Access Control programming details. And  
Refer to: DISARM /ARM/SLEEP/STAY the security system

## 4.2.1 Wiegand Keypad & RFID Card Reader, iButton Probe Wiring



### Wiegand keypad specifications:

26bit Wiegand (Default);  
8bit key press code

Maxim-Dallas iButton keys (iButton DS1990A – 64 Bit ID)) can be used to ARM/DISARM security panel or control selected output. Up to 800 iButton keys can be assigned to the system.

The First iButton key may be learned (recorded) by touching it to the reader. Without the need to send any SMS. The system will notify about successfully recording of the key into memory by shortly beeping twice via buzzer. The system will automatically assigns control function (ARM/DISARM).

The first key is the main key (MASTER) The total length of the bus up to 100 m. Depending of cable quality, and environment noise. If LED is without resistor. External 4.7k – 10k resistor required.

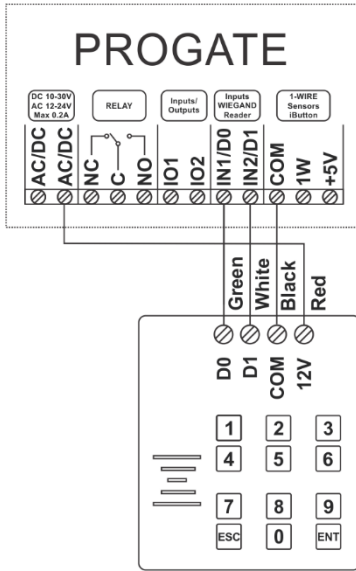


Figure 21 Wiegand keypad wiring

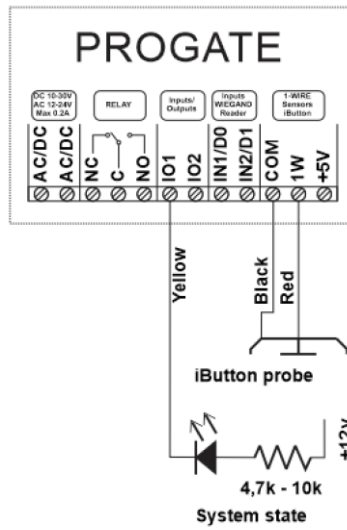


Figure 22 iButton connecting diagram

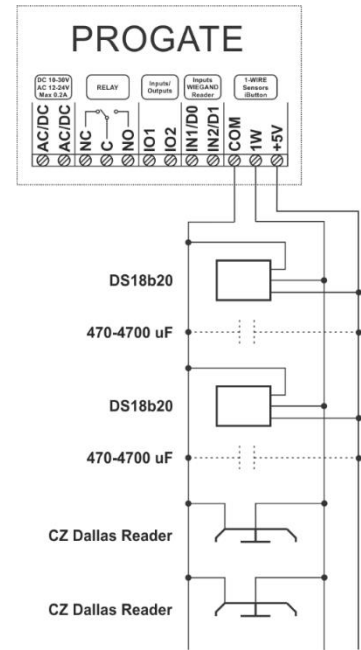


Figure 23 iButton connection diagram

## 4.2.2 Enter iButton, RFID, Phone numbers to the memory of the module

### First steps:

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

### Configurations methods:

Start automatic learning mode via mini USB cable (Sera2 software).  
 Start automatic learning mode via SMS command INST000000 063 1  
 Enter Keypad numbers manually via mini USB cable (Sera2 software).  
 Start automatic learning mode remotely via Sera2 software.

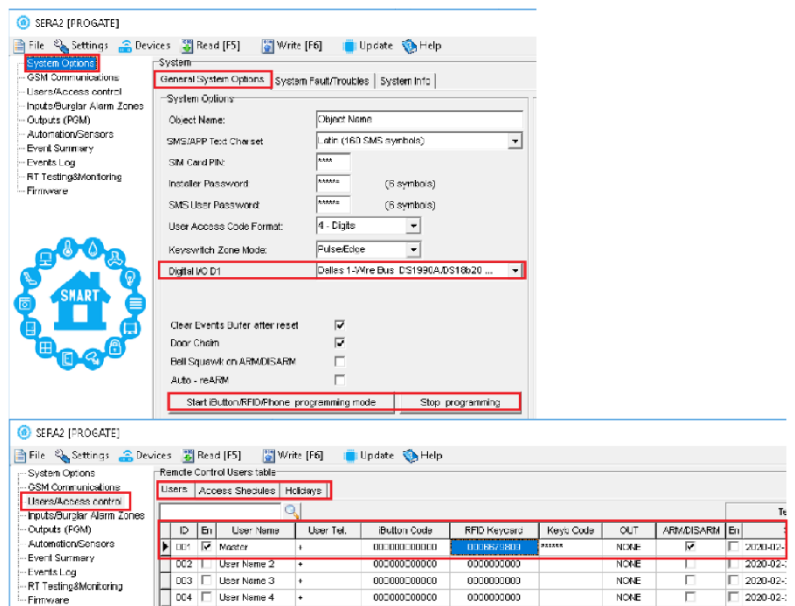
<https://youtu.be/VojAGa33rBY>

### If you want to edit existing configuration,

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

### Start automatic learning mode via mini USB cable (Sera2 software).

Go to Sera2> System Options> General system Options.  
 Select Dallas 1- Wire Bus (for iButton keys)  
 Press "Write"  
 Press "Start iButton/ RFID/ Phone programming mode."  
 Go to Sera2> Users/ Access control window.  
 Touch RFID keycards, iButton keys to the reader.  
 RFID keycard, iButton key numbers will appear in the list.  
 Go to System Options> General system Options and  
 Press "Stop programming" or wait until it will stop automatically.  
 Edit setting in the Users/ Access control window.  
 Press "Write"  
 Go to RT Testing & Monitoring> Hardware.  
 Press "Start Monitoring"  
 Go to RT Testing & Monitoring> Security Alarm Panel/ Access

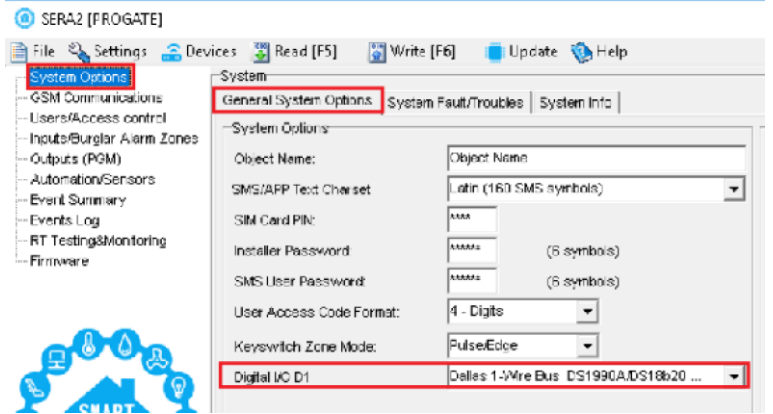


**Start automatic learning mode via SMS command INST000000 063 1**

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

**INST000000\_063\_S**

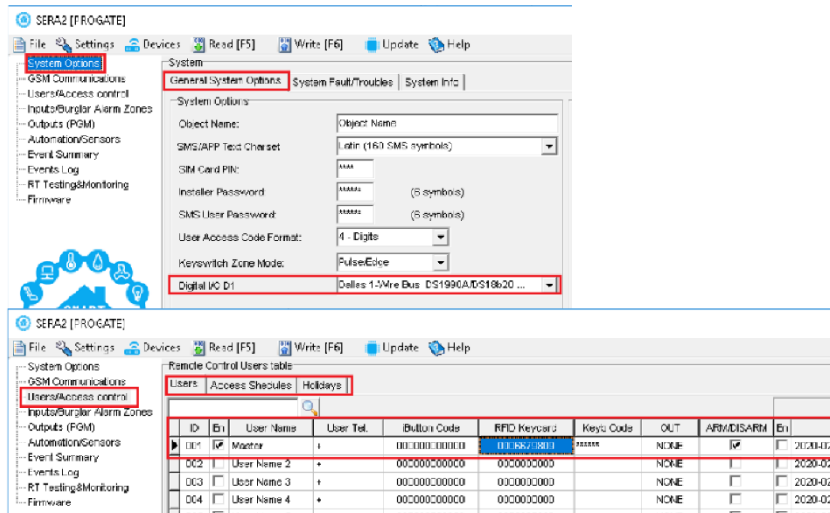
INST = Install. Configuration of the parameters.  
 000000= Installer's password  
 \_ = Space character  
 063= command code (iButton keys learning/deleting mode)  
 \_ = Space character  
 S=iButton keys entering/deletion mode.  
 0- Disable iButton keys learning mode,  
 1- Enable iButton keys learning mode,  
 2- iButton keys deleting mode,  
 Delete these keys from memory, which will be touched to the reader.



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

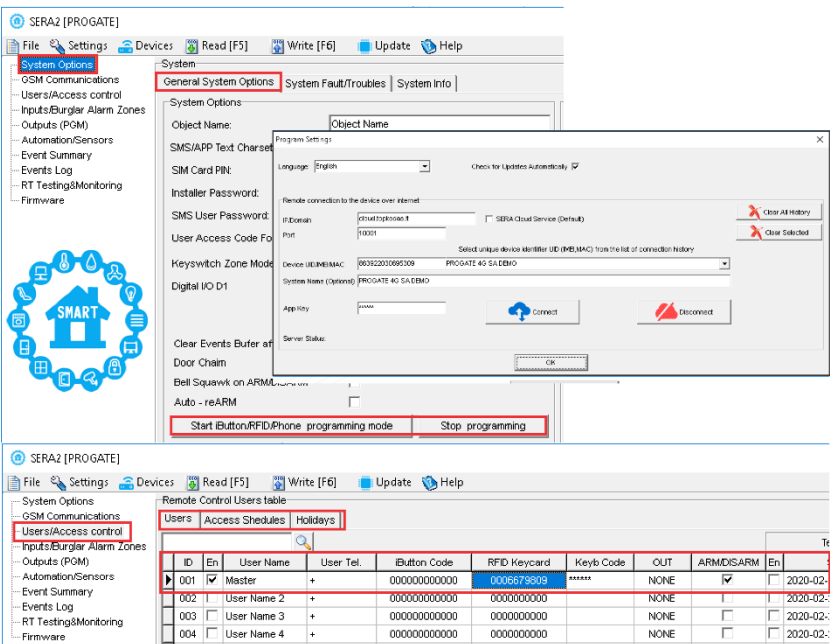
**Enter Keycard numbers manually via mini USB cable (Sera2 software).**

Go to Sera2> System Options> General system Options.  
 Select Dallas 1- Wire Bus (for iButton keys)  
 Press "Write"  
 Go to Sera2> Users/ Access control.  
 Enter RFID keycard, iButton key numbers  
 Edit other settings  
 Press "Write"  
 Go to RT Testing & Monitoring> Hardware  
 Press "Start Monitoring"  
 Go to Security Alarm Panel/ Access"  
 Touch the keycard to the RFID reader and iButton keys to the probe



**Start automatic learning mode remotely via Sera2 software.**

Start Sera2 software  
 Press "Connect remotely" button  
 Enter required parameter.  
 (Default App Key is 123456)  
 Press "Connect"  
 Go to Sera2> System Options> General system Options.  
 Select Dallas 1- Wire Bus (for iButton keys)  
 Press "Write"  
 Press "Start iButton/RFID/Caller ID Learning Mode"  
 Touch RFID keycards, iButton keys to the reader  
 Press "Stop programming" button  
 Or wait until the learning mode will stop automatically

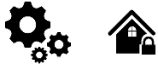






Refer to: Users & Access Control programming details.

## 4.3 Outputs



The module **Progate** has:

- 1 open drain (1A) output: RELAY. The output can be used for siren, relay, and lamp connection. This outputs can be controlled via short call or SMS. Output operation algorithms: Automation /CTRL, Siren, Buzzer, ARM state, Zones OK, Light Flash, inverting, pulse mode. Max current – (-V) 1000 mA.
- 2 open drain (20mA) outputs: I/O1 (20mA)... I/O2 (20mA). These outputs can be used for solid state relays, LED, to control devices up to 20mA.
- 1 output: D1 (10mA, Max Voltage 3,3V) for LED, solid state relays control. ! Max voltage 3,3V
- All outputs can be controlled via short call DIAL, SMS message, mobile, web app. This feature may be used for gate opening
- Output alarm parameters may be programmed.
- Programmable algorithms for outputs operation: CTRL/SMS/DIAL, SIREN, BUZER, ARM state, Zones OK, Light Flash, inverting, pulse mode

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

**i** Each output has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined output, for Example: Lights

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

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

### 4.3.1 Output PGM wiring. Bell, Relay, Led Wiring

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

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

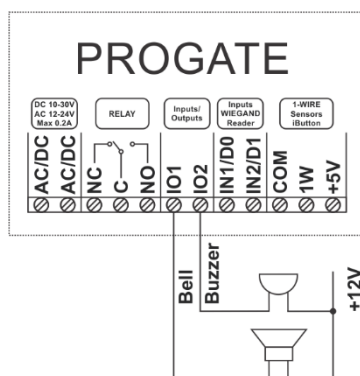


Figure 25 Bell, buzzer connection to I/O1, I/O2

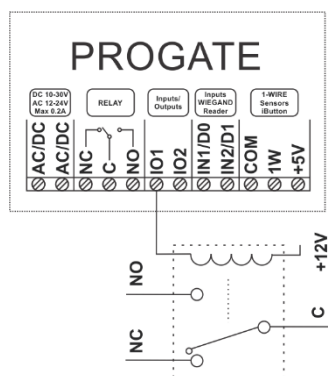


Figure 24 Relay connection to , I/O1, I/O2

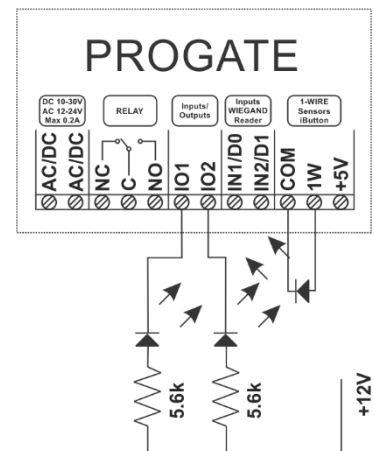


Figure 26 LED connection to I/O1, I/O2

**Output mode: timer, steady, pulse count.**

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

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

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

**Set output's parameters step by step:**

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

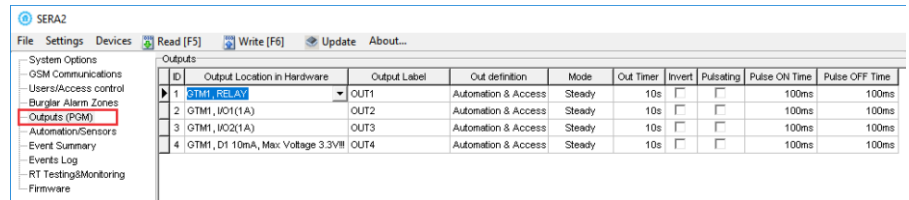


Figure 27Outputs (PGM) window

**If you want to edit existing configuration,**

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

**4.3.2 Control Outputs via SMS**

<code>USER123456_021_N#ST</code>	<p><b>Activate or deactivate selected output N.</b>          021= command code (Activate or deactivate selected output N)          N = output number          ST= output mode: 0 – deactivated output, 1- activated output</p>
----------------------------------	--

**4.3.3 Control Outputs via short call, iButton, RFID**

**4.3.4 Control Outputs via app**

**4.3.5 Output programming**



Output pulse counter

<https://youtu.be/V9vt10q-o8Q>



How to send commands to generate various pulse lengths (5s, 10s)

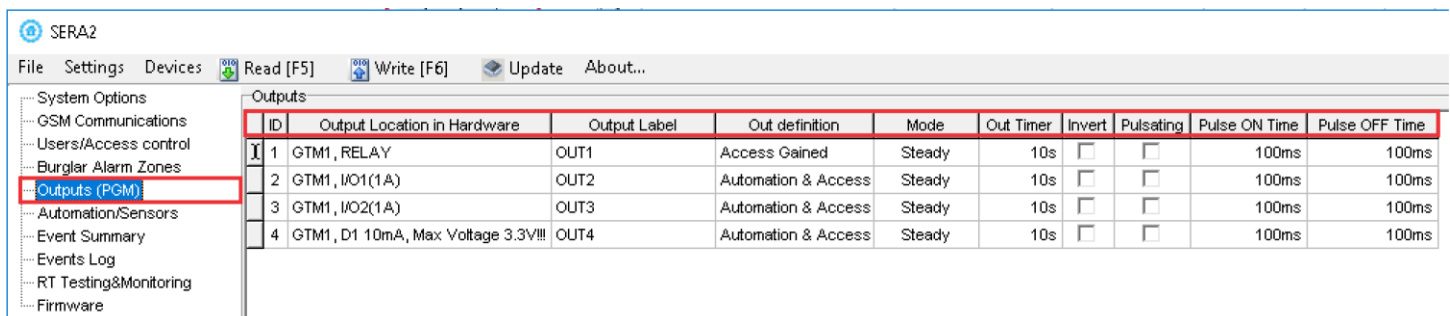
<https://youtu.be/KGvpfa38Iu0>

**Quick start outputs**

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

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

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

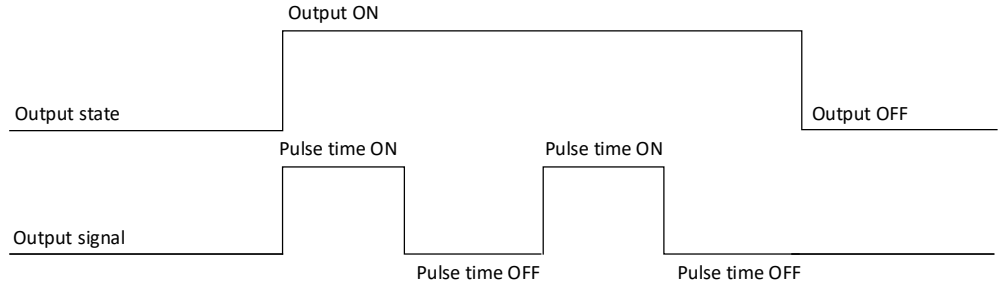


**If you want to edit existing configuration,**

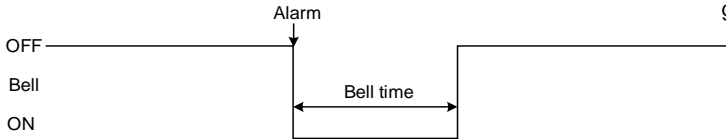
- You have to read it (press “Read” in the command line)
- Edit settings
- Write edited configuration (press “Write” in the command line)

**Outputs can be set as timers.**

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



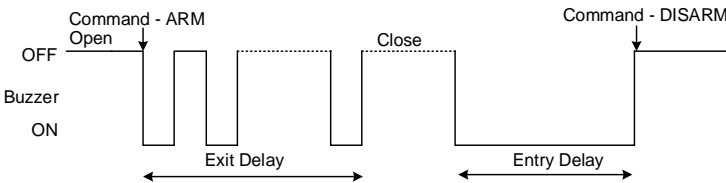
**Bell:** Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.



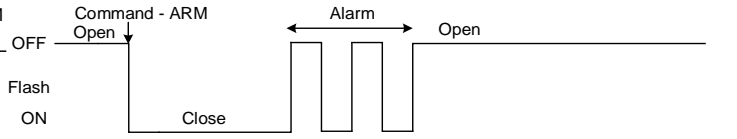
**ARM/DISARM:** Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.



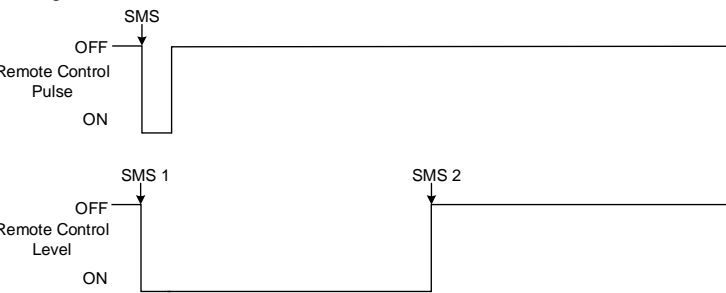
**Buzzer:** Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.



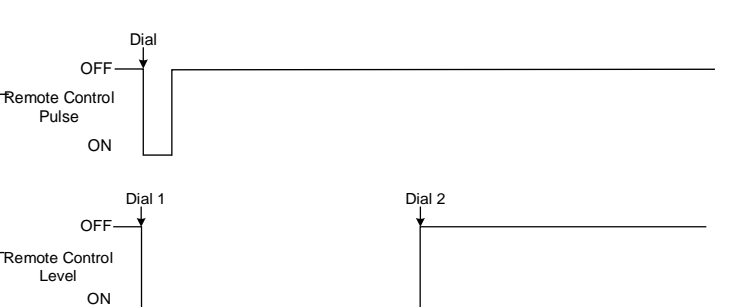
**Flash:** Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



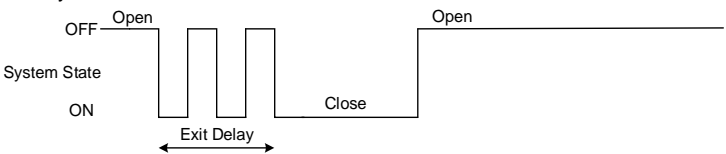
**Remote Control:** Output designed for connection of electrical devices which will be controlled by SMS message or phone call a) control by SMS message



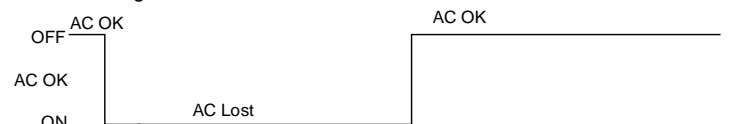
**Remote Control b) control by phone call**



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

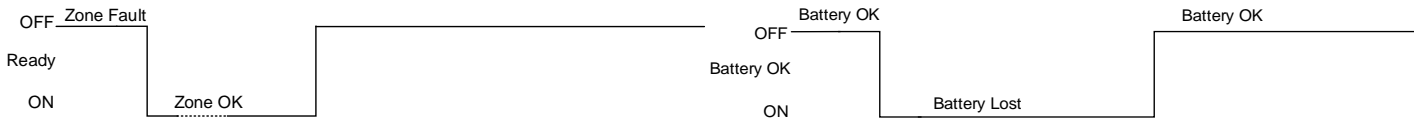


**AC OK:** Output for connection of indicator about control panel supply from alternating current



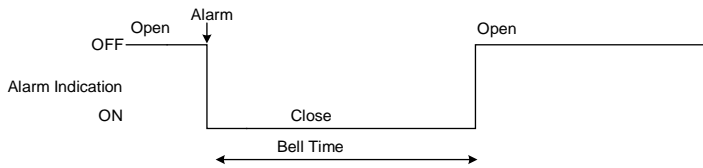
**Ready:** Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.

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



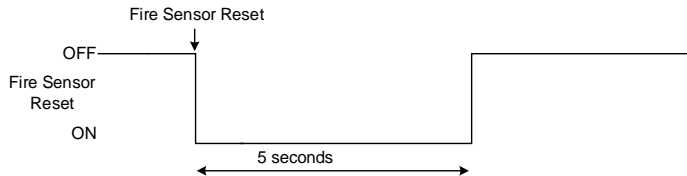
**Alarm indication:** Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.

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



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

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



### 4.3.6 Access control output with logging

If you want to edit existing configuration,

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

Set output definition to [Access Gained] . Sera2>Outputs

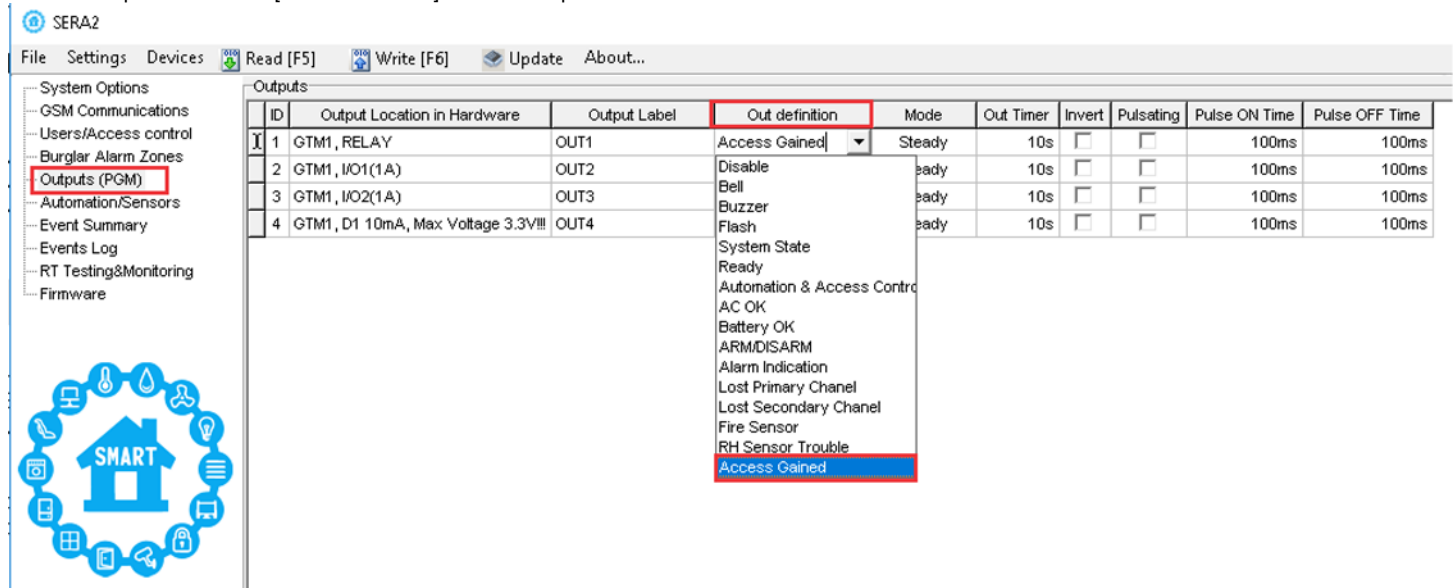


Figure 29 Outputs (PGM) window

This output could be controlled as following:

- If the user has right to ARM/DISARM system, it always has access to this output.
- If the user has not the right to ARM/DISARM the system (field near ARM/DISARM is not marked (Sera2> User/ Access control)), the user can access this output only if system is Disarmed.

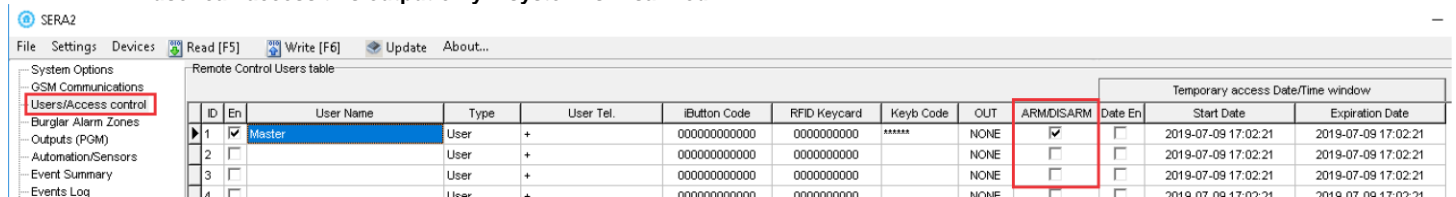


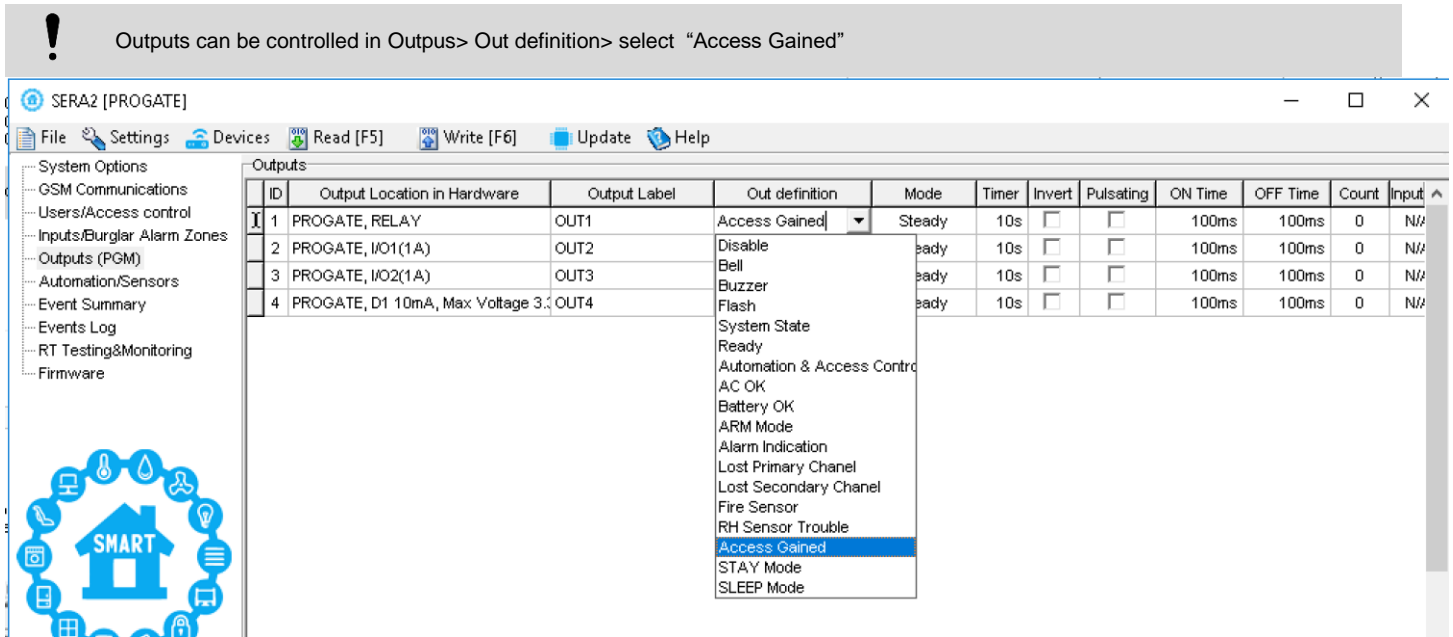
Figure 30 User/ Access control window

- If access is granted by user, 421 event Access granted is stored into the log. If not Access denied event 422 is stored to the log (Sera2> Events Log)

- if output will have definition [**Automation / CTRL**] it also can be controlled by user in any way but it will not generate 421 and 422 events

Event log e.g.

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



8. If you need to control outputs by short call or SMS, go to Sera2> Users/ Access control window and enter phone numbers of users, who will be able to control selected outputs via free short call.

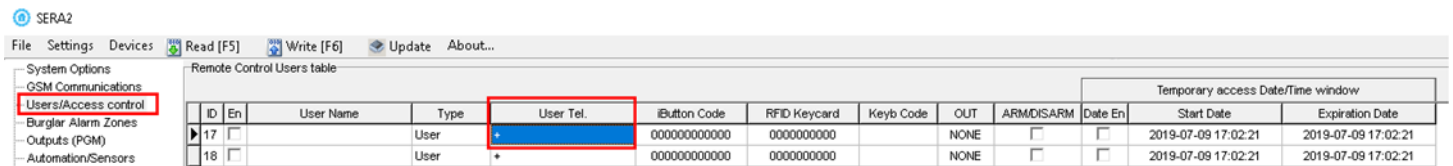


Figure 31 Users/ Access control window

9. Write configuration by pressing write icon
  - In order to control big power alternating current equipment, it is comfortable to use solid state relays.

Refer to: Outputs. Bell & PGM programming

## 4.4 How to set clock synchronization?

**If you received SMS messages with wrong date/ time, you need to set clock synchronization correctly**

You can select **clock synchronization** via:

### GSM modem

- (If you will not use mobile app and cloud service)

### Cloud Server

- (If you will use mobile app)
- SIM card must have data available
- Insert the SIM card in your smart phone and check is the internet available

**Or disable** 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

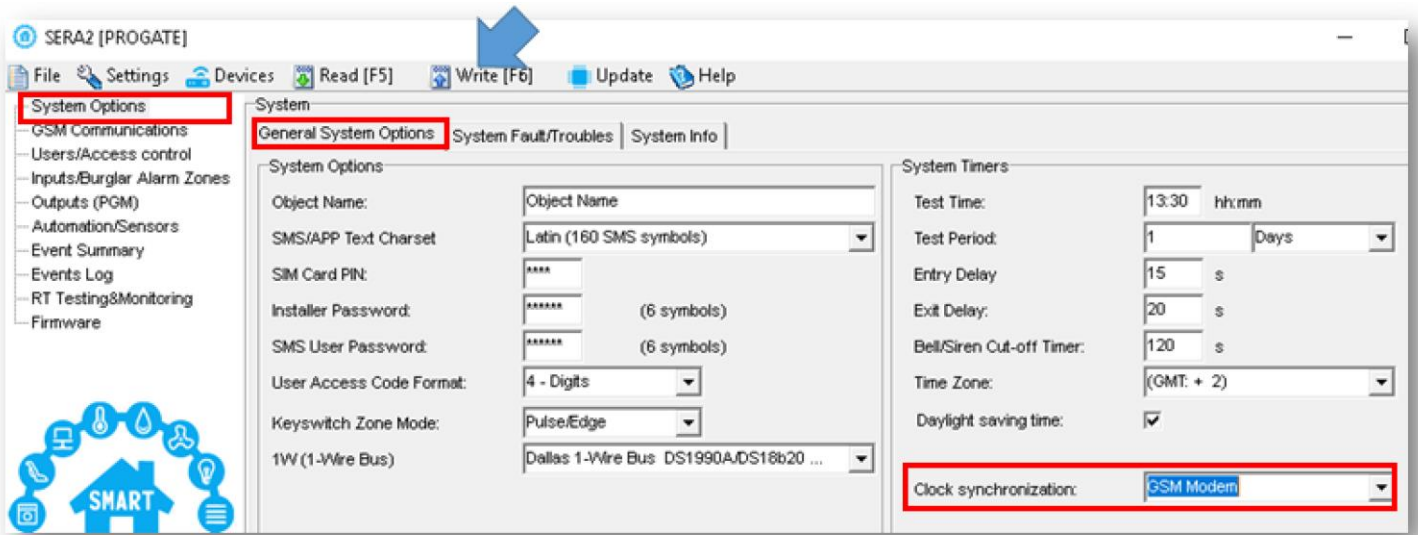


Figure 32 SERA2> System Options> General System Options

### Clock synchronization via Cloud server

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

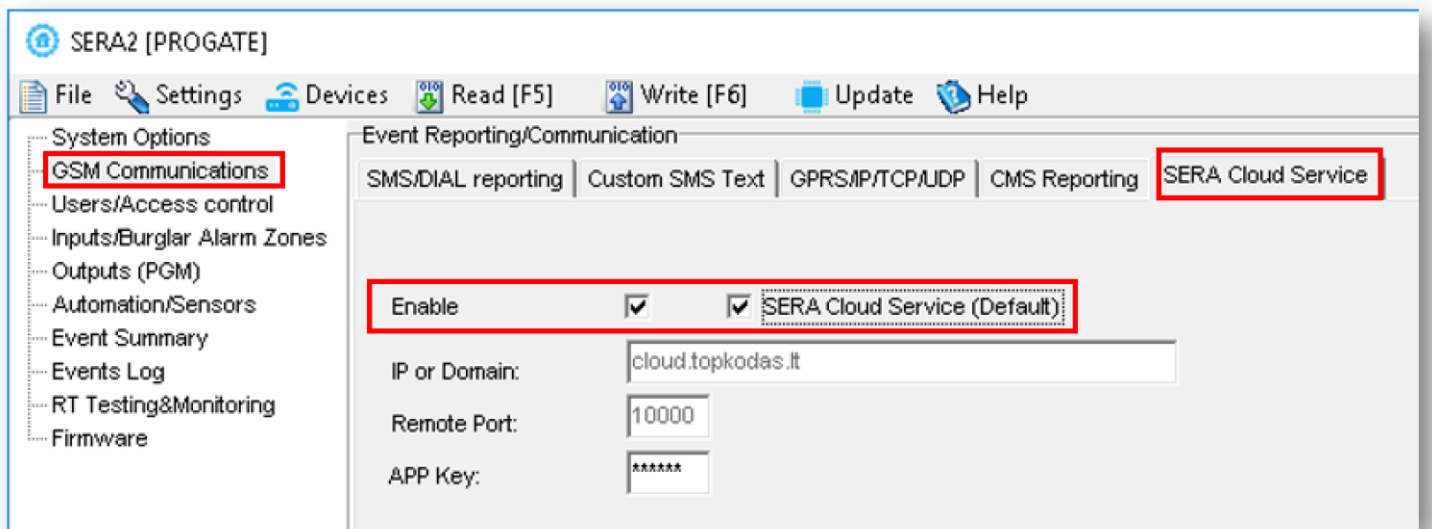
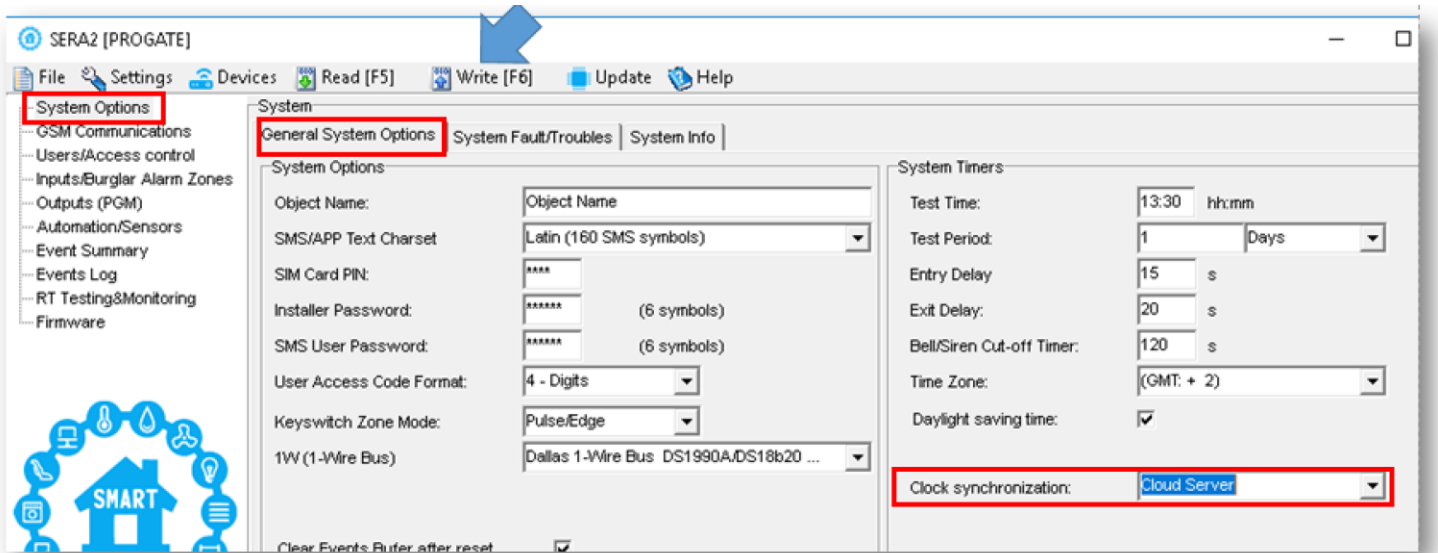


Figure 33 SERA2> GSM Communication> SERA Cloud Service

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

Figure 34 SERA2> System Options> General System Options



### If you want to edit existing configuration,

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



Figure 35 SERA2 Command line

## 4.5 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,

### 4.5.1 Humidity sensors AM2302/DHT22/AM2305/AM2306/AM2320/AM2321



Quick start humidity sensor AM2320

<https://youtu.be/CwXUOCbOrTQ>

Module should work with following sensors: Aosong 1-Wire bus Humidity Sensor AM2302, DHT22, AM2305, AM2306. Also a new smaller sensor exists AM2320 & AM2321.

Table 6 Sensors AM2302, AM2320/AM2321 specification

Manufacturers' Specification	AM2302	AM2320/AM2321
Operating Range	0–100	0–100
Absolute accuracy (%RH, 25°C)	±3% (10-90%) ±5% (<10, >90%)	±3% (10-90%) ±5% (<10, >90%)
Repeatability (%)	±0.3	±0.1
Long term stability (% per year)	0.5	0.5
1/e Response (sec)	5	5
Voltage supply (V)	3.3–5.5	3.1–5.5(AM2320) 2.6–5.5(AM2321)

The table lists values taken from datasheets. The Aosong data sheets do not specify maximum tolerances for most parameters, just 'typical' values. It would therefore seem that any particular device is not guaranteed to meet these specifications. For all the other devices the numbers above are the maximum tolerances and most also offer better 'typical' specifications.

Each AM2302 sensor connects on separate bus line to digital input D1 (Digital I/O D1 in Sera2). Total up to 1 AM2302 Aosong (Guangzhou) humidity sensor could be connected to Progate  
 Steps to start AM2320 and AM2302 sensors:

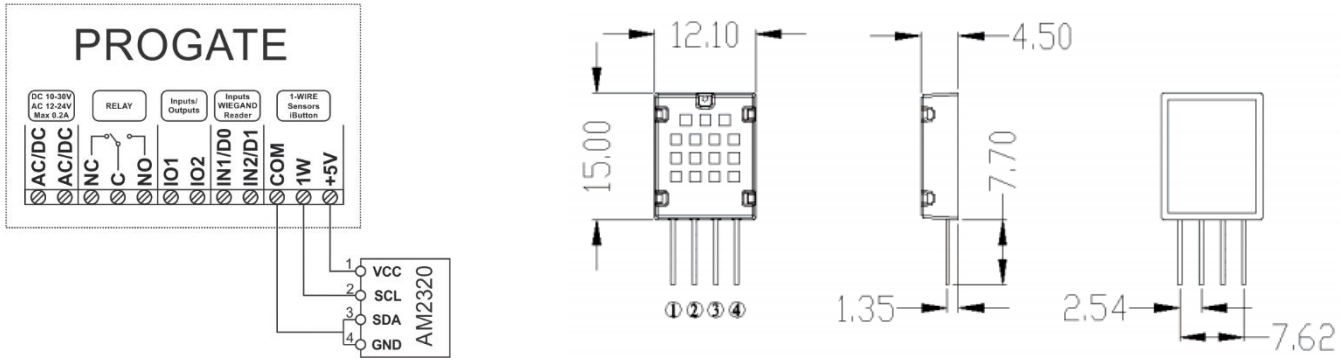


Figure 36 AM2320 connecting diagram

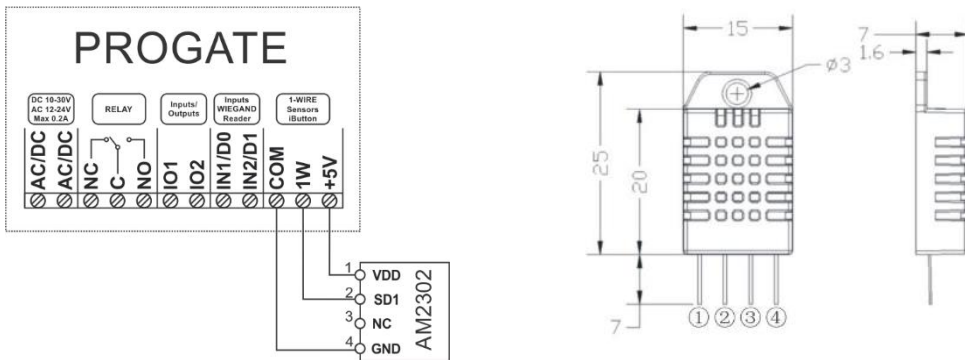


Figure 37 AM2302 connecting diagram

1. Connect AM2320 or AM2302 to the 1W according connection diagram.
2. Connect the module to the computer and connect the power supply.
3. Start free configuration program Sera2

**If you want to edit existing configuration,**

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



- Sensor's type should be select in the Sera2> System Options> General System Options window. Set 1W (1 Wire Bus) to Aosong 1- wire bus humidity/ temperature sensor....

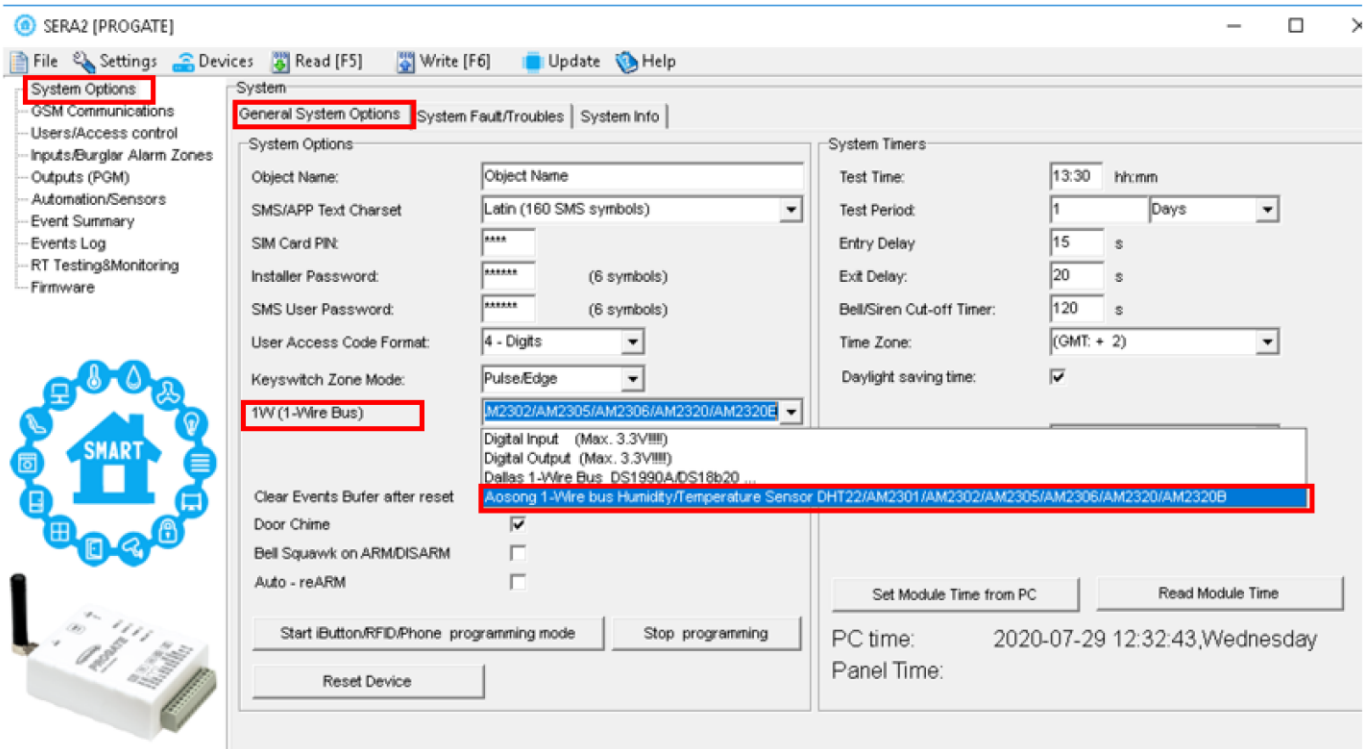


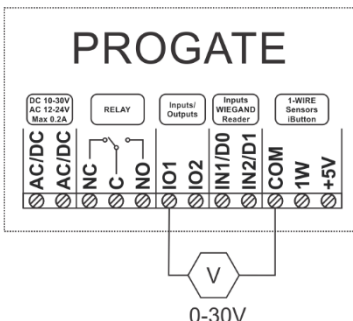
Figure 38 System Options> General System Options

- Write configuration, by pressing “Write” icon
- After module starts, wait a minute while sensor will be found on the bus.
- Read configuration, by pressing Read icon
- Go to Sera2> Automation/ Sensors window. The sensor will appear in the list automatically.
- Double click on the selected sensor's line.
- Set other parameters of the sensor MIN, MAX values Units etc.
- Write configuration to module



**Please visit:** [Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?](#)

#### 4.5.2 Analog inputs 0-30V



Steps to start analog sensors:

- Connect analog voltage sensors to I/O1, I/O2, according connection diagram.
  - The analog inputs can be used as security system zones or analog sensors.
- If analog inputs sensors is not in use, the inputs should be disabled in “Zones” or “Sensor” window.
  - Analog sensors should be calibrated and parameters should be set in the Automation/Sensors window. Sera2> Automation / Sensors. Sensors calibration is possible by changing multiplier, offset.

Refer to Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software

- When all changes has been done, the configuration should be written to module, by pressing write icon.

Figure 390-30V sensor connecting diagram

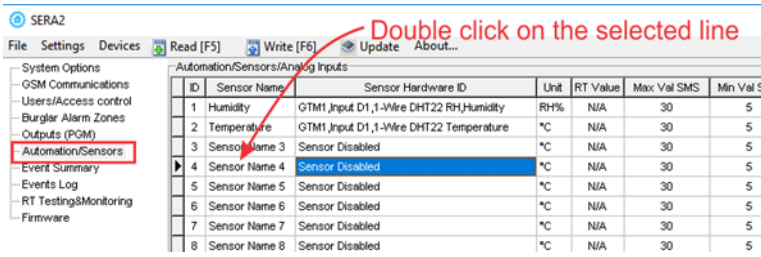


Figure 40 Automation/ Sensors window



Any automation voltage analog sensors 0-10V, can be connected to IN1-IN4 (has internal pull up resistor 5.1K) , and I/O1, I/O2

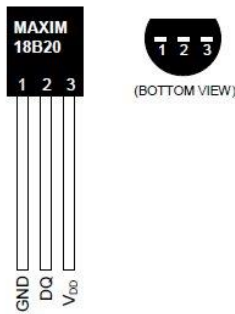


**Please visit:** [Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?](#)

### 4.5.3 Temperature sensors Dallas 1-wire DS18B20 installation & recommendations



The DS18B20 digital thermometer provides 12-bit Celsius temperature measurements. The DS18B20 communicates over a 1-Wire. Each DS18B20 has a unique 64-bit serial code, which allows multiple DS18B20s to function on the same 1-Wire bus. Thus, it is simple to use one to control many DS18B20s distributed over a large area. Applications that can benefit from this feature include HVAC environmental controls, temperature monitoring systems inside buildings, equipment, or machinery, and process monitoring and control systems.



#### Applications/Uses

- Consumer Products
- Industrial Systems
- Thermally Sensitive Systems
- Thermometers
- Thermostatic Controls

#### Key Features

- Measures Temperatures from -55°C to +125°C (-67°F to +257°F)
- ±0.5°C Accuracy from -10°C to +85°C
- Each Device Has a Unique 64-Bit code.

Figure 41DS18b20 sensor

#### 4.5.3.1 Wiring Dallas 1-wire DS18b20

- Connect 1-Wire sensors DS18b20 to D1 according connection diagram.

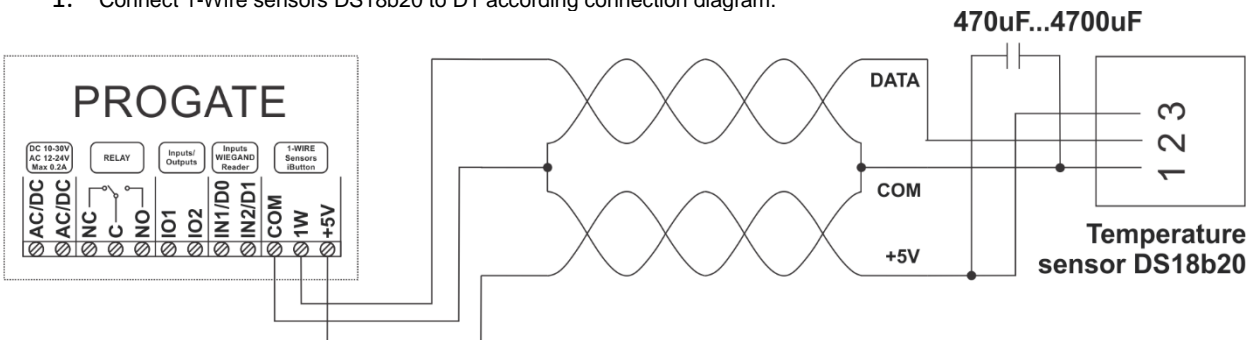


Figure 42DS18b20 connection with long distance UTP or FTP cable

- If you need to connect more sensors to the same input, connect them as a star or serial. Each line should be separated by 82-120 Ohm resistor

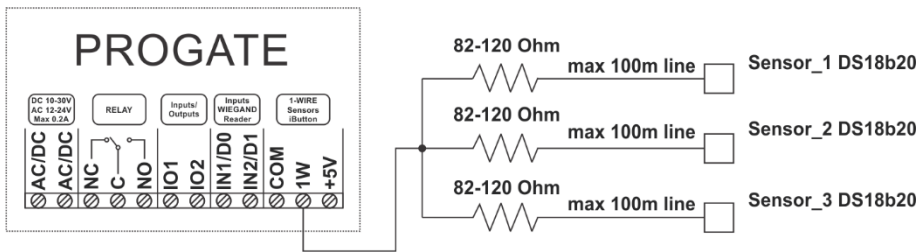


Figure 43 Star connection



The resistor must be as close as possible to the contacts of the module Progate.

Using cat 5 cable is best and will make it easier to maintain a working 1-wire network when you expand and add more sensors. The data and ground should use one twisted pair, for example blue/blue-white. A single wire from another pair is used for the 3.3 volt supply.

Don't double up wires on the assumption that this lowers resistance and is a 'good thing', it actually alters the impedance of the network and makes it less reliable. All unused wires in the cat 5 cable should be left unconnected (don't connect them to ground). When running a 1-Wire bus, Dallas recommend that you use an unshielded Cat5 cable for the bus. Do not use shielded cable as the capacitance increase will upset the network.

If you intend to have a large 1-Wire network, it is important that you design the network correctly, otherwise you will have problems with timing/reflection issues and loss of data. You must connect each sensor to a single continuous cable which loops from sensor to sensor in turn (daisy chain). This will reduce potential miss-reads due to reflections in the cable. Each sensor should have a maximum of 50mm (2") of cable connected off this main network. Even when using this method, connecting more than 10-15 sensors will still cause problems due to loading of the data bus. To minimize this effect, place a 100-120Ω resistor in series in the data line of each sensor before connecting to the network. The total length of the bus up to 100m. Depending of cable quality sensors number on bus, and environment noise. There is possibility to connect up to 32 devices.

Begin the installation by mounting additional devices in the cabinet using the stand-offs provided, then mount the cabinet in a dry, protected area with access to unstitched AC power. Install hardware in the sequence indicated in the following pages. Do NOT apply power until installation is complete.



All circuits are classified UL power limited except for the battery leads. Minimum ¼" (6.4mm) separation must be maintained at all points between power limited and non-power limited wiring and connections.



Please visit: [Temperature sensors Dallas 1-wire DS18b20 Configuration](#)

#### 4.5.3.2 Temperature sensors Dallas 1-wire DS18b20 Configuration



Step by step to start DS18b20 sensors:

##### If you want to edit existing configuration,

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

1. Connect 1-Wire sensors DS18b20 to D1 or D2, D3 according connection diagram. Connect the sensors as showed in [Wiring Dallas 1-wire DS18b20](#). If you need to connect more sensors to the same input, connect them as a star or serial.
2. Digital input 1W type should be select in the System Options> Digital I/O Settings window. Set digital input definition D1 to Dallas 1-Wire Bus option

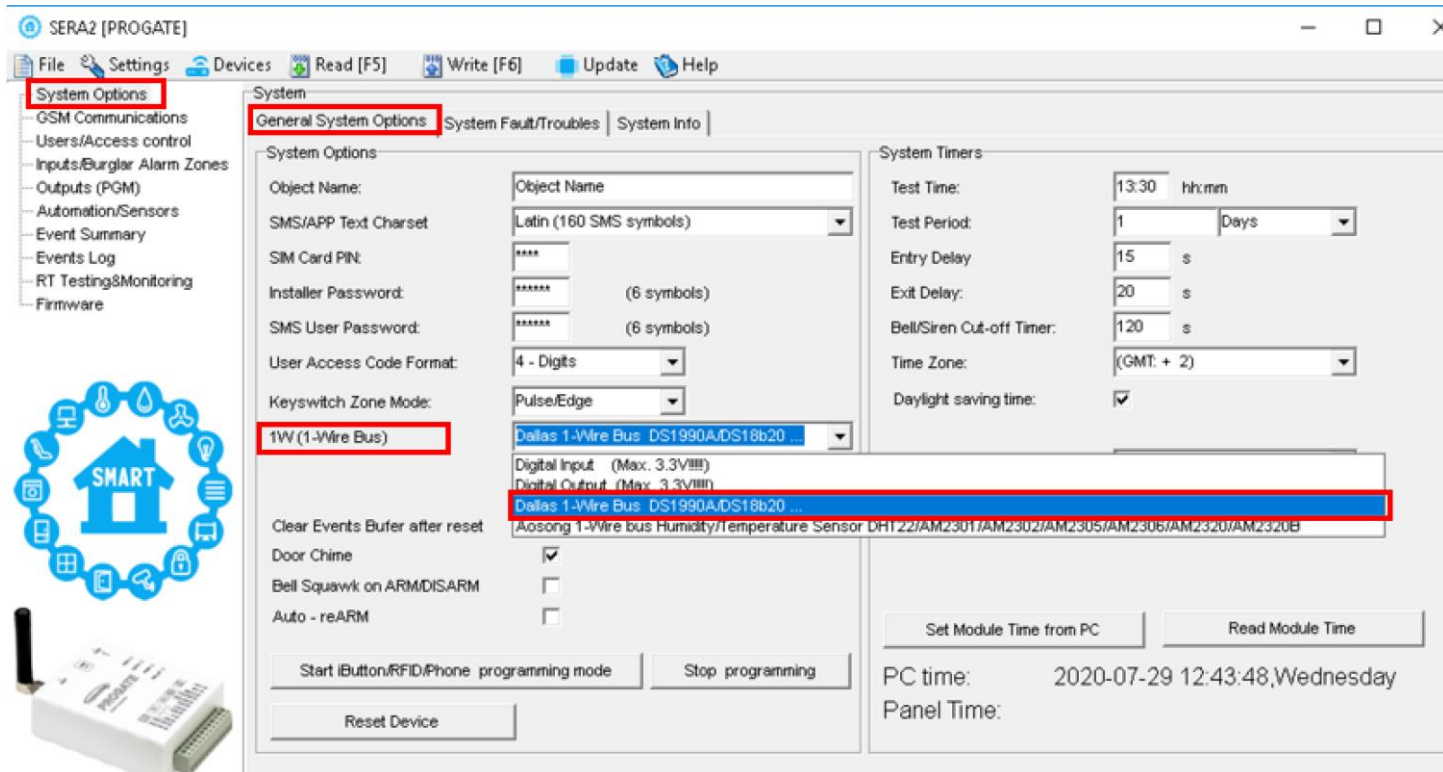


Figure 44 System Options > General System Options

1. Write configuration by pressing "Write" icon
2. Power the module.
3. After module starts. Within few seconds, it will automatically scans and registers all connected 1-Wire sensors on the bus.
4. Read configuration
5. Go to "Automation/ Sensors" window in the SERA2 software

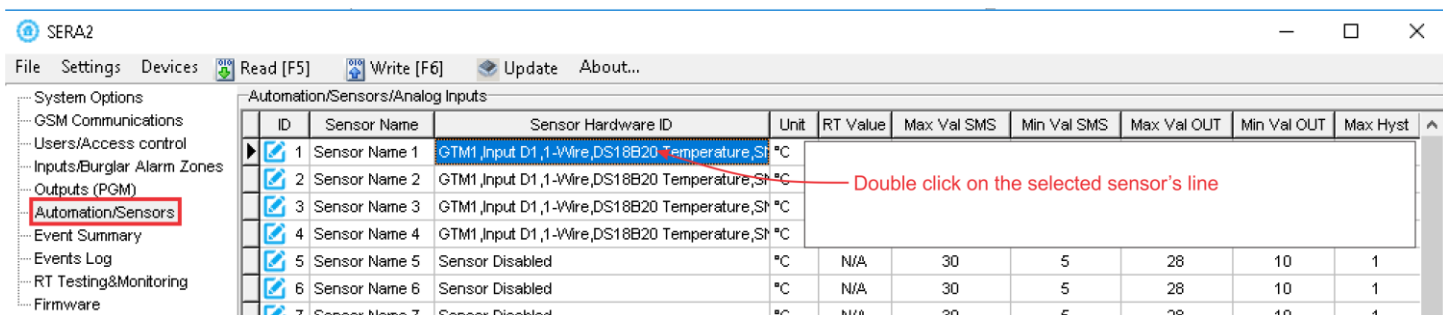


Figure 45 Automation/ Sensors window

6. Double click on the selected sensor's line. Set other parameters of the sensor MIN, MAX values Units etc. Every field explanation: Automation & Sensors Programming
7. Write configuration to module, by pressing "Write" icon



**Please visit:** [Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?](#)

#### 4.5.3.3 How to change temperature scale from Celsius to Fahrenheit

##### If you want to edit existing configuration,

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

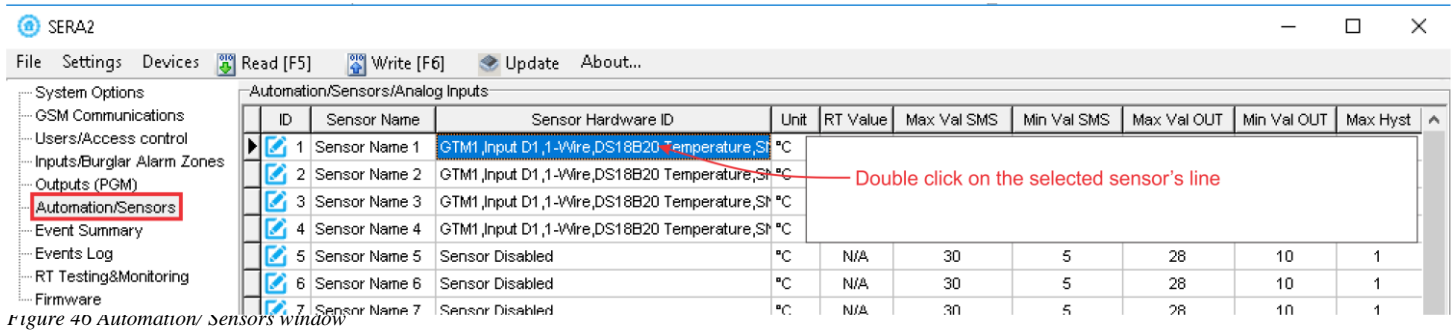


Figure 40 Automation/ Sensors window

1. Go to SERA2> Automation/ Sensors (double click on the sensor's line).
2. Enter Y (offset) and X (multiplier) values.
3. Change the units to Kelvin or Fahrenheit in the SERA2> Automation/ Sensors (double click on the sensor's line).

Y(offset)=273.15, X(multiplier)=1

**Celsius to Fahrenheit conversion**

Y(offset)=32, X(multiplier)=1.8

**Celsius to Kelvin conversion**



Refer to: Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software

#### 4.5.4 Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?



Testing Monitoring Automation AM2320

<https://youtu.be/-qklzGKELJI>



GSM Communication.  
Receive alarms to your mobile phone

<https://youtu.be/qFBT5zF42UQ>



Refer to: RT Testing & Monitoring. Hardware.

The list of alarm events with time and date stamp: RT Testing & Monitoring> Event Monitoring



Refer to: Real-time Testing & Monitoring > Event Monitoring

It is possible to receive alarm SMS to the mobile phone: GSM Communication> SMS/ Dial reporting



Refer to: Reporting to the user's mobile phone

Real time sensor values and states: RT Testing & Monitoring> Sensors/ Automation.



Refer to Real-time Testing & Monitoring > Sensors/ Automation

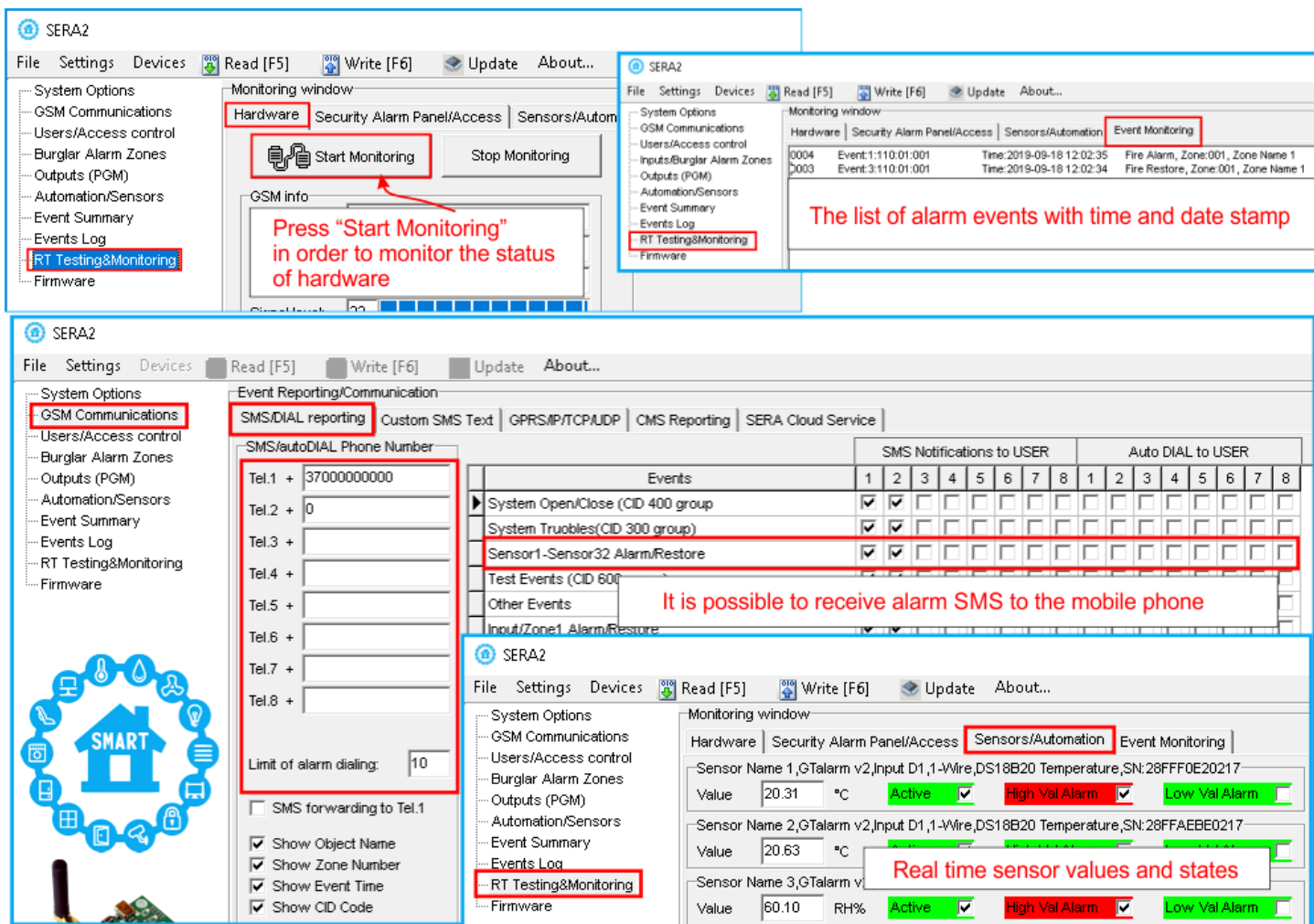


Figure 47 How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list

#### 4.5.5 How to edit alarm SMS text?

##### Step by step:

- Go to SERA2> Event Summary
- Edit text
- Press „Write“ in the command line

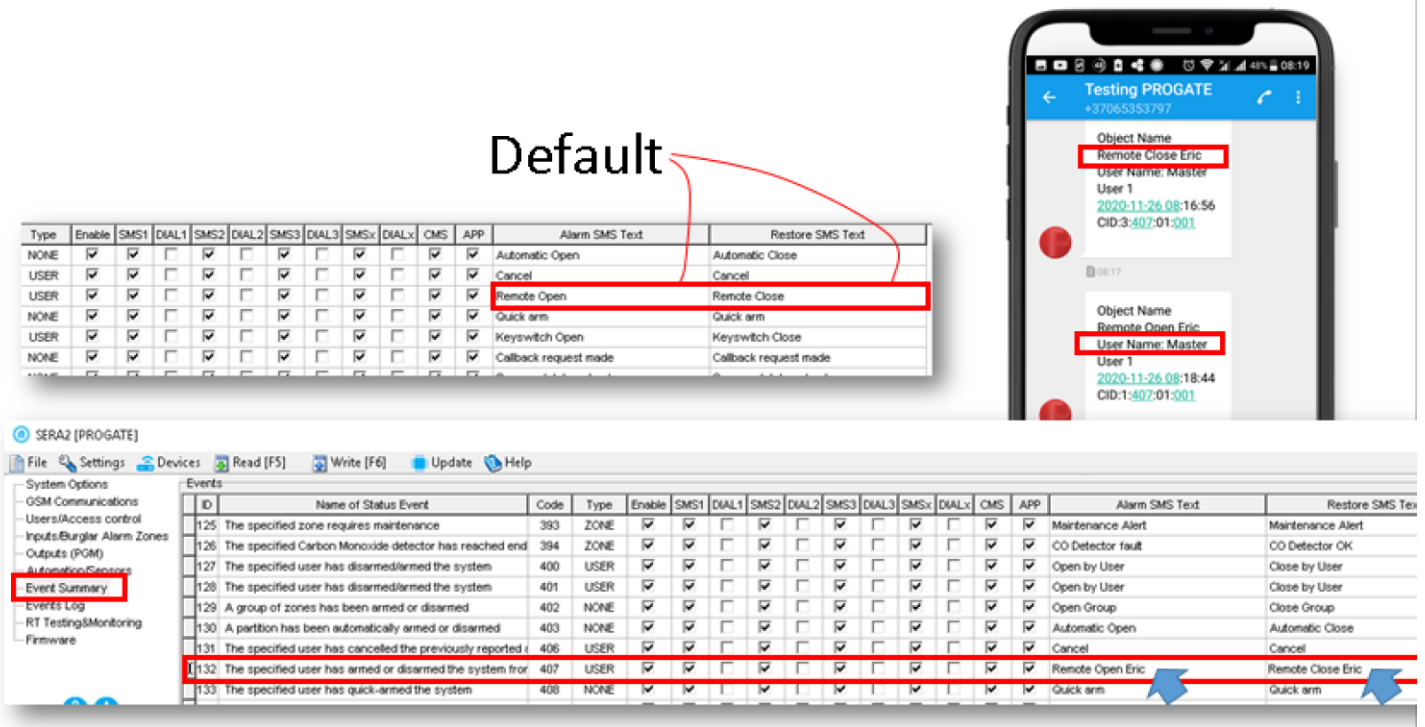


Figure 48 SERA2> Event summary

Go to SERA2> GSM Communications> SMS/ DIAL Reporting  
 Unmark  
 Press „Write“ in the command line

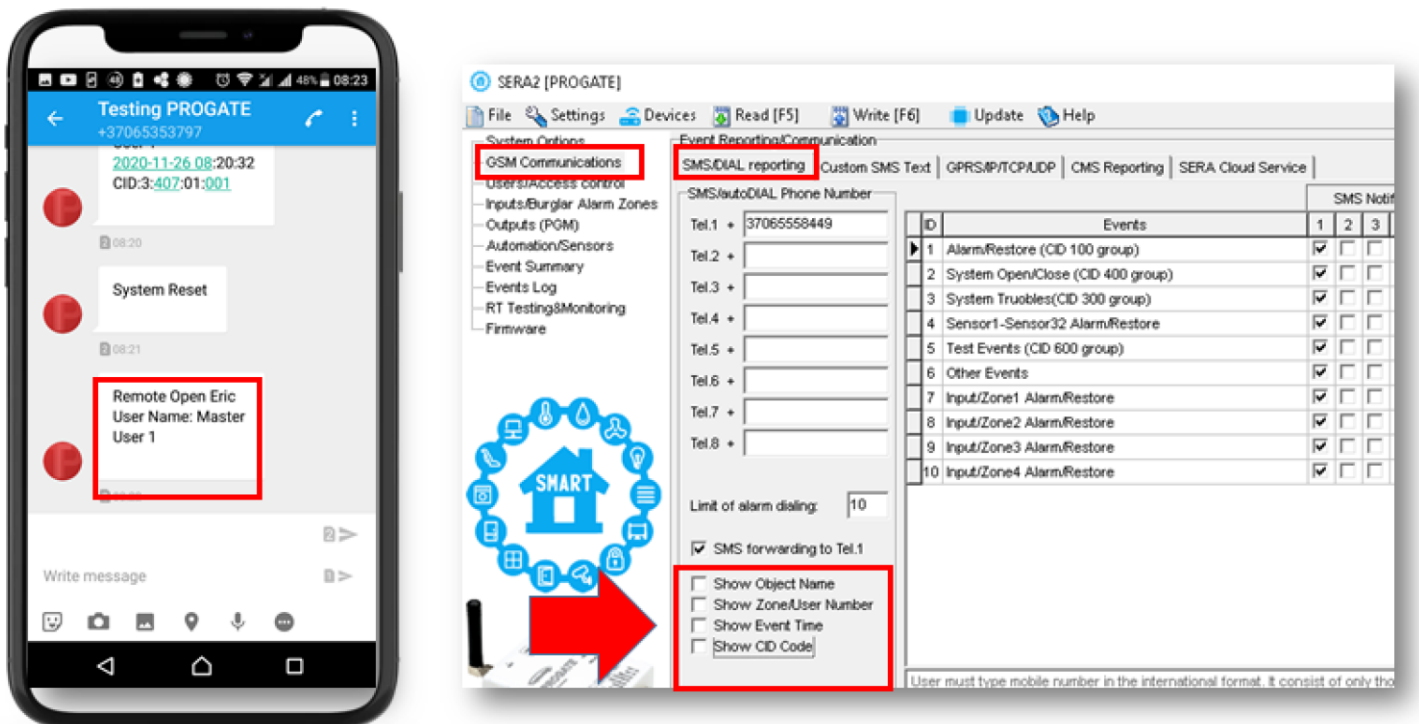


Figure 49 SERA2> GSM Communication> SMS/ DIAL reporting

Go to SERA2> Users/ Access control> Users  
 Edit user name  
 Press „Write“ in the command line

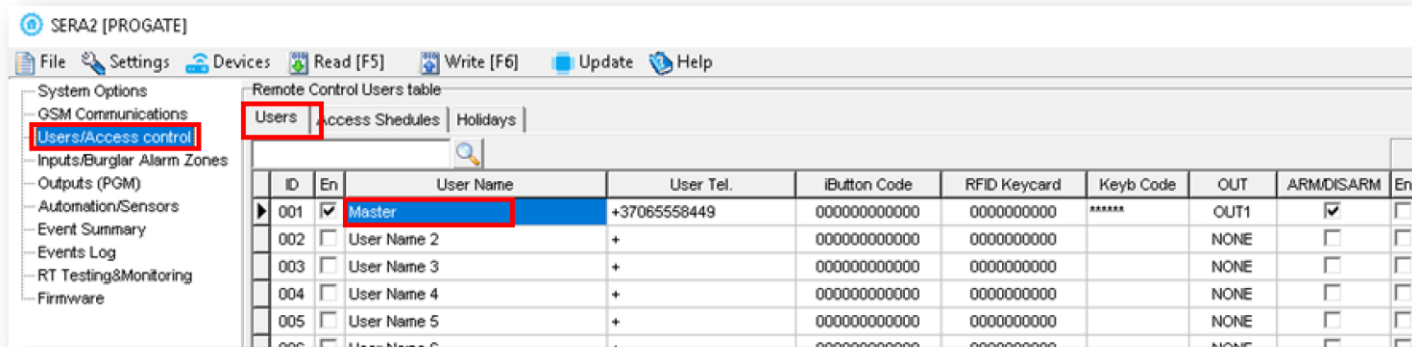


Figure 50 SERA2> User/ Access control> Users

#### 4.5.6 Burglar Alarm sensor zones wiring EOL NO NC



The module Progate has:

- In1, In2, I/O1, I/O2 Can be used or use it as security system's zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- I/O1, I/O2 with selectable type: NC/NO/EOL/EOL+TAMPER.

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

- Connect security system's sensors to module the as is shown in connection diagrams below
- Set the required parameters
- Write configuration by pressing „Write“ icon

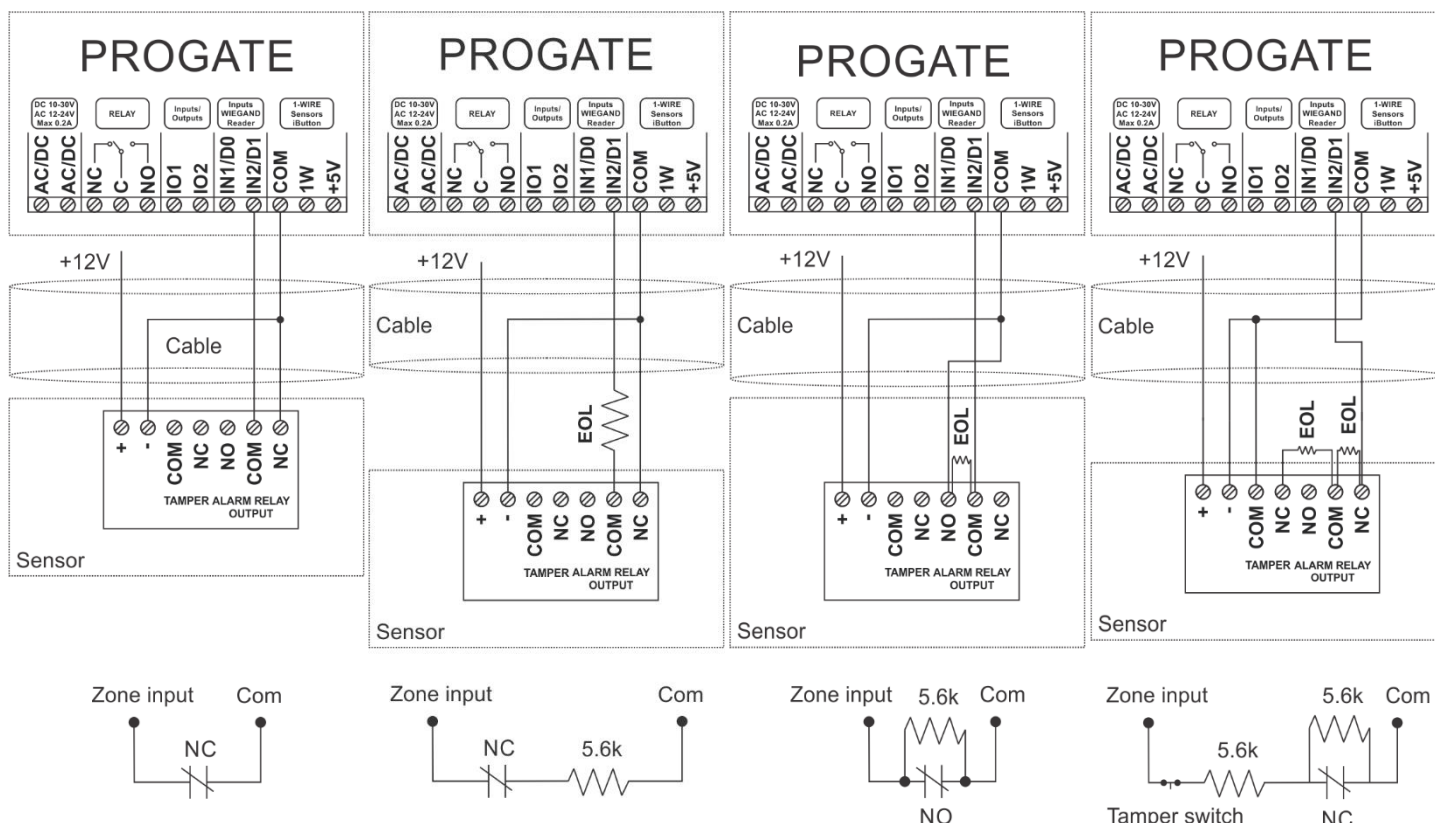


Figure 51 NC Contacts, No EOL

Figure 52 NC, With EOL

Figure 53 NO, With EOL

Figure 54 NC With EOL Wire Fault Recognition



All inputs has pull up resistors 10k

If you want to edit existing configuration,



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

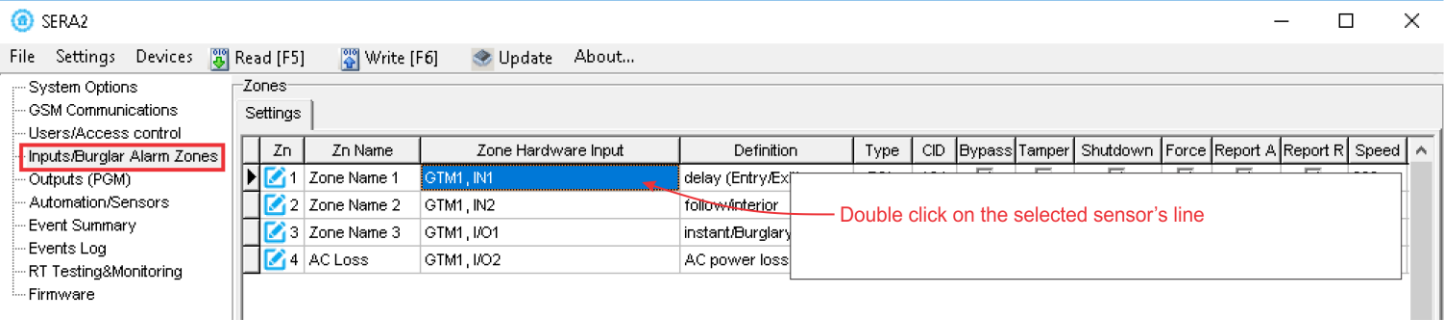


Figure 55 Burglar Alarm Zones window



Refer to: Zones programming

## 4.5.7 Fire alarm and Smoke sensors

### 4.5.7.1 Guidelines for Locating Smoke Detectors and CO Detectors



The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke and carbon monoxide alarms.

**Smoke Detectors.** Research indicates that all hostile fires in homes generate smoke to a greater or lesser extent. Detectable quantities of smoke precede detectable levels of heat in most cases. Smoke alarms should be installed outside of each sleeping area and on each level of the home.

Additional smoke alarms beyond those required for minimum protection be installed. Additional areas that should be protected include: the basement; bedrooms, especially where smokers sleep; dining rooms; furnace and utility rooms; and any hallways not protected by the required units.

On smooth ceilings, detectors may be spaced 9.1m (30 feet) apart as a guide. Other spacing may be required depending on ceiling height, air movement, the presence of joists, uninsulated ceilings, etc.

- Do not locate smoke detectors at the top of peaked or gabled ceilings; dead air space in these locations may prevent smoke detection.
- Avoid areas with turbulent air flow, such as near doors, fans or windows. Rapid air movement around the detector may prevent smoke from entering the unit.
- Do not locate detectors in areas of high humidity.
- Do not locate detectors in areas where the temperature rises above 38°C (100°F) or falls below 5°C (41°F).

Where required by applicable laws, codes, or standards for a specific type of occupancy, approved single- and multiple-station smoke alarms shall be installed as follows:

- (1) In all sleeping rooms and guest rooms.
- (2) Outside of each separate dwelling unit sleeping area, within 6.4 m (21 ft) of any door to a sleeping room, the distance measured along a path of travel.
- (3) On every level of a dwelling unit, including basements.
- (4) On every level of a residential board and care occupancy (small facility), including basements and excluding crawl spaces and unfinished attics.
- (5) In the living area(s) of a guest suite.
- (6) In the living area(s) of a residential board and care occupancy (small facility).

**CO Detectors.** Carbon monoxide gas moves freely in the air. The human body is most vulnerable to the effects of CO gas during sleeping hours. For maximum protection, a CO alarm should be located outside primary sleeping areas or on each level of your home.

The electronic sensor detects carbon monoxide, measures the concentration and sounds a loud alarm before a potentially harmful level is reached.

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10°C or exceed 40 °C.
- Near paint thinner fumes.
- Within 5 feet (1.5 meters) of open flame appliances such as furnaces, stoves and fireplaces.
- In exhaust streams from gas engines, vents, flues or chimneys.
- In close proximity to an automobile exhaust pipe; this will damage the detector.

**Progate.** Begin the installation by mounting additional modules in the cabinet using the stand-offs provided, then mount the cabinet in a dry, protected area with access to unswitched AC power. Install hardware in the sequence indicated in the following pages. Do NOT apply power until installation is complete.

### 4.5.7.2 [4-Wire] Smoke detector Wiring



Connect the 4-wire smoke detectors and a relay as shown in the figure below.

#### If you want to edit existing configuration,

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

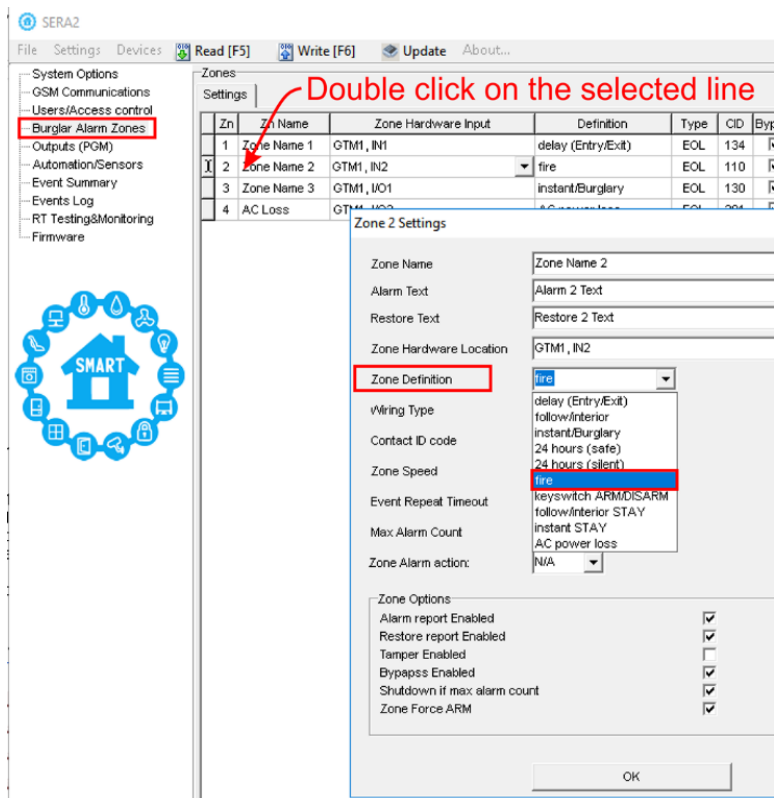
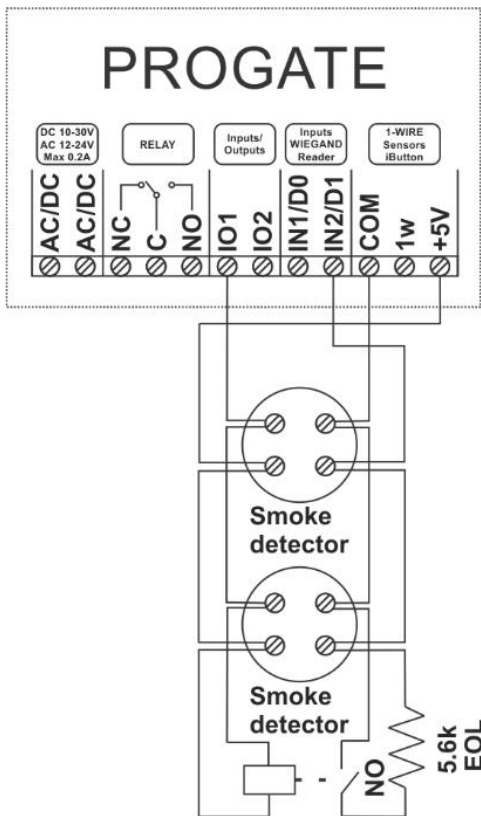


Figure 56 Burglar Alarm Zones window

Figure 57 4-Wire Smoke Detector Installation

Install the 4-wire smoke detectors with 18 gauge wire. If power is interrupted, the relay causes the control panel to transmit the Fire Loop Trouble report. To reset (unlatch), connect the smoke detector's negative (-) to a PGM.

The parameters of the zone should be defined as a "Fire Zone". If a line short occurs or the smoke detector activates, whether the system is armed or disarmed, the control panel will generate an alarm. If the line is open, the "Zone Fault" report code is sent to the monitoring station or to the user, if programmed.

1. Connect the [4-wire] smoke detector.
2. Connect the power supply.
3. Install SERA2 software.
4. Go to "Burglar Alarm Zones" window. Double click on required input. Set "Zone definition" to "Fire".
5. Write configuration by pressing "Write" icon.



Refer to: Zones programming

## 5 Programming

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

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

### 5.1 SERA2 Uploading/Downloading Software



We recommend programming the module Progate with SERA2 software

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

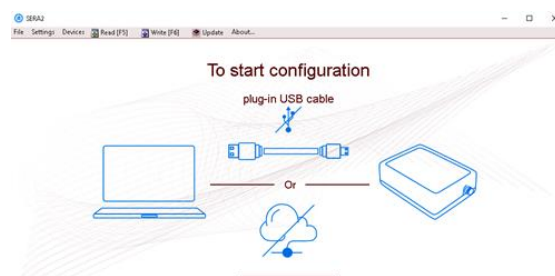


Figure 58How to start configuration with Sera2 software

Start the software SERA2. Go to „Start“> „All programs“> „SERA2“> „SERA2 “ or go to installation directory and click „SERA2.exe“.

**Connection of the module to your PC**

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

**Work with the software SERA2**

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

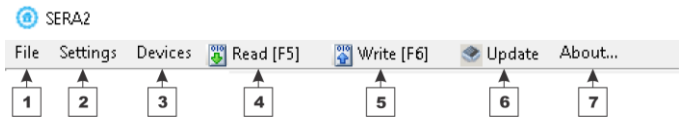


Figure 59 Command line

**!** Each time after configuring the module press Write **W** 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

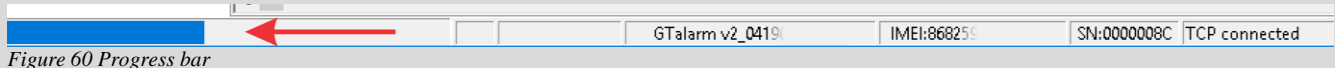


Figure 60 Progress bar

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

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

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

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

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

- !** Press “Read” icon first to read the configuration from the module, the press “File>Save us” and save the configuration.
- !** Save the Events log file and send these files with the question to the seller.

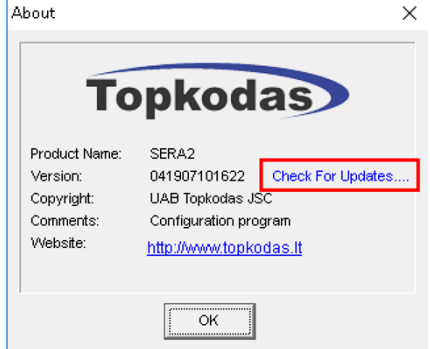


Figure 61 Go to „Update“ in the command line

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

**!** An unlimited number of modules can be configured remotely on the same computer at the same time. The configuration reading and writing speed does not decrease because the processes are running in parallel. Many Sera2 programs could be opened and used at the same time.

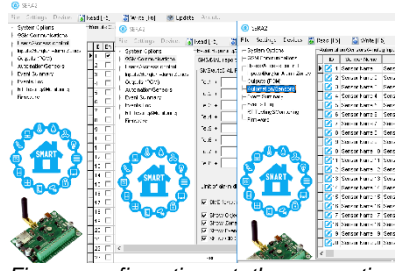
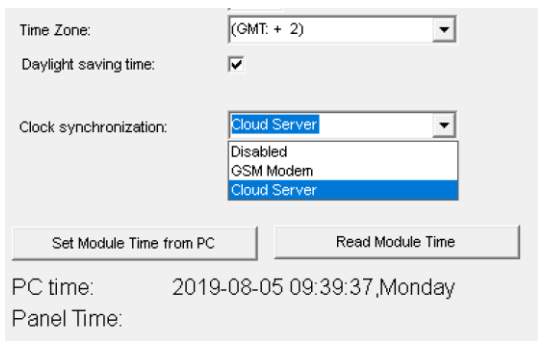


Figure configuration at the same time  
62 Unlimited number of modules

**5.2 General system options programming**





The system comes equipped with internal real-time clock (RTC) with battery that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly. SERA2 software provides the ability to select the Time Zone and The user may also choose Set module time from PC, which instantly provides the exact PC time. When the system is connected to the monitoring station via IP connection the date and time will be automatically synchronized with the monitoring station. It is possible to select automatically time synchronization with: GSM Modem, Cloud Server or disable it.

Figure 63 Clock, time Zone and clock synchronization.  
Sera2> System Options> General System Options

**!** If the module has been connected first time to the power supply, or power supply has been disconnected for a long time, the time of the module should be set again.

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

**System Options > General system Options**

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

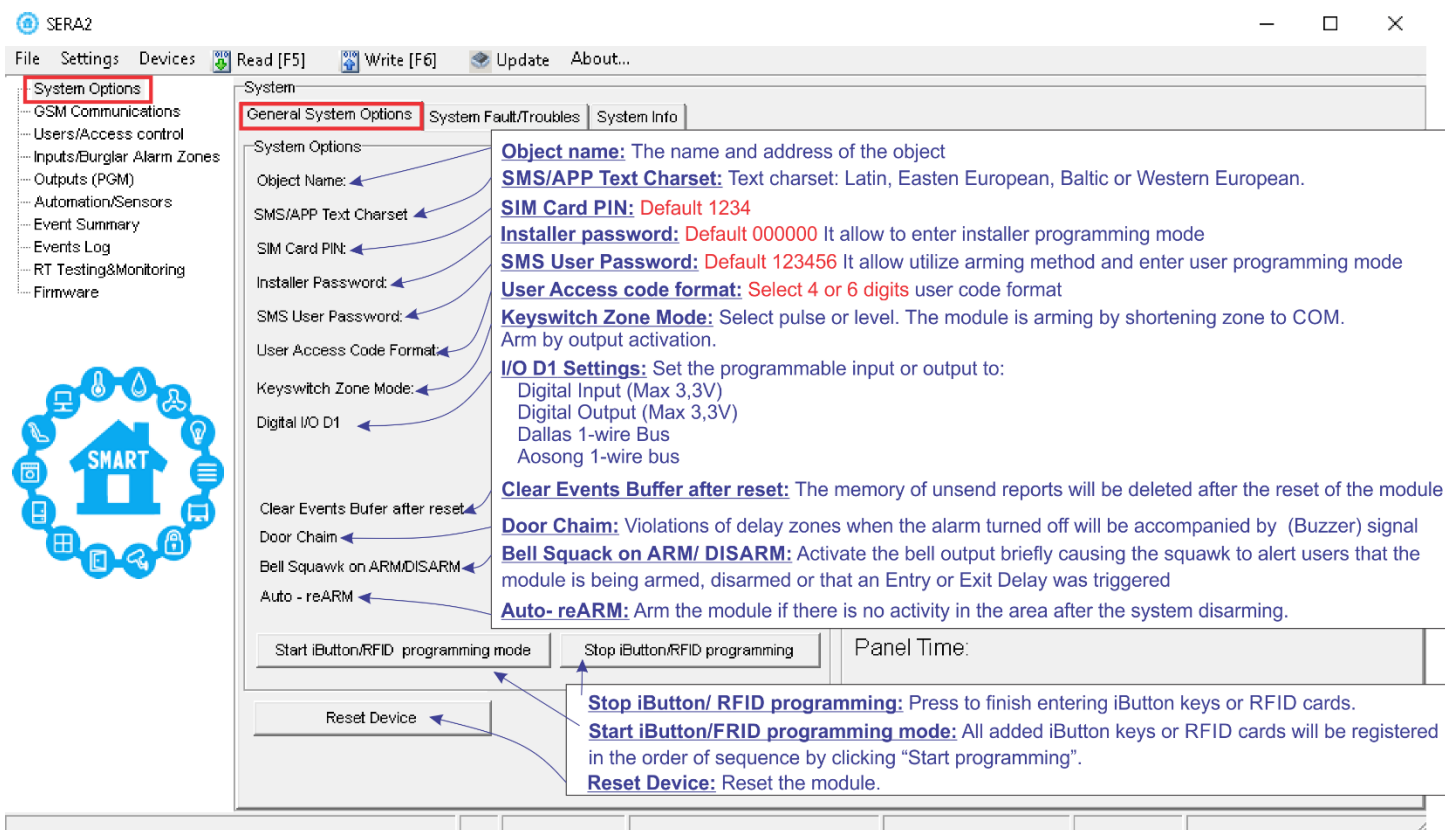


Figure 64 System Options> General System Options

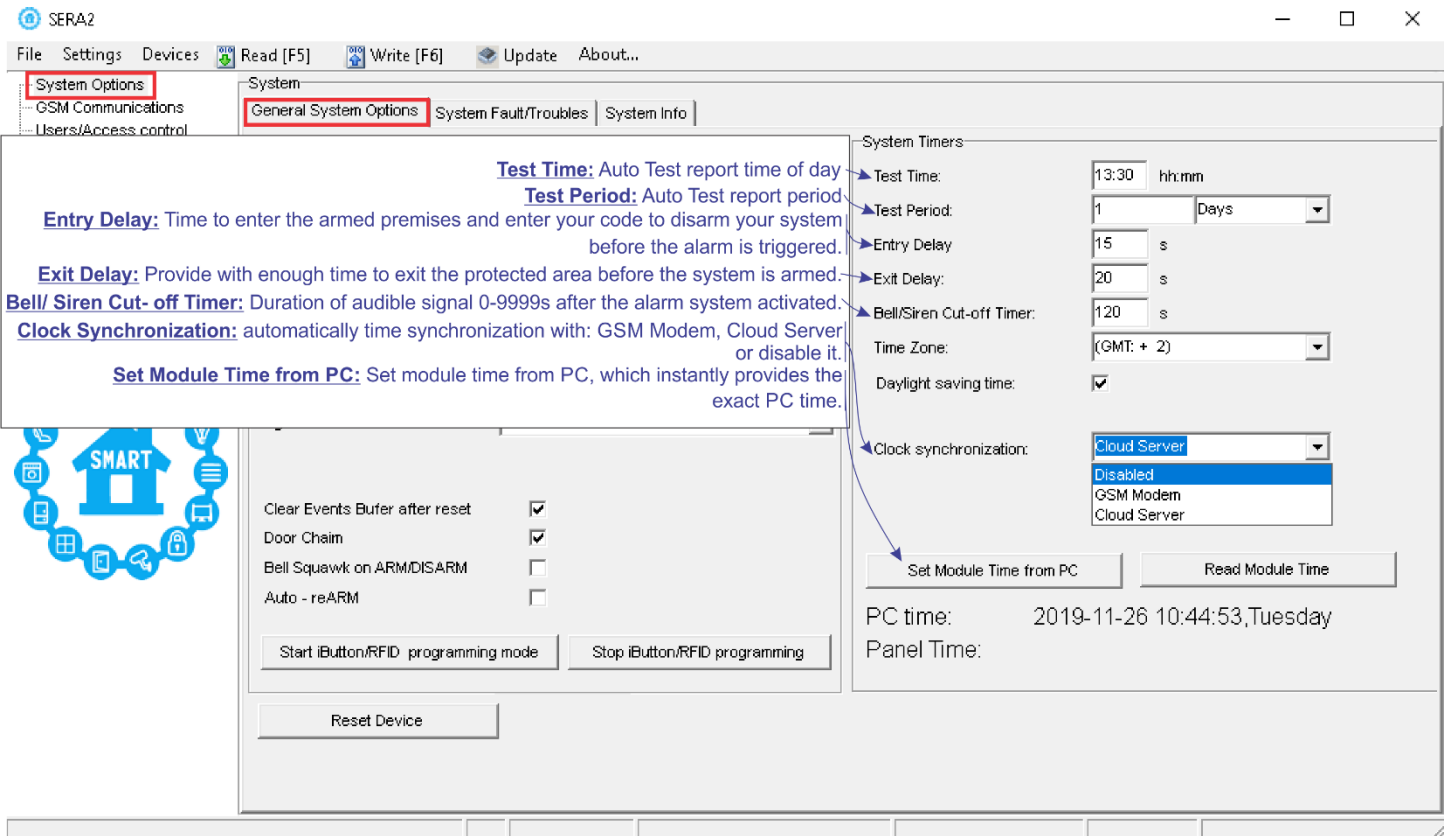


Figure 65 System Options > General system options window

### 5.3 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.

**System Options** > **System Fault/Troubles**

ID	Trouble	Enable	Restrict ARM
1	Battery trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Clock trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	BUS trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Tamper trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Fire loop trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	SIM card trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	Zone antimasking trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	GSM network trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Fault/Troubles Global Settings**

Trouble Event Limit:   
Reset Trouble Event Counter After:  min

**System Voltage (Low Battery) settings**

Low System Voltage Alarm:  V  
System Voltage Restore:  V  
Event Delay:  s

**Global Tamper Recognition:**

Tamper Disable  
 Trouble when disarmed / alarm as per zone when armed  
 Trouble always  
 Audible alarm when disarm / alarm as per zone when armed

**Legend:**

- GSM network trouble:** SIM card is not registered with the GSM network provider
- Zone antimasking trouble:** Do not available in this module
- SIM card trouble:** Not available or impossible to read SIM card.
- Fire loop trouble:** The trouble is occurring with your smoke detectors.
- Tamper trouble:** The zone(s) that was tampered
- BUS trouble:** Do not available in this module.
- Clock trouble:** The time and date has not been set.
- Battery trouble:** Power supply or backup battery voltage is low, needs to be recharged, or replaced
- Enable:** The system will detect a marked trouble
- Restrict Arm:** In case of such trouble, the arming activation will be restricted.
- Trouble Event Limit:** Allowable number of the same trouble event
- Low System Voltage Alarm:** The system is running on the backup battery and voltage is dropped below allowed value.
- System Voltage Restore:** The voltage has been restored and has been reached defined value.
- Event Delay:** System low voltage trouble event report delay.
- 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.
- Trouble always:** Generates Trouble Only (when armed or disarmed).
- 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.
- Tamper Disable:** The module will not generate an alarm or trouble.

Figure 66 System Options > System Fault/ Troubles window

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

## 5.4 Zones programming



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

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

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

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

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

- i** The difference between stay and sleep zone types: "stay" zone type has delay zone timeout, in "sleep" zone type delay zone becomes instant
- i** The system will NOT activate siren and keypad buzzer only when Instant, Silent zone types is violated.
- i** Any Delay type zone will operate as Instant type zone when the system is armed in the Stay mode. When the system is fully armed, the Delay type zone will operate normally.
- i** If the zone is not used, it must be disabled.

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren/bell and the keypad buzzer and send the SMS text message to the listed

user phone number. The system will cause tamper alarm under the following conditions: If the enclosure of a detection device, siren/bell, metal cabinet or keypad is opened, the physical tamper switch will be triggered. If needed to get tamper alarms, the field near "Tamper Enabled", should be marked. In that case, all tamper and tamper alarm notification by SMS text message is enabled.

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

1. Install SERA2 software.
2. Connect the module to the computer via mini USB cable. Device> Progate
3. Go to Zones window in the SERA2 software
4. Set the required parameters
5. Write configuration by pressing „Write“ icon

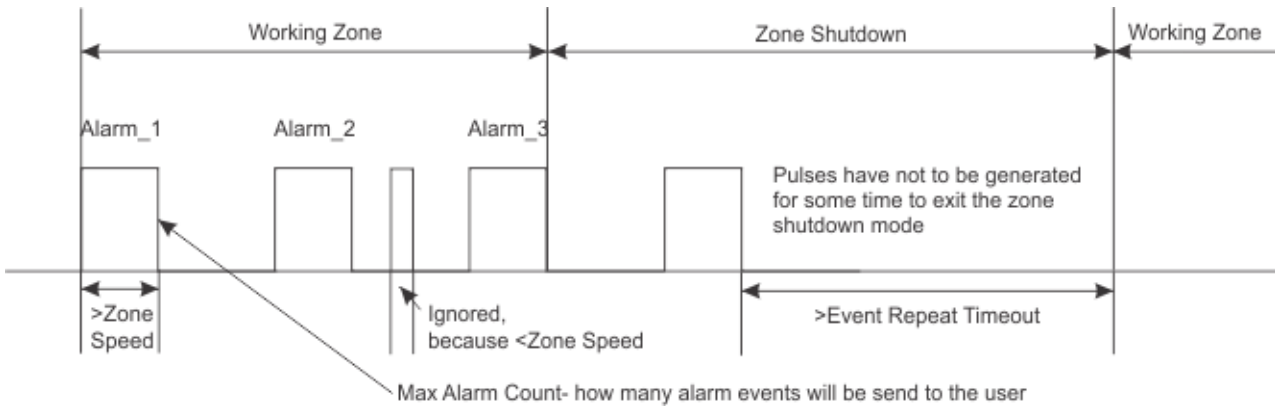


Figure 67 The explanation of Zone Speed, Max Alarm Count, Event Repeat Timeout

**Zone 1 Settings**

Zn	Zn Name	Zone Hardw
1	Zone Name 1	GTalarm v2, IN1
2	Zone Name 2	GTalarm v2, IN2
3	Zone Name 3	GTalarm v2, IN3
4	AC Loss	GTalarm v2, IN4
5	Zone Name 5	GTalarm v2, IO1
6	Zone Name 6	GTalarm v2, IO2

**Zone 1 Settings**

- Zone Name
- Alarm Text
- Restore Text
- Zone Hardware Location
- Zone Definition
- Wiring Type
- Contact ID code
- Zone Speed
- Event Repeat Timeout
- Max Alarm Count
- Zone Alarm action

**Zone Options**

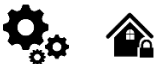
- Alarm report Enabled
- Restore report Enabled
- Tamper Enabled
- Bypass Enabled
- Shutdown if max alarm count
- Zone Force ARM

**Explanations:**

- Alarm Text:** It is possible to customize alarm text
- Restore Text:** It is possible to customize restore text
- Zone Hardware Location:** Select the zone hardware input
- Wiring Type:**
  - EOL End of line resistor. Input type with resistor.
  - NC The alarm will be send when the circuit between input and ground (-V) will be broken.
  - NO The alarm will be send when the input will be connected with ground (-V)
- Contact ID code:** The module will automatically generate the reporting event when transmitting to the CMS.
- Zone 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:** Insensitive time to recurrent zone events
- Max Alarm Count:** 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.
- Zone Alarm action:** Determines which output will be activated
- Alarm report enabled:** The system will report alarm event and log it to the event buffer
- Restore report enabled:** The system will report restore event and log it to the event buffer
- Tamper Enabled:** The system will detect a tamper condition with one or more sensors on the system
- Bypass Enabled:** The system will allow zones to be Manually Bypassed.
- Shutdown if max alarm count:** 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:** Only force zones can be bypassed when the module is Force armed. Fire Zones cannot be Force Zones.

Figure 68 Inputs/ Burglar Alarm Zones window

## 5.5 Outputs. Bell & PGM programming



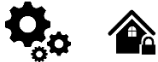
ID	Output Location in Hardware	Output Label	Out definition	Mode	Out Timer	Invert	Pulsating	Pulse ON Time	Pulse OFF Time
1	GTM1, RELAY	OUT1	Disable	Steady	10s			100ms	100ms
2	GTM1, IO1(1A)	OUT2	Bell						
3	GTM1, IO2(1A)	OUT3	Buzzer						
4	GTM1, D1 10mA, Max Voltage 3.3V!!!	OUT4	Flash						

**Mode:** Steady: Steady ON/OFF mode  
**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.  
**Pulsating ON Time:** Pulsating mode pulse ON duration.  
**Pulsating OFF Time:** Pulsating mode pulse OFF duration.

**Access Gained:** If user has right to ARM/DISARM system, it always has access to this output. If ARM/DISARM flag is not set user can access this output only if system is Disarmed (Open).  
**RH Sensor Trouble:** Output for RH Sensor trouble operation. In this mode output can automatically reset Humidity sensor if trouble occurs.  
**Fire Sensor:** 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.  
**Lost Primary Channel:** Output where a continuous signal is generated when communication with primary channel was lost.  
**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.  
**ARM/ DISARM:** Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.  
**Battery OK:** Output for connection of indicator about control panel supply from battery.  
**AC OK:** Output for connection of indicator about control panel supply from alternating current.  
**Automation & Access 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  
**Ready:** Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.  
**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.  
**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.  
**Buzzer:** Output for buzzer connection. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.  
**Bell:** Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.  
**Disable:** Output disabled

Figure 69 Outputs (PGM) window

## 5.6 Users & Access Control programming details.



Users/ Access Control > Remote Control Users Table

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

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



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



**Expiration Date:** Temporary access expiration date and time  
**Start Date:** Temporary access start date and time  
**Date EN:** Temporary access enable  
**ARM/ DISARM:** If this check box is checked, a user will be able to ARM/DISARM the module by dialing.  
**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  
**Key Code:** Key button code might be entered manually. 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  
**iButton Code:** 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. iButtons must be from 01 family  
**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.  
**Type:** Reserved for future uses  
**User Name:** The name of users who will be able to control the module should be entered in this column.  
**En:** Reserved for future uses

Figure 70 Users/ Access control window

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

Figure 71 Users/ Access Control > Users, Users Access Control> Access Schedules and Users/ Access Control> Holidays window

Go to Sera2> System Options> General system Options  
 Set 1W (1-Wire Bus) to Dallas 1-Wire Bus  
 Set time zone  
 Set clock synchronization  
 Press "Write"

Go to Sera2> System Options> General system Options.  
 Press "Start iButton/ RFID/ Phone programming mode."  
 Go to Sera2> Users/ Access control window.  
 Touch RFID keycards, iButton keys to the reader.  
 Call to the module from your mobile  
 RFID keycard, iButtons code, phone number will appear in the list.  
 Go to System Options> General system Options and  
 Press "Stop programming" or wait until it will stop automatically.  
 Edit setting in the Users/ Access control window.  
 Press "Write"

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

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

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

Suppose you must create a Cleaning Crew schedule. The schedules are to be set up as follows: Monday-Friday 5 p.m.-1 a.m., Saturday and Sunday 8 a.m.-1 p.m., no holidays. This becomes three separate schedules, as follows.

2 Monday-Friday, 5 p.m.-11:59 p.m. (Remember, the time range cannot cross midnight, so 11:59 p.m. is the limit.)

3 Tuesday-Saturday, 12:00 a.m.-1:00 a.m.

4 Saturday-Sunday, 8:00 a.m.-1:00 p.m.

Note: Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, schedules that contain that specific Holiday type will work. The Holiday allows users to further customize how the panel works. For example, the user can block access to a building on that day, or grant special access during that day. Each Holiday added is considered a full day, extending from midnight to midnight.

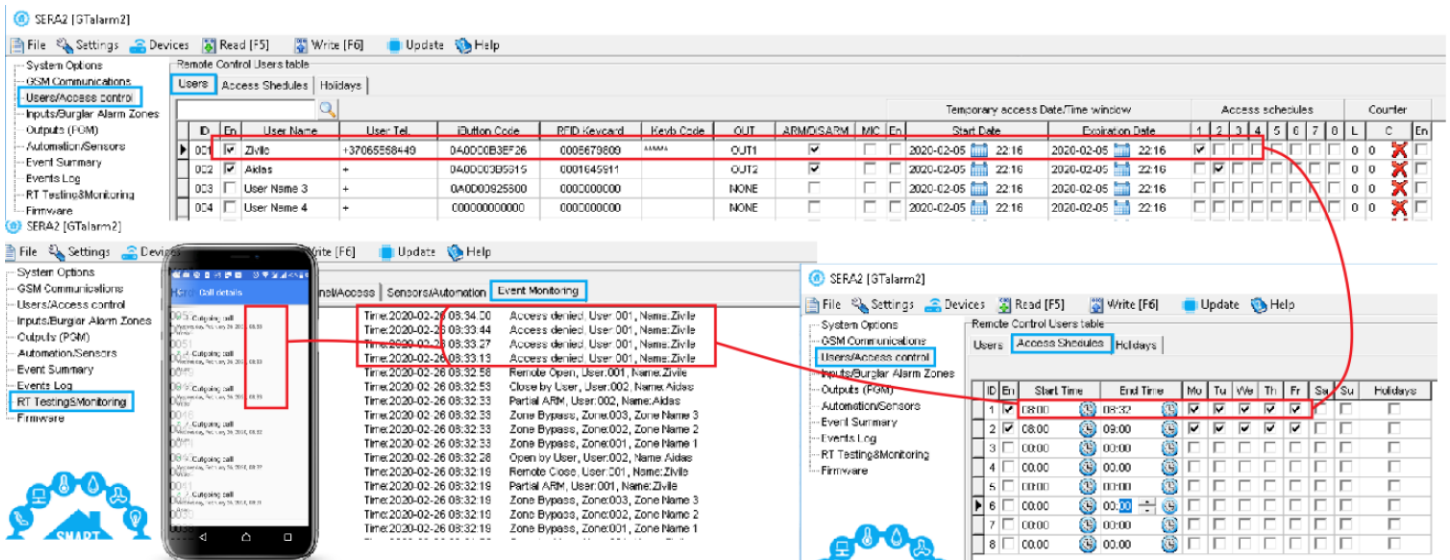


Figure 72 The example of schedule

## 5.7 DISARM /ARM/SLEEP/STAY the security system



System Options > System Fault/ Troubles

In this window System trouble settings could be configured

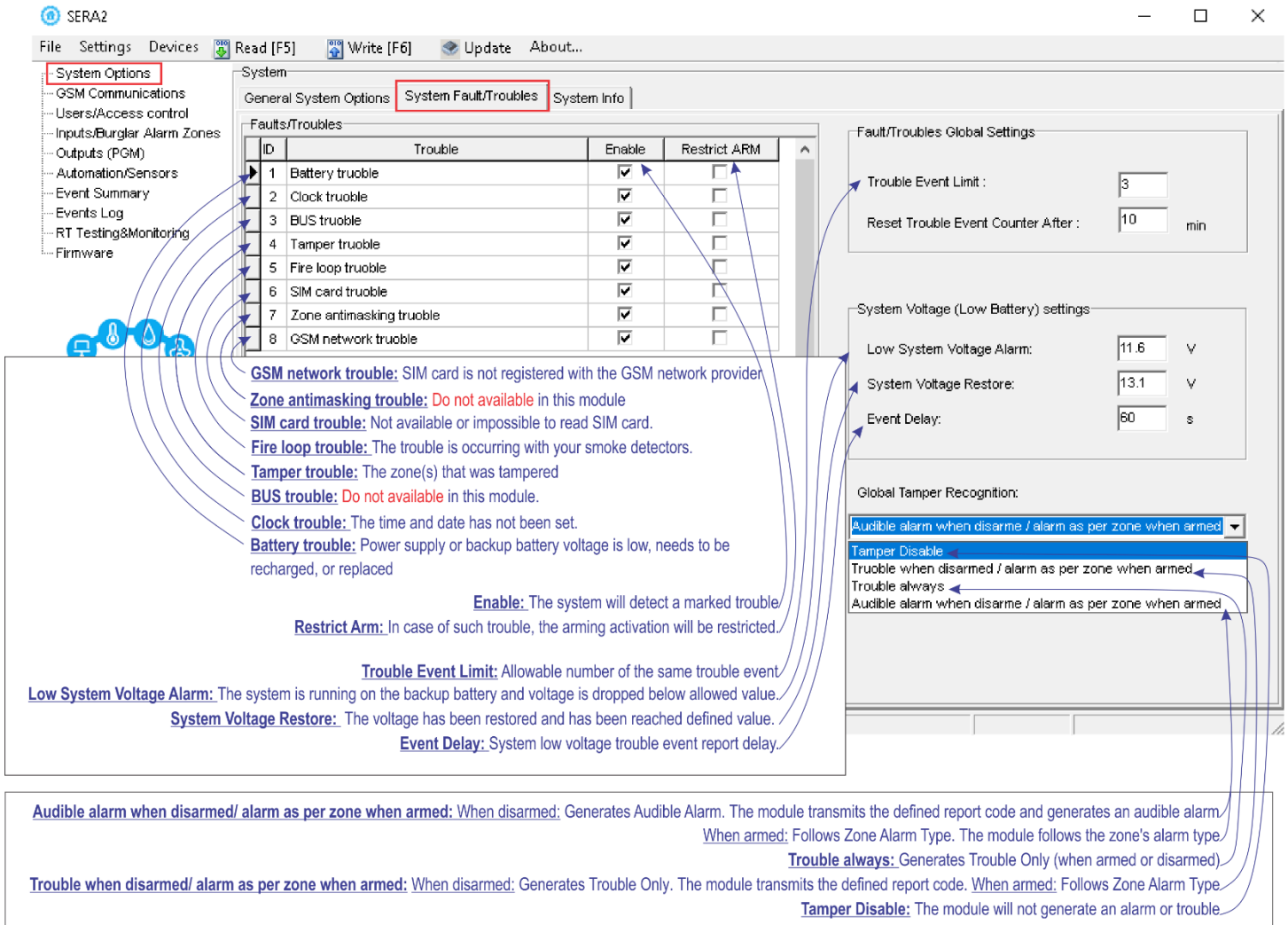


Figure 73 System Options> System Fault/ Troubles

The system can be armed in one of four modes DISARM, ARM, SLEEP, STAY. By default, it is allowed to arm the system while the following system faults are present:

- Low battery.
- Battery dead or missing.
- Battery failed.
- Date/time not set.
- GSM connection failed.
- GSM/ GPRS antenna failed.

If needed, restrict arm, when such trouble occur, check near such trouble in the System options> System Fault/Troubles window. And in case of such trouble, the arming activation will be restricted.

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

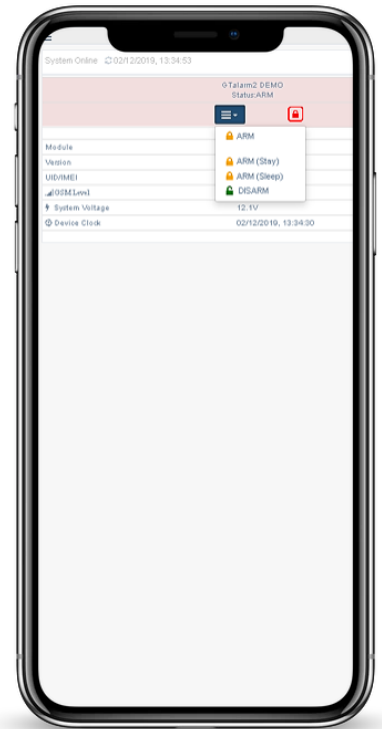


Figure 74 Arm/ Disarm via mobile app



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

**Remote Control Users table**

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+	000000000000	0000000000	*****	NONE	<input checked="" type="checkbox"/>		2019-09-17 15:42:59	2019-09-17 15:42:59
2	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
3	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
4	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
5	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
6	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
7	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	
8	<input type="checkbox"/>	User	+	+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-09-17 15:42:59	

**Temporary access Date/Time window**

September 2019

Mon Tue Wed Thu Fri Sat Sun

26 27 28 29 30 31 1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

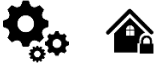
16 17 18 19 20 21 22

23 24 25 26 27 28 29

**Expiration Date:** Temporary access expiration date and time  
**Start Date:** Temporary access start date and time  
**Date EN:** Temporary access enable  
**ARM/ DISARM:** If this check box is checked, a user will be able to ARM/DISARM the module by dialing.  
**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  
**Keyb Code:** Key button code might be entered manually. 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  
**iButton Code:** 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. iButtons must be from 01 family  
**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.  
**Type:** Reserved for future uses  
**User Name:** The name of users who will be able to control the module should be entered in this column.  
**En:** Reserved for future uses

Figure 75 Users/ Access control window

## 5.8 Reporting SMS&Dial in Case of Alarm Events



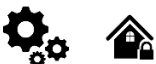
The system supports up to 8 user phone numbers identified as User 1 through 8 for monitoring purpose: receive alarm phone calls via GSM connection and SMS text messages from the system. When the system is armed or disarmed by free of charge phone call or SMS text message, the system sends a confirmation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

By default, once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number. To permit/deny system arming/disarming by phone call and SMS text message that contain a valid SMS password, configuration by SMS text message that contain a valid SMS password from any phone number, please refer to the following configuration methods.

**!** The system will NOT transmit any data to monitoring station while configuring the system remotely via GPRS network. However, during the remote connection session, the data messages are queued up and transmitted to the monitoring station after the configuration session is over. SERA2 software provides remote system configuration ability via Internet using TCP/IP server on SERA2 software. The connection can be established on the system via GPRS network. After the remote system configuration is complete the session will automatically expire in 20 minutes. Alternatively, the connection with the server can be terminated at any time by sending an SMS text message.

**!** NEVER add a phone number of the device's SIM card as a user phone number!

### 5.8.1 Reporting to the user's mobile phone



GSM Communications > SMS DIAL Reporting

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

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

1. The system activates the siren/bell. The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.
2. The system attempts to send an SMS text message (if programmed), containing the violated name. The system will send SMS text messages regarding each violated zone separately.
  - a) If the user phone number is unavailable, it will attempt to send the SMS text message to the next listed user phone number, assigned to the same zone as the previous one. The user phone number may be unavailable due to the following reasons: mobile phone was switched off or was out of GSM signal coverage.

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

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

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



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

ID	Events	SMS Notifications to USER								Auto DIAL to USER							
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
2	System Open/Close (CID 400 group)	<input checked="" type="checkbox"/>															
3	System Troubles(CID 300 group)	<input checked="" type="checkbox"/>															
4	Sensor1-Sensor32 Alarm/Restore	<input checked="" type="checkbox"/>															
5	Test Events (CID 600 group)	<input checked="" type="checkbox"/>															
6	Other Events	<input checked="" type="checkbox"/>															
7	Input/Zone1 Alarm/Restore	<input checked="" type="checkbox"/>															
8	Input/Zone2 Alarm/Restore	<input checked="" type="checkbox"/>								<input checked="" type="checkbox"/>							
9	Input/Zone3 Alarm/Restore	<input checked="" type="checkbox"/>															
10	Input/Zone4 Alarm/Restore	<input checked="" type="checkbox"/>															

Figure 76 GSM Communication> SMS/ DIAL reporting

### 5.8.2 Custom SMS Text



GSM Communication > Custom SMS Text

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

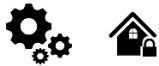
ID	Text Description	SMS Text
1	Alarm	Alarm
2	Restore	Restore
3	Open	Open
4	Close	Close

Figure 77 GSM Communications> Custom SMS Text

### 5.9 Reporting to the Central Monitoring Station



## 5.9.1 GPRS/ IP/ TCP/ UDP details programming



GSM Communication > GPRS/ IP/ TCP/ UDP

The GPRS/ IP/ TCP/ UDP window let you set GPRS, IP, TCP and UDP parameters

SERA2

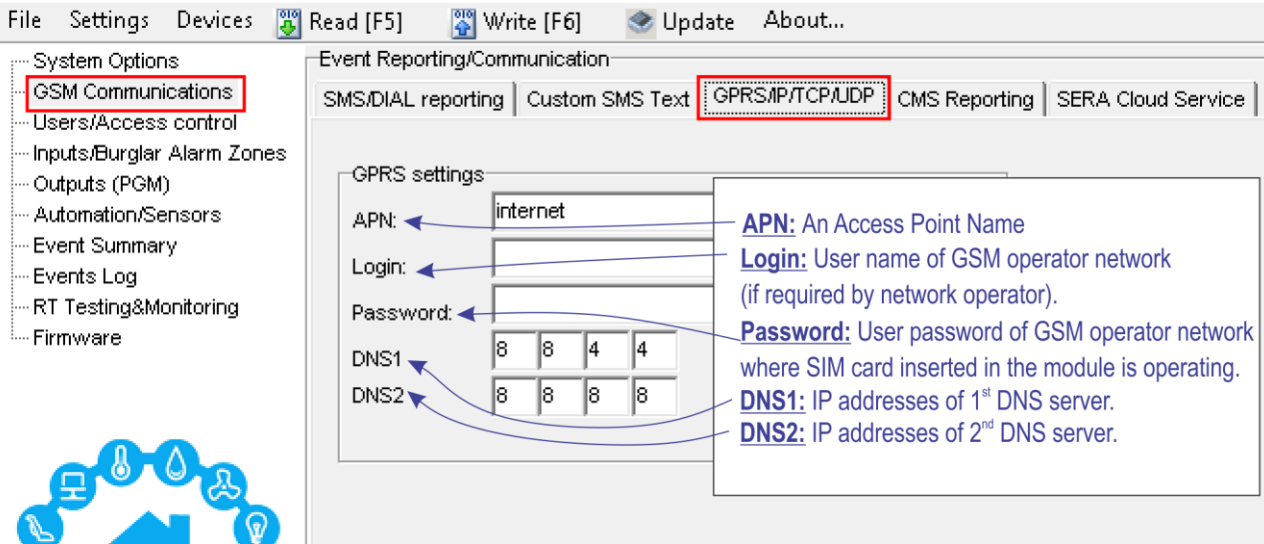


Figure 78 GSM Communications > GPRS/IP/TCP/UDP

## 5.9.2 Central Monitoring Station details programming



GSM Communication > CMS Reporting

The CMS Reporting window let you set reporting to central monitoring station parameters

The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the central monitoring station when the CMS (Central Monitoring Station) mode is enabled, set to GPRS.

When using the CMS mode, the data messages transmitted to the monitoring station will gain the highest priority for the delivery, therefore based on the communication method a constant and stable connection with the monitoring station must be ensured. In case of connection failure, the system will attempt to restore the connection and if the monitoring is unavailable for a lengthy period of time, the system switch to backup CMS.

**!** The module will NOT send any data to the monitoring station while remote connection, remote firmware update is in progress. However, during the remote connection session process, the data messages will be queued up and transmitted to the monitoring station after the remote connection session is over, while during the remote firmware update process NO data will be queued up and all data messages will be lost.

**!** Phone calls via GSM network to the listed user phone number in case of alarm are disabled by force when MS mode is enabled.

### Data Messages – Events

The system supports the following communication methods and protocols:

- GPRS network –SIA IP protocol (ANSI/SIA DC-09-2012; configurable as encrypted and non-encrypted).
- SMS –SMS to User text format.

Initially, the system communicates via primary connection with the monitoring station. By default, if the initial attempt to transmit data is unsuccessful, the system will make additional attempts until the data is successfully delivered. If all attempts are unsuccessful, the system will follow this pattern:

1. The system switches to the backup connection that follows in the sequence (presumably - Backup 1).
2. The system then attempts to transmit data by the backup connection.
3. If the initial attempt is unsuccessful, the system will make additional attempts until the data is successfully delivered.
4. The system ends up with all unsuccessful attempts.

If all attempts by all set connections are unsuccessful, the system will wait until the delay time (by default – 1200 seconds) expires and will attempt to transmit data to the monitoring station again starting with the primary connection.

Figure 79 GSM Communication > CMS Reporting window

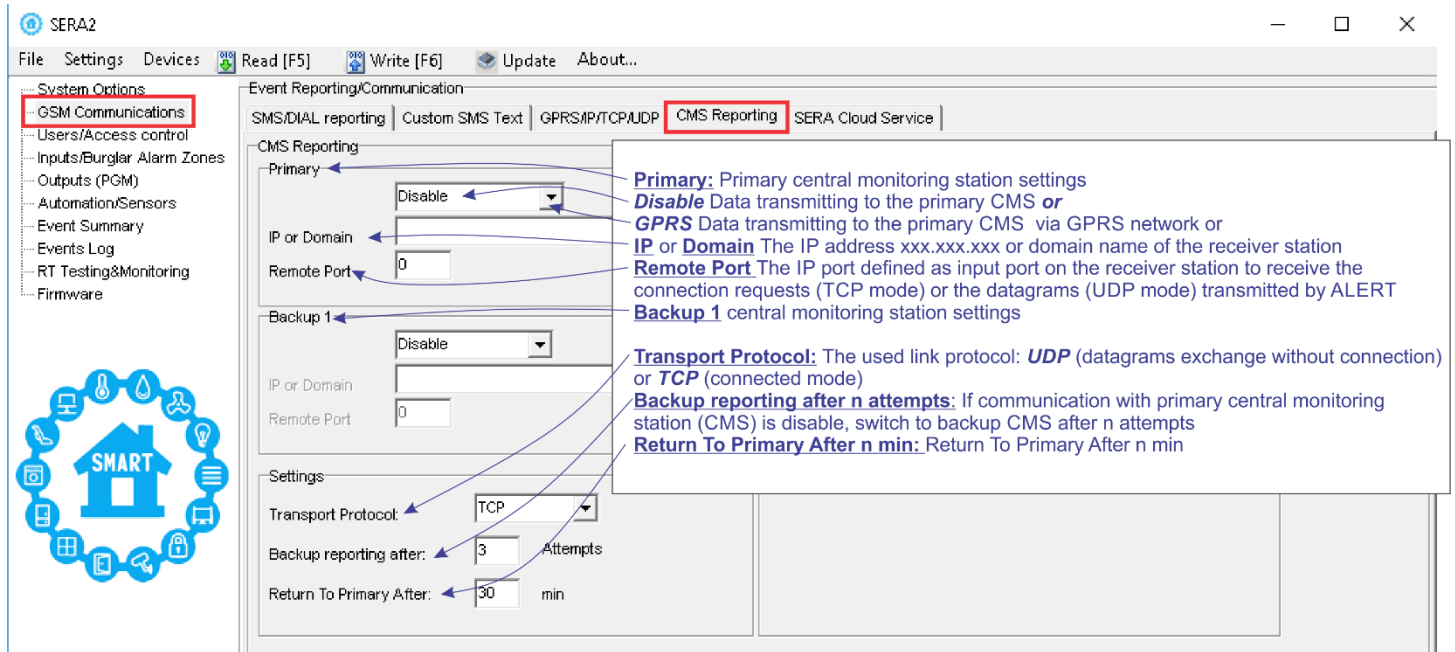


Figure 80 GSM Communications> CMS Reporting window

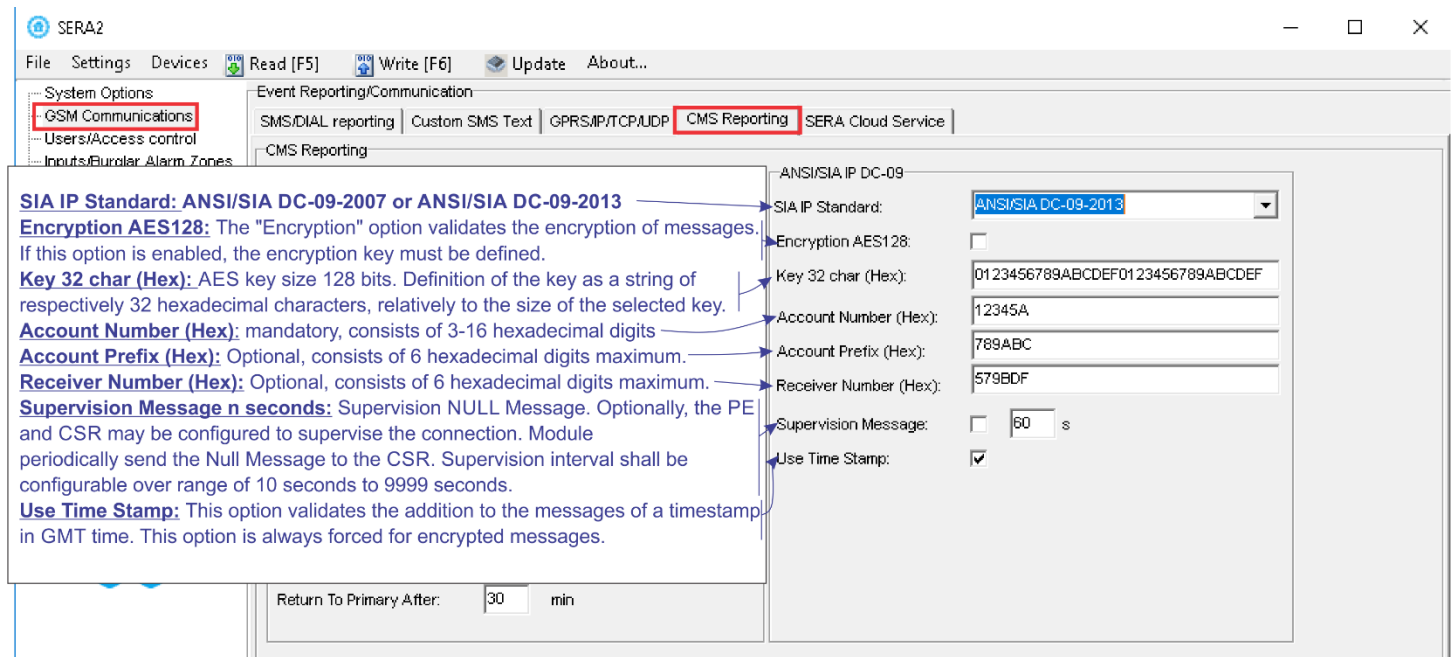


Figure 81 GSM Communication> CMS Reporting window

## 5.10 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.

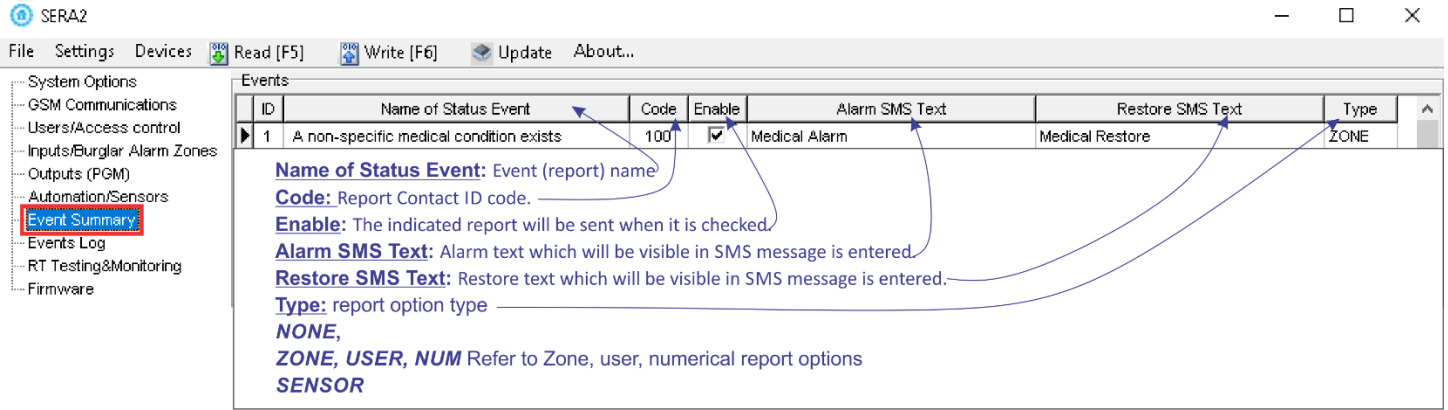
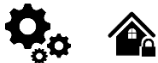


Figure 82 Event Summary window

## 1.1. RT Testing & Monitoring. Hardware.



RT Testing & Monitoring > Hardware

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

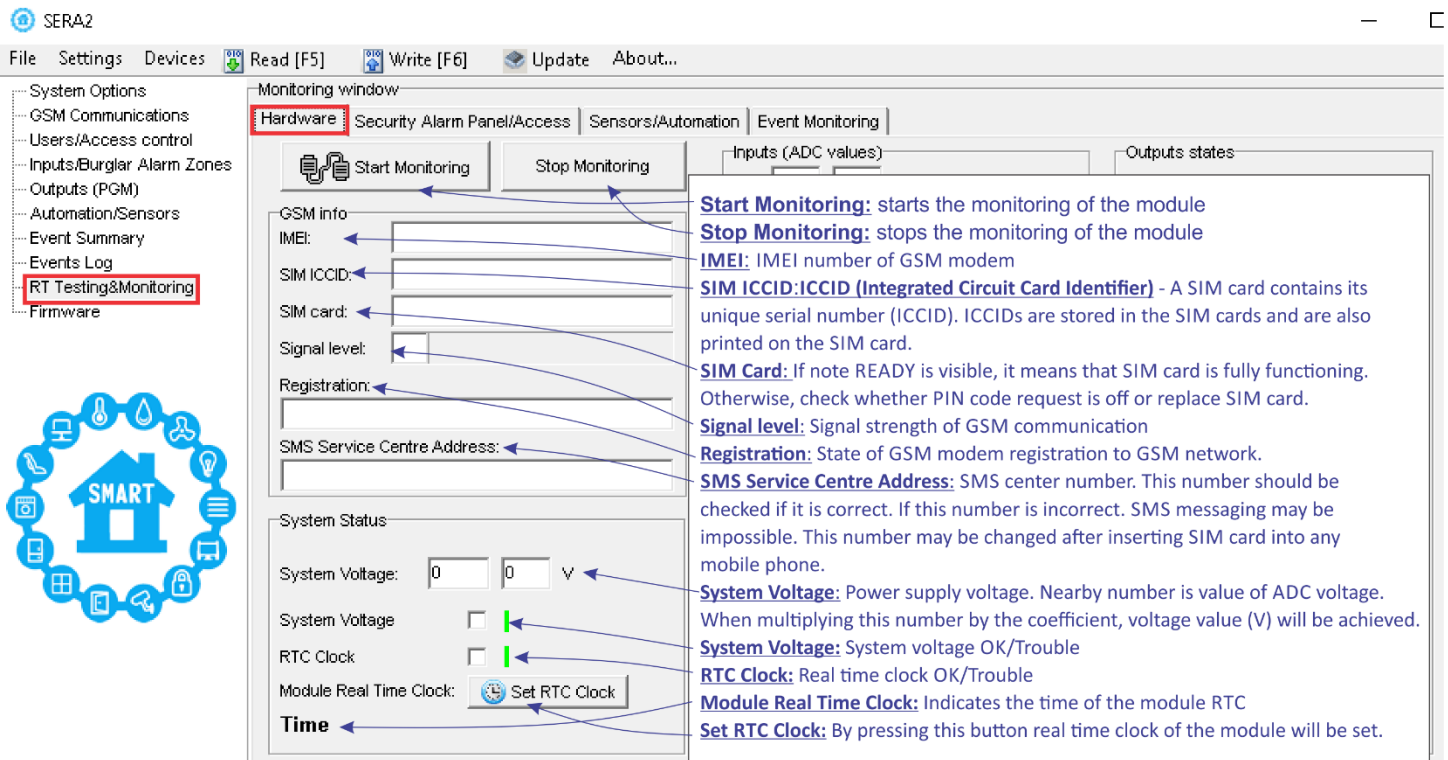


Figure 83 RT Testing Monitoring > Hardware window



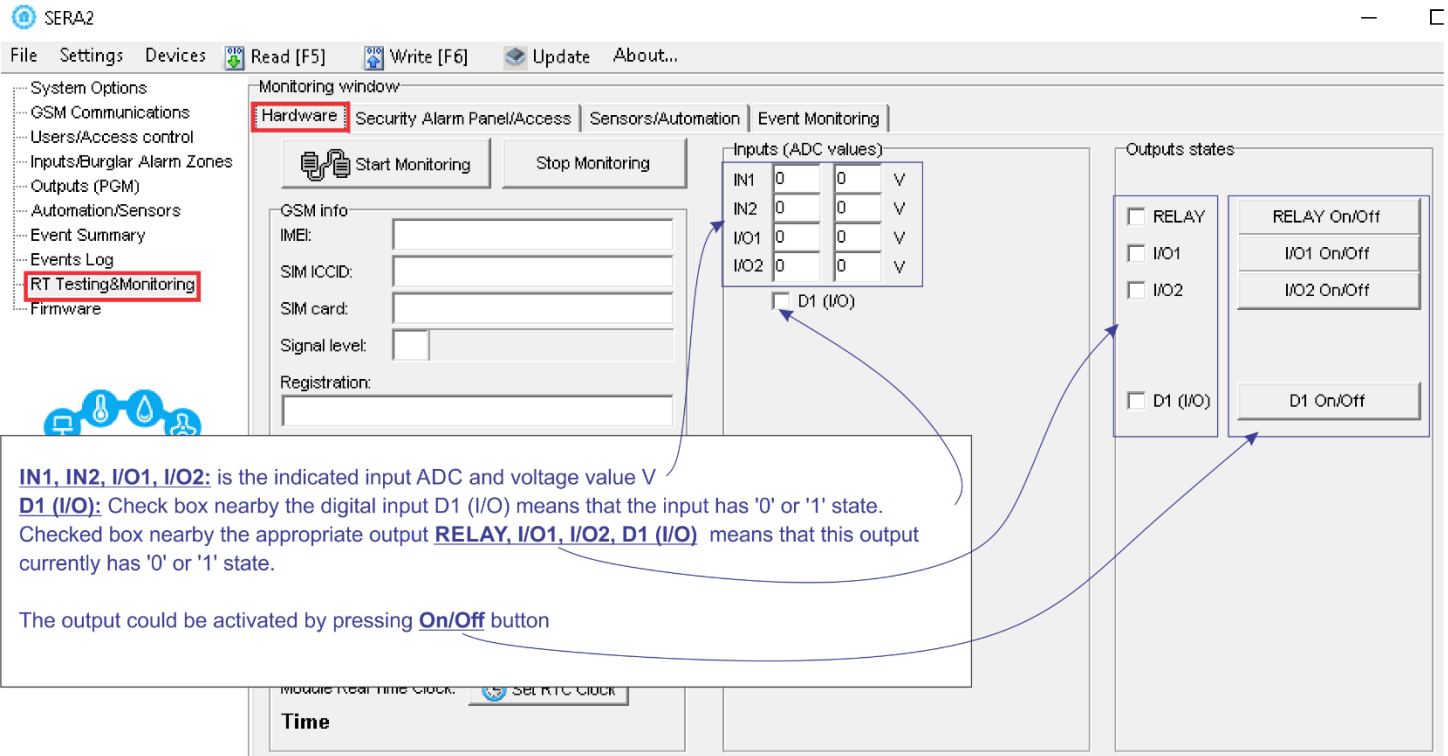


Figure 84 RT Testing Monitoring > Hardware window

## 5.11 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.

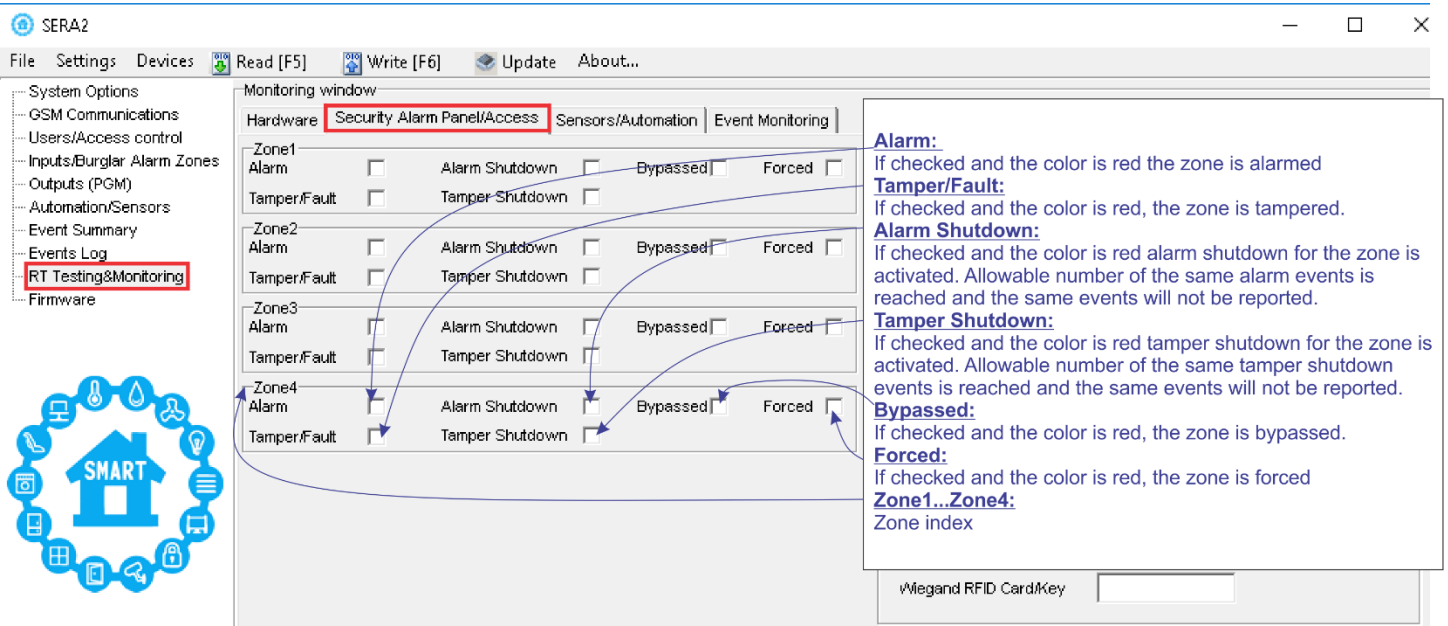


Figure 85 RT Testing Monitoring > Security Panel/ Access window

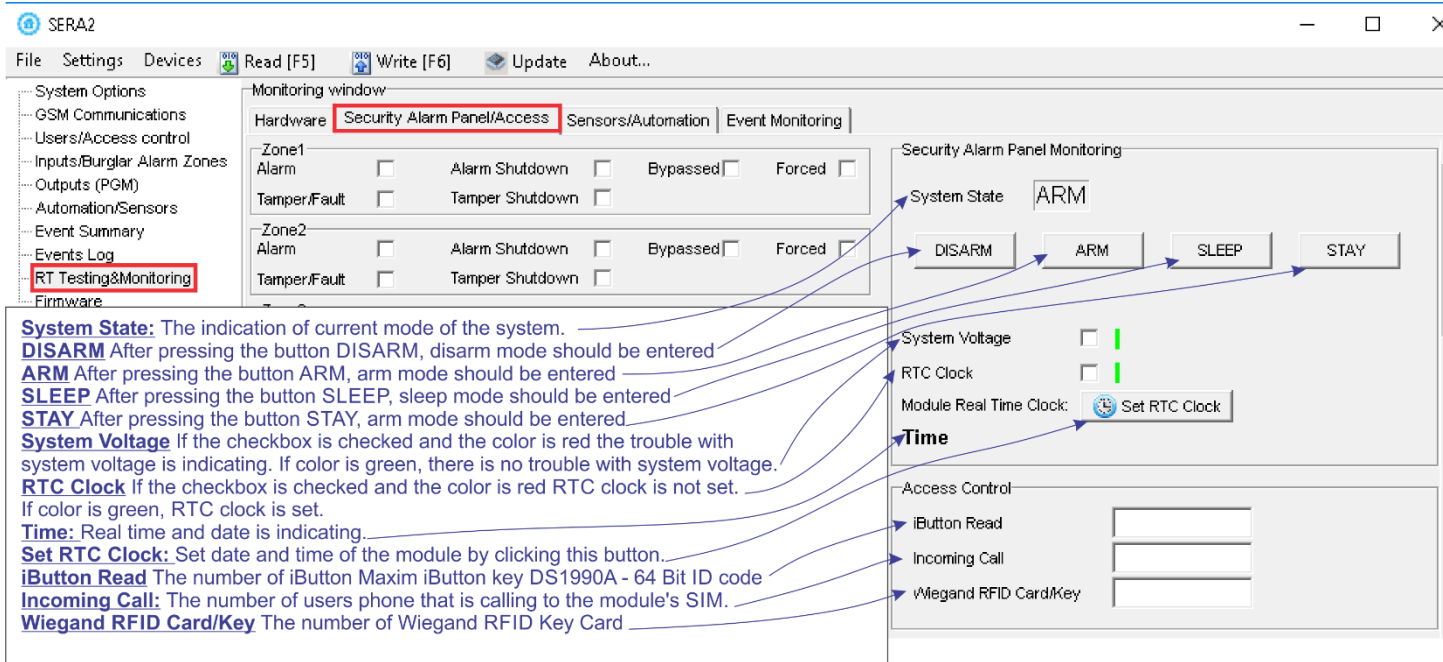


Figure 86 RT Testing Monitoring> Security Alarm Panel/ Access window

## 5.12 Automation & Sensors Programming



### The most important information due to automation with the module Progate

**Sensors.** The module can receive signals from standard sensors that produce a standard analog or pulse output. Sensor's parameters should be set by SERA2 software.

**Remote Monitoring, Control** It is possible to monitor, control or log data by using GSM GPRS network from almost any location around the world. The data transmitting via GPRS using TCP/IP protocol; the GSM module connects to the internet via a GPRS channel to SeraServer server tool who registering all devices. The connection is established by the SERA2 configuration tool using unique id. The SeraServer is designed to make setup and use fast and easy setup and configuration.

**Remote monitoring.** Using the GSM, GPRS remote access from the simplest application, viewing data to more sophisticated uses, such as sending a text message when an alarm occurs or transmitting a data log file over the internet from a remote location to a central office. A user can access this data anytime, anywhere.

**Testing & Monitoring.** You need to monitor the temperature, humidity maybe even the security

**Localized Monitoring Systems.** Perfect for many applications, SeraServer technology can be used in labs, clean rooms, museums, warehouses, computer rooms, food processing/storage, hospitals, and greenhouses, as well as HVAC, pharmaceutical, electronic assembly, and many more environments. Depending on your specific application, you can monitor ambient temperature, humidity, or use a thermocouple or other process. Sensor with analog voltage/current or pulse output, and make the data available anywhere. The Sera Server can be configured quickly and easily you can even use a SERA2 program.

Step by step to set the parameters of security system:

#### Installation:

- Install the module Progate and sensors (PIR, smoke detectors, door contacts)
- Connect the GSM antenna to the antenna connector. Insert the SIM card in the SIM card holder. Ensure that PIN request function is disabled. Connect the battery
- Connect the power supply
- Connect the sensors (PIR, smoke detectors, door contacts) to the module Progate, according connecting diagrams
- Connect Bell, Siren to the output of the Progate, according connecting diagram
- Connect Wiegand keypad and RFID reader, according connecting diagram

#### Configuration:

- Install SERA2 software
- Connect the module to the computer via mini USB cable.
- Configure sensors parameters
- Configure PGM outputs
- Enter user phone numbers for system parameters monitoring
- Read information about arming/ disarming and systems operation algorithm
- Enter user phone numbers for remote control of the outputs
- Set reporting to server details
- Read event Log
- Real time sensors inputs, system outputs monitoring
- Sometimes it is useful security system's details for automation purpose:

## 1.1. Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software



Step by step to start DS18B20 sensors:

3. Connect 1-Wire sensors DS18B20 to D1 or D2, D3 according connection diagram.
4. Digital input type D1,D2,D3 should select in the System Options> Digital I/O Settings window. Set digital input definition D1, D2, D3 to Dallas 1-Wire Bus option

Figure 87 System Option> General System Options window

8. Write configuration by pressing "Write" icon

Figure 88 Command line

9. Power the module.
10. After module starts. Within few seconds, it will automatically scans and registers all connected 1-Wire sensors on the bus.
11. Read configuration
12. Go to "Automation/ Sensors" window in the SERA2 software

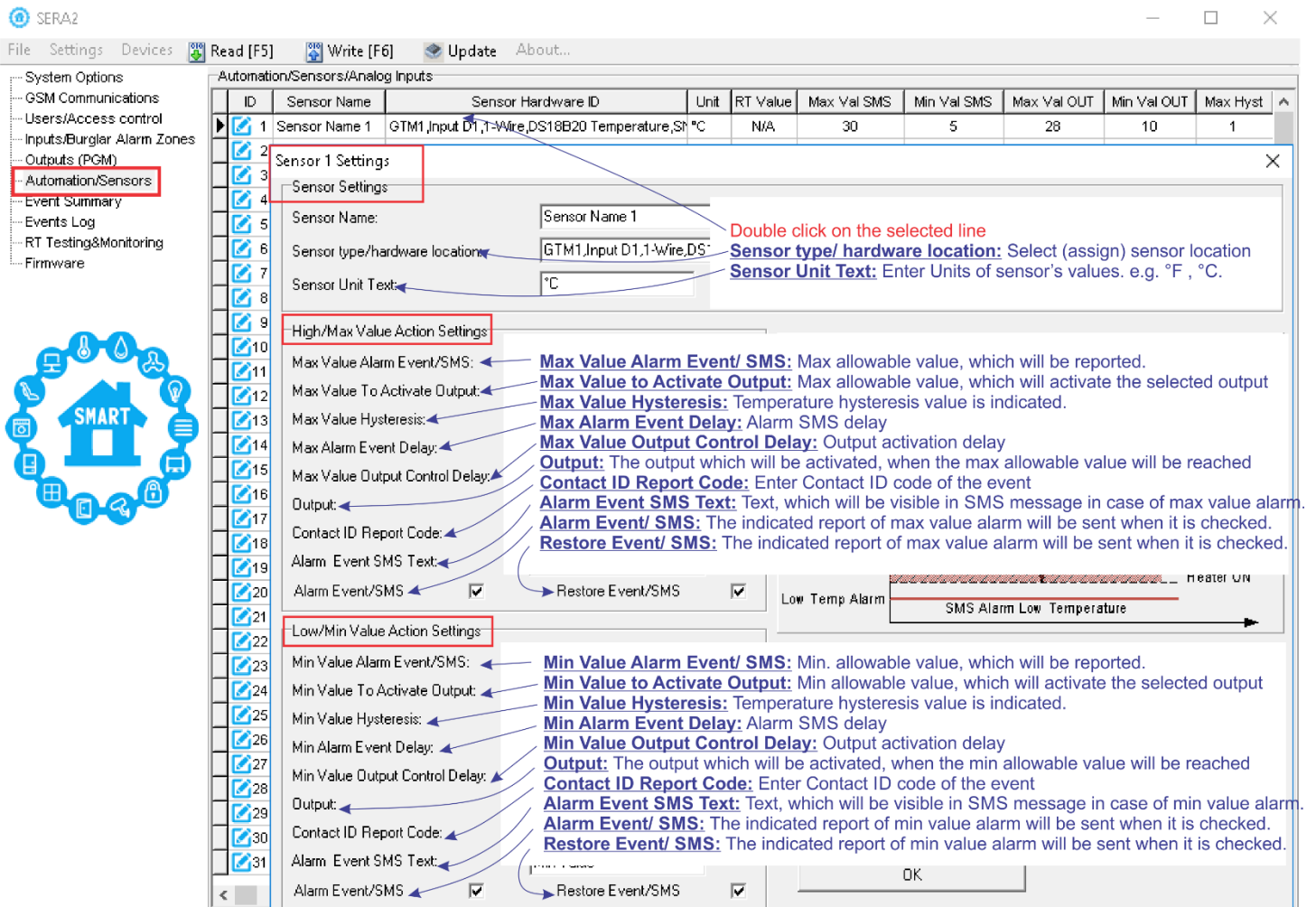
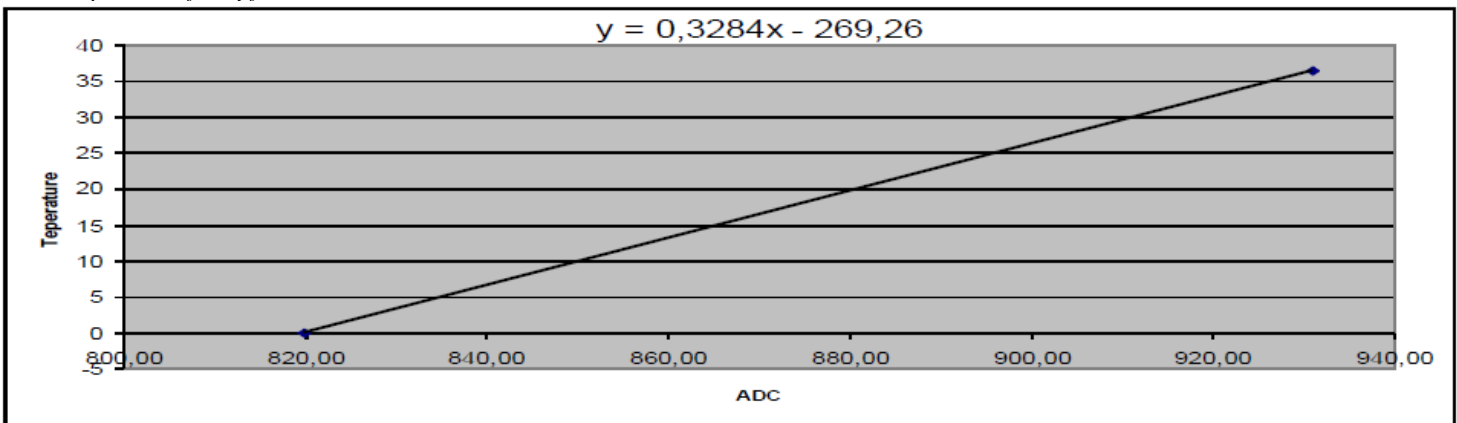


Figure 89Automation/ Sensors window

13. Double click on the selected sensor's line. Set other parameters of the sensor MIN, MAX values Units etc. Every field explanation:Automation & Sensors Programming
14. Write configuration to module, by pressing "Write" icon



Table 7 Explanation of every field in "Automation/ Sensors" window



26	<b>X-multiplier= Mult Coef Correction</b>	X-multiplier coefficient. Following the equation "Temperature=X*ADC+Y"to calculate X and Y coefficients. Measure temperature in two points at least.
27	<b>Y-offset= Sum Coef Correction</b>	Y-offset coefficient. Following the equation "Temperature=X*ADC+Y"to calculate X and Y coefficients. Measure temperature in two points at least.
	<b>Temperature= X*ADC+Y</b>	

Figure 90 how to calculate X-multiplier and Y-offset with excell chart.

## 5.12.1 How does smart thermostat, alarm system works?

The module will keep the home at a stable temperature

„Min Value To Activate Output“ temperature is great for helping prevent home from going below certain temperatures by turning on heating when the set limits are reached. Turn off the heating, when comfort zone is reached.

The smartphone will alert user if there are unusual temperature changes at home.

„Min Value Alarm“ temperature can prevent the pipes from freezing, even if the heating system is broken. The module Progate will inform the user (send alarm SMS and call)

Temperature control system relies upon a controller, which accepts a temperature sensor as input. It compares the actual temperature to the desired control temperature, or set point, and provides an output to a control element. An on-off controller will switch the output only when the temperature crosses set point. For heating control, the output is on when the temperature is below the set point, and off above set point. Since the temperature crosses the set point to change the output state, the process temperature will be cycling continually, going from below set point to above, and back below.

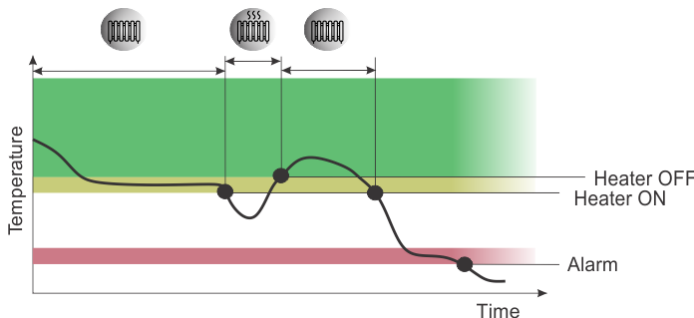


Figure 91 How does thermostat work

## 5.12.2 How to prevent the output from frequently changes according to minute temperature changes

ON/OFF control action turns the output ON or OFF based on the set point. The output frequently changes according to minute temperature changes as a result, and this shortens the life of the output relay or unfavorably affects some devices connected to the Temperature Controller. To prevent this from happening, a temperature band called hysteresis is created between the ON and OFF operations.

In cases where this cycling occurs rapidly, and to prevent damage to contactors and valves, an on-off differential, or “hysteresis,” is added to the controller operations. This differential requires that the temperature exceed set point by a certain amount before the output will turn off or on again.

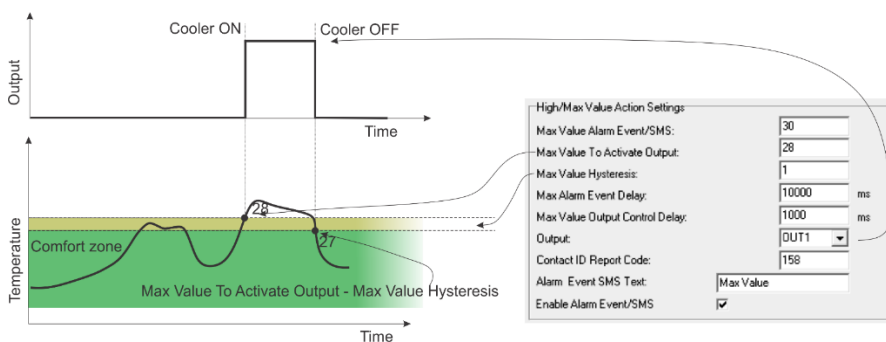
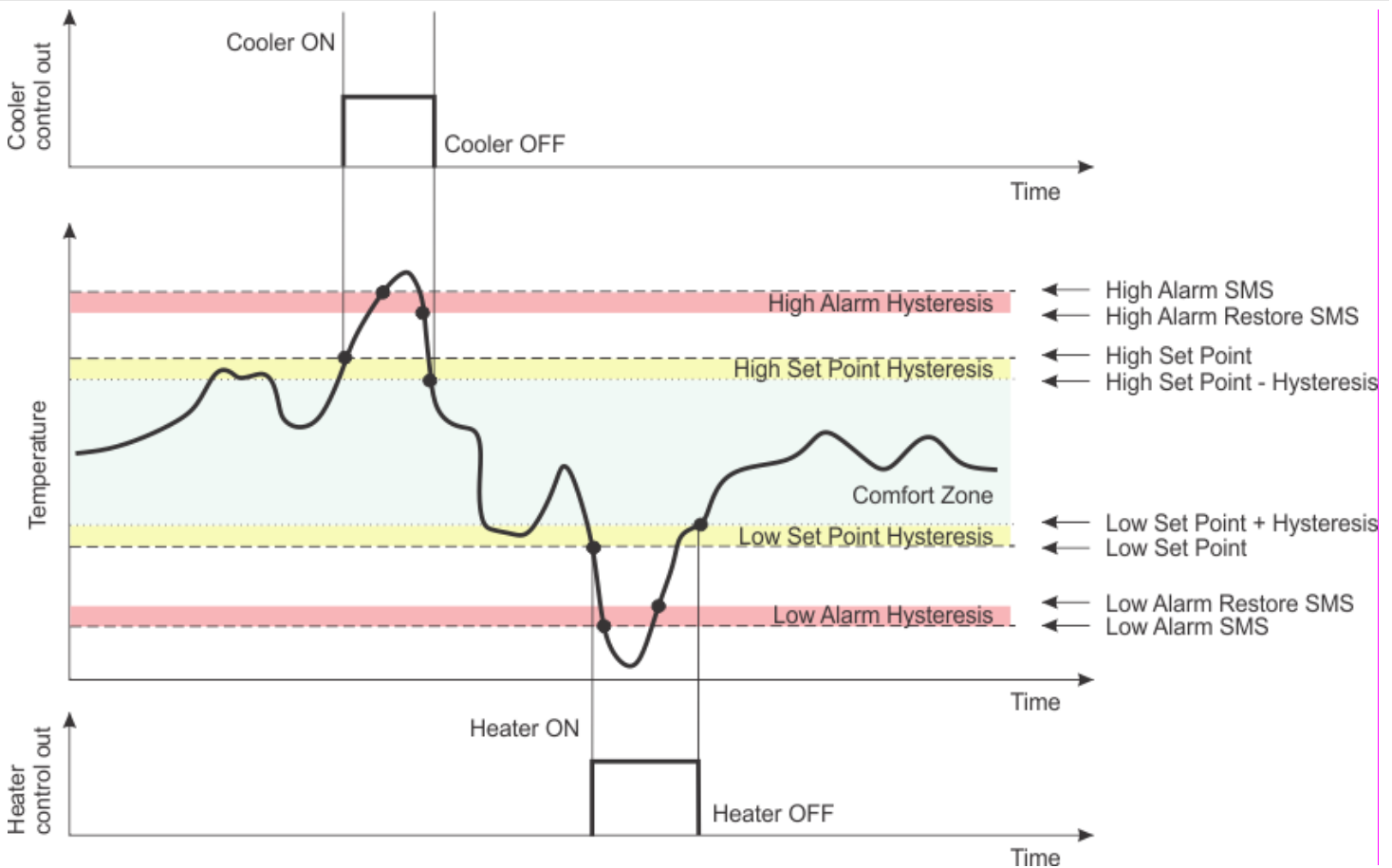


Figure 92 The example of configuration. Sera2> Automation/ Sensors. Double click on the selected line.



Max Value hysteresis is the same hysteresis for Output activation and for alarm event.

### 5.12.3 The example of heating, cooling control with the module Progate



High/Max Value Action Settings	
Max Value Alarm Event/SMS:	30
Max Value To Activate Output:	28
Max Value Hysteresis:	1
Max Alarm Event Delay:	10000 ms
Max Value Output Control Delay:	1000 ms
Output:	OUT1
Contact ID Report Code:	158
Alarm Event SMS Text:	Max Value
Enable Alarm Event/SMS	<input checked="" type="checkbox"/>

Figure 93 The example of sensor's setting

The module activates the output at the set point. The event recovers from the hysteresis value.

**Temperature 28 degrees** – OUT1 will be activate after 1000ms. „Max Alarm Event Delay“prevents from OUT1 activation in response to short-term temperature fluctuations, for example because of window or door opening.

**Temperature 30 degrees** –alarm SMS with the text "Max Value" will be send after 10000ms

If the hysteresis set to 1. The system will work as follows:

Set point = 28 degrees

When temperature rise to 28 degrees, turn on the cooler. When temperature drops to 27 degrees, the system will turn off the cooler.

ON- OFF control switches the output either full ON or full OFF, depending on the input set point and hysteresis values. The hysteresis value indicates the amount the process value must deviate from the set point to turn on the output. With hysteresis set to 0, the process value would stay closer to the set point, but the output would switch ON and OFF more frequently, and may result in the output "chattering".

In order to control big power alternating current equipment, it is comfortable to use solid state relays.

AC/DC adapter with the voltage 10V - 14V and current  $\geq 1A$  might be used to powering the module. We recommend to use TPS12 power supply with the deep discharge protection. The solution with Progate module will gives a call and send SMS warning when the battery voltage reaches the limit. [https://www.topkodas.lt/Downloads/TPS12\\_UM\\_EN.pdf](https://www.topkodas.lt/Downloads/TPS12_UM_EN.pdf)

## 5.13 Data Transmitting to Server & Remote Control



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

It was discussed in [GPRS/ IP/ TCP/ UDP details programming](#)

### 5.13.1 TCP/ IP Remote Control



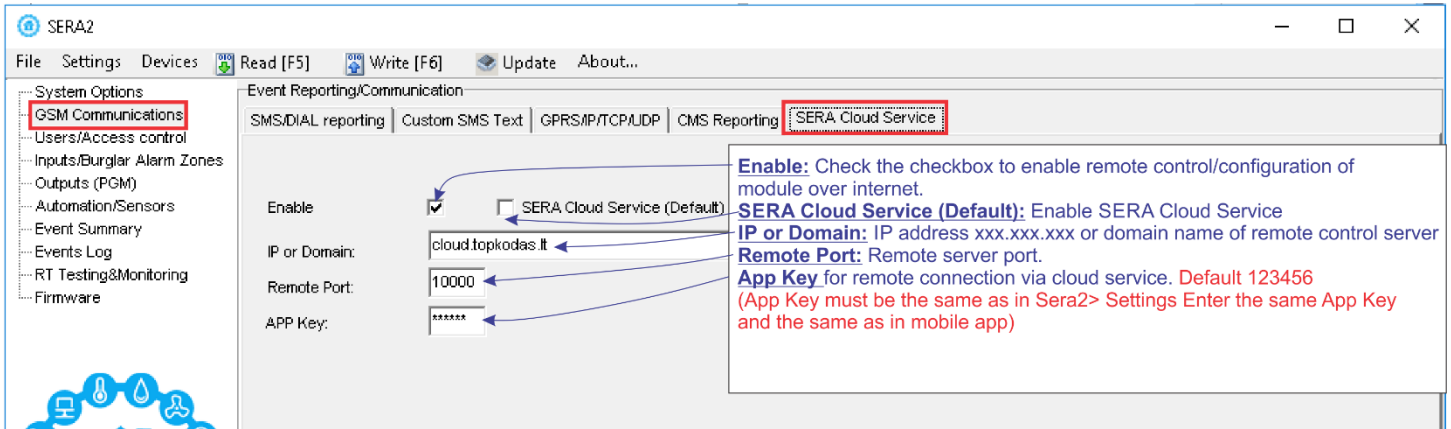


Figure 94 GSM Communication > SERA Cloud Service window

### 5.14 Events Log



#### Events Log

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

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

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

Communication with monitoring station status.

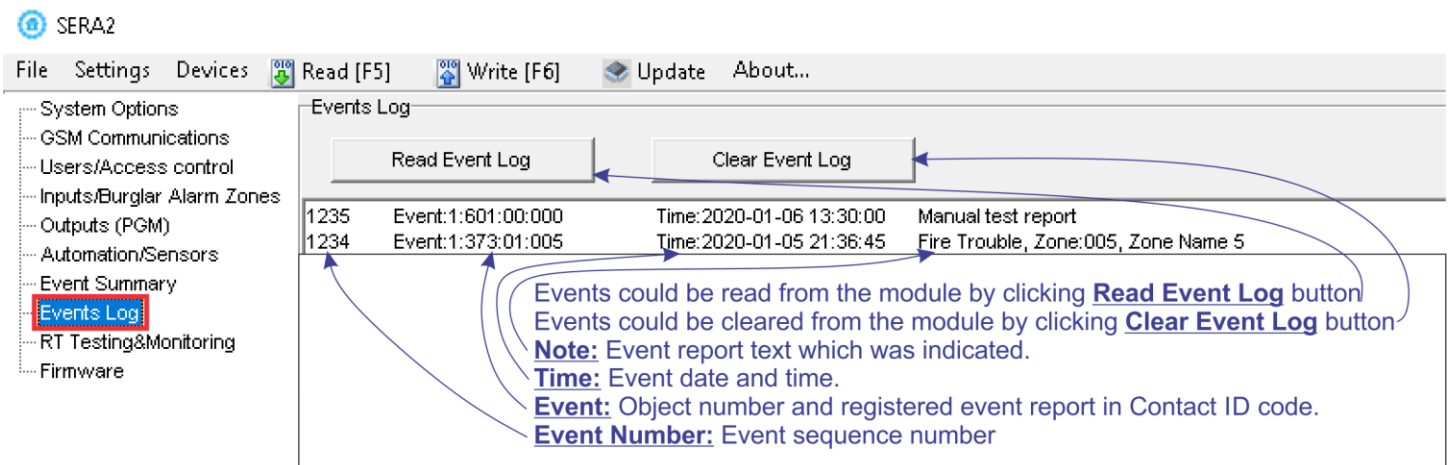


Figure 95 Events Log window.

### 5.15 Remote Monitoring, Control, Configuration, FW update over the internet



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

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

**How does it works?**

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

Progate ↔ SERA Cloud Server [cloud.topkotas.lt] ↔ SERA2

Or


Progate ↔ SERA Cloud Server [cloud.topkotas.lt] ↔ Standard web browser. Firefox, Chrome etc.

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

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

**Steps to activate Remote control over internet:**

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

 SERA2

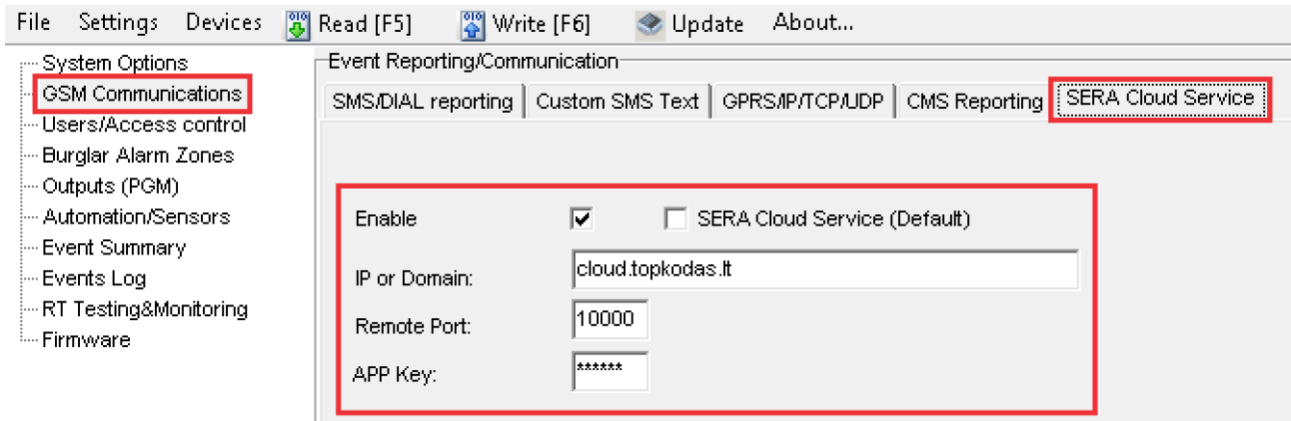


Figure 96 GSM Communication> Sera Cloud Service window

**6. Go to Sera2> GSM Communication> CMS Reporting**

 SERA2

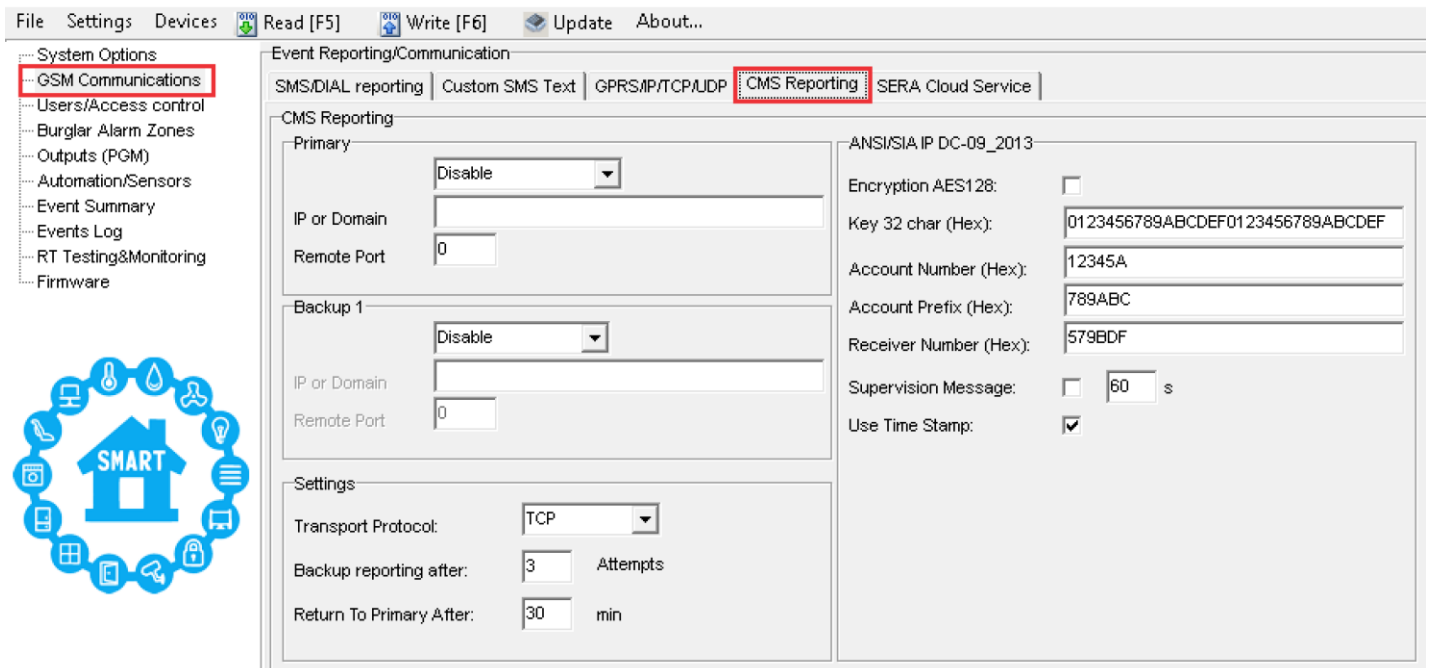


Figure 97 GSM Communication> CMS Reporting window



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

**GPRS network settings**

`INST000000_008_APN#LOGIN#PSW#`

008= command code (GPRS network settings)  
 APN=31 symbols  
 LOGIN=31 symbols  
 PSW=31 symbols

**Remote control of the module over the Internet.**

`INST000000_009_ADDR#PORT#PING#KEY#`

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

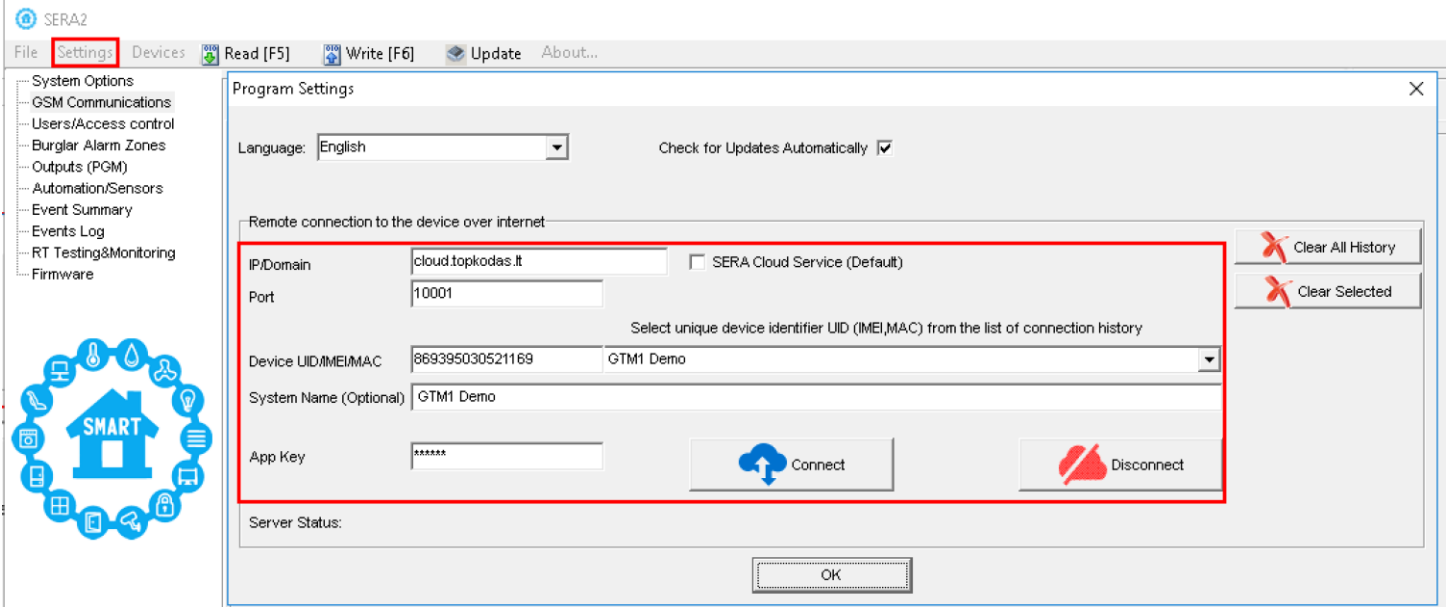


Figure 98 Command line> Settings window

- Sera2> Settings Check “SERA Cloud Service (default)” checkbox.
- Enter Device UID/IMEI. Press *Connect* button and wait till connection will be established. In the bottom in the task bar appears TCP connected notification.

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

## 5.16 Testing & Monitoring Automation



### 5.16.1 Real-time Testing & Monitoring > Sensors/ Automation

RT Testing & Monitoring > Sensors/ Automation

The Sensors/ Automation window let you see real time sensors states: is the sensor active, does it reaches high or low value alarm.

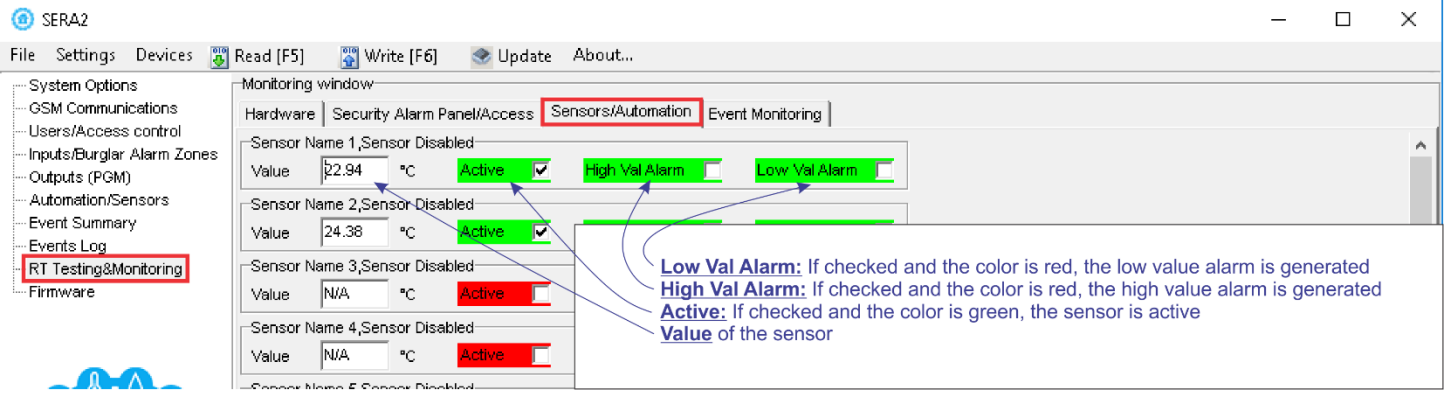


Figure 99 RT Testing & Monitoring > Sensors/ Automation window

## 5.16.2 Real-time Testing & Monitoring > Event Monitoring



RT Testing & Monitoring > Event Monitoring

The Event Monitoring window will show real time events information

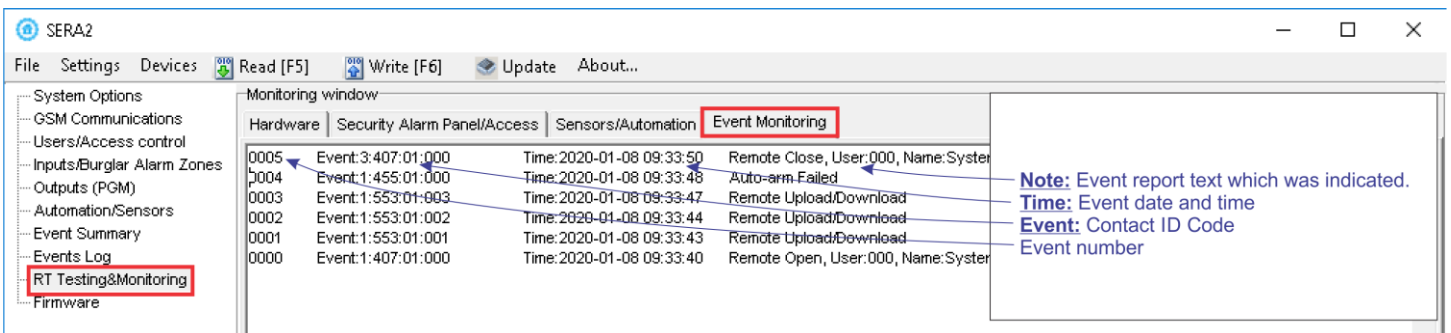


Figure 100 RT Testing & Monitoring > Event Monitoring window.

## 6 Info: Hardware, Firmware, Bootloader, Serial No & Updates



System Options > System Info

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

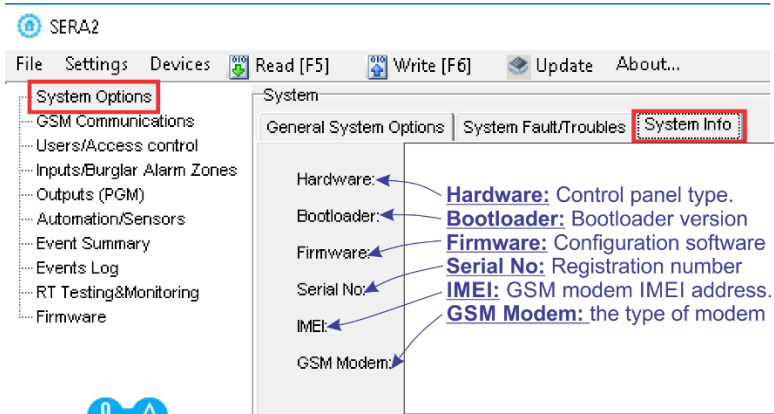


Figure 101 System Options > System Info window.

## 6.1 Firmware Update

### Firmware

This window let you update the firmware of the module.

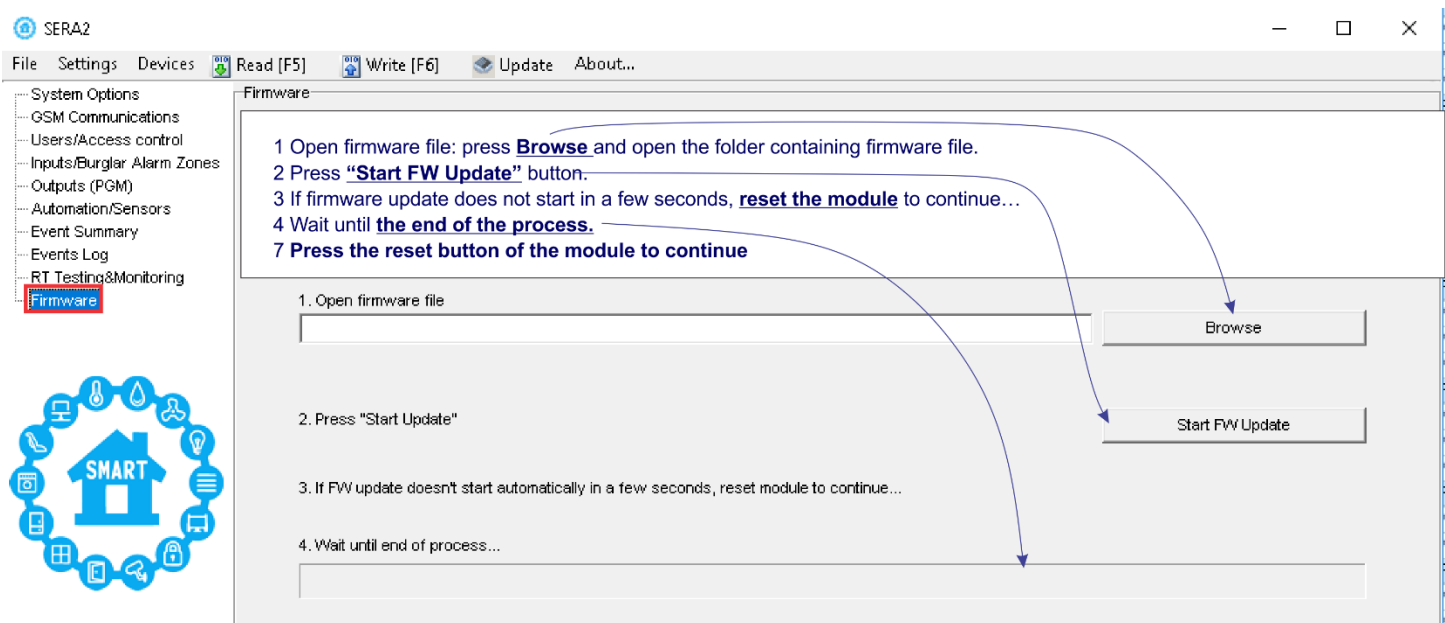


Figure 102 Firmware window

## 7 Recommendations for the user & installer



What should you do, if you noticed, that **there is Sensor trouble in the "Event Log" window?**

0009	Event:1234:1:110:01:006	Time:2017-02-14 08:51:41	Note: , Fire Alarm, Zone:006
0010	Event:1234:1:380:00:001	Time:2017-02-14 08:53:30	Note: , Sensor Trouble, Zone:001

Figure 103Sera2> Events Log window

1. It is comfortable to use "RT Testing&Monitoring" window. Red field indicates sensor's troubles.
2. Go to Automation/ Sensors window, disabling this sensor and press "Write". Maybe there is the problem with sensor's connection to the module.
3. If the problem still exist, please read, save and send the configuration to the seller. Describe what and how is connected to zone: 001 and send this information to the seller.

## 8 Remote control and configuration using SMS Commands



Users allowed:  
 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

Installers allowed:  
 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  
 Enter/ deleting user phone numbers  
 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 – 6-digit password used for system control and request for information. By default, installer code is 000000, which is highly recommended to change.



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

- Identification:  
 INST – Install used for module's configuration.  
 - Installer's or user's password.  
 - space character  
 - Command code.  
 - space character  
 - First configuration array  
 - space character  
 - Second configuration array  
 - etc.

- Identification:  
 USER – User used for module's control.  
 - Installer's or user's password.  
 - space character  
 - Command code.  
 - space character  
 - First configuration array  
 - space character  
 - Second configuration array  
 - etc.

## 9 The table of installers commands



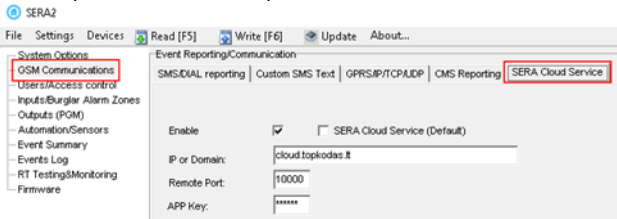
SMS commands with **correct INST password** can be send from any phone number. Keep INST password in secret!



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

Table 8 The table of installers commands

<p><code>INST000000_001_N#TEL#SMS#DIAL#System</code>  <code>open close</code></p>	<p><b>Programming of users telephone numbers to send SMS and to make a call if the event occur:</b>          001= programming user's tel. numbers for DIAL and send SMS          N = user ID number 1-8          TEL = user's telephone number (max 16 digits) without (+) country code, operator's code and user's telephone number included. The end symbol #;          SMS = event filter for sms. 1- send event, 0- don't send event. Sequence of the events 1.2.3...n For example: 001000          DIAL = event filter for DIAL. 1-DIAL if the event occur, 0-don't DIAL Sequence of the events 1.2.3...n For example: 101000          # = delimiter</p> <p><b>e.g.: INST000000 001 1#3706666666#0001000000#0000011111#</b></p> <p>Event filter eiliskumas:          1-reserved          2-system open close          .....          .....          10-Input/Zone4 Alarm/Restore</p>
<p><code>INST000000_002_ID</code></p>	<p><b>Delete user's phone number according the user ID number. Phone number used for receive user's information.</b>          002= command code (deleting user's numbers according the user ID number)          ID = user ID number from 1 to 8</p>
<p><code>INST000000 004 ID#TEL#OUT#OPT#NAME#</code></p>	<p><b>To enter user's telephone number for remote control via short call</b></p> <p><b>USER NAME-only Latin characters is allowed inside SMS</b>          004= command code (enter user's telephone number for remote control via short call)          ID = user ID number 001-800</p>

	<p>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, 1-10.          OPT = DIAL function: 0 – disabled 1 – enabled, Sequence from the left to the right</p> <p><b>OPT:</b>  <b>1-ARM/DIARM</b>  <b>2-Reserved (GTIarm2 =MIC)</b></p>
<code>INST000000 005 TEL#</code>	<p><b>To delete user's phone number for remote control, according phone number</b>          005= command code (delete user's phone number for remote control, according phone number)          TEL = user's phone number (max 16 digits) without (+) comprised of country code, operator's code and user's telephone number. User's phone number must be the same as in the memory of the module.</p>
<code>INST000000_006_N</code>	<p><b>Delete user's phone number whose ID number is N.</b>          006= command code (Delete user's phone number according user's ID number )          N = user's ID number from 001 to 800.</p>
<code>INST000000_007_P#PER#HH:mm#</code>	<p><b>Automatic periodical test settings</b>          007= command code (Automatic periodical test)          P= 0-test disabled, 1- test period by 24 hours, 2- period by minutes          PER= automatic test sending period from 1 to 99999 days or minutes          HH-hours 0-23 ,          mm- minutes 0-59</p> <p><b>e.g. INST000000 007 2#1#14:50#</b> The test will be send every 1 minute</p>
<code>INST000000_008_APN#LOGIN#PSW#</code>	<p><b>GPRS network settings</b>          008= command code (GPRS network settings)          APN=31 symbols          LOGIN=31 symbols          PSW=31 symbols</p>
<code>INST000000 009 ADDR#PORT#</code> <code>INST000000 009 ADDR#PORT#PING#</code>	<p><b>SERA cloud Service Parameters</b>          009= command code (Remote control of the module over the Internet)          ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain text length of up to 47 characters)          PORT= TCP port number from 1 to 65535          Default parameters is in the picture below. We recommend do not change these parameters.</p> 
<code>INST000000_010_E</code>	<p><b>To activate the connection to the remote control server</b>          010= command code (To activate the connection to the remote control server)          E= 1-enabled, 0-disabled</p>
<code>INST000000_019_N#P</code>	<p><b>To change the operation algorithm of the output</b>          019= command code (To change the operation algorithm of the output)          N = output number from 1 to 10          P = output operation algorithm. 0 – output disabled, 1 – Bell, 2- buzzer, 3- flash led, 4- system state LED, 5-LED „system ready“, 6- Automation &amp; access control, 7- AC OK, 8 – Battery OK, 9- ARM/DISARM 10-alarm indication, 11- Lost Primary chanel 12- Lost secondary chanel 13- Fire sensor14-RH Sensor trouble , 15- Access Gained</p>
<code>INST000000_020_N</code>	<p><b>Invert output state</b>          020= command code (outputs inversion)          N = output number from 1 to 10.</p>
<code>INST000000_021_N#ST</code>	<p><b>Output activation or deactivation</b>          021= command code (Output activation or deactivation)          N = output number 1-10          ST = output mode 0 – OFF, 1- ON</p>
<code>INST000000_022_N#TIME#</code>	<p><b>Output activation for the time interval</b>          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.</p>
<code>INST000000_030_ST</code>	<p><b>Change security system's mode (ARM/DISARM/STAY/SLEEP)</b>          030= command code (Change security system's mode)          ST = 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP</p>
<code>INST000000_031_ZN#BYP</code>	<p><b>Zone bypassing by sms command</b>          031= command code (Zone bypassing)          ZN = zone number from 1 to 32          BYP= 1 – zone bypass 0- zone active.</p>

<b>INST000000_063_S</b>	<b>iButton keys learning/deleting mode</b> 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
<b>INST000000_070_N#VALUE #</b>	<b>Programming of max sensors value upon reaching, the SMS message with „High Alarm“ text will be sent</b> 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
<b>INST000000_071_N#VALUE #</b>	<b>Programming of minimal sensors value upon reaching the SMS message with „Low Alarm“ text will be sent</b> 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
<b>INST000000_072_N#VALUE#</b>	<b>Programming of sensor max value upon reaching the selected output will be activated.</b> 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.
<b>INST000000_073_N#VALUE#</b>	<b>Programming of sensor min value upon reaching the selected output will be activated.</b> 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.
<b>INST000000 090 NEW_INST_PSW</b>	<b>Change installer's password</b> (Installers password should be changed before exploitation of the module) 090= command code (Change of installer's password) NEW_INST_PSW = New Installer's password.
<b>INST000000 091 NEW_USER_PSW</b>	<b>Change user's password</b> (User's password should be changed before exploitation of the module) 091= command code (Change user's password) NEW_USER_PSW = New user's password.
<b>INST000000_092</b>	<b>Remote reset of the module via SMS messages</b> 092= command code (Remote reset of the module via SMS messages )
<b>INST000000 093 yyyy/MM/dd#HH:mm#</b>	<b>Time of the module setting via SMS message</b> 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
<b>INST000000_094_TEL#SMS</b>	<b>SMS from the module forwarding to the other phone number</b>  <b>SMS from the module forwarding to the other phone number</b> <b>094= command code (SMS from the module resending to the other phone number)</b> <b>TEL = phone number to which will be forwarded sms textSMS = sms text that will be send to the referred number.</b> <b>TEL=86161111111 local number arba international format e.g. +370616111111</b>  <b>INST000000 094 +37061611111#Hello</b>  <b>SMS text =Latin Charset</b> SMS from the module forwarding to the other phone number094= command code (SMS from the module forwarding to the other referred phone number)TEL = phone number to which will be forwarded sms textSMS = sms text that will be send to the referred number  TEL=861611111111 local number arba international format e.g. +370616111111 INST000000_094_+370616111111#Hello international must be with '+' local without'+' 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"
<b>INST 000000_095_E</b>	<b>Zone Walk Test request</b> 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
<b>INST000000 096</b>	<b>Fire sensors reset.</b>
<b>INST000000_100_N</b>	<b>System state request:</b>

	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 The table of users commands

**!** The phone number must be in the **Sera2> Users/ Access control** list if USER123456 commands will be used. If the phone number is not in the list, the sms commands from this phone number will be blocked.

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

Remote Control Users table											Temporary access Date/Time window		
ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MIC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+37000000000	00000000000	000000000	*****	NONE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input type="checkbox"/>		User	+	00000000000	000000000		OUT1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Table 9 The table of user's commands

<b>USER123456_020_N</b>	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.
<b>USER123456_021_N#ST</b>	<b>Activate or deactivate selected output N.</b> 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
<b>USER123456_022_N#TIME#</b>	<b>Output activation for the time interval</b> 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.
<b>USER123456_030_ST</b>	<b>Change security system's mode (ARM/DISARM/STAY/SLEEP)</b> 030= command code (Change security system's mode (ARM/DISARM/STAY/SLEEP) ST = Security system mode 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP
<b>USER123456_031_ZN#BYP</b>	Enter user phone number in <b>the Sera2&gt; Users/ Access control</b> list <b>Zone bypassing by sms command</b> 031= command code (Zone bypassing) ZN = zone number from 1 to 32 BYP= 1 – zone bypass 0- zone active.
<b>USER123456_094_TEL#SMS</b>	<b>SMS from the module forwarding to the other phone number</b> 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
<b>USER123456_100_N</b>	<b>System state request:</b> 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).  <b>Only for the firmware versions &gt; 190926</b>

## 11 APP configuration

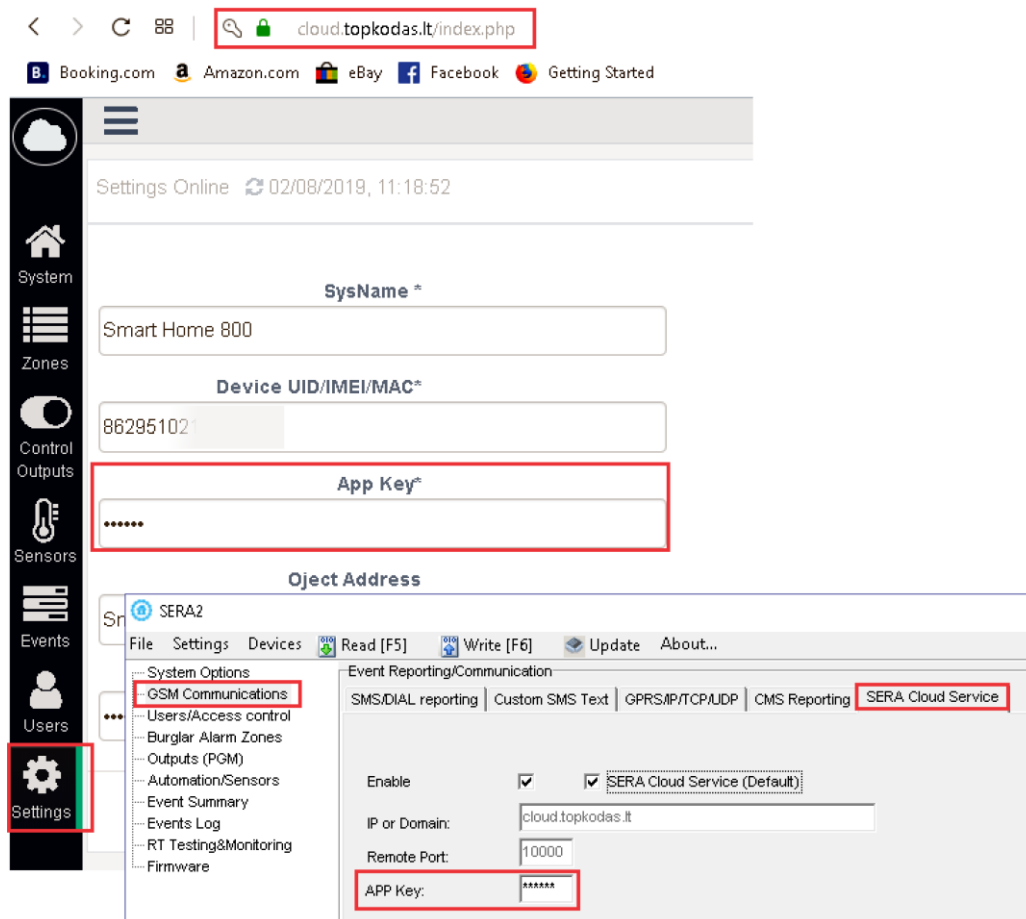


Figure 104 <https://cloud.topkodal.it/index.php>> Settings and GSM Communications> Sera Cloud Service windows

App key in module and APP must be the same. IMEI (device UID) you can find on the modem of the module or in SERA program System Options> System info.

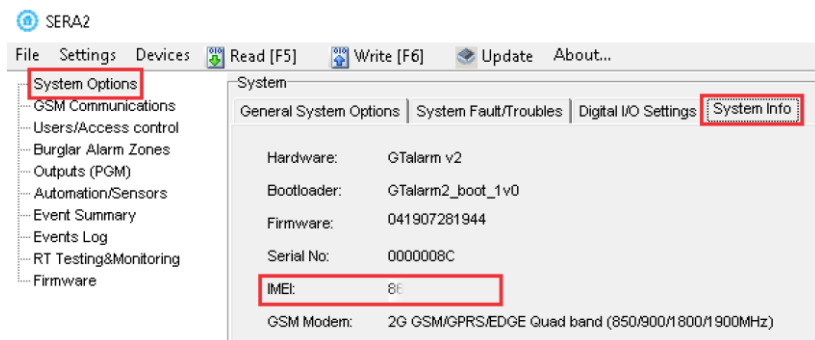


Figure 105 System Options> System Info window

## 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;

Products 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 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.