TOPKODAS

GTCOM2

Installation & Programming Manual

GSM Communicator

PSTN Contact ID to GSM SMS Text Converter

Reporting security panel messages to the SIA-09 CMS (Central Monitoring Station) receiver

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

DESCRIPTION

A cost-effective solution that provides GSM/GPRS connectivity for any non-GSM PSTN security alarm panel DSC, Paradox, UTC Interlogix (CADDX), Innerrange, Texecom, Honeywell, Crow and Pyronix.

GTCOM2 GSM Communicator is special for converting the PSTN Ademco Contact ID codes to readable SMS notifications and SIA-09 IP over GPRS network to central monitoring station (CMS).

The GSM communicator converts the Contact ID codes of the alarm panel's PSTN communicator into:

- Readable SMS text and CALL
- Mobile App Push Notifications
- SIA-09 CMS Central monitoring station receiver

Also you will get extra features in the same module:

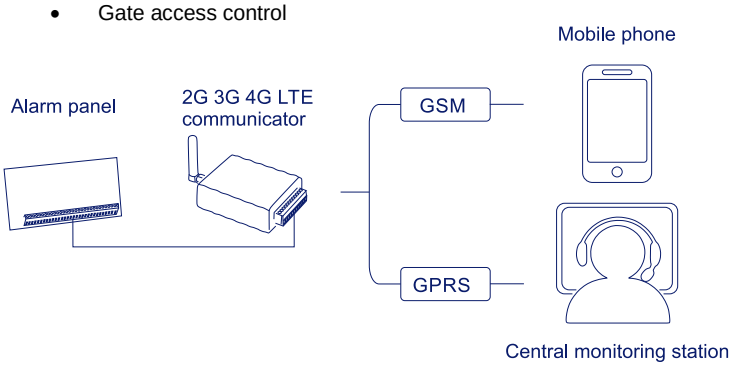
- ARM/DISARM security panel remotely using APP, Call, SMS
- Access Control: Gates, Doors, etc …
- Control Thermostat. Can be connected up to 32 temperature sensors.

FEATURES

- Connects to the Panel's Landline Dialer.
- Reporting to:
  - 8 cellular numbers through SMS
  - 8 cellular numbers Alarm calls
  - Android / iOS **SERANOVA** app push notifications.
  - Reporting system events to a central monitoring station receiver using Internet Protocol Event Reporting with event type Contact ID. IP communication data is sent using the **SIA IP DC-09** standard protocol, which supports Ping supervision, AES128 Encoding, TCP/IP or UDP/IP via GSM GPRS. The supported versions of **SIA DC-09** standards:
    - ANSI/SIA DC-09-2007
    - ANSI/SIA DC-09-2012
    - ANSI/SIA DC-09-2013.
- Works with Android/iOS **SERANOVA** app and Web Apps:
- Provides SMS and push notifications about events.
- Allows remote system Arm/Disarm.
- Enables remote control of connected devices (lights, gates, ventilation systems, heating, sprinklers, etc.).
- Features remote temperature monitoring.
- Multiple methods for remote control and monitoring:
  - Android / iOS / WEB-based **SERANOVA** APP allowing control system from any OS device from anywhere
  - SMS-based communication for system control
  - Control of the device by call
  - For your convenience, a web app compatible with standard web browsers for better accessibility.
- Built-in access control features. Access control for gates, doors, barriers, and more.
- Thermostat and automation support for up to 32 digital sensors, ideal for various temperature-sensitive environments.
- Remote configuration and control via GPRS connection, USB with SERA2 software, or the free **SERANOVA** app
- Firmware update via USB or remotely via GPRS with the SERA2 software.
- Built-in access control features.
- Events log buffer. **3072 events**.
- Built-in real-time clock

APPLICATIONS

- GTCOM2 communicator is cost-effective upgrade for existing security panel:
  - Functions as a gateway with third-party PSTN/non-2G/3G/4G LTE alarm panels, using 2G/3G/4G LTE and IP networks for transmitting data to **central monitoring stations (CMS)** or users via SMS and app notifications.
  - **Capable of simulating PSTN line**, interpreting DTMF Contact ID messages, and sending SMS via GSM network. Compatible with DTMF dialing and Ademco Contact ID (SIA DC-05 standard).
  - Supports **SMS notifications** for up to 8 users about system events based on alarm panel settings.
- Allows control of the primary alarm panel from GTCOM2, with status visible in the app.
- Enables GTCOM2 control from the alarm panel with status display on the keyboard.
- Home automation
- Gate access control



*Alarm panel must support DTMF (tone) dialing and Ademco Contact ID data format according to SIA SIA DC-05 standard.

Download SERANOVA APP by Scanning the QR Code

GET IT ON Google Play

Download on the App Store

The meaning of icons in the manual:

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

Contents

1 GENERAL INFORMATION

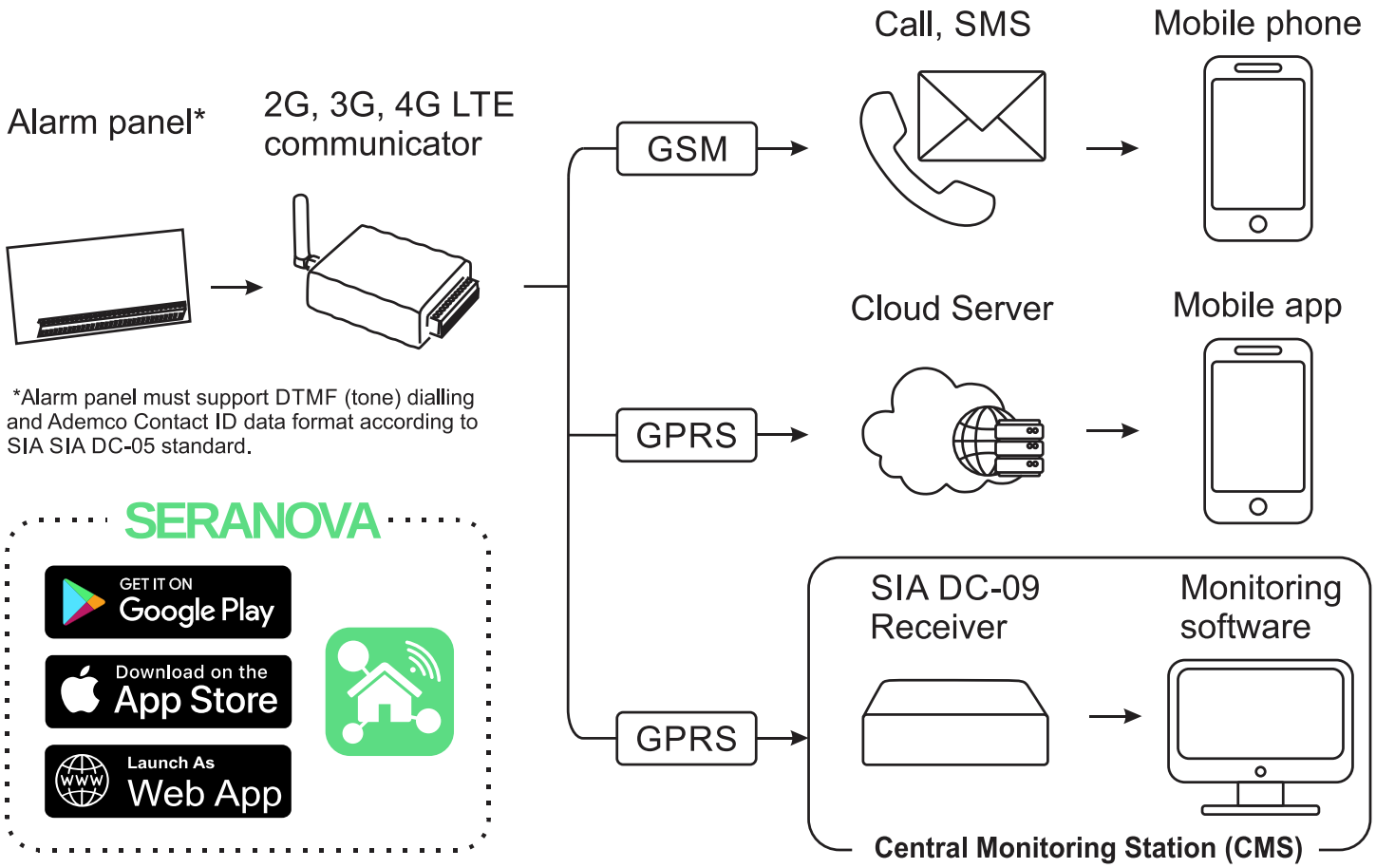


Figure 1 Structural schematic with usage

- The GTCOM2 module sends GSM-based SMS alerts about security system events to users.
- Converts Contact ID DTMF data from any security panel's PSTN communicator into SMS; transmits to central monitoring stations (CMS) using the SIA DC-09 IP protocol, ensuring compatibility with SIA DC-09 receivers.
- Displays the security panel status on the SERANOVA mobile app.
- Synchronizes statuses between the GTCOM2 and the primary alarm panel for control and monitoring, which are accessible through both the app and keyboard.
- In the event of an alarm or other occurrence, it sends sequential SMS messages (SMS1, SMS2... SMSn) and calls (DIAL1, DIAL2… DIALn) to each of the 8 users.

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

IN1, IN2 inputs:
- Burglary alarm zones. Input type NC/NO/EOL/EOL+TAMPER 2.2K + 2.2K;
- 10K pull up resistor;
- Analog input 0-10V;
- Response time;
- Time of repeatable Alarm/Restore;
- Commutation of selected output;

Inputs/outputs I/O1, I/O2:
Programmable output;
- Open Drain 24V/1A ,
- Short Circuit Protection
- Overvoltage Protection (Active Clamp)
- Overcurrent Protection

Programmable Input:
- NC, NO or EOL=5.6kΩ (settable)

Digital 1-Wire interface 1W:
800 iButton users - DS1990A,
up to 32 temperature sensors DS18b20
Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321;

Protocol to Central monitoring station (CMS):
ARC – Alarm receiving center
SIA IP DC-09 protocol:
- Standards supported:
  - DC-09-2007,
  - DC-09-2012,
  - DC-09-2013,
  - DC-09-2021
- Backup channel: Yes
- UDP/TCP: Yes
- AES128 bit encryption: Yes
- Ping Supervision Messages: Yes
- Time Stamp synchronization: Yes

Wiegand interface D0,D1 (DATA0/ DATA1):
- Wiegand Keypad / RFID reader;
- Wiegand Keypad / RFID reader:
- 26-bit,34bit Wiegand RFID card format
- 4-bit, 6-bit, 8-bit Keypad PIN/CODE format
- The total length of the bus from 10 to 100m.

Module control:
ARM/DISARM of the security system via:
- Free SERANOVA app (Android, IOS, web)
- 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

Buffer for unsent events:
Nonvolatile flash events log 3072 events

5V power source output:
- Voltage 5V
- Current limit 100mA

Power supply voltage:
- DC 10-16 V / 200mA max
- Max. Allowed ripple voltage 100mV.

Consumption current:
In standby mode less than 50 mA.
In dialing or SMS/GPRS sending mode less than 200 mA.

Environmental parameters:
Storage temperature range
from -40 to +85 ºC / -40 to 185 ºF
Operational temperature range
from -30 to +75 ºC / from -22 to 167 ºF
Max relative humidity:
0-90% RH @ 0… +40°C (0-90% RH @ +32… +104°F) (non-condensing)

Package weight 90g

Module weight: 43g

Overall dimensions of the module:
73x62x26mm

1.2 Used definitions and terms

Term	Description
Alarm Log	Records of system events
Arming/Disarming	The process to activate or deactivate the system's security.
Authorized user	A person with a mobile number registered in the GTCOM2 module. Multiple users with equal rights can be added.
Backup battery	The secondary power source of the system. In case of a main power failure, the backup battery will take over.
Bell squawk	Siren signals indicating arming (2 short beeps) and disarming (1 long beep). Default is off.
Bypass/Activate Zone	Allows disabling a compromised zone for arming. The zone is ignored if breached while armed and stays bypassed till disarmed.
Caller ID	Identifying the caller's phone number.
COM	Negative power supply terminal.
Configuration	Setting system parameters such as phone numbers, 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	Countdown initiated upon violation of a Delay-type zone. If disarmed before expiry, no alarm triggers.
EOL	(End of line resistor) input type with resistor.
Event	The information that the user receives.
Event Log	Recorded system events. Logs actions, configurations, and info messages.
Exit Delay	Time after arming for users to leave the secured area.
Fault	An issue preventing normal system operations. The system can diagnose and notify of faults via SMS.
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	Regular system test event with date, status, signal strength etc.
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	Indicates a zone's condition: violated or restored.
+V	Positive power supply terminal.

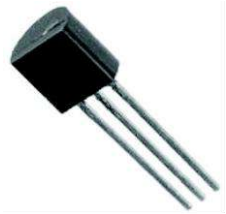
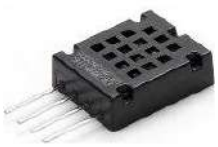
1.3 Package content

Table 1 Standard package content

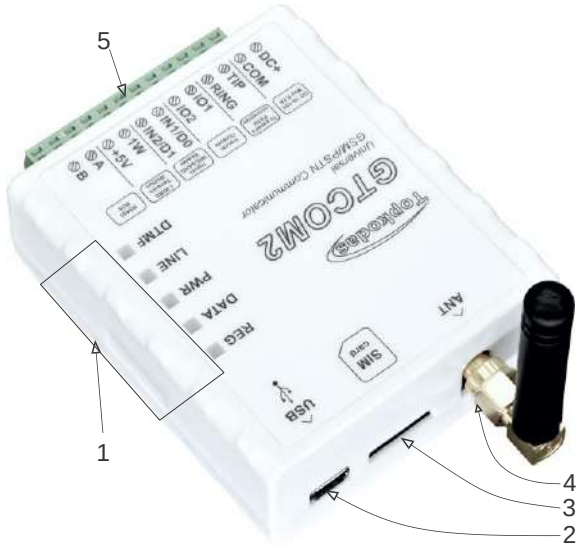
	
GTCOM2 module – 1 pcs	Shipping Package - 1 pcs

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

Table 2 Additional, under request package content

			
Cellular Antenna 2.5 dBi L-Type SMA Connector	4G LTE Antenna 3dBi SMA male Adhesive Mount 2m Cable	4G LTE Antenna 7dBi SMA male Magnetic 2m Cable	4G LTE Antena 5dBi SMA male Magnetic 2m Cable
			
Waterproof Temperature Sensor DS18B20 cable 1m	Temperature sensor DS18B20	Digital Temperature/Humidity Sensor Am2305	Humidity sensor AM2320
			
iButton DS1990A-F5+ key	iButton probe with LED indicator	Mini USB cable	Wiegand keypad & RFID reader

1.4 General view of the module



1. **LED Indication**: See Table 3 for the meaning of LEDs.
2. **Mini USB** Connector: Used for module configuration and firmware updates.
3. **SIM** Card Holder: Push-push type for Nano SIM.
4. **ANT** GSM Antenna Connector.
5. **Terminal Block**: For power supply and input/output connections.

1.5 Meaning of LEDs and contacts

Table 3 Meaning of LEDs

Name	Indication variations	Meaning
WDG (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 data has been sent.
LINE (blue)	Lights continuously	The security control panel has picked up a handset Off-hook
	OFF	The security control panel has not picked up a handset On-hook
DTMF	Blinking 5-10ms	DTMF tones are receiving from the control panel
	Blinking 1s	DATA OK. Data received correctly.

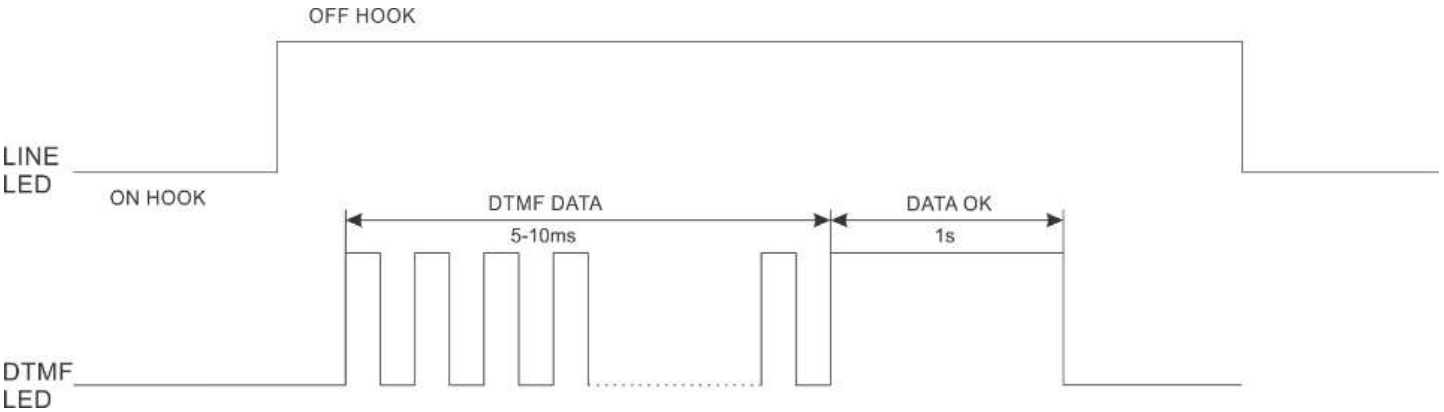


Figure 2 Meaning of LINE and DTMF LEDs

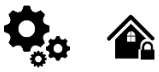
LINE (blue) LED lights continuously, when central panel OFF HOOK DTMF LED is blinking (5-10ms). When DTMF LED lights for 1s, data received correctly.

Table 4 Terminal block. Contacts.

Name	Optional functions and Description	
DC+	DC	10-16V
	Max	0.2A
COM	Common terminal (negative)	
TIP	Terminal to connect with security control panel TIP terminal	
RING	Terminal to connect with security control panel RING terminal	
I/O1-I/O2	Programmable functions	Digital input (zone) NC/NO/EOL/EOL+Tamper [1]
		Open drain output 16V/1A
		Analog voltage input 0-16V
IN1/D0 … IN2/D1	Programmable functions	Input/Zone with pull up resistor 10K to the VD+. Used for gate position or security sensors
		Can be configured NC/NO/EOL/EOL+Tamper
		Wiegand interface. Inputs D0 and D1 used for Wiegand RFID reader, keypad
1W	Programmable functions	Digital output (Max 3.3V)
		Digital input (Max 3.3V)
		Dallas 1-Wire bus. For iButton DS1990A and temperature sensors DS18B20
		Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
	Max available voltage	+3,3V
	Max available current	10mA
+5V	Power supply for external temperature, humidity sensors	
	Max available voltage	+5V
	Max available current	100mA
A	RS485 bus A contact	
B	RS485 bus B contact	

[1] If the zone used for security system purpose 5.1k pull-up resistor should be connected

2 QUICK START



- Settings can be saved to file and quickly written to other communicators.
- Two access levels for configuring the device for CMS administrator and for installer.
- Remote configuration and firmware updates.

2.1 Requirements of the Security Control Panel

The security control panel should meet the following requirements:

- Support the Ademco Contact ID protocol in accordance with the SIA DC-05 standard.
- Support dialing in DTMF tones.
- Support the transfer of Contact ID data in DTMF tones.
- It is recommended that the control panel supports automatic Contact ID codes.

2.2 Requirements for SIM card

- **Any SIM card could be used.** The GTCOM2 module is not locked to a specific GSM network. This means users can use a SIM card from any GSM service provider that offers SMS and calling capabilities.
- For controlling the module via a short call, the SIM card should have a Caller ID option, which is typically available. If your card cannot identify a caller, please contact your GSM service provider or use another SIM card.
- To insert the SIM card into the holder, ensure the card's circuitry faces downward and the card's key (cut angle) faces upward. The card holder is of the "Push-Push" type, meaning the card is secured after one push and released after a second push.
- Avoid forcing the SIM card into its holder to prevent damage to the SIM card holder.

Do not insert the SIM card forcefully, as this may damage the SIM card holder.

Data usage can be enabled or disabled, but to use the remote cloud service, data must be enabled.

2.3 Preparation

Before you begin, ensure that you have the necessary items:

- A USB cable (Mini-B type) for configuration.
- At least a 4-wire cable for connecting the communicator to the control panel.
- A flat-head screwdriver, 2.5mm in size.
- A cellular antenna with sufficient gain, if network coverage in the area is poor.
- An activated Nano-SIM card (with the PIN code request disabled).
- The specific installation manual for your security control panel.

2.4 Fastening

Mounting on DIN rail

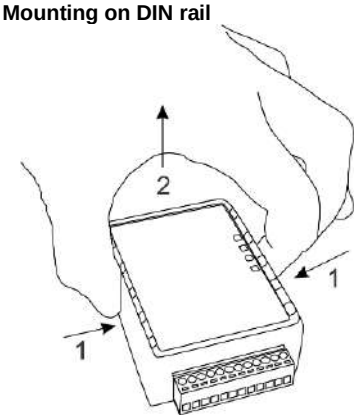


Figure 3 remove the top lid

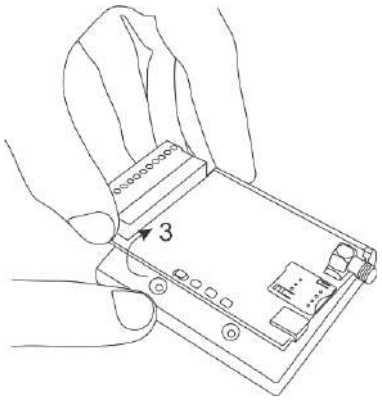


Figure 4 Remove the PCB board

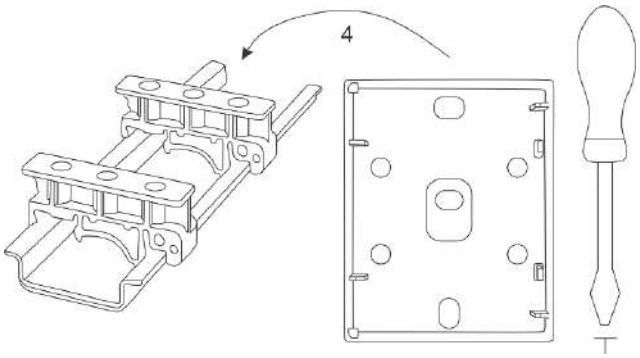


Figure 5 Fasten DIN rail adapters to the base of the case

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

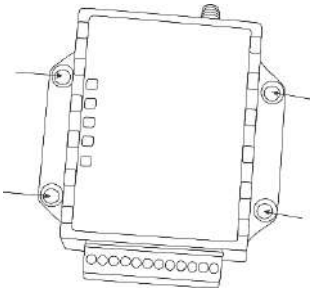


Figure 6 fasten the base of the case

2.5 Configuration methods

It is possible to configure device in following methods:

- **SERA2** software via **USB** (recommended)
- **SERA2 remote** connection over internet Cloud service
- **SERANOVA app**
- **SMS text commands**. For more details, see:

2.6 SERA2 software

SERA2 software is intended for GTCOM2 configuration locally via USB port or remotely via 'SERA Cloud Service' internet GPRS/LTE 2G/3G/4G network. This software simplifies system configuration process. SERA2 software is free, which you can download from our website: https://www.topkodas.lt/Downloads/SERA2_Setup.exe

2.6.1.1 SERA2 Software Installation:

- Visit http://topkodas.lt and download the SERA2 software.
- Locate and open the folder containing the SERA2 software installation files. Click on "SERA2 setup.exe."
- If the installation directory is correct, click [Next]. To choose a different directory, click [Change], specify the desired installation directory, and then click [Next].
- Verify the entered information and click [Install].
- Once the SERA2 software installation is successful, click [Finish].

2.6.1.2 Configuration using SERA2 software

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

- Download and install and open free SERA2 configuration & Diagnostic software: https://www.topkodas.lt/Downloads/SERA2_Setup.exe
- Connect the controller to a computer using a mini-USB cable.
- The program will automatically recognize the connected device and will automatically open the controller configuration window.
- [Menu > Read] will read configuration of device and show current settings of device.
- [Menu > Write] will save the settings made in the program to the device.
- [Menu > File > Save] will save the settings into a configuration file. You can upload the saved settings to other Devices later. This allows to quickly configure multiple devices with the same settings.

- [Menu > File > Open] will allow to choose a configuration file and open saved settings.
- If you want to revert to default settings, go to Update in the command line and update FW. Or press [Menu->File->Restore Default]

2.7 SERA Cloud Service: Remote Connection to the Module via Internet Using the SERA2/SERANOVA

GSM Communication > SERA Cloud Service

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

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

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

Remote Connection Capabilities:

- Access to the SERANOVA app (Android, iOS, WEB) or SERA2 windows software.
- Remotely configure system parameters, monitor hardware status, input voltage, temperature sensors, and GSM network levels.
- Update the module's firmware and read the event log.

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

- Use SERANOVA app (Android, IOS, WEB)
- Use SERA2 windows software remotely via internet.
  - Configure system parameters
  - Monitoring of hardware system status, input voltage, including temperature sensors, GSM network parameter levels.
  - Update the module's firmware.
  - To read event log

How it Works:

- **Connection Protocol**: A GPRS/LTE-backed TCP/IP protocol.
- **Connecting Platform**: Connects through GPRS/LTE to the SERA cloud server using the module's unique IMEI (UID).
- **Communication Pathways:**
  - GTCOM2 (device) ↔ [SERA Cloud Service] ↔ SERA2 (configuration software) for system setup and management.
  - CTCOM2 ↔ [SERA Cloud Service] ↔ SERANOVA app (compatible across Android, iOS, and standard web browsers like Firefox, Chrome, etc.)
- **SERA Cloud Server's Role**: Creates a communication tunnel between GTCOM2 and SERA2/SERANOVA app, facilitating two-way communication through the TCP protocol.

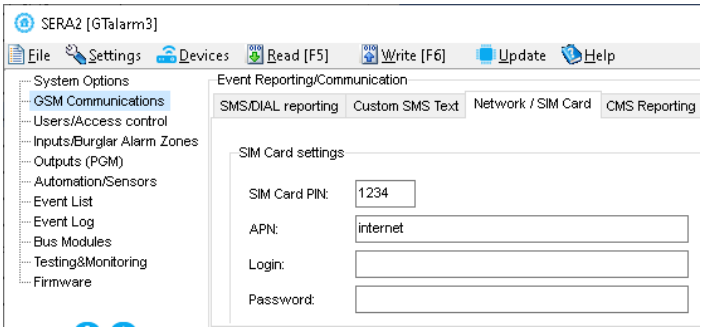
Note: Ensure GPRS service is active on the module's SIM card. If it's not automatically activated, contact your GSM provider. A data plan is recommended, with the module consuming 10-50MB monthly on average.

GPRS/LTE Mobile Data Requirements:

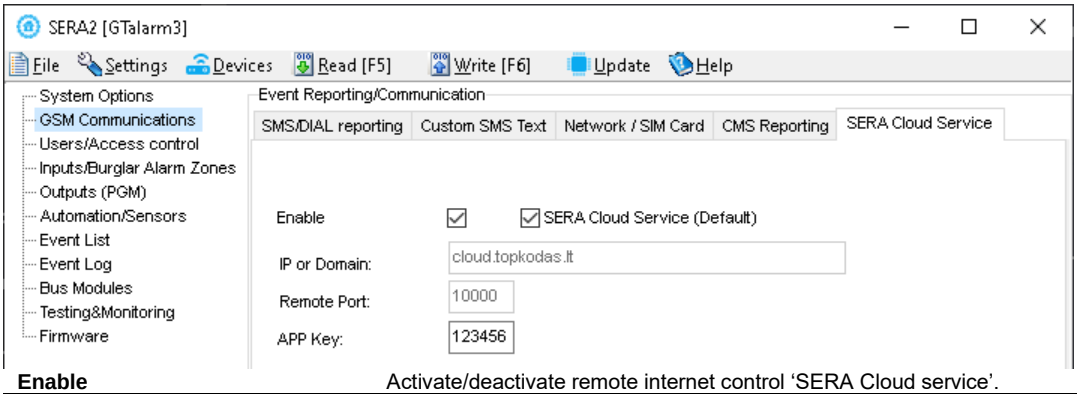
- Any active SIM card can be used. The module is not locked to any specific network and can work with any SIM card that supports SMS and calls.
- Employ a SIM card with a data plan enabled.
- Estimated data consumption: Between 10 to 50MB monthly.

Setting Up Remote Control:

- Install the SERA2 software.
- Navigate to 'SERA2>GSM Communications>Network/SIM Card' tab to configure APN, login, and password (details provided by your network provider).
- Go to 'SERA2>GSM Communications>SERA Cloud Service' tab and activate [SERA Cloud Service] with default settings.
- Press [Write] to save the configuration.



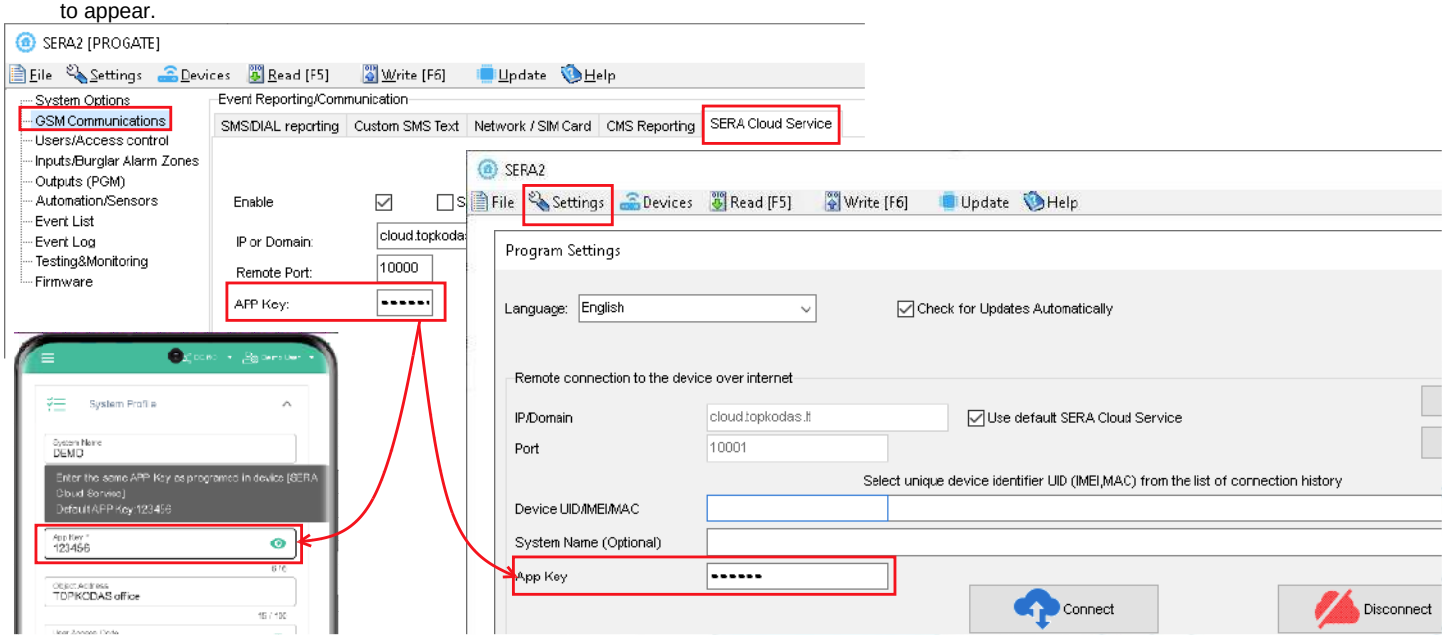
> **!** Make sure the correct APN is set. Using the wrong APN may result in data and VoLTE not working. Consult your network provider for the correct APN details.



Enable	Activate/deactivate remote internet control 'SERA Cloud service'.
IP or Domain	Set to either IP (xxx.xxx.xxx) or domain (default: cloud.topkodas.lt).
Remote Port	The default port is 10000; make sure the firewall is not blocking this port.
App Key	Server encryption key. Default value set to 123456.

Steps to connect remotely to device via internet using **[SERA Could Service]:**

- Insert the SIM card into the module.
- **Ways to get device IMEI (UID):**
  - **First call** to module. The caller will receive a greeting SMS with the IMEI of the module.
  - By sending an **SMS command**: INST000000,100,1
  - Run **SERA2** and connect device to USB. Go to: SERA2 > System Options > System Info.
- Check "SERA Cloud Service (default)" checkbox.
- To connect, use the module's UID (IMEI) and AppKey (default:123456)
- Use the same AppKey (default:123456) in the module and in SERA2 or SERANOVA for remote connection.
- Click the **[Connect]** button. Wait for a 'TCP connected' notification to appear.



If needed, APN/Password/Login/IP/Domain/ Port /PING time /KEY can be set by SMS commands

GPRS network settings

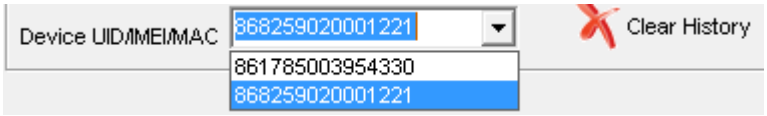
INST000000␣008␣APN#LOGIN#PSW#

- **008**: Command code
- **APN**: Access Point Name (31 char. max).
- **LOGIN**: User login (31 char. max).
- **PSW**: Password (31 char. max).

Remote control of the module over the Internet.

INST000000␣009␣ADDR#PORT#PING#KEY#

- **009**: Command code.
- **ADDR**: IP address (format xxx.xxx.xxx.xxx) or domain (up to 47 characters).
- **PORT**: TCP port number (1 to 65535).
- **PING**: Ping time =600
- **KEY**: App Key (Default is 123456).



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

2.8 SERANOVA (Android/iOS/Web) app

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

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

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

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

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

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

SERANOVA

GET IT ON Google Play

Download on the App Store

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

2. **Register** or sign in to your account.
3. **How Get IMEI**: To add a system, the device's IMEI is required. Obtain the IMEI by:
   - Making the initial call to the device. The first caller becomes the owner and administrator and receives an SMS with the IMEI from GTCOM2. Copy the IMEI, which serves as the module's UID and allows connection to the free SERANOVA app.
   - Sending an IMEI request SMS command INST000000␣100␣1 to the controller's SIM card number. The sender will receive an SMS response with complete device information, including the IMEI.

- Reading the IMEI via USB using the SERA2 configuration program from *System Options* > *System Info*

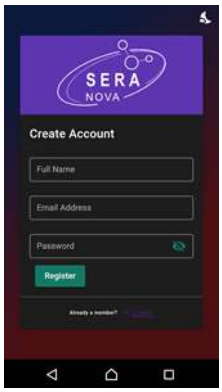
4. Add new system to the app

- Enter the IMEI (UID) you copied from the SMS or SERA2 system information
- Enter App Key (default: 123456).
- Enter the **User Access Code** (default: 123456). Without a user access code, the system cannot operate. This code serves as both the user ID and password within the system. Each user must have a unique code, which is located in the user table. The system administrator creates and provides these codes to each user.
- Phone number of system
- Enter system name.
- Press [SAVE].

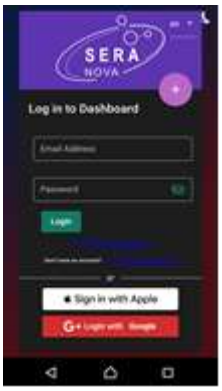
5. How to add a new user

- New users must download the SERANOVA app. Create an account, login with his email and password
- System owner or administrator goes to *SERANOVA> Menu> Users> [Add new User]*
- To enable a user to log in to the system, the owner must enter the user's email and user code (with which the system will be operated. This is the user ID and password). This is enter the user email that was used to create the SERANOVA account. Enter User code (Default 1234), Phone number, Set Output for control, User privileges: admin or user

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



1.Install SERANOVA app
2.Create account



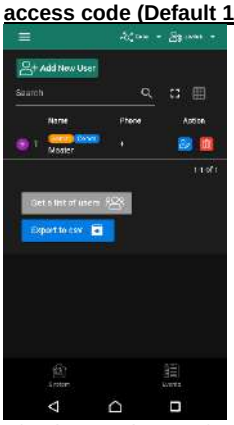
3.Log In
4. The first person to call the GTCOM2 SIM card number becomes the owner and administrator.

5. GTCOM2 sends a message with the IMEI
6. Enter the IMEI and App Key (Default 123456), **Enter User access code (Default 123456)**

7. The system is now manageable

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

9. Select pulse or level



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

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

How to add additional system (unlimited number) to SERANOVA app:

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

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

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

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

3 WIRING & INSTALLATION

Preparation procedure of the module GTCOM2.

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

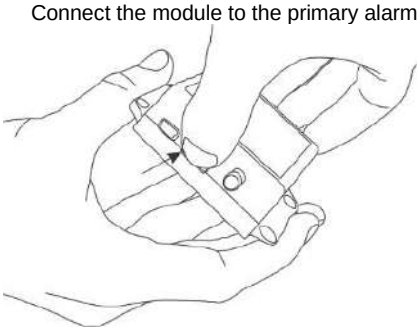


Figure 7 Insert the SIM card

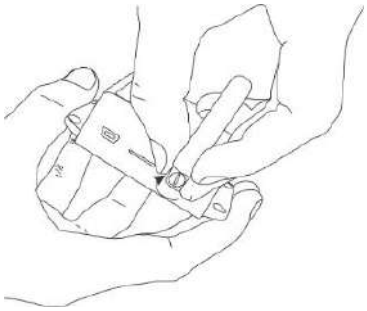


Figure 8 Screw the GSM antenna

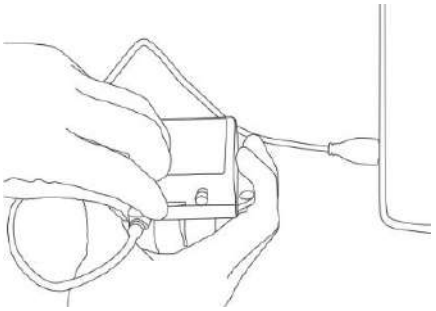


Figure 9 connect the module to the computer

3.1 Communicator wiring methods

- The GTCOM2 module enhances third-party security systems with PSTN communicators by providing GSM/LTE/IP connectivity.
- It uses a RING/TIP PSTN interface to connect to security panels, converting Ademco Contact ID data into SMS for up to 8 users, and reports to the CMS using the SIA IP DC-09 protocol.
- With two digital inputs, the GTCOM2 monitors the security panel's ARM/DISARM/STAY states and other alarms, immediately sending SMS and calls upon siren activation and reporting to the CMS.
- With two outputs, GTCOM2 controls ARM/DISARM states and remote gate access, linking to keyswitch-configured zones for partition control.
- The module's status synchronizes with the control panel, shifting between ARM and DISARM as required. It also displays the system status on the SERANOVA mobile app.

The GTCOM2 can be connected to a security panel in two ways:

1. Connection solely to the PSTN communicator for receiving all events from the security panel, and relaying these events as **readable SMS** to user mobiles, as **push notifications** to the Android/iOS **SERANOVA** App, and to the **Central Monitoring Station receiver** via the internet using the SIA DC-09 protocol.
2. Connection to the PSTN communicator with added remote ARM/DISARM control of the alarm panel through a keyswitch zone.

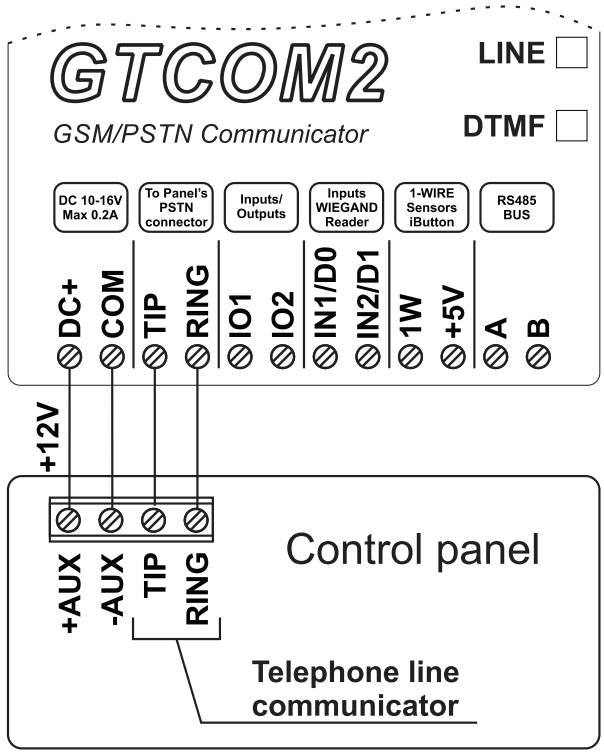


Figure 10Communicator wiring diagram

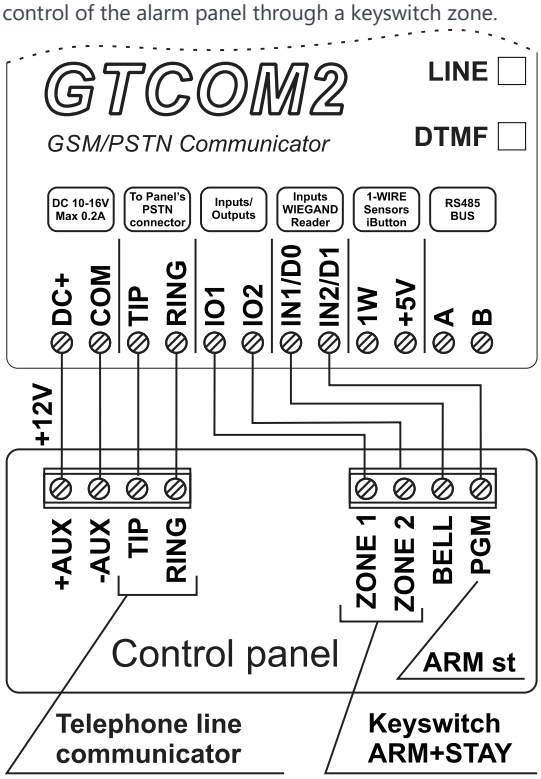


Figure 11 ARM the panel via keyswitch zone

3.2 Programming the Primary PSTN Alarm Panel

The configuration of the panel's PSTN communicator should be similar to event transmission to the monitoring station receiver using the CONTACT ID DTMF protocol. The module can work with any central panel that has a PSTN communicator and adheres to the Ademco Contact ID data format as per the SIA DC-05 standard. Additionally, the central panel must support phone number dialing using DTMF tones. (Note: Pulse dialing is not supported by the GTCOM2).

Configuring the Panel's PSTN Communicator for CONTACT ID DTMF Protocol:

- Ensure the central panel supports the Ademco Contact ID format (SIA DC-05) and DTMF tone dialing (Note: Pulse dialing is incompatible with GTCOM2).
- Activate the panel's PSTN dialer
- Set a 4-digit communicator account (e.g., "1234").
- Input the monitoring station receiver's phone number (GTCOM2 responds to any number over 2 digits). **
- Set communication dialing options to [DTMF Dialing].
- Set Communications protocol to [DTMF Contact ID].
- If available, activate [Contact ID Automatic Reporting Codes].
- Enable relevant PSTN communication events (Open/Close/Alarm/Restore/Maintenance/Test).

Panel's Settings for Two-Way ARM/DISARM Synchronization*:** *[APP/Call/SMS/iButton] <->GTCOM<->PANEL<-> [Panel Keyboard]*

- **Set Panel PGM to monitoring ARM status in level (steady) Mode**
  - Activation event: [ARM Area1]
  - Deactivation Event: [DISARM Area1]
  - Mode: [Steady]
  - NO/NC depending of GTCOM22 input keyswitch settings.
  - In our example set to [NO]
- **Set Panel Keyswitch Zone to Momentary (Pulse) Mode) to receive ARM/DISARM signals from the GTCOM2 [System Armed state] Output PGM.**
  - Zone Type: [Keyswitch Momentary] (Pulse)
  - Area Assignment: [Area 1] (Set AREA you want to control)
  - Keyswitch Action: [ARM/DISARM]

*The communicator supports the SIA Ademco CONTACT ID data package protocol (as per the SIA DC-05 standard).
**The telephone number and data transfer format are DTMF (tone).
*** Two-way ARM/DISARM synchronization allows the USER to control the panel via the panel's keyboard as well as remotely from the GTCOM2 APP/WEB/SMS/iButton/RFID/Call. This ensures that the GTCOM2 APP displays the same system status as the security panel's keyboard.

GTCOM2 do not accept pulse dialing from PSTN communicator

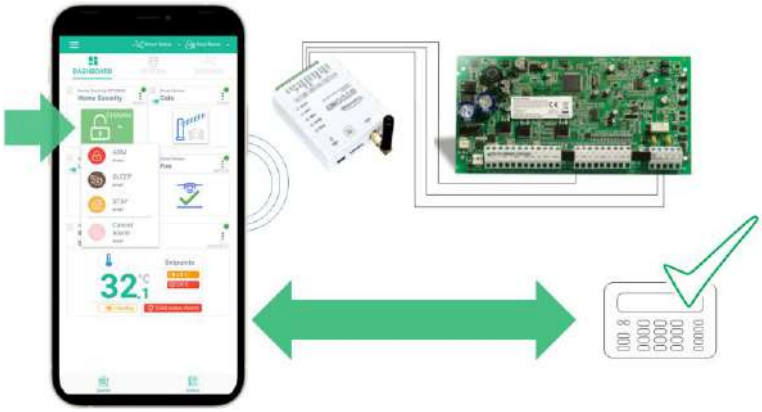
3.3 Remote ARM/DISARM of Primary Alarm Panel Using GTCOM2 with SERANOVA App

It is possible:
- To control primary alarm panel from **SERANOVA** app and see the panel status
- To control primary alarm panel from keypad and see the same status in **SERANOVA** app

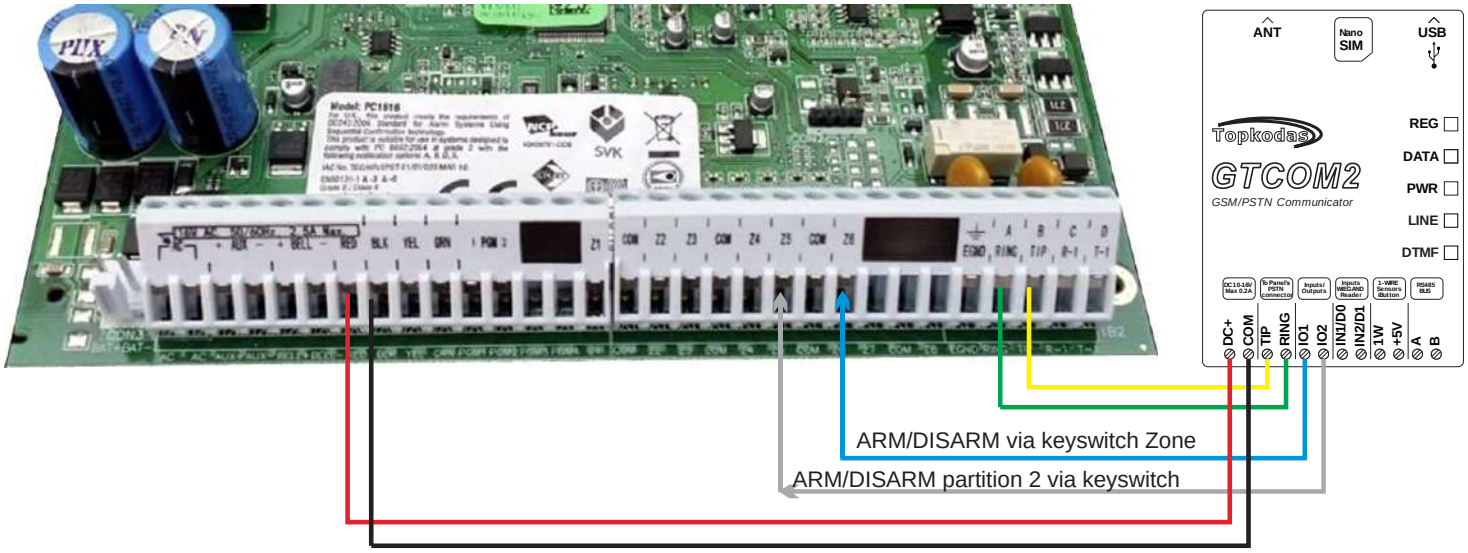
GTCOM2 & Primary Alarm Panel Synchronization
Synchronize alarm panel status with the GTCOM2 SERANOVA app in two ways:

1. Through primary panel events: GTCOM2 updates its SERANOVA app status with each Open/Close event from the main panel.
2. Via the panel's PGM output ARM state: a faster method, but it requires an extra wire to the PGM for status monitoring.

Open/Close synchronization allows panel control via keypad or remotely through the GTCOM2 **SERANOVA** app /web/SMS/call, ensuring the app reflects the panel's actual status.

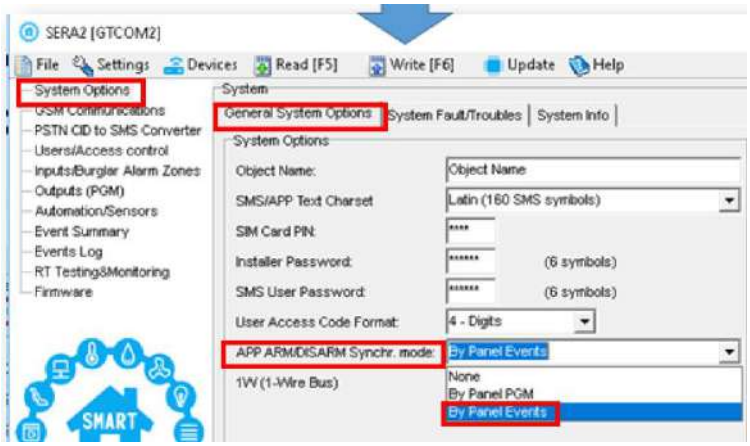


3.3.1 GTCOM2 and primary alarm panel synchronization [by Panel's EVENTS]



Wiring:

- TIP/RING
- GTCOM PGM -> Panel Keyswitch (pulse mode)



Set system status synchronization mode [By Panel Events]:

- Go to *SERA2> System Options> General System Options*
- Set App ARM/DISARM Synchr mode to **[By Panel Events]**

Set module PGM action on ARM/DISARM command from APP/CALL/SMS/iButon/RFID

- Out Definition: [Activate by ARM/DISARM Command]
- No: [1] (this is partition number)
- Mode: [Pulse]
- Timer: [2s] (this is PGM pulse time on ARM/DISARM command)

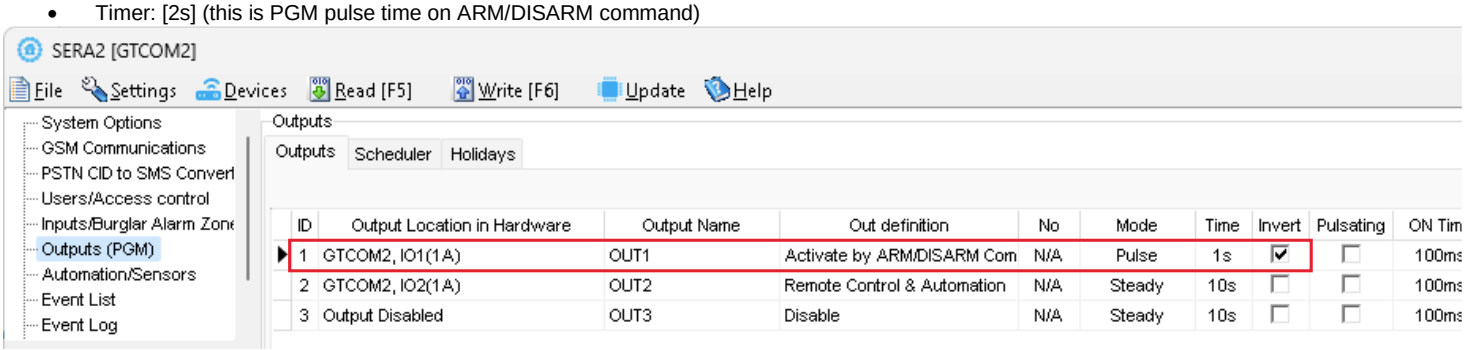
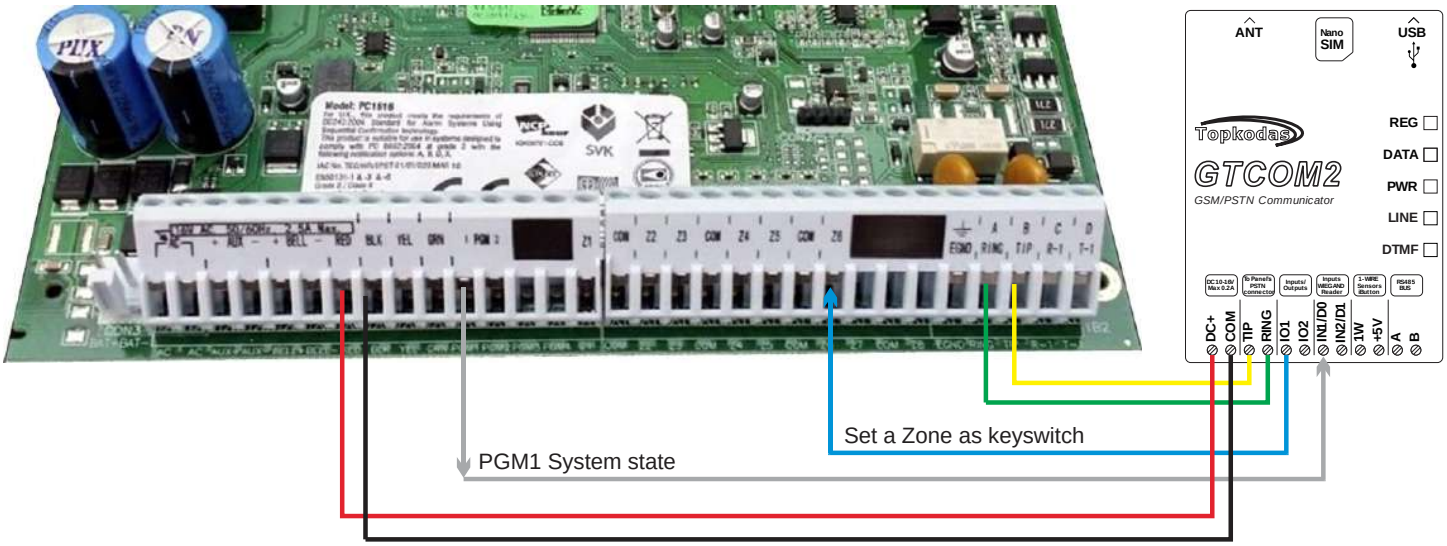


Figure 12SERA2> Outputs (PGM)

3.3.2 GTCOM2 and primary alarm panel synchronization [by Panel's PGM]

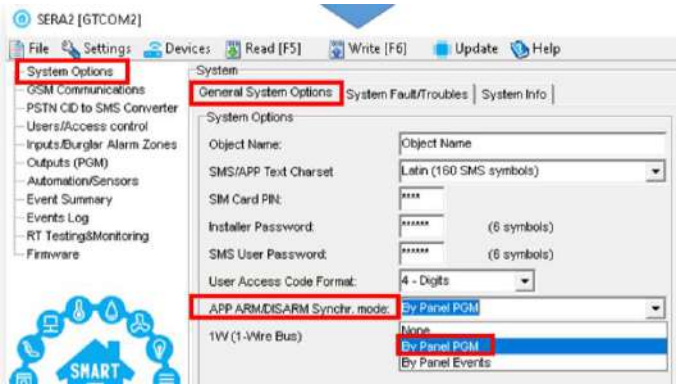


Wiring:

- TIP/RING
- GTCOM PGM -> Panel Keyswitch zone (Pulse mode)
- GTCOM Keyswitch <- Panel PGM (Level Mode)

Set system status synchronization mode [By Panel PGM]:

- Go to *SERA2> System Options> General System Options*
- Set App ARM/DISARM Synchr. mode to **[By Panel PGM]**



Set GTCOM2 keyswitch zone

- Go to *SERA2> Inputs> Burglar Alarm Zones and set:*
- Keyswitch Zone Mode: [Level] (Steady)
- Definition: [keyswitch ARM/DISARM]
- Type: [NC]
- Press [Write]

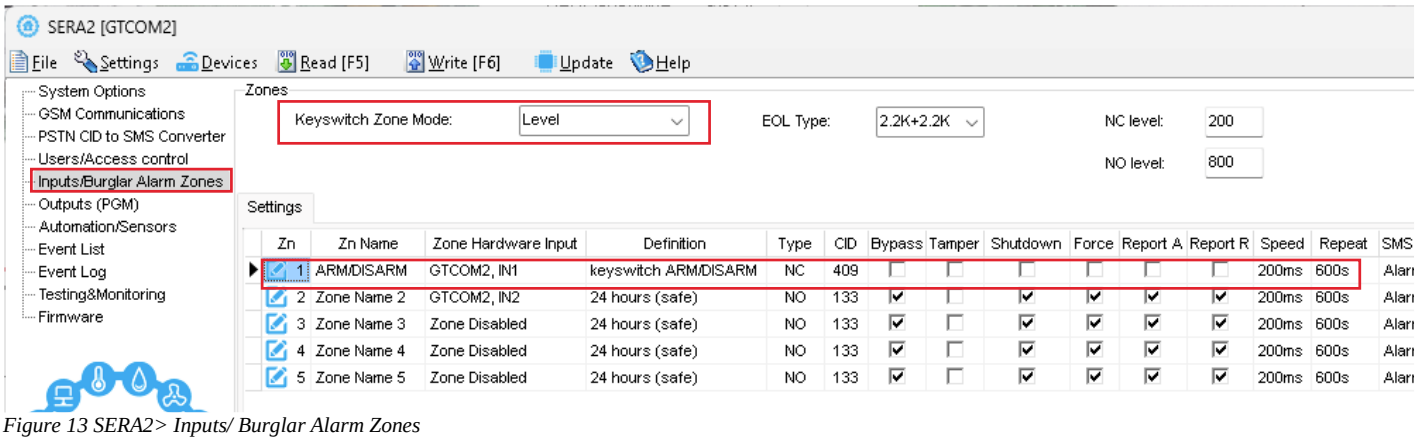


Figure 13 SERA2> Inputs/ Burglar Alarm Zones

Set module PGM action on ARM/DISARM command from APP/CALL/SMS/iButon/RFID

- Out Definition: [Activate by ARM/DISARM Command]
- No: [1] (this is partition number)
- Mode: [Pulse]
- Timer: [2s] (this is PGM pulse time on ARM/DISARM command)

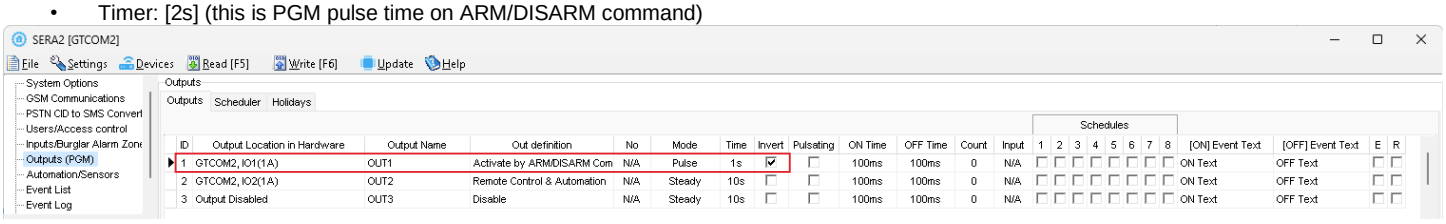
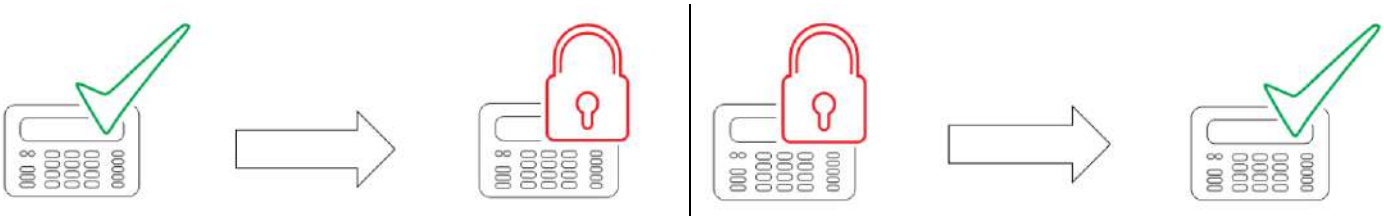


Figure 14 SERA2> Outputs (PGM)

3.4 How to Test Synchronization between GTCOM2 and the Primary Alarm Panel

STEP by STEP:

- Navigate to SERA2 > RT Testing & Monitoring > Hardware.
- Click the **[Start Monitoring]** button.
- Press **[I/O1 On/Off]** button.
- Observe the change in Inputs (ADC values); they should switch from 1 to 0 or 0 to 1.
- The status of the primary panel should change accordingly.



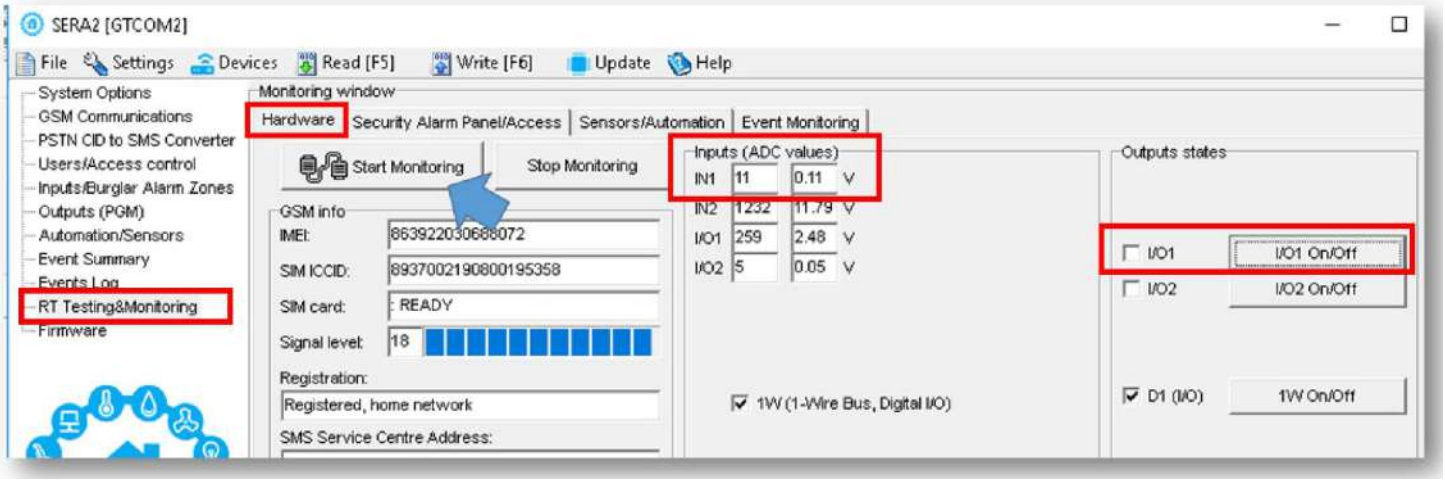


Figure 15 SERA2> RT Testing & Monitoring> Hardware

- Go to SERA2> RT Testing & Monitoring> Security Alarm Panel/ Access
- The status of GTCOM2 module should change

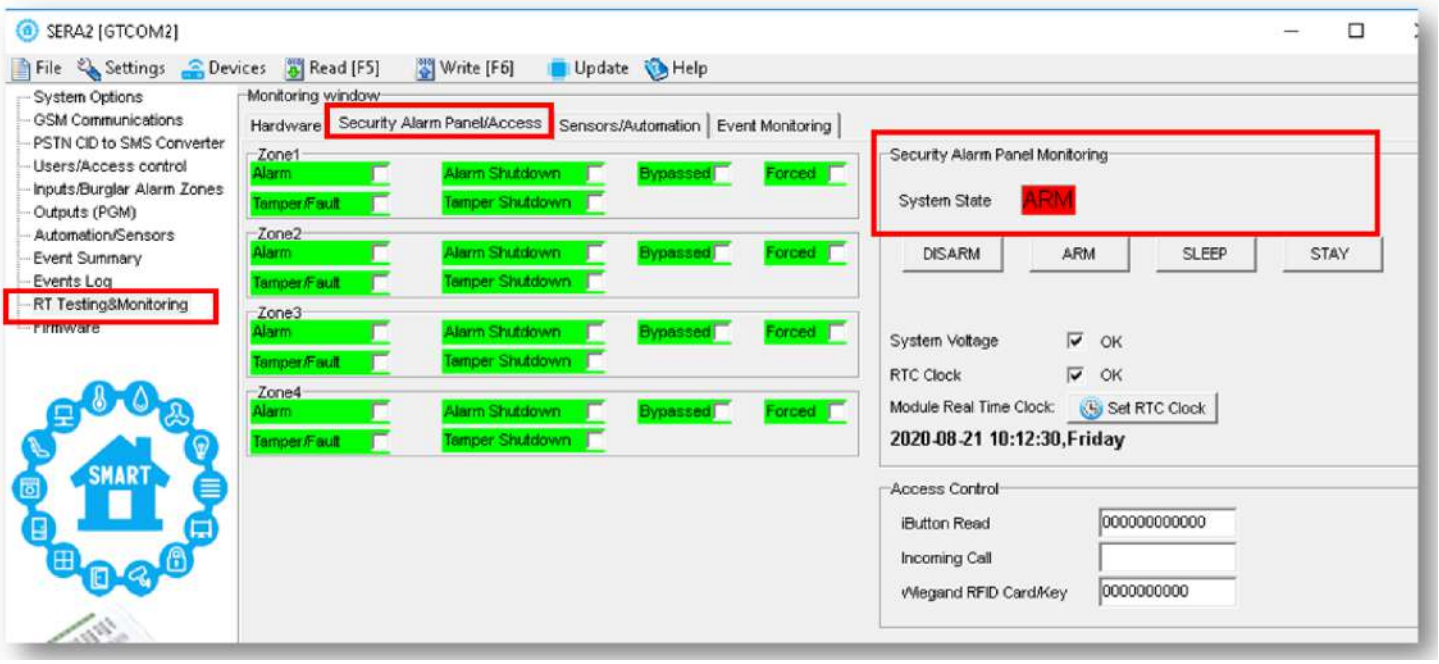


Figure 16 SERA2> RT Testing & Monitoring> Security Alarm Panel/ Access

You will see the same process on your smartphone in the mobile app as well.

3.5 GTCOM2 Communicator - Converter for Ademco Contact ID codes into SMS text

The GTCOM2 communicator simulates the operation of a PSTN phone line and receives Contact ID messages from the security control panel.

All information from the security control panel to the module is transferred in DTMF tones. The security control panel must support tone (DTMF) dialing and data transfer using the CONTACT ID protocol in DTMF tones. Pulse format is not supported.

From the security control panel receives CONTACT ID message as follows:
ACCT MT Q XYZ GG CCC S

ACCT - 4-digit number.
MT - message type 18 or 98 CONTACT ID message.
Q - event qualifier:
- 1 = Alarm, new event or opening
- 3 = Restore or closing
- 6 = event state report

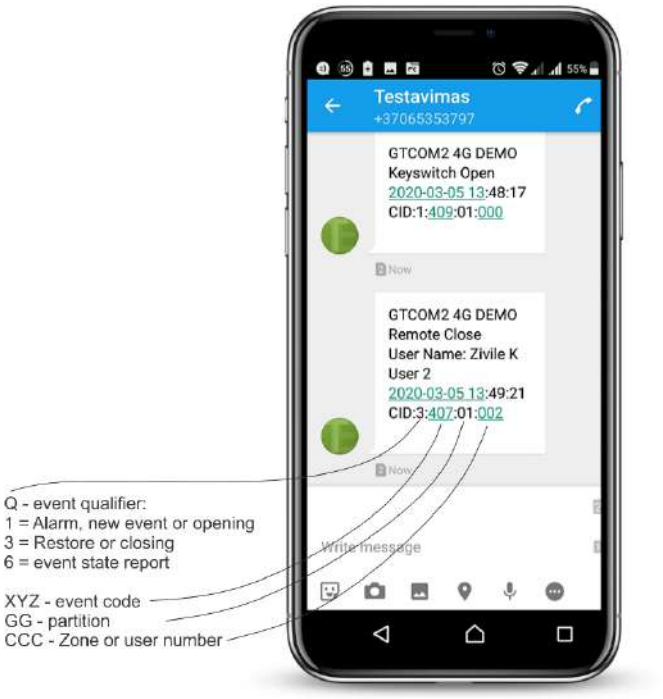
XYZ - event code (3-digit Hex 0-9,B-F) see annex
GG - 2-digit subtype number.
CCC - Zone or user number depending on what type of message has been received.
S - Control sum of the message.
The following message codes are being described in order to convert CONTACT ID message into SMS text:

O:XYZ:GG:CCC

- Q: Event qualifier
- XYZ: Event code
- GG: Partition
- CCC: Zone/user number.

CONTACT ID messages are described in Sera2> PSTN CID to SMS converter window in 3 tables: [XYZ], [GG], [CCC]

Event description text can be modified, allowing for the generation of desired text for every received CONTACT ID message.



Steps for setting up Contact ID protocol to SMS text conversion in Sera2:

- Go to *Sera2 > GSM Communication > SMS/DIAL Reporting*. Enter phone numbers, mark '**Other Events**', and edit other settings.
- Go to *Sera2 > PSTN CID to SMS Converter > [XYZ] Contact ID Event Code*. Edit text in "Alarm SMS Text", "Restore SMS Text", and select event type as: ZONE/USER/NONE.
- Go to *Sera2 > PSTN CID to SMS Converter > [CCC] User/Zone Name*. Enter User/Zone Name.
- Edit partition name in *Sera2 > PSTN CID to SMS Converter > [GG] Group or Partition* window.
- Enter phone numbers for remote control in Sera2 > Users/Access Control window. And mark ARM/DISARM checkbox
- Click [Write]

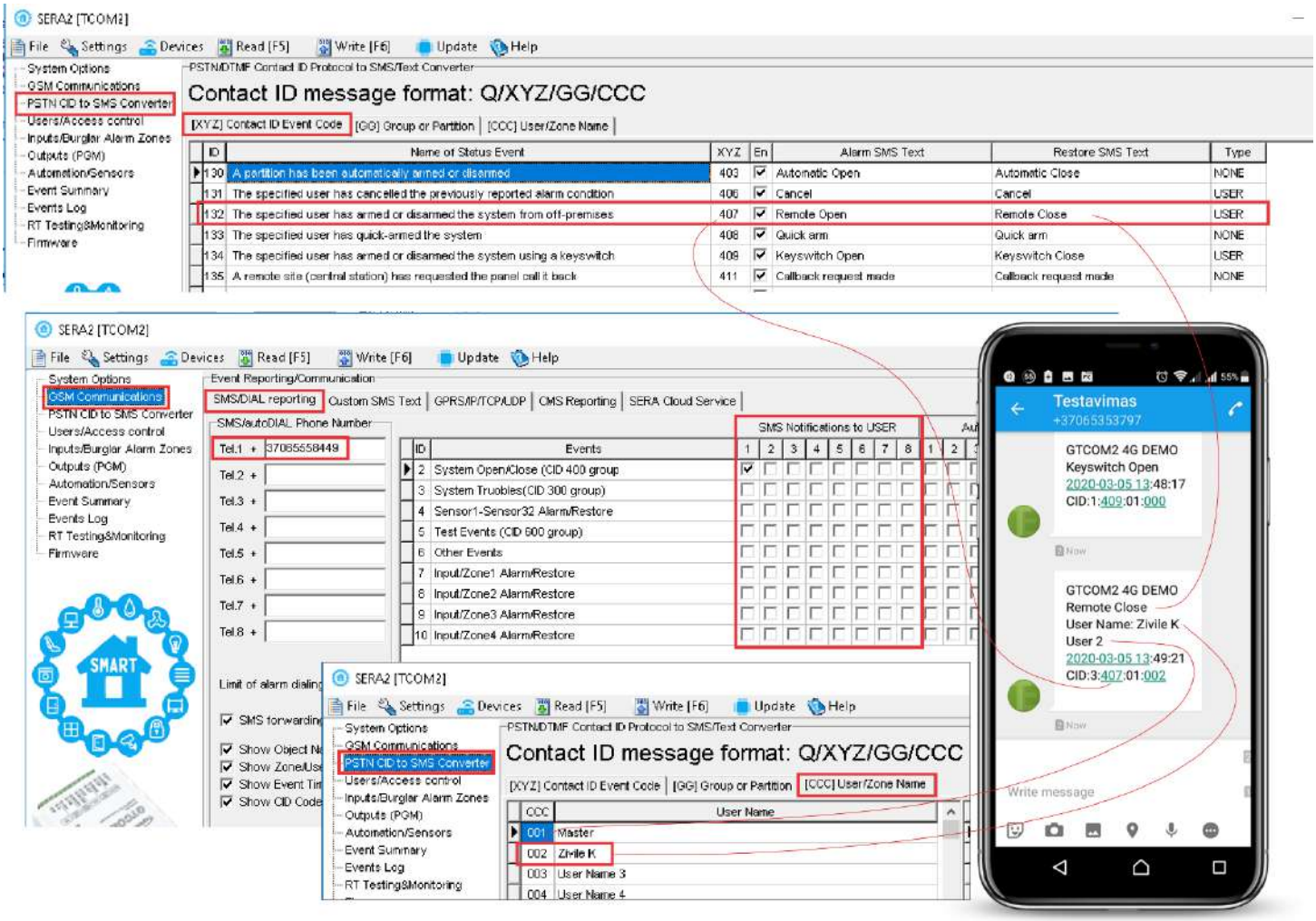
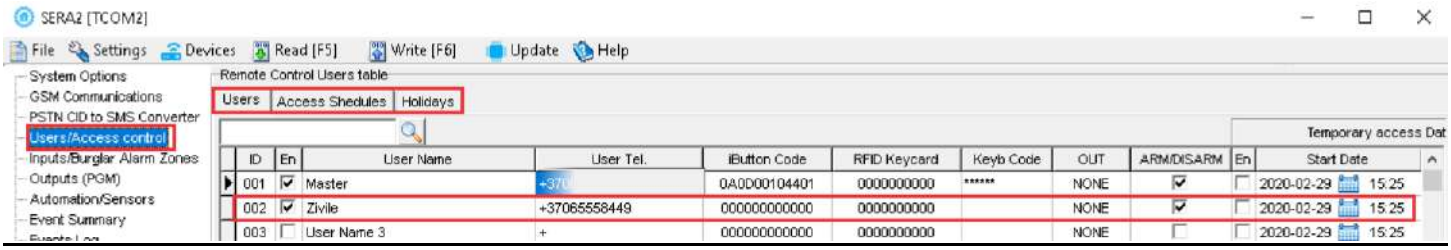


Figure 17 Sera2> PROGATE> PSTN CID to SMS Converter



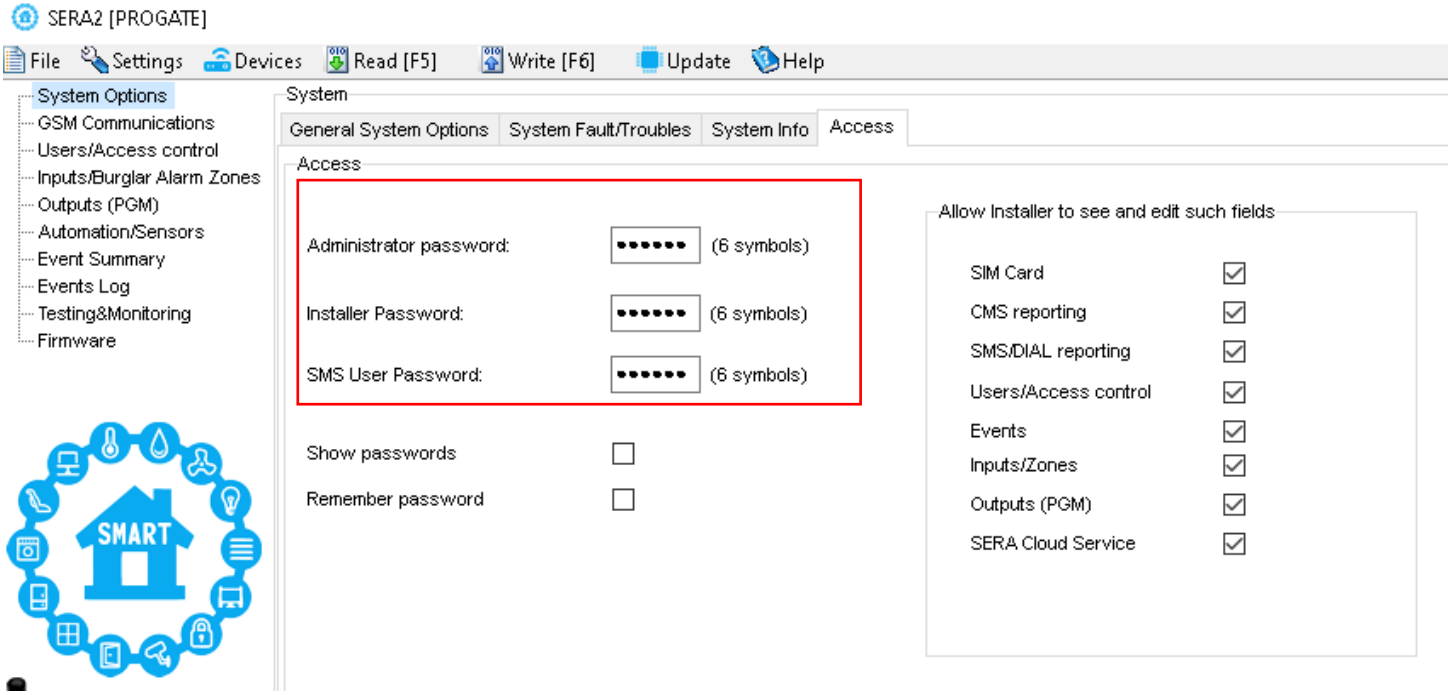
Refer to:
[Access control. Arming/Disarming methods]
[Users & Access Control programming details.]
[DISARM /ARM/SLEEP/STAY the security system]
[Reporting SMS&Dial in Case of Alarm Events]

4 SYSTEM ACCESS: CODES, PASSWORDS, AND PERMISSIONS

4.1 Default Codes/Passwords and Explanations

Table 5 Default passwords and explanations

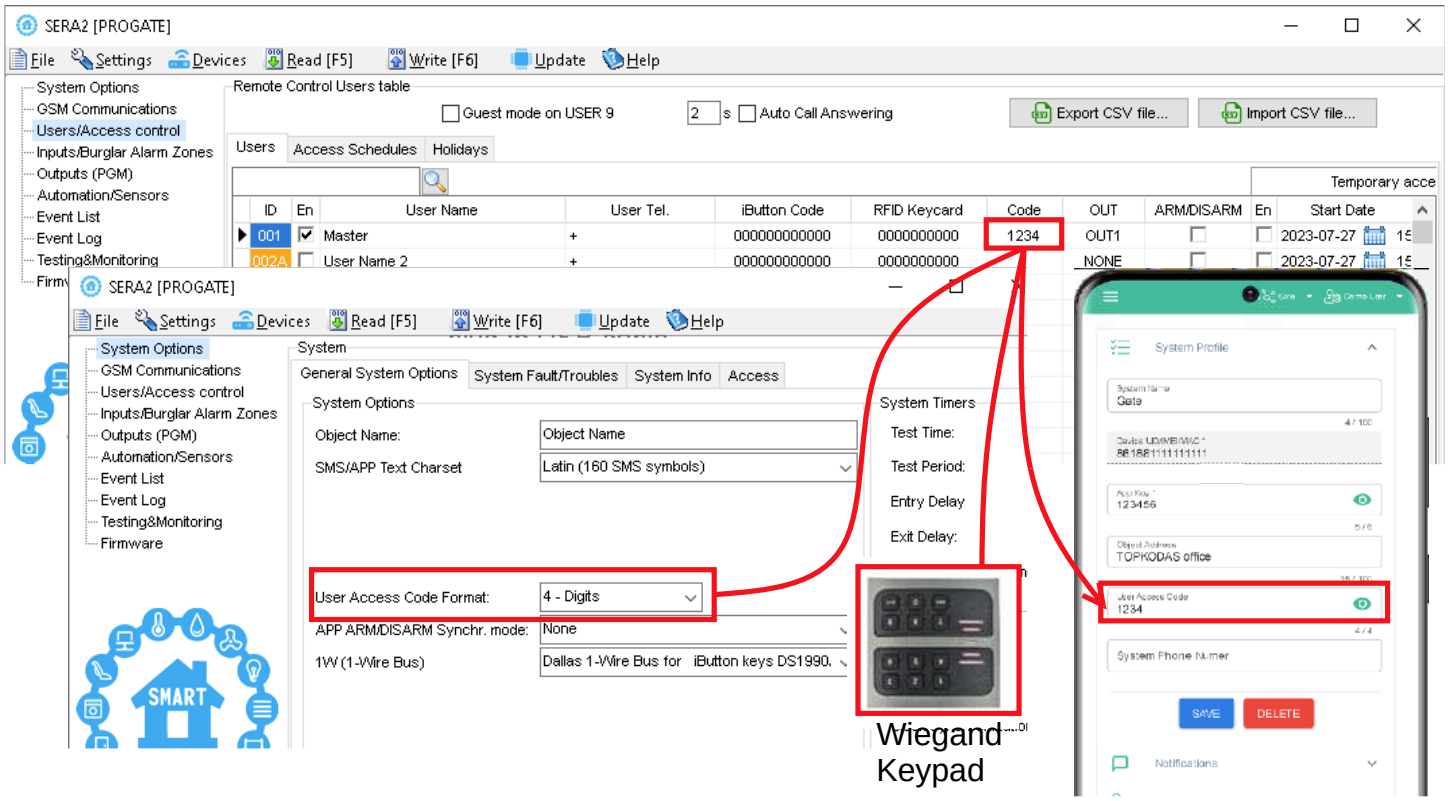
Password	Default	Location in SERA2	Explanation
Administrator password	123456	SERA2> System Options> Access	The **'Administrator password**' allows full module configuration access. The system administrator can adjust device settings, update firmware, and set permissions for the **Installer**, specifying which parameters they can modify. This ensures protection of sensitive data such as IP addresses, phone numbers, and other confidential information.
Installer Password	000000	SERA2> System Options> Access	The 'Installer password' allows sending SMS commands with INST identification and provides access to SERA2's programming mode. However, the Installer can only modify or see those module settings in SERA2 that the system administrator has granted permission for. Refer to section *9.1* for more details.
SMS User Password	123456	SERA2> System Options> Access	The '**SMS User Password'** permits sending SMS commands with **USER** identification. The user phone number must also be authorized for remote or SMS control. The default SMS user password is 123456, used for module control with USER commands. Refer to section *9.2* for more details.
App Key	123456	SERA2> GSM Communications> Sera Cloud Service	The **'APP Key**' links to the **'SERA Cloud service'**, allowing remote access through the **SERA2** or **SERANOVA** app. For a successful connection, the code must match on both the device and app. ! For users with multiple systems, use the same '**App Key'** across all systems. Different App Keys on the same SERANOVA account can cause functionality issues.
User Code (APP/Keyboard)	123456	SERA2> Users/Access> Users Table[Code] column	The **'User Code**' is a unique identifier for controlling the system via the **SERANOVA** app or **Wiegand keypad**. The default **Master Code** is 1234 or 123456, based on the format. ! This code must match on the device and in the **SERANOVA** app under *Settings > System Profile > User Access Code*. Without the correct code, users cannot control the system.
SIM card PIN	1234	SERA2> GSM Communications> Network/SIM Card	It is automatically ignored if pin request in SIM card is disabled



4.2 User codes for access control via keypad and SERANOVA app

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

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



4.3 Access control. Arming/Disarming methods

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

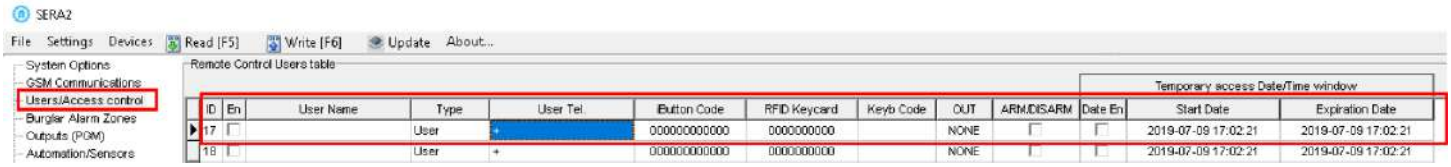
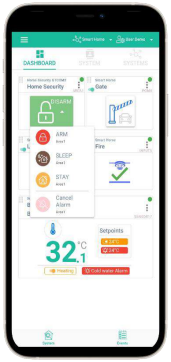


Figure 18Users/ Access control window

Arming and Disarming the System Using the SERANOVA Mobile/Web App

Press on ARM, ARM (Stay), ARM (Sleep), or DISARM in the Mobile/Web App > System window.
How to start Android app see section: *2.8 SERANOVA (Android/iOS/Web) app*
Add new system in app

- Default App Key: 123456
- Default User Access Code: 123456
- Go to SERA2> System Options> General System Options
- IMEI:



Arm/Disarm by call

- From one of the 800 registered numbers, dial the system's number to arm/disarm or turn off the alarm.
- Unlisted numbers are ignored.
- Calls are free as the system rejects them after recognizing the number.
- Toggle arming permissions for specific numbers in the “Users & Remote Control” settings.

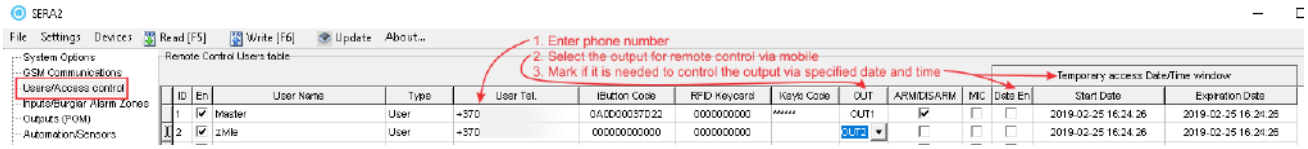


Figure 19 ARM/ DISARM by call settings

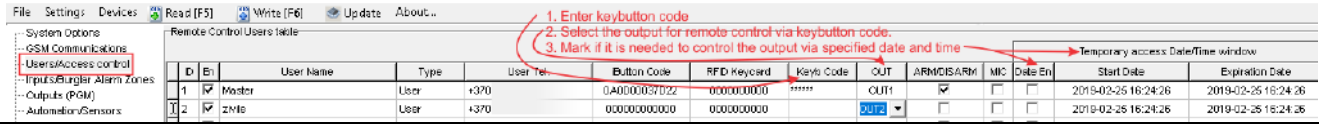
Arm/Disarm via SMS

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

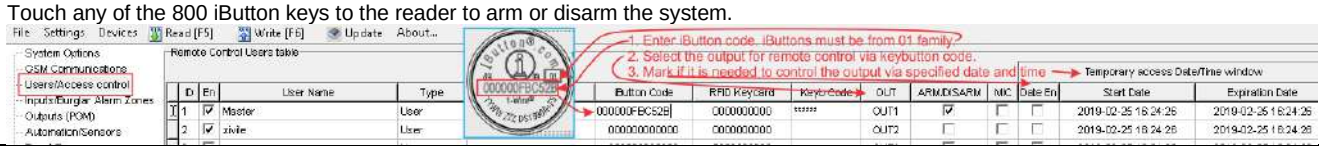
Arm/Disarm by Wiegand keypad

- Arm or disarm using the Wiegand Keypad by entering the User/Master Code.
- To cancel arming, re-enter the code during the exit countdown.
- Disarm and turn off alarms by entering a valid user or master code.



Arm/Disarm by iButton key

Touch any of the 800 iButton keys to the reader to arm or disarm the system.



Arm/Disarm by RFID key card, keyfob

Touch one of the 800 available RFID keycards to the Wiegand keypad to arm or disarm the system.

If you want to edit existing configuration,
Press [Read]
Edit settings
Write edited configuration press [Write]

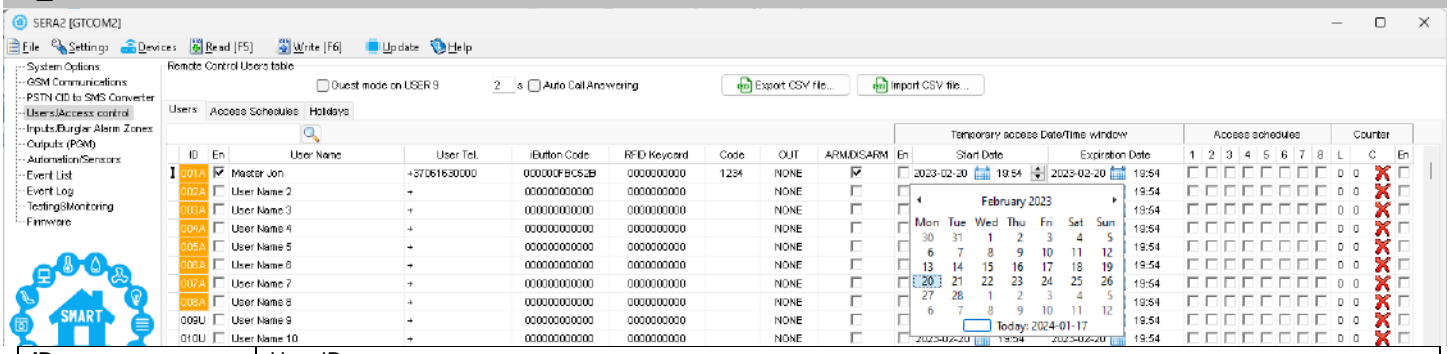
More information about how to configure Arming/ Disarming:

4.4 Users & Access Control programming details.

SERA2>Users/ Access Control > Remote Control Users Table

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



ID	User ID	
En	User Enabled	
User Name	The name of users who will be able to control the module should be entered in this column.	
User Tel.	In this column, you need to enter the phone numbers of the users who will be able to control the module with a call. User number should be entered with international code.	
iButton Code	iButton Maxim iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000	
RFID Keycard	RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000	
Keyb Code	Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000	
OUT	The selected output is activated if the user makes a call from this number. Preferred output may be assigned to each user's number. Thus different users are able to control different objects.	
ARM/DISARM	If this checkbox is ticked, the user will be able to activate/deactivate the security system with a call.	
MIC	If checked, by calling from the specified phone, the controller responds and you can hear what's going on in the premises	
Temporary access	**Date EN**	Temporary access enable
	Start Date	Temporary access start date and time
	Expiration Date	Temporary access expiration date and time
Access Schedules	Access Schedules enable users to control the system within specific time intervals	

The GTCOM2 module offers User Access Schedules, allowing system control within set time intervals for actions like ARM/DISARM, output control via iButton readers, cards, the SERANOVA app, or calls. For instance, users can manage specific outputs from 12:00 a.m. to 6:00 a.m. daily. Set and view these schedules in the 'Users > Access Schedules' tab."

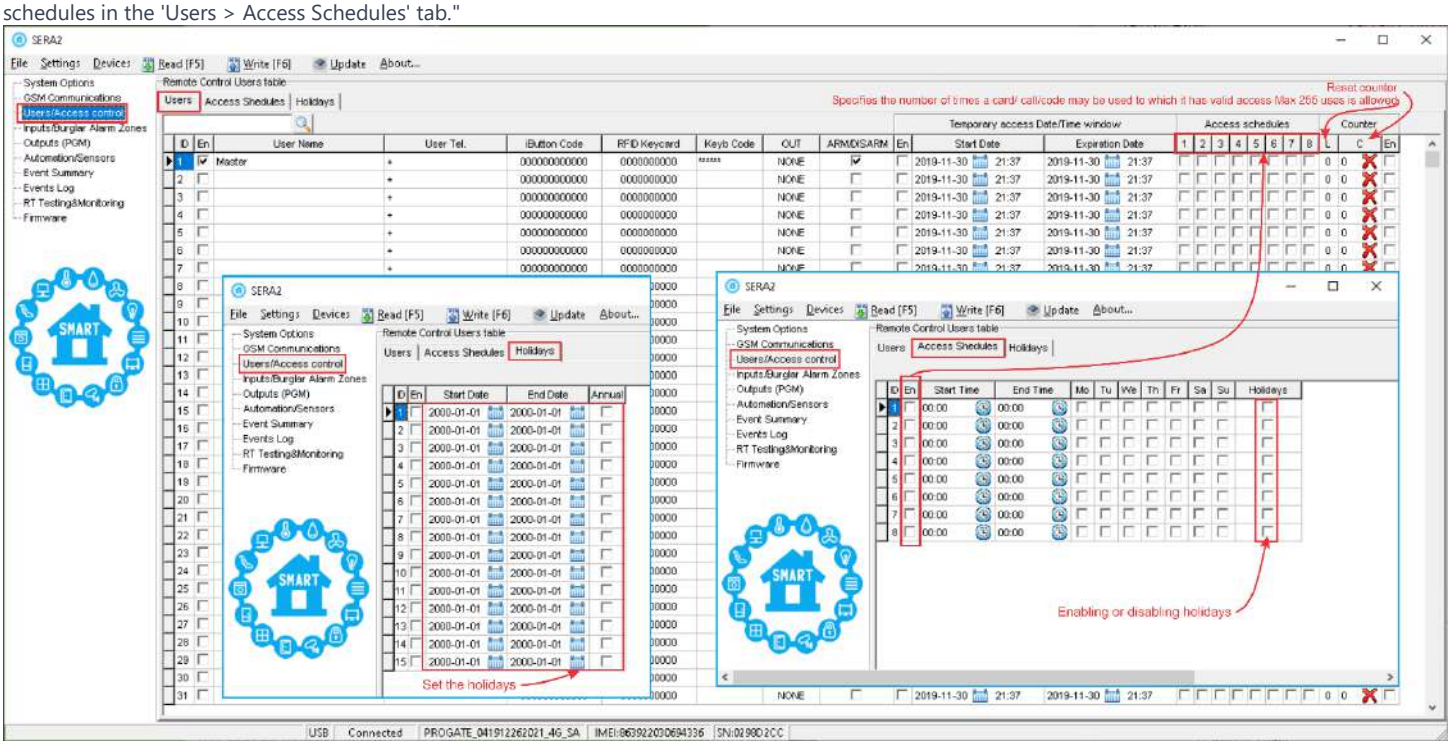


Figure 20 Users/ Access Control > Users, Users Access Control> Access Schedules and Users/ Access Control> Holidays window

Set System Clock and Time Zone:

- Navigate to: *Sera2 > System Options > General System Options.*
- Set your desired time zone and synchronize the clock.
- Press [Write].
- See: *8.2 Real-time clock Time Zone and Synchronization*

RFID/iButton/Phone Programming:

- Go to: Sera2 > System Options > General System Options.
- Press: [Start iButton/RFID/Phone programming mode]
- Open: Sera2 > Users/ Access control window.
- Touch RFID keycards or iButton keys to the reader.
- Call the module from your mobile. The list should include scanned RFID cards, iButtons codes and phone numbers.
- Navigate back to: System Options > General System Options.
- Press [Stop programming] (or wait for automatic stop).
- Adjust settings as needed in the Users/ Access control window.
- Press [Write].

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

An example of user access:
Let's say need to create a Cleaning Crew schedule as follows: Monday-Friday from 5 p.m. to 1 a.m., and Saturday-Sunday from 8 a.m. to 1 p.m., excluding holidays. This results in three schedules:

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

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

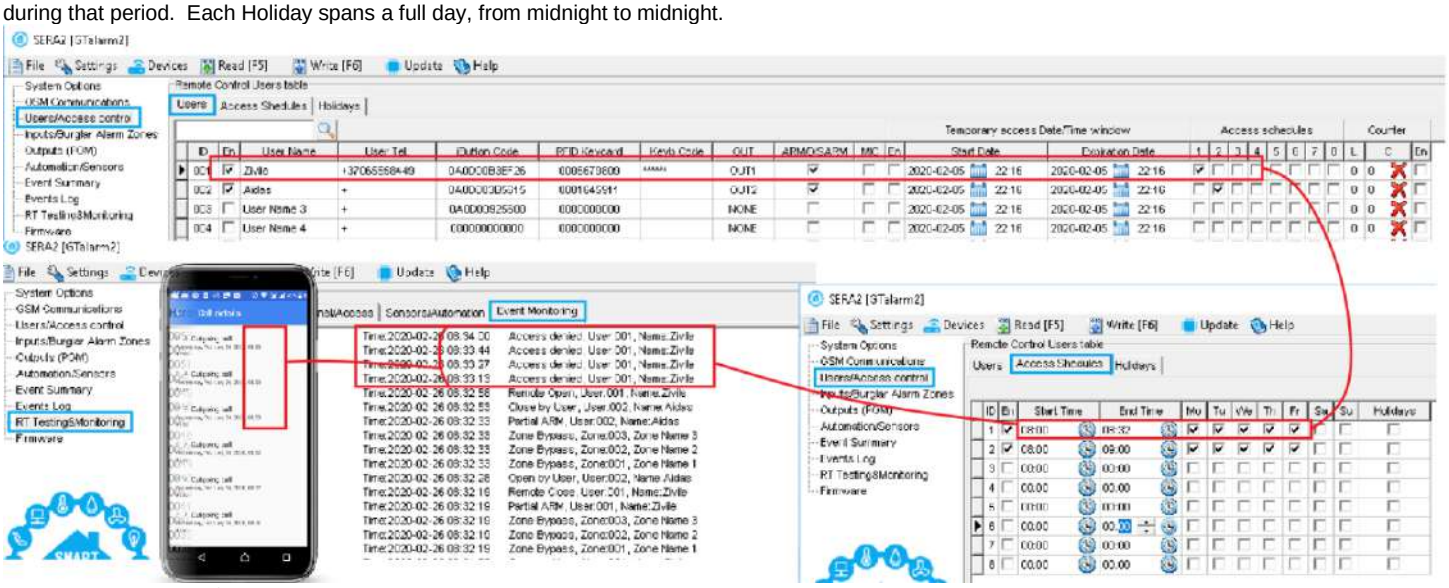


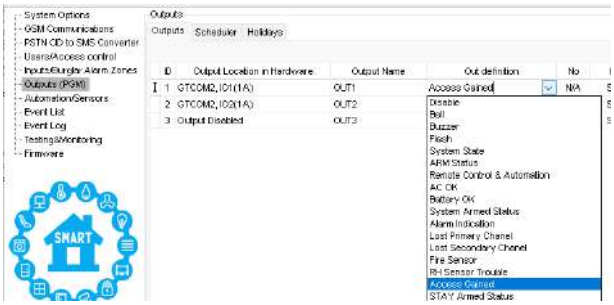
Figure 21 the example of schedule

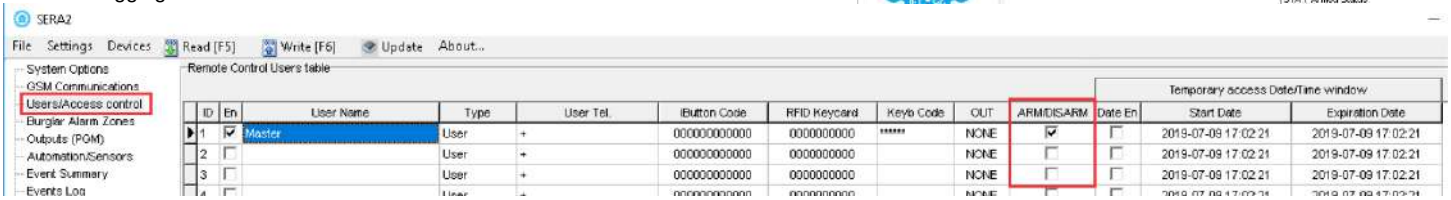
The module can be controlled only by these users, whose phone numbers entered in the memory of the module

Exclusive Control of the GATE/Door only for ARM/DISARM Authorized Users

Configuring **[Access Gained]** Output

- Define the output as [Access Gained] to permit user control when the system is disarmed (Sera2 > Outputs).
- Users with ARM/DISARM privileges can always access this output.
- Users without ARM/DISARM privileges can access the output only if the system is disarmed (unchecked in Sera2 > User/Access Control).
- Access attempts are logged: 'Access Granted' (421) or 'Access Denied' (422) in the Event Log (Sera2 > Events Log).
- Outputs with [Automation / CTRL] definition can be user-controlled without logging events 421 or 422.





Event log e.g.

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

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

Wiegand keypad specifications:
Wiegand Terminals: **D0 / D1**
26bit, 34bit Wiegand (Default);
Keypad Operation: 4bit, 6bit, 8-Bit Burst Output. Each single key press as 4,6,8-bit code

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

Figure 22 Wiegand keypad wiring

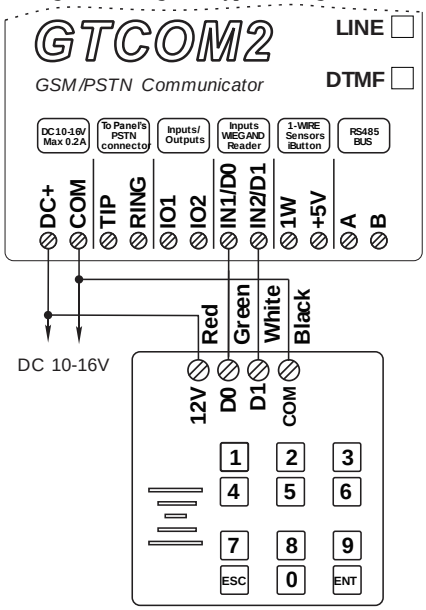


Figure 23iButton connecting diagram

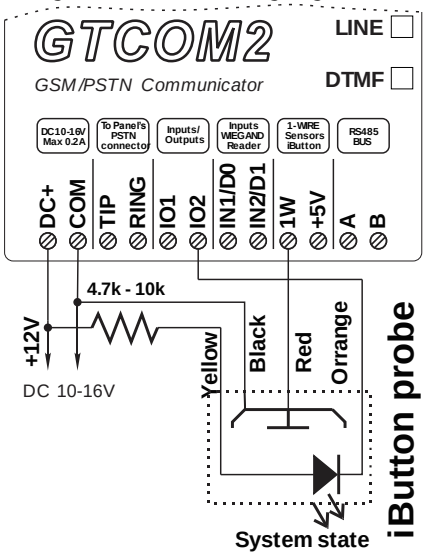
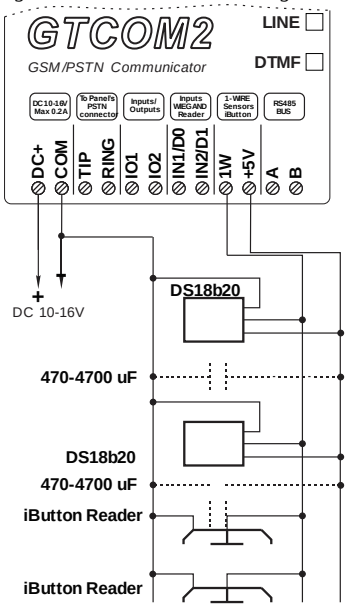


Figure 24 iButton connection diagram



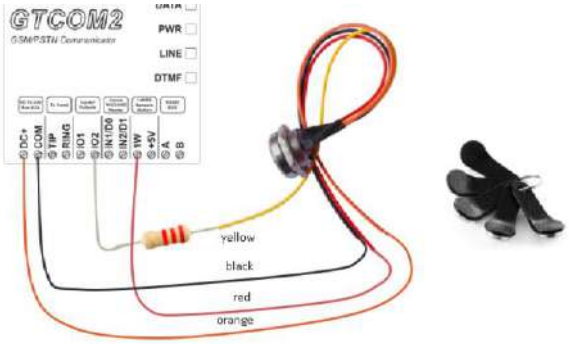


Figure 25 iButton probe wiring

4.6 Programming 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.

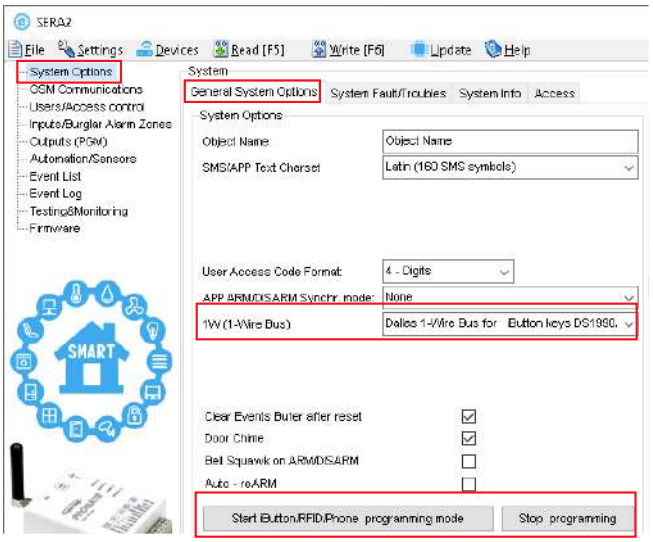
Configuration methods:
- Start automatic learning mode via mini-USB cable (SERA2 software).
- Start automatic learning mode via SMS command INST000000␣063␣1
- Enter Keycard numbers manually via mini-USB cable (SERA2 software).
- Start automatic learning mode remotely via SERA2 software.

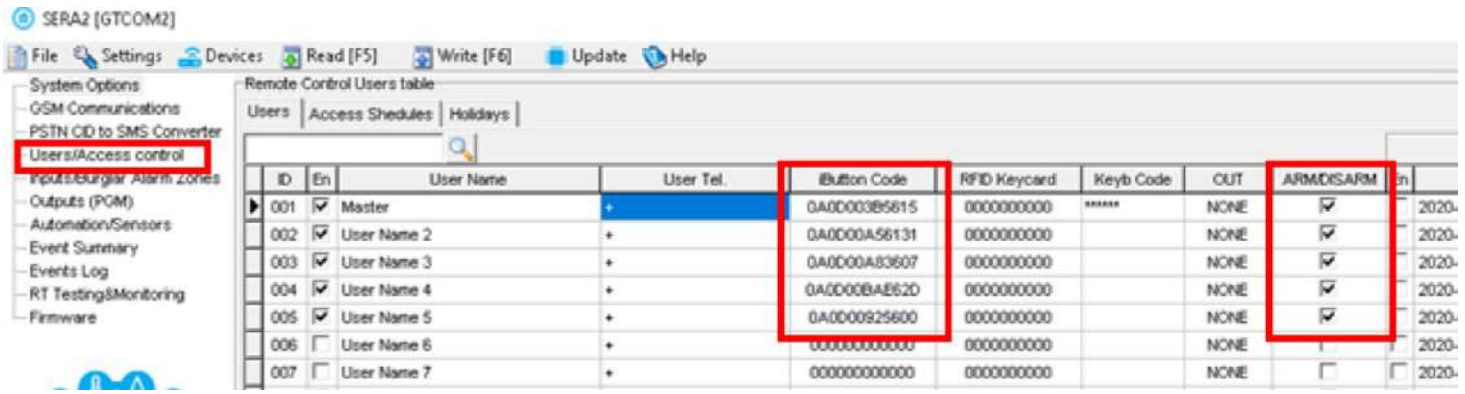
- The First iButton key could be learned (recorded) by touching it to the reader. Without the need to send any SMS. The first key is the main key (MASTER)
- The system will notify about successfully recording of the key into memory by shortly beeping twice via buzzer.
- The system will automatically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

Output definition should be set as “System State”. Go to SERA2> Outputs (PGM)> Set Out definition to “System State” press [Write]

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

- Navigate to *SERA2 > System Options > General System Options.*
- Select 1W (1- wire Bus) to the 'Dallas 1-Wire Bus' option (for iButton keys).
- Click on [**Write**].
- Click on [**Start iButton/RFID/Phone Programming Mode**].
- Navigate to *SERA2 > Users/Access Control*.
- Touch the RFID keycards or iButton keys to the reader. The key numbers will appear in the list.
- To finish, go back to *System Options > General System Options* and click on [**Stop Programming**].
- You can edit additional settings in the Users/Access Control window. Remember to click [**Write**] after making changes.
- Go to *RT Testing & Monitoring > Hardware* and click on [**Start Monitoring**].
- Go to *RT Testing & Monitoring > Security Alarm Panel/Access*
- Touch the keycard to the RFID keypad. Check ARM/DISARM action.





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

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

Start the automatic key programming mode remotely via SERA2 software.

- Start SERA2 software
- Go to *SERA2>Settings* and
- Enter required parameters: IMEI/UID and App Key
- Press [**Connect**]
- Go to *SERA2> System Options> General system Options.*
- Select Dallas 1- Wire Bus (for iButton keys)
- Press [**Write**]
- Press [**Start iButton/RFID/Caller ID Learning Mode**]
- Touch RFID keycards, iButton keys to the reader
- Press **[Stop programming]** button
- Or wait until the learning mode will stop automatically

Start the automatic key programming mode by SMS command

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

- Send SMS message: INST000000␣063␣1
- You will receive the message: iButton/RFID/Caller ID Learning Mode is Switched ON
- Touch RFID keycards to the RFID reader.
- Sent the message: INST000000␣063␣0
- You will receive the message: iButton/RFID/Caller ID Learning Mode Stopped
- IButton keys deleting mode. Delete these keys from memory, which will be touched to the reader. Sent the message: INST000000␣063␣2

Refer to: *Error! Reference source not found.*

5 OUTPUTS

The module GTCOM2 has:

- 2 outputs: I/O1 (1A) … I/O2 (1A).
- 1 output: **1W** (10mA, Max Voltage 3,3V) for LED, solid state relays control. ! Max voltage 3,3V
- Outputs can be controlled via short call, SMS, RFID, iButton, or the **SERANOVA** app. This is particularly useful such as gate opening.
- Output alarm parameters may be programmed.
- The system supports automatic scheduling, including holidays.
- Programmable algorithms for outputs operation: CTRL/SMS/DIAL, ARM state, inverting, pulse mode

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

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

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

5.1 Schematic and Wiring of Outputs

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.

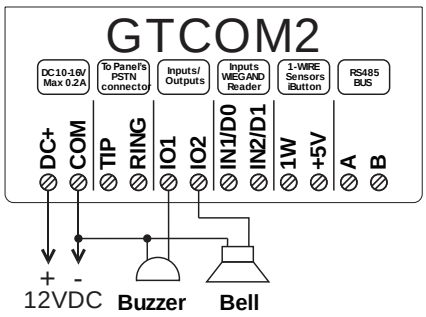


Figure 26 Bell, buzzer connection to I/O1, I/O2

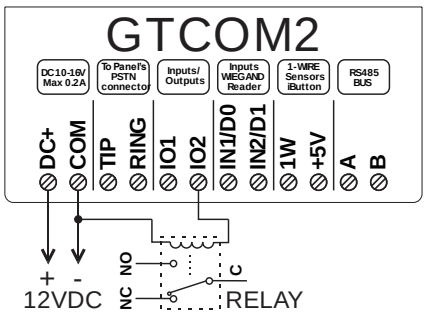


Figure 27 Relay connection to , I/O1, I/O2

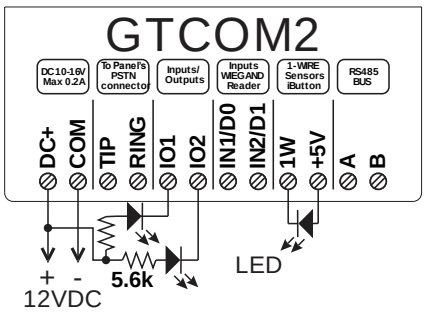


Figure 28 LED connection toI/O1, I/O2

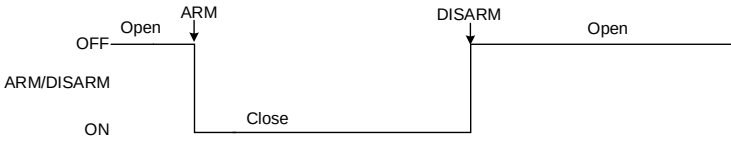
5.2 Output Programming

- Install SERA2 software. For more information look at *2.6 SERA2 software*
- Connect the module to the computer via mini USB cable. Device> GTCOM2
- Go to Outputs (PGM) window in the SERA2 software
- 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.
- State type: flash, timer, steady mode.
- If necessary, output operation might be inverted.
- Write configuration by pressing [Write}
- 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.
- Press [Write]

Refer to:

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

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



6 INPUTS

The module PROGATE has:

- **2 analog inputs IN1, IN2 (0-10V)** 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 (0-10V)** 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 input (1W (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,

- IN1, IN2, I/O1, I/O2 Can be used as inputs to detect System state on the main Alarm Panel as well as Gate position or security system's zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- Connect sensors to module the as is shown in connection diagrams below
- Set the required parameters
- Write configuration by pressing [Write] button

Inputs IN1 and IN2 has internal pull up resistors 10k

Input/Zones wiring NC/NO/EOL/Tamper

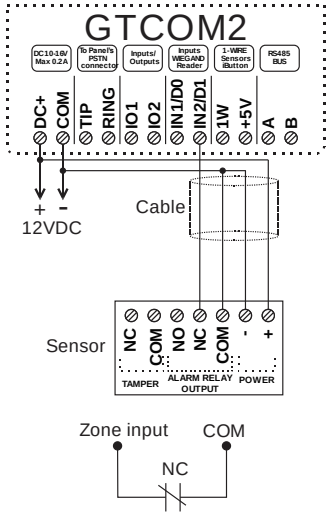


Figure 29NC Contacts, No EOL

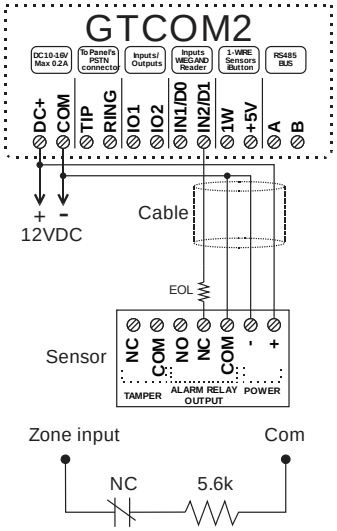


Figure 30 NC, With EOL

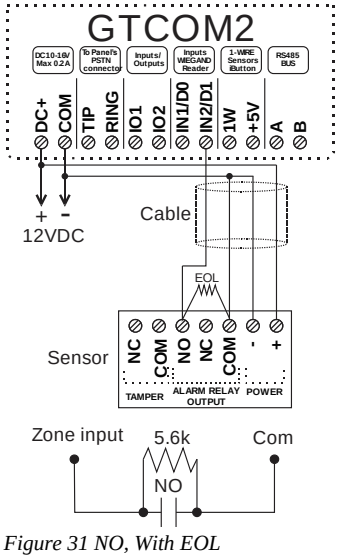


Figure 31 NO, With EOL

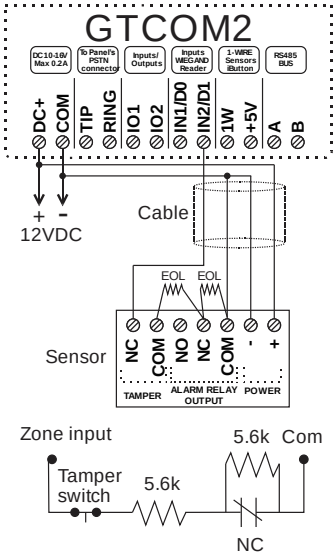


Figure 32NC With EOL Wire Fault Recognition

Programming of inputs Refer to: :

7 SENSORS & AUTOMATION

Sensor Compatibility: Accepts signals from analog 0-10V or digital sensors, configurable with **SERA2** software.
Worldwide Access: Utilizes GSM GPRS networks for global data monitoring and control via **SERANOVA** app or WEB
Applications:

- Enables versatile remote access for data viewing, alarm notifications, and data logging from any location.
- Suitable for monitoring various environmental such as temperature and humidity.
- Applicable in labs, museums, warehouses, and more

7.1 Humidity sensors AM2302/DHT22/AM2305/AM2306/AM2320/AM2321

The module supports Aosong 1-Wire bus Humidity Sensors AM23xx series: AM2302, DHT22, AM2320, AM2305, and AM2306.

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 contains datasheet values: Aosong specifies 'typical' values without maximum tolerances
Sensor AM23xx sensor connects on 1-Wire bus line to digital input **1W**. One AM23xx Aosong humidity sensor can be connected to GTCOM2

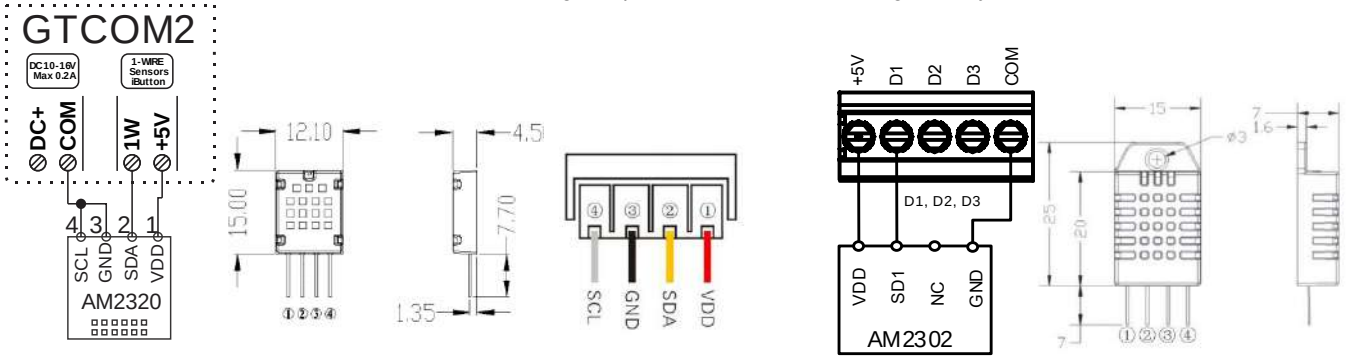
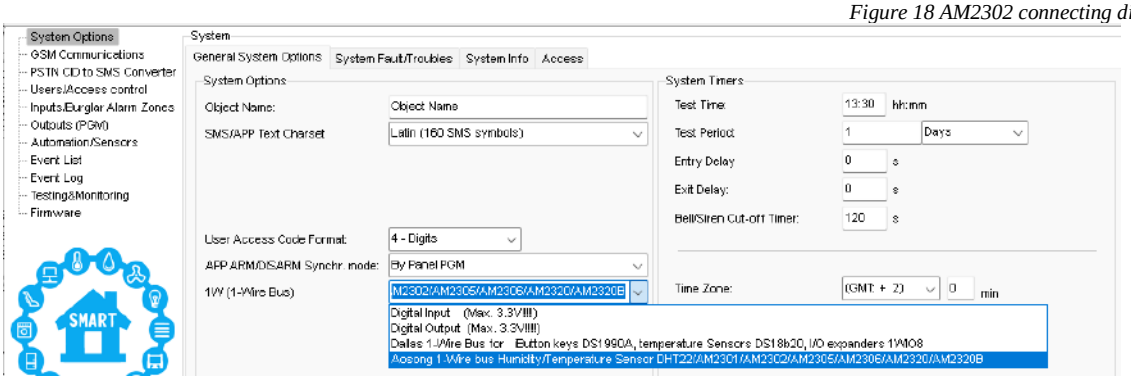
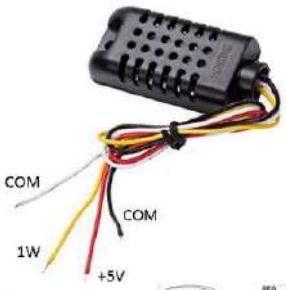


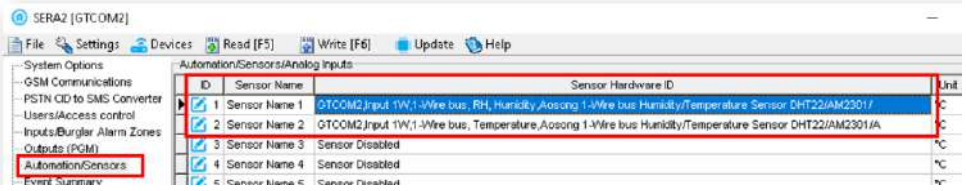
Figure 18 AM2302 connecting diagram





Steps to start AM23xx, AM2320, AM2305 sensors:

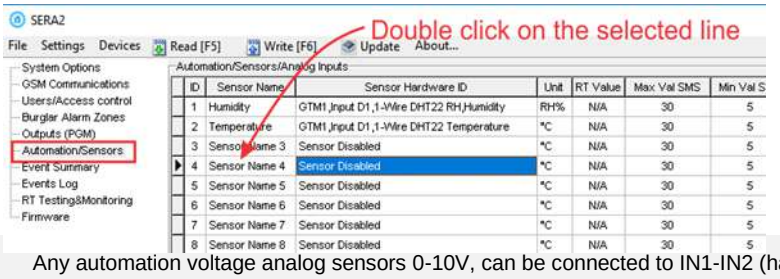
- Connect the sensor to 1W contact according to the connection diagram.
- Navigate to *SERA2>System Options>General System Options* and set **1W (1-Wire Bus)** to [Aosong 1-Wire bus Humidity/Temperature Sensor].
- Press [Write].
- Power on the module.
- Wait for the sensor to be detected on the bus.
- Press [Read].
- Navigate to SERA2 > Automation/Sensors. Locate the desired registered sensor in the sensor table and double-click on its line.
- Configure the required parameters.
- Press [Write].
- Press [Read] (Wait until you will see the note, that “Configuration was received”)
- Go to *SERA2> Automation/ Sensors*
- You will see the connected sensor in the list

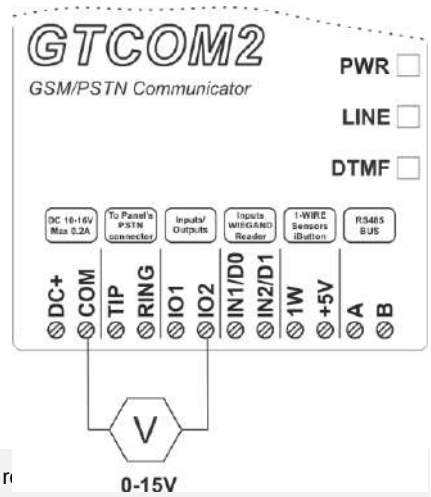


Imortant! Do not change polarity! It will damage the sensor

7.2 Analog Inputs 0-10V Setup

- Connect analog voltage sensors to I/O1 and I/O2 as per the diagram.
- Use analog inputs for security zones or sensors.
- Disable unused inputs in 'Zones' or 'Sensor' window.
- Calibrate sensors and set parameters in 'Automation/Sensors' (Sera2 > Automation / Sensors), adjusting multiplier and offset.
- For detailed setup, see *Error! Reference source not found.*
- Save changes to the module by clicking [Write].

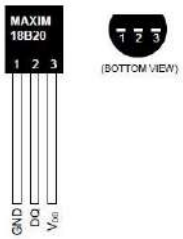




! Any automation voltage analog sensors 0-10V, can be connected to IN1-IN2 (has internal pull up r

7.3 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.

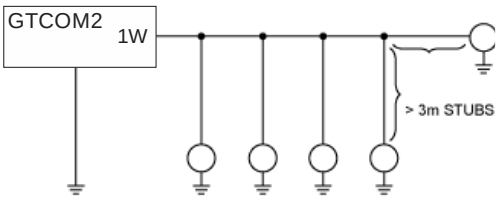


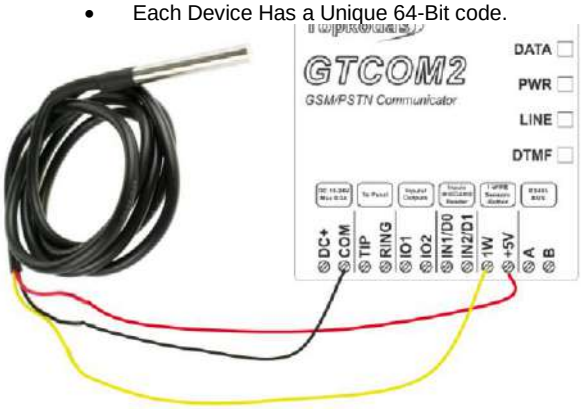
Applications/Uses

- 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.





! ***Imortant!*** Do not change polarity! It will damage the sensor

Connect 1-Wire sensors **DS18b20** to terminal **1W** according following topologies:

- Linear topology: slaves are attached to the 1-Wire bus with insignificant (< 3m) branches or "stubs."
- Star topology. The 1-Wire bus is split at or near the master end and extends in multiple branches of varying lengths. There are slave devices along, or at the ends of, the branches. When a stub is connected to a 1-Wire bus, there is an impedance mismatch at the branch point.; Each branch line should be separated by 82-120 Ohm resistor

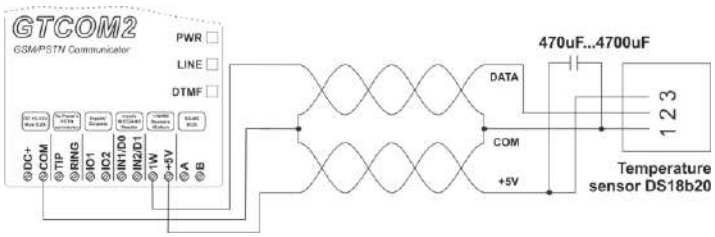


Figure 33 DS18b20 connection with long distance UTP or FTP cable

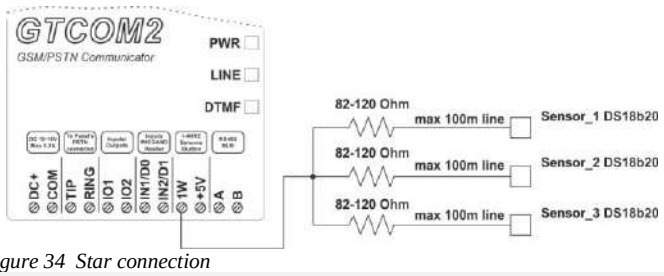
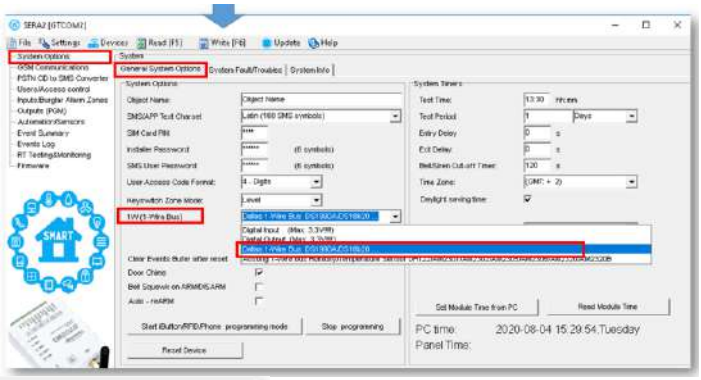
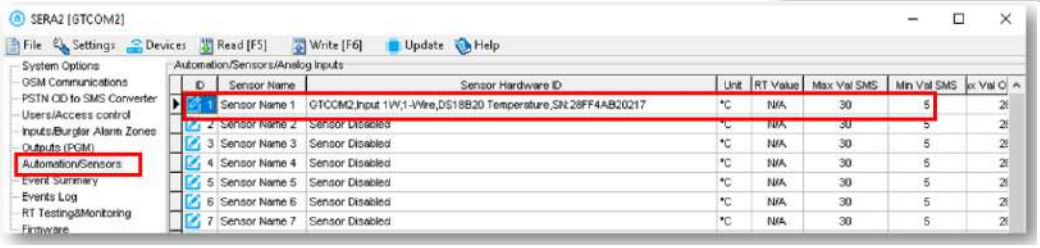


Figure 34 Star connection

! The line resistor must be as close as possible to the contacts of the module GTCOM2.

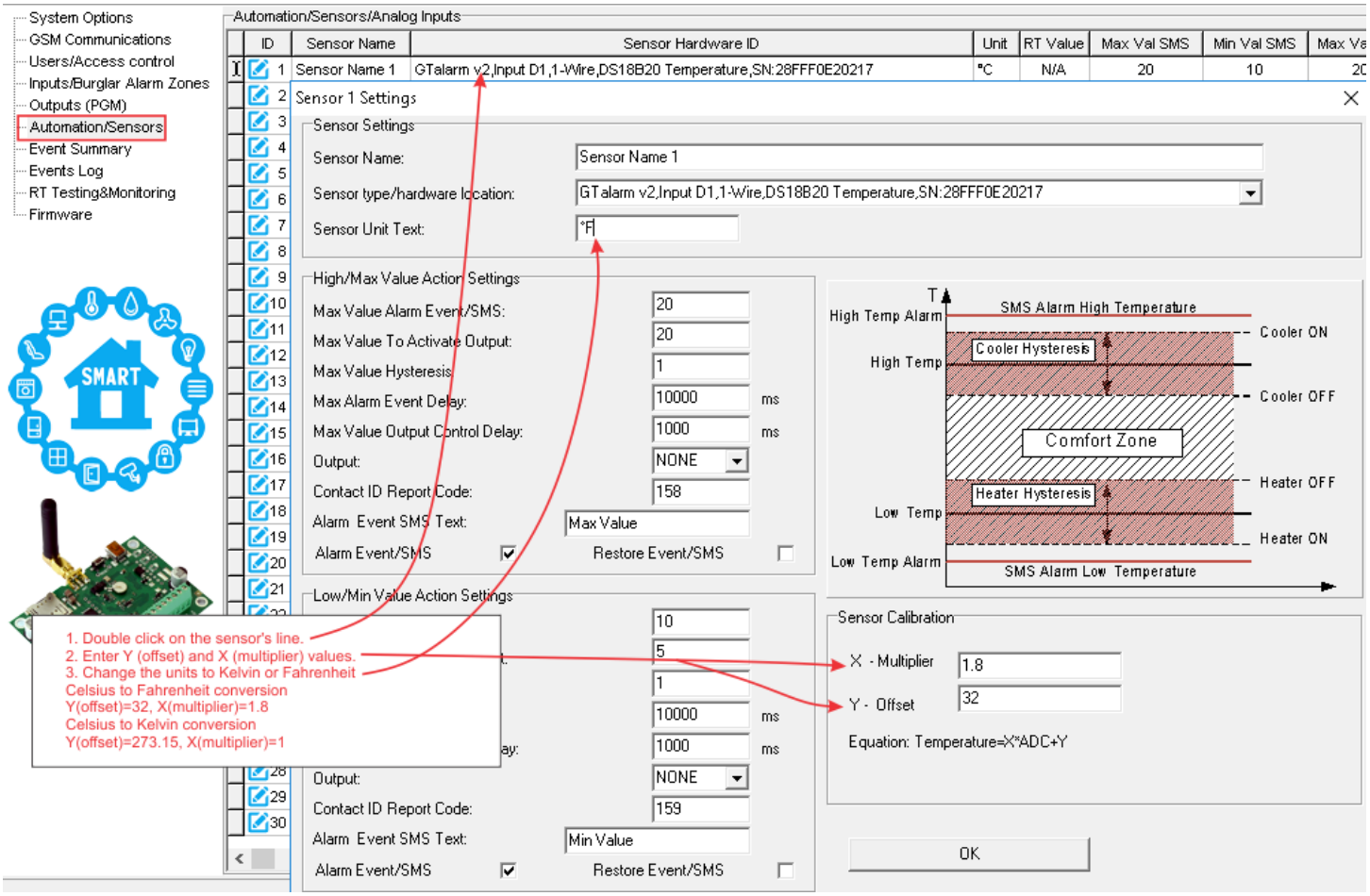
- Go to SERA2> System Options> General System Options
- Set 1W (1- Wire Bus) to Dallas 1-Wire Bus DS1990A/ DS18b20…
- Press [Write]
- Press [Read] (Wait until you will see the note, that “Configuration was received”)
- Go to SERA2> Automation/ Sensors
- You will see the connected sensor in the list





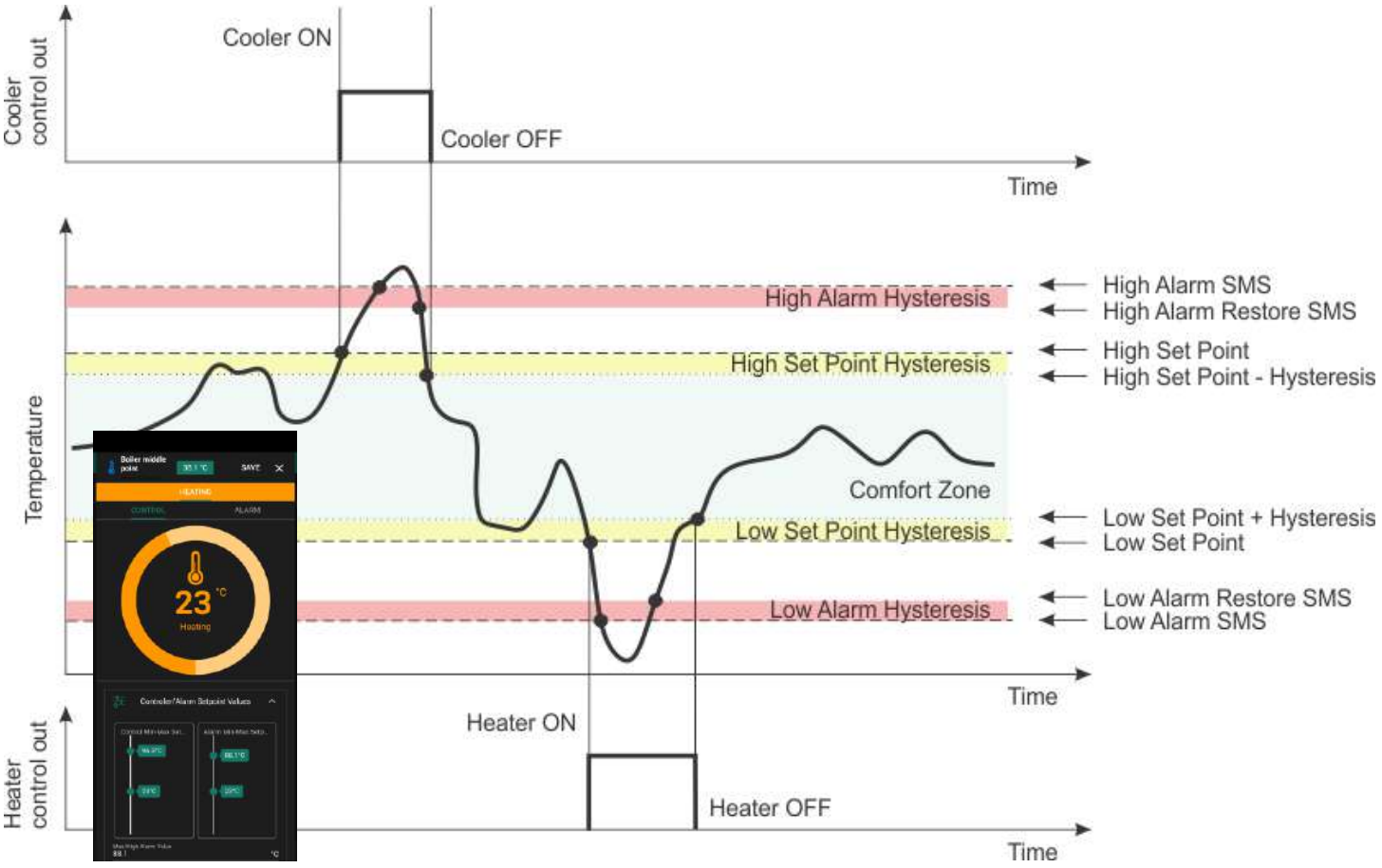
- Double click on the selected line
- Edit settings
- Press [Write]

7.4 How to change temperature scale from Celsius to Fahrenheit



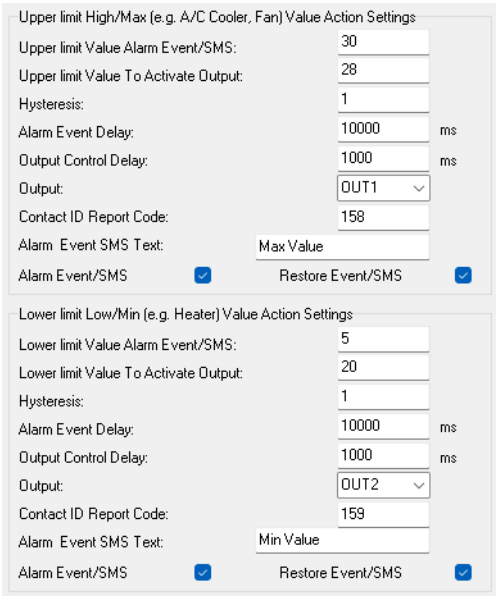
- Double click on the sensor’s line
- Enter Y (offset) and X (multiplier) values
- Change the units to Kelvin or Fahrenheit
  - **Celsius to Fahrenheit conversion:** *Y (offset)=32, X (multiplier)= 1.8*
  - **Celsius to Kelvin conversion:** *Y (offset)= 273.15, X (multiplier)=1*

7.5 Example of Thermostat Control for Heating and Cooling



The system utilizes four set points for comprehensive temperature management, catering to both cooling and heating requirements:

1. **Upper Limit for Output Control (Cooling Set Point)**: Activates cooling when temperature exceeds this set point. For instance, if set to 28 degrees, the system activates the cooling output (e.g., OUT1) after a delay of 1000ms to prevent false activation from short-term temperature increases.
2. **Upper Limit for Temperature Alarm (Cooling Alarm Set Point)**: Triggers an SMS alarm if temperature surpasses this higher threshold. For example, at 30 degrees, the system sends an 'Overheat' SMS alarm after a delay of 10000ms.
3. **Lower Limit for Output Control (Heating Set Point)**: Activates heating when temperature falls below this set point to maintain warmth. For example, with a set point of 20 degrees, the heating output (e.g., OUT2) engages after a specific delay, ensuring the premises stay warm.
4. **Lower Limit for Temperature Alarm (Heating Alarm Set Point)**: Sends an SMS alarm if temperature drops below this threshold, preventing conditions like freezing. If set to 5 degrees, an 'Antifreeze' SMS alarm is sent, indicating the temperature is dangerously low.



Hysteresis and System Behavior:

- Hysteresis value prevents frequent toggling of the system, reducing output 'chattering'. It ensures the system operates smoothly around set points, activating or deactivating outputs only when the temperature sufficiently deviates from the target.
- ON-OFF control method switches the output entirely ON or OFF, maintaining temperature within the hysteresis range of the set points.

For high-power AC equipment control in heating or cooling systems, using solid-state relays is recommended for their reliable performance and efficient load handling."

7.6 How to test the sensors

- Real-time hardware status: Go to RT Testing & Monitoring > Hardware, then press [Start Monitoring].
- View the list of alarm events with timestamps: Navigate to RT Testing & Monitoring > Event Monitoring.
- To receive alarm notifications via SMS to your mobile phone: Go to GSM Communication > SMS/Dial reporting.
- For real-time sensor values and states: SERA2 > Access RT Testing & Monitoring > Sensors/Automation.
- To save the configuration, press [Write].

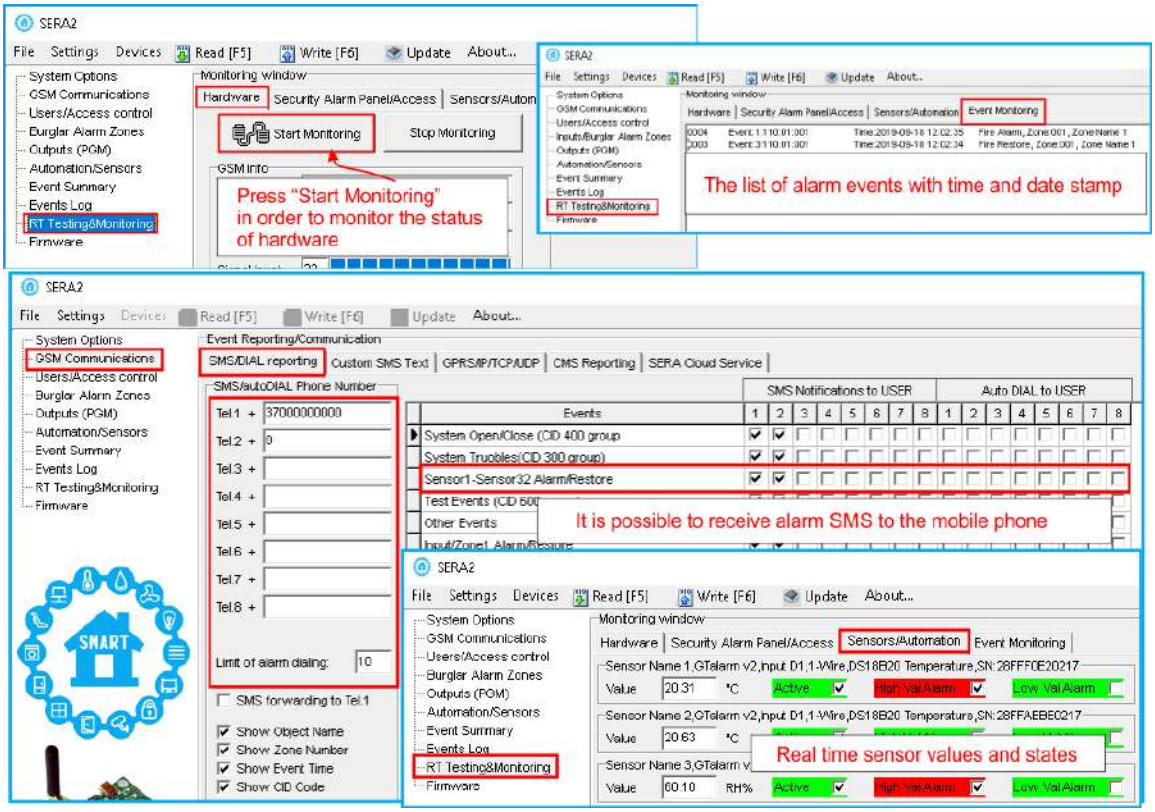
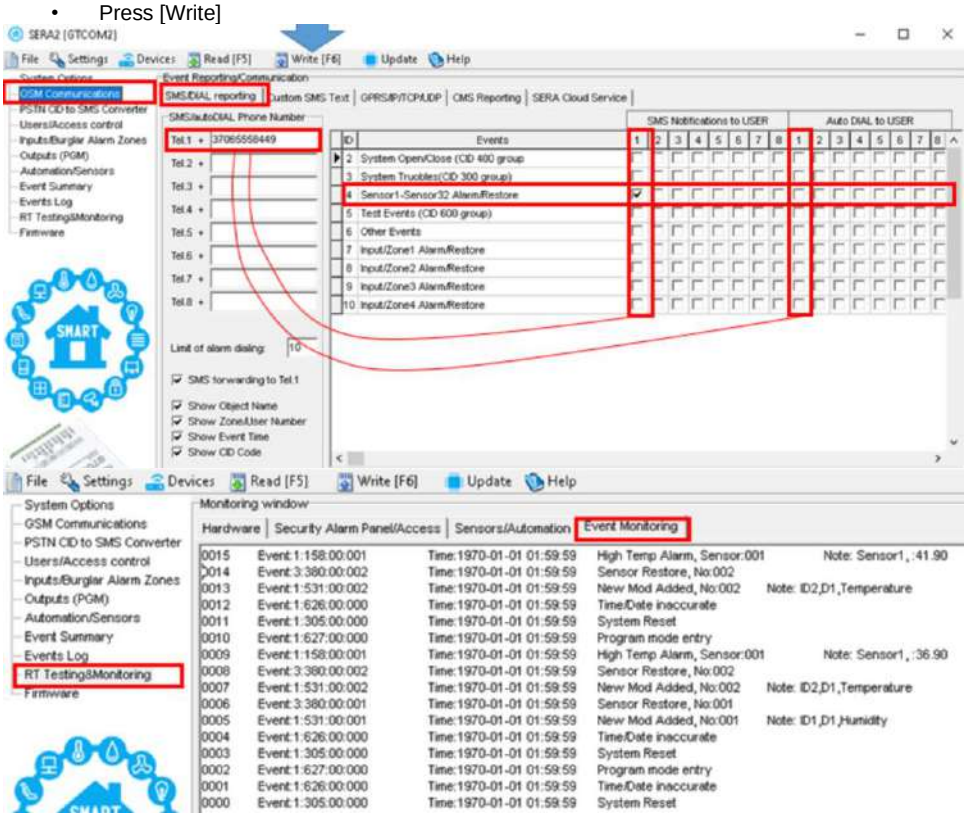


Figure 35 How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list

How to receive SMS alarms

- Go to SERA2> GSM Communications> SMS/ Dial reporting
- Enter phone number
- Mark alarm events
- Press [Write]



What to Do if You Detect a Sensor Trouble in the "Event Log" Window?

- Use the "RT Testing & Monitoring" Window: Sensor troubles are highlighted in red in this window.
- Navigate to the Automation/Sensors window, deactivate the problematic sensor, and then press [Write]. It's possible the issue might be related to the sensor's connection to the module.
- If the issue persists, ensure you save the configuration. Next, send this configuration to the seller. Be detailed in your description: specify the issues, mention connections related to zone: 001, and provide any other relevant information before forwarding it to the seller.

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

8 Programming with SERA2 configuration software

The SERA2 software is a configuration tool for the GTCOM2 module, allowing local configuration via USB or remote configuration via the GPRS/LTE network. It simplifies the system configuration process by enabling use of a personal computer. We recommend programming the GTCOM2 module with SERA2 software. Here's how to install and start it:

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

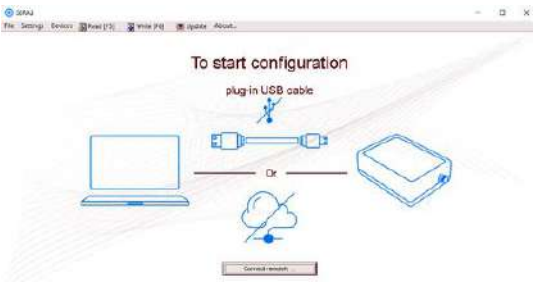


Figure 36Sera2 software

Connection of the module to PC

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

Work with the software SERA2

If you are sure that the module is fully connected to PC and power supply, please go to Devices > GTCOM2

Figure 37 Command line

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

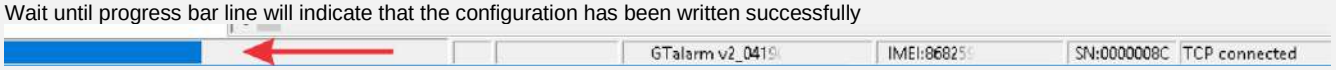


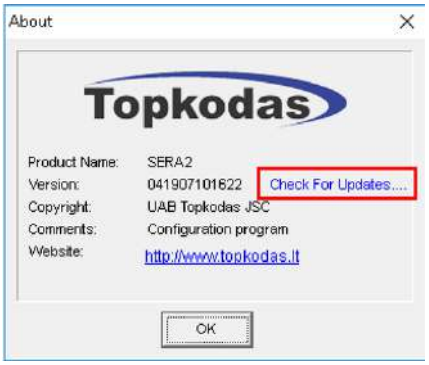
Figure 38 Progress bar

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

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

To receive software updates:

- Go to **Settings** and select "**Check for Updates Automatically**". The program will notify you when a new update is available.
- Start the update process when prompted.
- Connect the module to your computer using a mini-USB cable.
- Write the update to the GTCOM2 module by pressing the [Update] button in the SERA2 software.
- If you want to update the module manually, press [Update]



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

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

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

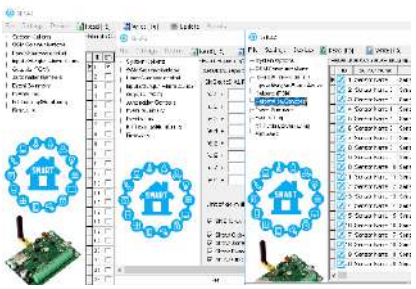
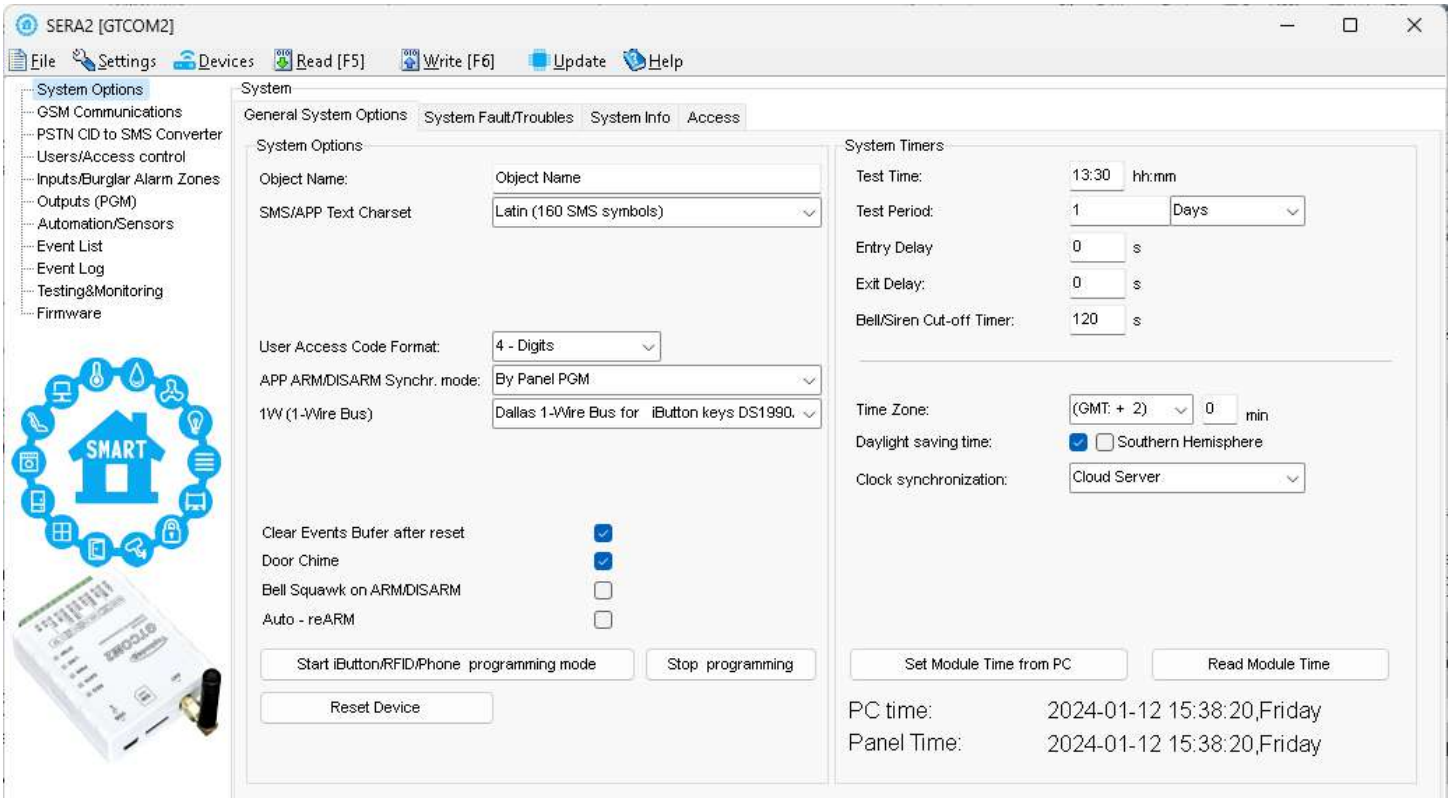


Figure 39configuration at the same time. Unlimited number of modules

8.1 General system options programming

System Options > General system Options

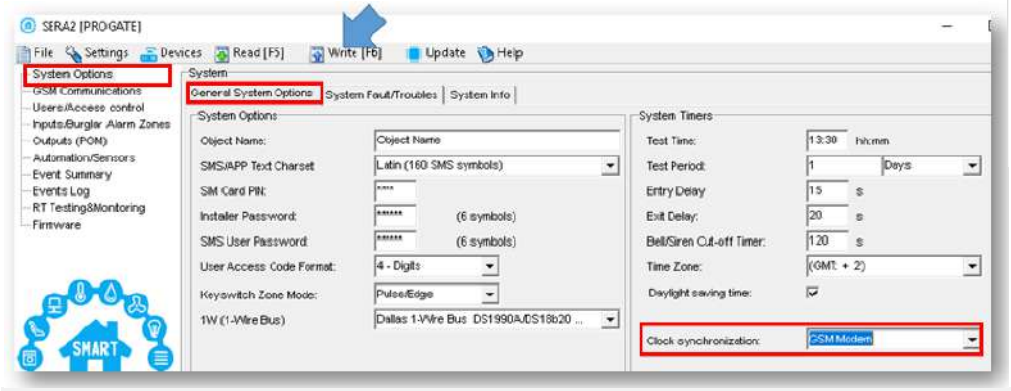
The general system options settings let you control system options, system general settings, systems timers, let you program iButton keys and reset the module

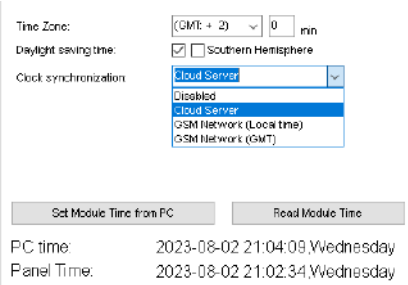


Object Name	System name
SMS/APP Text Charset	Text charset: Latin, Easten European, Baltic or Western European.
User Access code format	Select 4 or 6 digits user code format
App ARM/DISARM Synchr mode:	Sets algorithm how to synchronize main Alarm panel system state with GTOM2 SERANOVA App • By Panel PGM • By Panel Events
1W (1-Wire Bus)	1W Digital I/O Mode. 1-Wire bus / Digital Input / Digital Output
Clear Event Buffer After Reset	When the cell is checked, the memory of unsent reports will be deleted after the module resetting
Door Chime	When this box is checked, violations of set Delay zones at the alarm turned off will be accompanied by keyboard audible (Buzzer) signal
Bell squawk on ARM/ DISARM	The module can activate the bell output briefly causing the squawk to alert users that the module is being armed, disarmed or that an Entry or Exit Delay was triggered. Enable or disable the desired option.
Auto re-ARM	The module can be programmed to arm the module if there is no activity in the area after the system disarming.
Start iButton/RFID programming	All added iButton keys or RFID cards will be registered in the order of sequence by clicking Start programming
STOP iButton/RFID programming	To finish entering iButton keys or RFID cards, click Stop programming button
Test Time	Auto Test report time of day
Test Period	Auto Test report period
Entry Delay	This delay gives you time to enter the armed premises and enter your code to disarm your system before the alarm is triggered.
Exit Delay	The system will trigger the Exit Delay Timer to provide you with enough time to exit the protected area before the system is armed.
Bell/ Siren Cut – off Timer	Duration of audible signal (sirens, Bell) after the alarm system activated. Time shall be written in seconds, duration from 0 to 9999.
Time Zone	System time zone.
Daylight saving time	Sets day light saving automatically
Clock Synchronization	Set how to synchronize clock
Set module time from PC	To set the clock click Set time from PC button and the clock will be set using computer's clock.
Read module time	To read the clock of module.

8.2 Real-time clock Time Zone and Synchronization

The SERA2 software provides options for setting the PROGATE real time clock's 'Time Zone' and 'Daylight Saving' automatically, which is essential for modules with automatic schedules to avoid incorrect schedule activations due to time zone errors.

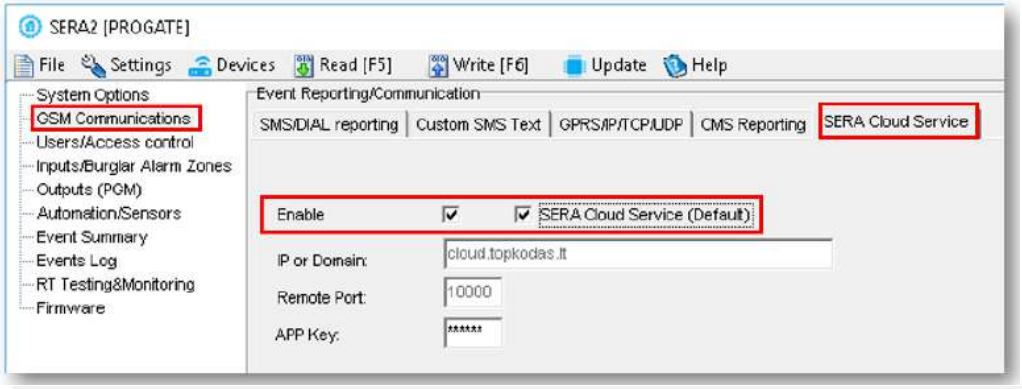




If the module has been connected first time to the power supply, or power supply has been disconnected, the time of the module should be set again by auto synchronization or manually.

System clock can be synchronized in following ways:

1. **Cloud Server**. Synchronize by [SERA Cloud Service]. SIM card must have mobile data and [**SERA Cloud Service**] must be enabled.
2. **GSM Network (Local time).** Select this if cellular network provides local time format.
3. **GSM Network (GMT).** Select this if cellular network provides GMT time format.
4. **Disabled**. If you want to set time manually.
5. **Central monitoring station:** Via the IP SIA DC-09 protocol, the system's date and time will automatically synchronize with the station when connected
6. **Direct PC synchronization**: Users can set the module's time directly from their PC for immediate synchronization.



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

8.3 GSM Communicator Programming

8.3.1 Event Notifications via SMS & DIAL

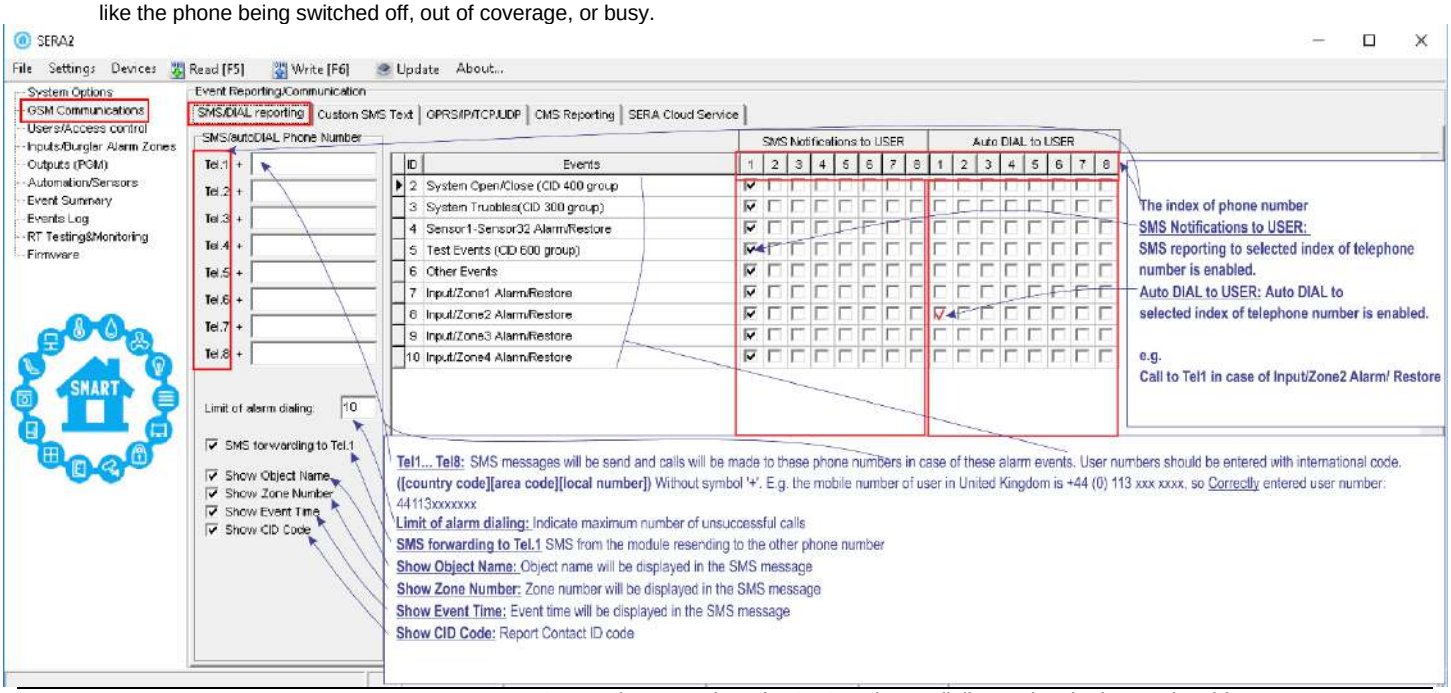
GSM Communications > SMS DIAL Reporting

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

The system allows setting up to 8 users to receive notifications via SMS or/and calls (DIAL). These notifications, sent through GSM, include alarms and system status updates, such as gate openings or system arming/disarming. Users can configure their phone numbers and select specific events for alerts in the 'GSM Communications > SMS DIAL Reporting' settings.

For alarm situations like zone or tamper violations, the system follows this sequence:

- It sends an SMS with the zone's name. If the user's phone is off or out of GSM coverage, the system sends the SMS to the next listed number. Each zone triggers a separate SMS. The process repeats as programmed.
- If set, the system also calls the first listed user's number for each violation. If unavailable, it tries the next number in the set order, due to reasons like the phone being switched off, out of coverage, or busy.

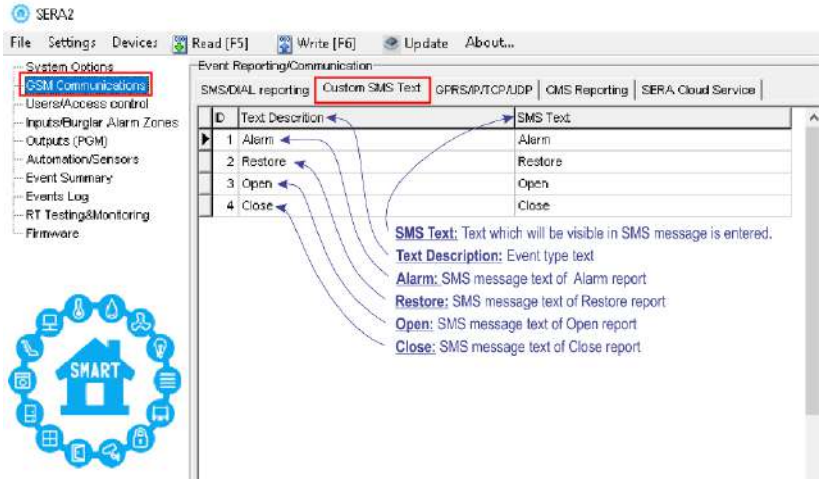


The SMS/auto DIAL Phone Numbers	Enter up to 8 user phone numbers for SMS and auto-dialing, using the international format **[Country code][Area code][Local number]** without the '+' symbol. For example, a UK number +44 (0) 113 xxx xxxx should be entered as 44113xxxxxxx. Incorrect formats would be 440113xxxxxxx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

8.3.1 Custom SMS Text

GSM Communication > Custom SMS Text

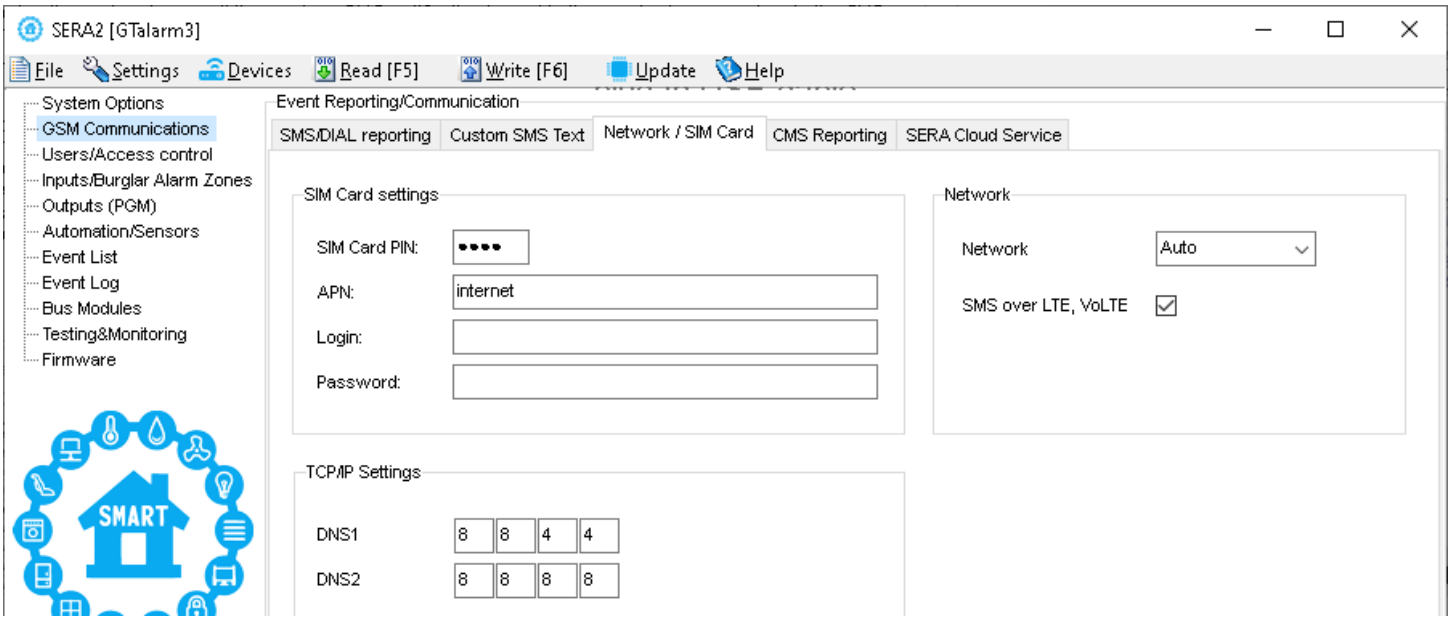
The Custom SMS Text options let you enter the text that will be send to the user in case if the alarm event occur.



Text Description: Event type text
SMS Text: Text which will be visible in SMS message is entered.
Alarm: SMS message text of Alarm report
Restore: SMS message text of Restore report
Open: SMS message text of Open report
Close: SMS message text of Close report

8.3.2 Network/SIM Card/GPRS/LTE programming

GSM Communication > Network/SIM Card



APN: An Access Point Name
Login: User name of GSM operator network (if required by network operator).
Password: User password of GSM operator network where SIM card inserted in the module is operating.
DNS1: IP addresses of 1st DNS server.
DNS2: IP addresses of 2nd DNS server.

8.3.3 Central Monitoring Station details programming. Reporting to the Central Monitoring Station (CMS)

GSM Communication > CMS Reporting

This window allows you to configure the parameters for reporting to a central monitoring station (CMS).

In CMS mode, messages sent to the monitoring station are prioritized. Due to this prioritization, it's crucial to maintain a consistent and reliable connection with the CMS. Should the connection be interrupted, the system will try to re-establish it. If the CMS remains inaccessible for an extended period, the system will switch to a backup CMS.

Data Messages – Events

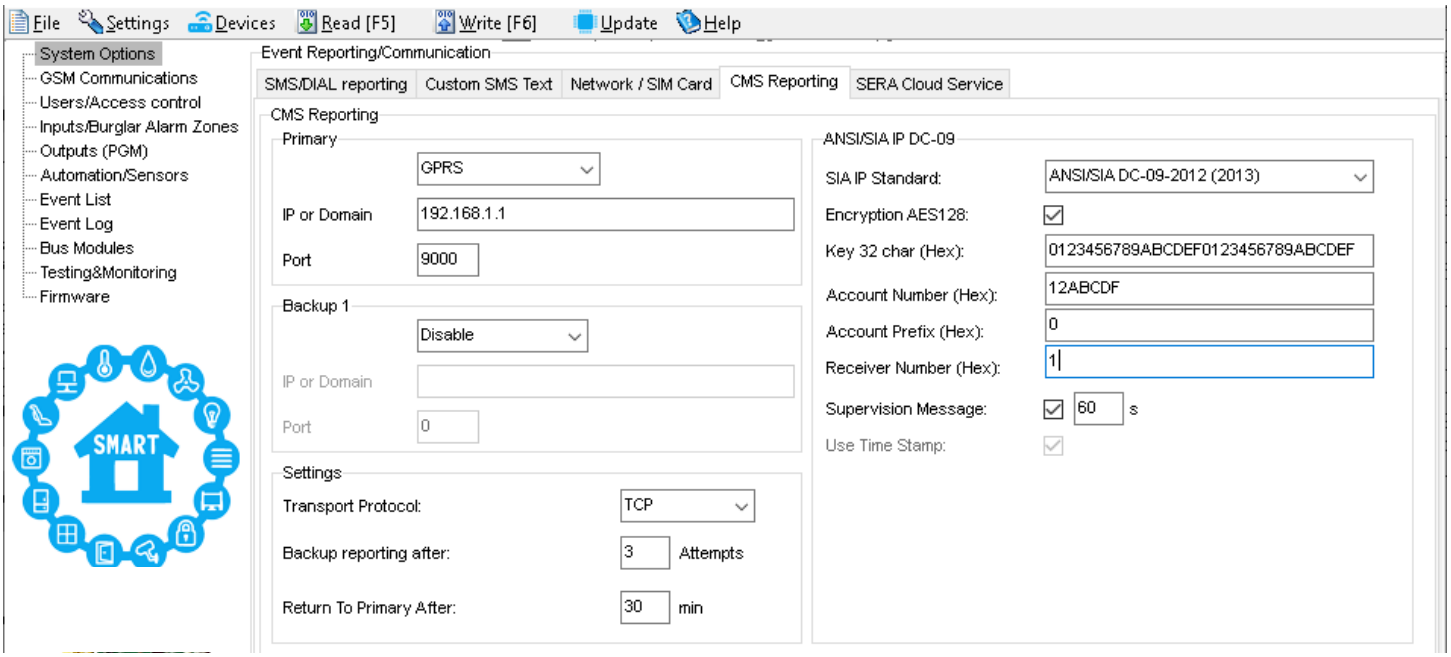
The system supports the following communication methods and protocols:

- GPRS network –SIA IP protocol (ANSI/SIA DC-09-2012; configurable as encrypted and non-encrypted).
- All events to CMS are transmitted according SIA-IP ANSI/SIA DC-09- 2013 standard message body in ADM-CID format Contact ID DC-05.

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:

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

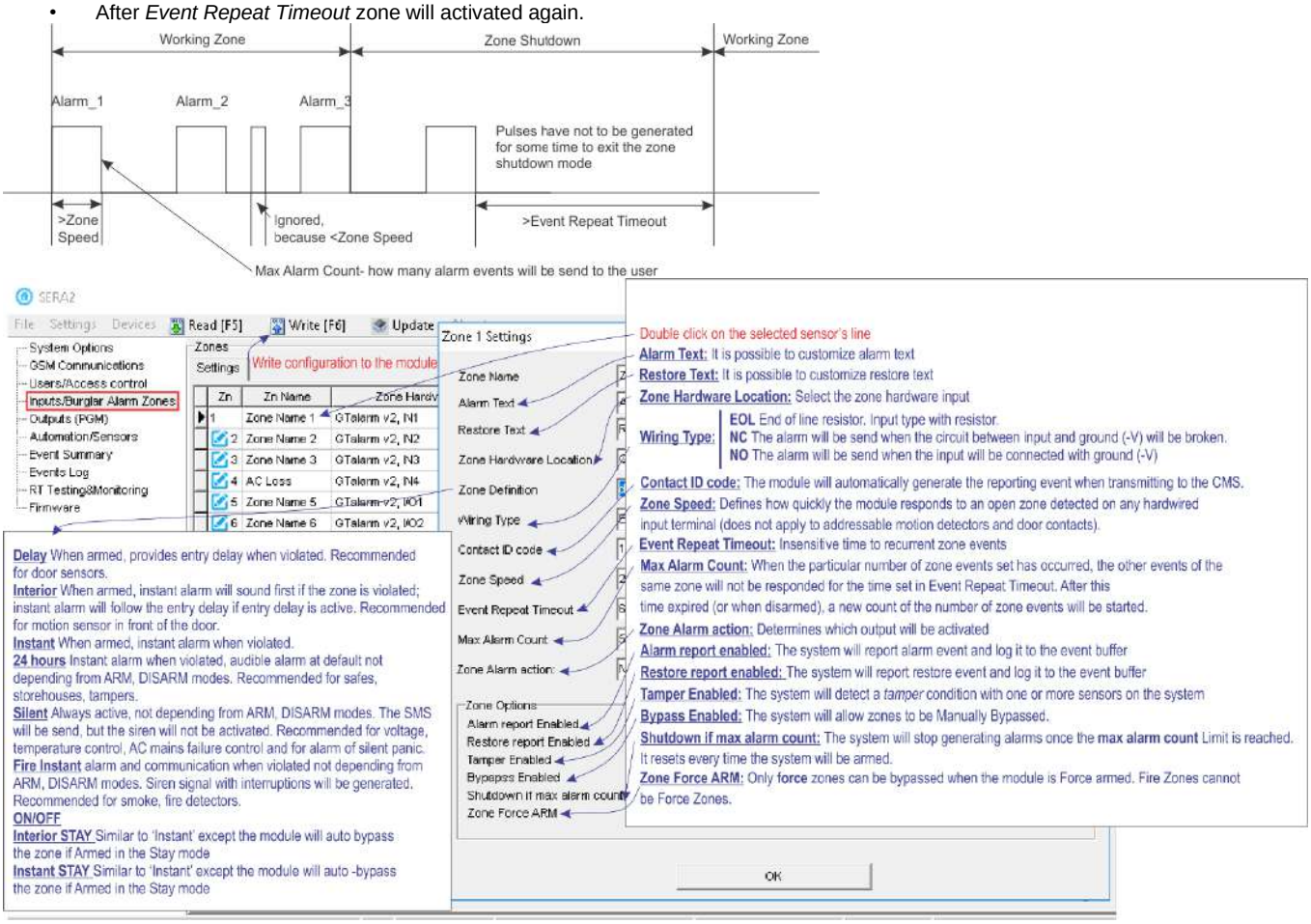


CMS Reporting	Primary central monitoring station settings
Primary	Primary central monitoring station settings
GPRS or Disable	Data transmitting to the primary CMS via GPRS network or data transiting Disable
IP or Domain	The IP address xxx.xxx.xxx or domain name of the receiver station.
Remote Port	The IP port defined as input port on the receiver station to receive the connection requests (TCP mode) or the datagrams (UDP mode) transmitted by ALERT.
Backup 1	Backup 1 central monitoring station settings
Transport Protocol (TCP or UDP)	The used link protocol: UDP (datagrams exchange without connection) or TCP (connected mode).
Backup reporting after n attempts	If communication with primary central monitoring station (CMS) is disable, switch to backup CMS after n attempts
Return To Primary After n min	Return To Primary After n min
Encryption AES128	The "Encryption" option validates the encryption of messages. If this option is enabled, the encryption key must be defined.
Key 32 char (Hex)	AES key size 128 bits. Definition of the key as a string of respectively 32 hexadecimal characters, relatively to the size of the selected key.
Account Number (Hex)	mandatory, consists of 3-16 hexadecimal digits
Account Prefix (Hex)	Consists of 6 hexadecimal digits maximum. If not used enter ”0”
Receiver Number (Hex)	Optional, consists of 6 hexadecimal digits maximum.
Supervision Message n seconds	Supervision NULL Message. Optionally, the PE and CSR may be configured to supervise the connection. Module periodically send the Null Message to the CSR. Supervision interval shall be configurable over range of 10 seconds to 9999 seconds.
Use Time Stamp	This option validates the addition to the messages of a timestamp in GMT time. This option is always forced for encrypted messages.

8.4 Inputs/Zones programming

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

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



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.
Zone definition:
Delay When armed, provides entry delay when violated. Recommended for door sensors.
Interior When armed, instant alarm will sound first if the zone is violated; Instant alarm will follow the entry delay if entry delay is active. Recommended for motion sensor in front of the door.
Instant When armed, instant alarm when violated.
24 hours instant alarm when violated, audible alarm at default not depending from ARM, DISARM modes. Recommended for safes, storehouses, tampers.
Silent Always active, not depending from ARM, DISARM modes. The SMS will be send, but the siren will not be activated. Recommended for voltage, Temperature control, AC mains failure control and for alarm of silent panic.
Fire Instant alarm and communication when violated not depending from ARM, DISARM modes. Siren signal with interruptions will be generated. Recommended for smoke, fire detectors.
ON/OFF
Interior STAY Similar to 'Instant' except the module will auto bypass the zone if Armed in the Stay mode

8.1 Outputs PGM programming

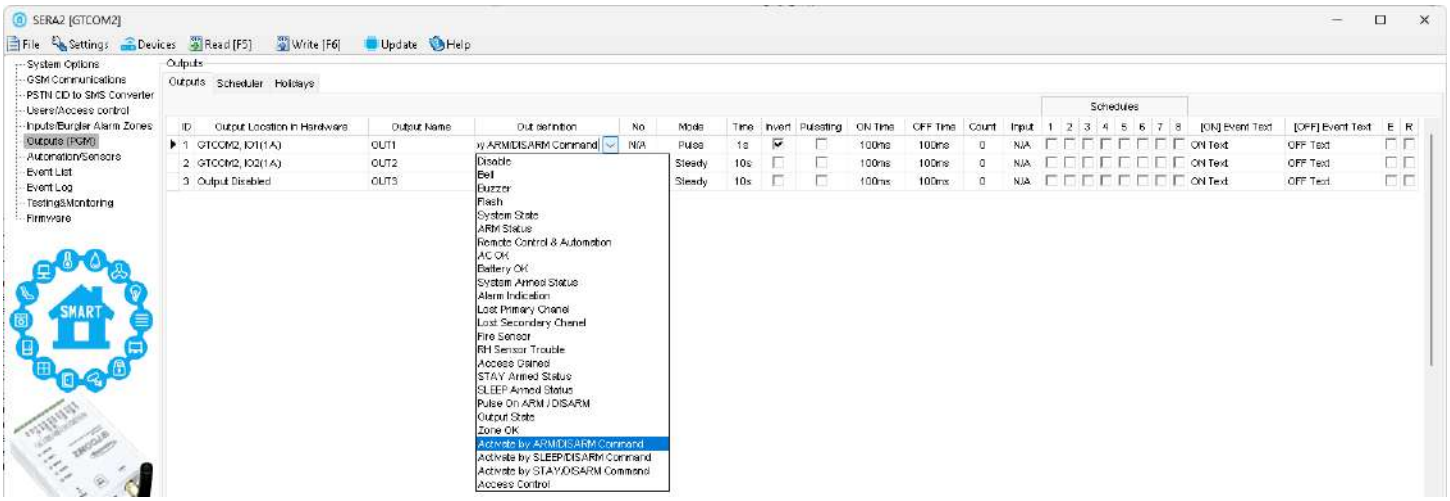
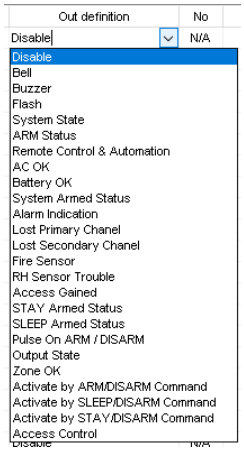


Figure 40 Outputs (PGM) window

ID	Output index number.
Output Location in Hardware	The outputs hardware location.
Output Label	Output name
Out definition 	Output Operation Mode Selection: • **Disable**: Output is deactivated. • **Bell**: Connects to a sounder (siren). Emits a continuous or pulsating signal (for fire) upon alarm activation. • **Buzzer**: Emits a pulse during Exit Delay and a continuous tone during Entry Delay or disturbances. Acts as a keypad buzzer when the system is deactivated. • **Flash**: Pairs with a light indicating system status. Pulsates during Exit Delay, remains continuous during alarms, and stops upon DISARM. • **System State**: For light indicators showing system status. Pulsates during Exit Delay, remains steady during alarms, and stops when system is disarmed. • **ARM Status**: Activates the output when the security system is armed. • **Remote Control &Automation:** Mode to remotely control electrical devices via App, SMS, or phone call. Also allows automated control based on events e.g. thermostat or schedules. • **AC OK**: Indicates the panel's AC power supply. • **Battery OK**: Indicates battery power supply for the control panel. • **System Armed Status**: Connects to a light indicating system status. Continuous signal when the system is armed. • **Alarm Indication**: Indicates alarm status. Emits a continuous signal upon alarm event of the system. • **Lost Primary channel**: Emits a continuous signal if the primary CMS communication channel fails. • **Lost Secondary channel**: Emits a continuous signal if the backup CMS communication channel fails. • **Fire Sensor**: Resets fire sensor operation. Changes status for 5 seconds before reverting. • **RH Sensor Trouble**: In this mode, the output can automatically reset the humidity sensor if a malfunction occurs. • **Access Gained:** If a user has the right to ARM/DISARM the system, they always have access to control this output. If the ARM/DISARM flag isn't set, a user can access this output only if the system is disarmed. • **STAY Armed Status**: This output activates when the system is set to Armed STAY mode. • **SLEEP Armed Status**: This output activates when the system is set to Armed SLEEP mode. • **Pulse on ARM/DISARM**: Generates an impulse when the system is armed or disarmed. • **Output State**: Reflects the state of a selected output, for example, an LED output can mirror Output 1 if [No]=1. • **Zone OK**: Indicates when all security system zones are not violated. A continuous signal indicates the system's readiness. • **Activate by ARM/DISARM Command**: Activates when the system receives an ARM/DISARM command. • **Activate by SLEEP/DISARM Command**: Activates when the system receives a SLEEP/DISARM command. • **Activate by STAY/DISARM Command**: Activates when the system receives a STAY/DISARM command. • **Access Control**: This mode allows the output to be used for gate or door access control. It logs every user access event, and if activated by a call, it stores the phone number.
Mode	Output Control Mode: • **Pulse**: This mode generates a single impulse signal According [Time] parameter when the output is activated. • **Steady**: This mode maintains the output in either an ON or OFF state once it's activated. • **Pulse Count**: In this mode, upon activation, the output produces a series of impulses based on the specified [Count] parameter.
Time	Then [**Mode**]=Pulse, Pulse time duration can set from 1 to 999999 sec.
Invert	Output Inversion is activated
Pulsating	Pulsating mode is activated. Then output is activated it will pulsate according pulse [**ON time**] and [**OFF Time**]
Pulse ON Time	Pulsating mode pulse ON duration.
Pulse OFF Time	Pulsating mode pulse OFF duration.

8.2 Sensors Programming & Automation/Sensors/Analog Inputs Programming

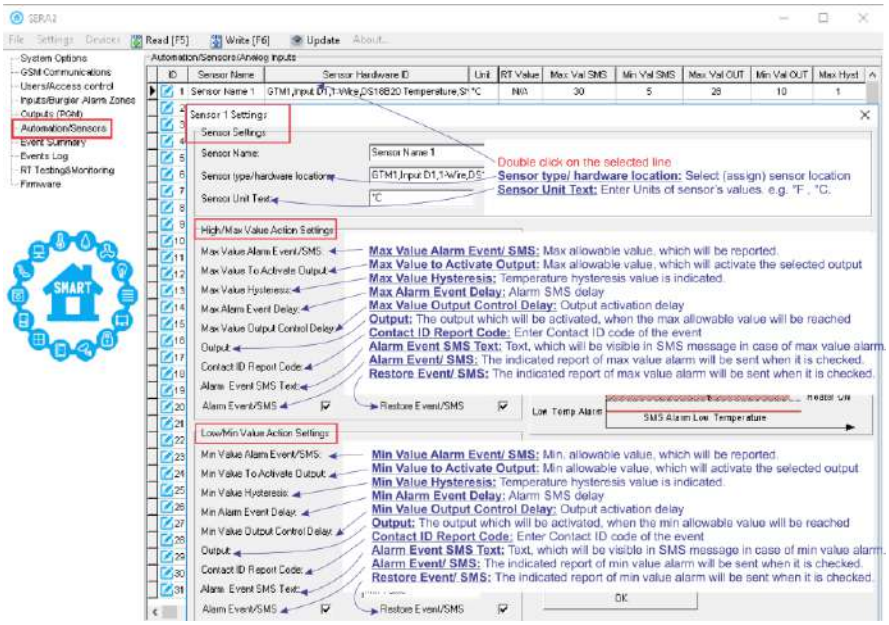
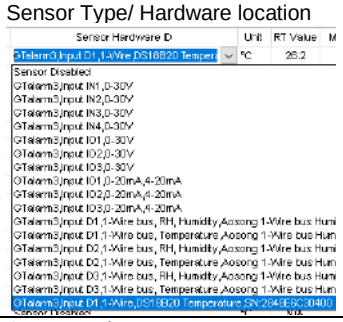
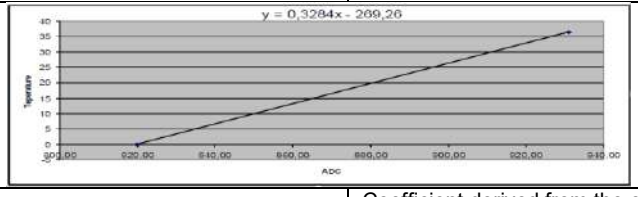
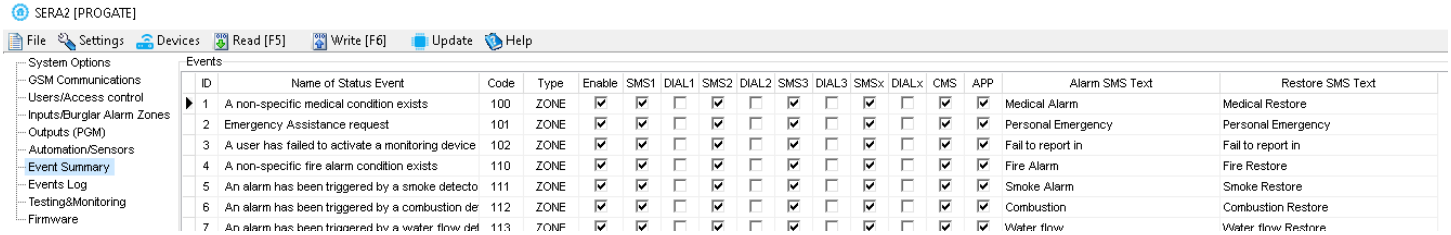


Table Column	Field name in Sensor Form	Column/Field Description
Sensor Name	Sensor Name	Sensor name
Sensor Hardware ID	Sensor Type/ Hardware location 	Location of sensor connected to the module: Specify which sensors are connected to the module. Sensor disabled: Check if the sensor is deactivated. GTCOM2, Input IN1…IN2, 0-30V: Assign voltage input ranging from 0-30V to IN1…IN2. GTCOM2, Input 1W, 1-Wire DHT22 RH, Humidity: Assign digital input D1…D3 for 1-Wire DHT22 RH Humidity sensor. GTCOM2, Input 1W, 1-Wire DHT22 RH, Temperature: Assign digital input D1…D3 for 1-Wire DHT22 RH Temperature sensor. 1-Wire Temperature sensors: Assign digital input 1W for 1-Wire DS18b20 Temperature sensor.
Unit	Sensor Unit Text	Specify the unit used for the sensor.
Max Val SMS	Max Value Alarm Event/ SMS	Define the maximum temperature value that triggers a report.
Max Val OUT	Max Value To Activate Output	Set the maximum temperature value to activate a specific output.
Max Hyst	Max Value Hysteresis	Specify the hysteresis value for the upper set point.
Max SMS Delay	Max Alarm Event Delay	Set the delay for SMS/App notifications when the upper limit is reached.
Max OUT Delay	Max Value output Control Delay	Determine the delay for output control when the upper limit is hit.
Max OUT	Upper Limit/Max>Output	Select the output that will be triggered when the maximum temperature value is hit.
Max Alarm SMS	Alarm Event SMS Text	Enter the text to be displayed in the SMS message when the set temperature limit is exceeded.
Max SMS en	Enable Alarm Event SMS	Check to send the indicated high temperature report.
Min Val SMS	Min Value Alarm Event/ SMS	Define the minimum temperature value that triggers a report.
Min Val OUT	Min Value To Activate Output	Set the minimum temperature value to activate a specific output.
Min Hyst	Min Value Hysteresis	Specify the hysteresis value for the lower set point.
Min SMS Delay	Min Alarm Event Delay	Set the delay for SMS/App notifications when the lower limit is reached.
Min OUT Delay	Min Value Output Control Delay	Determine the delay for output control when the lower limit is hit.
Min OUT	Lower Limit/Min>Output	Select the output that will be triggered when the minimum temperature value is hit.
Min Alarm SMS	Alarm Event SMS Text	Enter the text to be displayed in the SMS message when the set temperature limit is exceeded.
Min SMS en	Enable Alarm Event/ SMS	Check to send the indicated low temperature report.
Calibration: Temperature= X*ADC+Y		
Mult Coef Corr.	X-multiplier	Coefficient derived from the equation “Temperature = X*ADC + Y”. Measure temperature in at least two points to calculate X.
Sum Coef Corr.	Y-offset	Coefficient derived from the equation “Temperature = X*ADC + Y”. Measure temperature in at least two points to calculate Y.
Max CID	Contact ID Report Code	Input report codes in Ademco CID or SIA DC09 format. The module can set default report codes, and they can be modified. For custom notifications, add text in the “Alarm SMS Text” field.
Min CID	Contact ID Report Code	
RT Value		After connecting to the module and selecting the [Read] icon, this field displays the real-time sensor value.

8.1 Event List (Events)

Event List

The Event List (Events) table contains Contact ID codes of events and enables users to change the text that will be reported if the event occurs.



ID	Name of Status Event	Code	Type	Enable	SMS1	DIAL1	SMS2	DIAL2	SMS3	DIAL3	SMSx	DIALx	CMS	APP	Alarm SMS Text	Restore SMS Text
1	A non-specific medical condition exists	100	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Medical Alarm	Medical Restore
2	Emergency Assistance request	101	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Personal Emergency	Personal Emergency
3	A user has failed to activate a monitoring device	102	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Fail to report in	Fail to report in
4	A non-specific fire alarm condition exists	110	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Fire Alarm	Fire Restore
5	An alarm has been triggered by a smoke detecto	111	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Smoke Alarm	Smoke Restore
6	An alarm has been triggered by a combustion de	112	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Combustion	Combustion Restore
7	An alarm has been triggered by a water flow del	113	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Water flow	Water flow Restore

Figure 41 Event List window

ID	Report sequence number
Name of Status Event	Event (report) name
Code	Report Contact ID code.
Enable	The indicated report will be sent when it is checked.
Alarm SMS Text	Alarm text which will be visible in SMS message is entered.
Restore SMS Text	Restore text which will be visible in SMS message is entered.
Type	None – Type is not assigned USER – Refer to USER Report Options ZONE – Refer to Zone Report Options NUM – Refer to Numerical Report Options

8.2 Events Log

Events Log

The Event Log displays events stored in a nonvolatile flash memory buffer, recording each new event. It has a capacity of up to 3072 event records.

The event log allows to chronologically register up to 3072 time stamped records regarding the following system events:

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

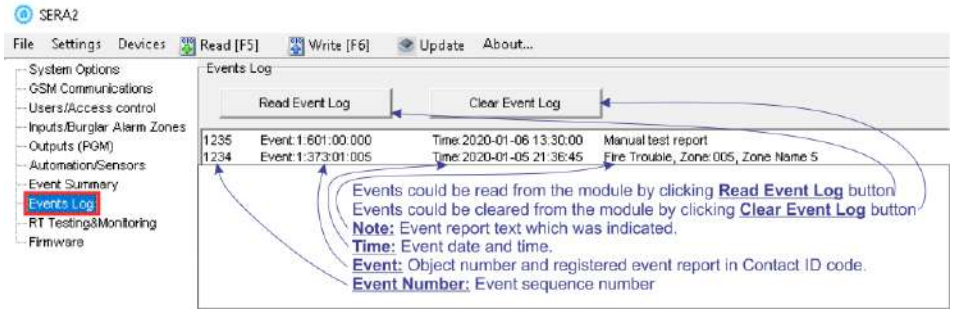


Figure 42Events Log window.

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

If you notice 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

- Check the 'RT Testing & Monitoring' window, where a red field indicates sensor issues.
- In the 'Automation/Sensors' window, you can temporarily disable the sensor and click [Write].
- The issue might be with its connection. Ensure the sensor connection is properly done.
- Check the wire length. Excessively long cables can cause poor communication between the controller and the sensor.
- If the issue persists, consider replacing the sensor.

8.3 Real-Time Testing & Monitoring of Hardware

RT Testing & Monitoring > Hardware

System hardware can be monitored in real time via USB or TCP Cloud connections. The Hardware Monitoring window provides real-time data on inputs, outputs, system state, voltages, sensors, and GSM network status.

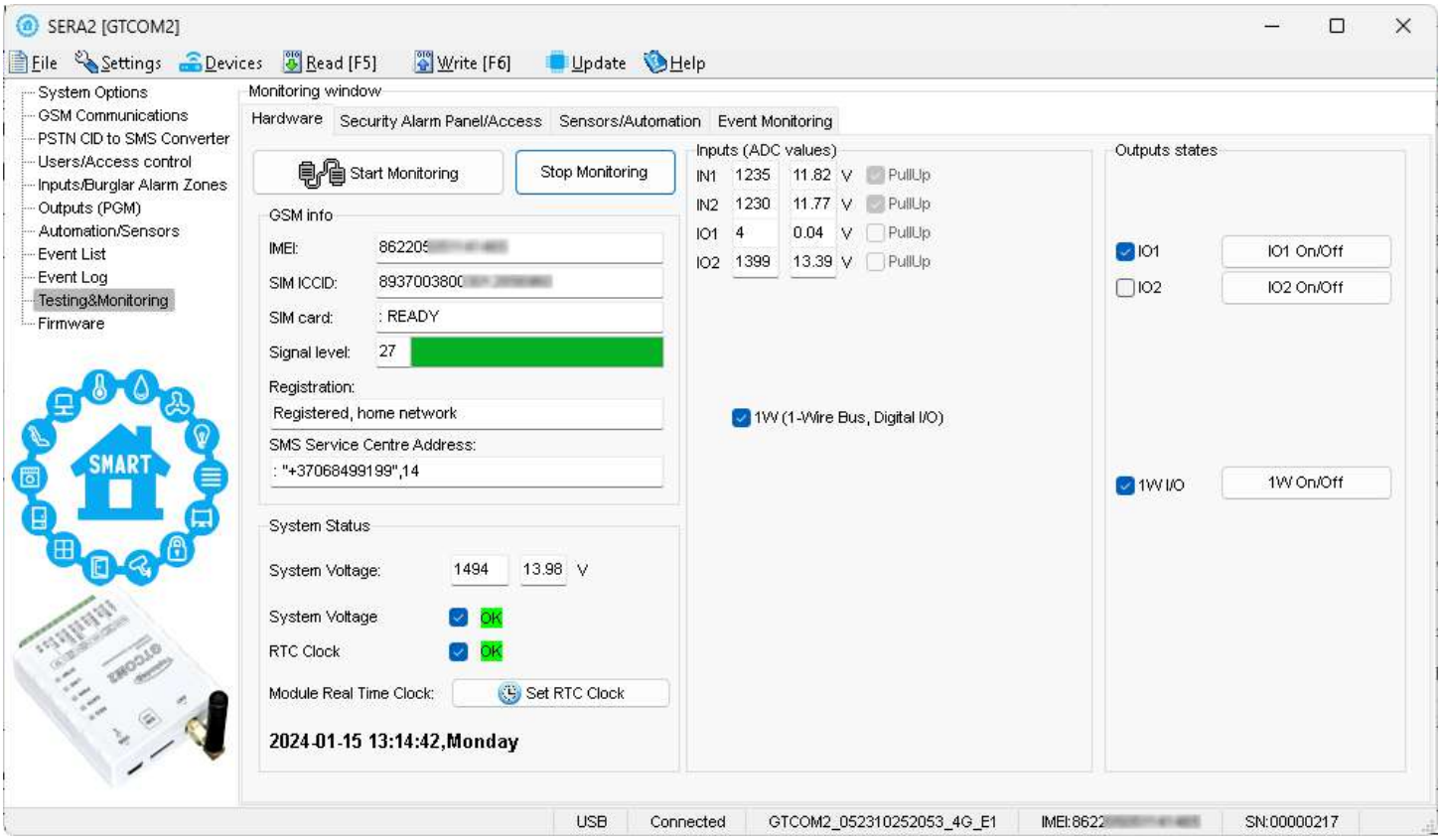
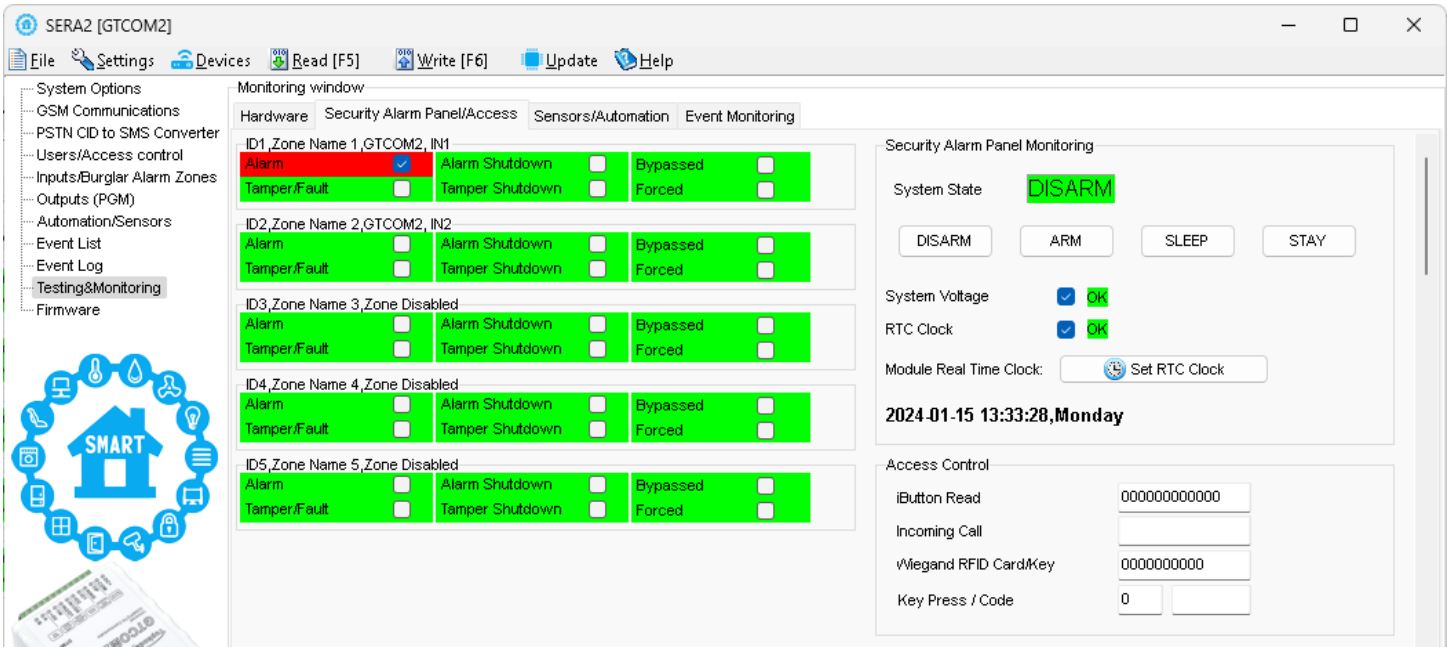


Figure 43RT Testing & Monitoring > Hardware window

Start Monitoring	Pressing **Start Monitoring** button starts the monitoring of the module.
Stop Monitoring	Pressing **Stop Monitoring** button stops the monitoring of the module.
IMEI	IMEI number of GSM modem available in the module
SIM ICCID	**ICCID (Integrated Circuit Card Identifier)** - A SIM card contains its unique serial number (ICCID). ICCIDs are stored in the SIM cards and are also printed on the SIM card.
SIM Card	If note READY is visible, it means that SIM card is fully functioning. Otherwise, check whether PIN code request is off or replace SIM card.
Signal level	Signal strength of GSM communication
Registration	State of GSM modem registration to GSM network.
SMS Service Centre Address	SMS center number. This number should be checked if it is correct. If this number is incorrect. SMS messaging may be impossible. This number may be changed after inserting SIM card into any mobile phone.
System Voltage	Power supply voltage. Nearby number is value of ADC voltage., voltage value (V) will be achieved.
System Voltage	System voltage OK/Trouble
RTC Clock	Real time clock OK/Trouble
Module Real Time Clock	Indicates the time of the module RTC
Set RTC Clock	By pressing this button real time clock of the module will be set.
Inputs IN1…IN2	IN1…IN2 is the indicated input ADC and voltage value V.
I/O1…I/O2	I/O1…I/O2 is the indicated voltage ADC value and current ADC value mA.
I/O1…I/O2 On/Off	Checked box nearby the appropriate input/output **I/O1…I/O2** means that this input/output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button
1W (I/O) On/Off	Checked check box nearby the digital outputs **1W (I/O)** means that the 1-Wire Bus currently has ‘0’ or ‘1’ state.

8.3.1 RT Testing & Monitoring Security Alarm Panel/ Access



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

8.3.2 Real-time Testing & Monitoring > Event Monitoring

RT Testing & Monitoring > Event Monitoring	The Event Monitoring window will show real time events information

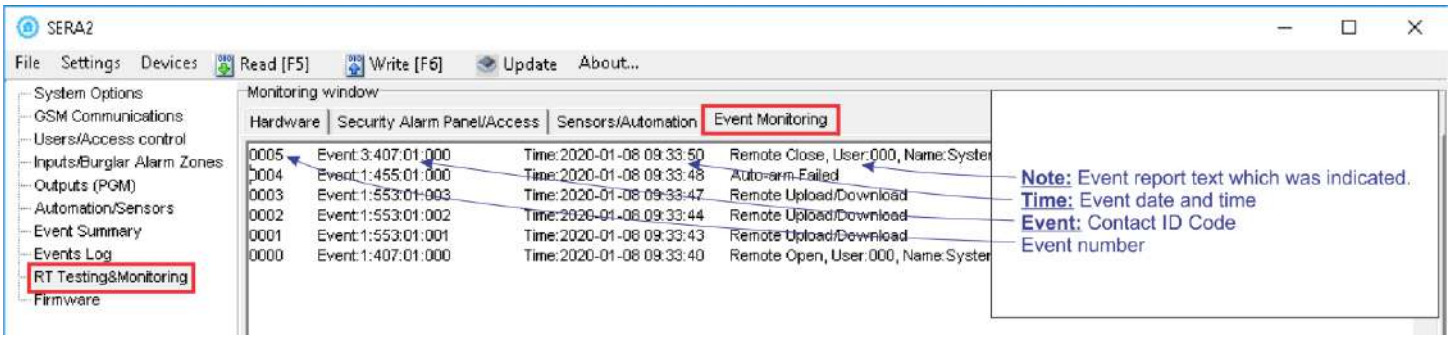


Figure 44 RT Testing & Monitoring > Event Monitoring window.

8.4 SERA2 Remote Configuration, Firmware Updates, Monitoring, and Logging

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

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

How does remote connection work?

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

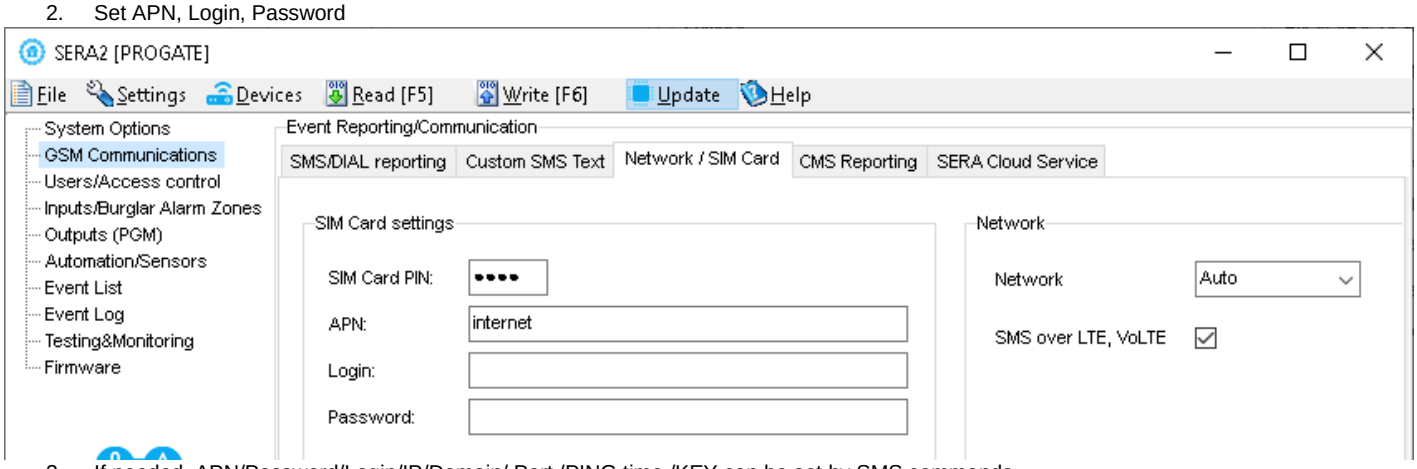
PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→SERA2 Configuration software (Windows)
Or
PROGATE ←→ SERA Cloud Server [cloud.topkodas.lt] ←→SERANOVA app (Web,Android,IOS) https://seranova.eu/login

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

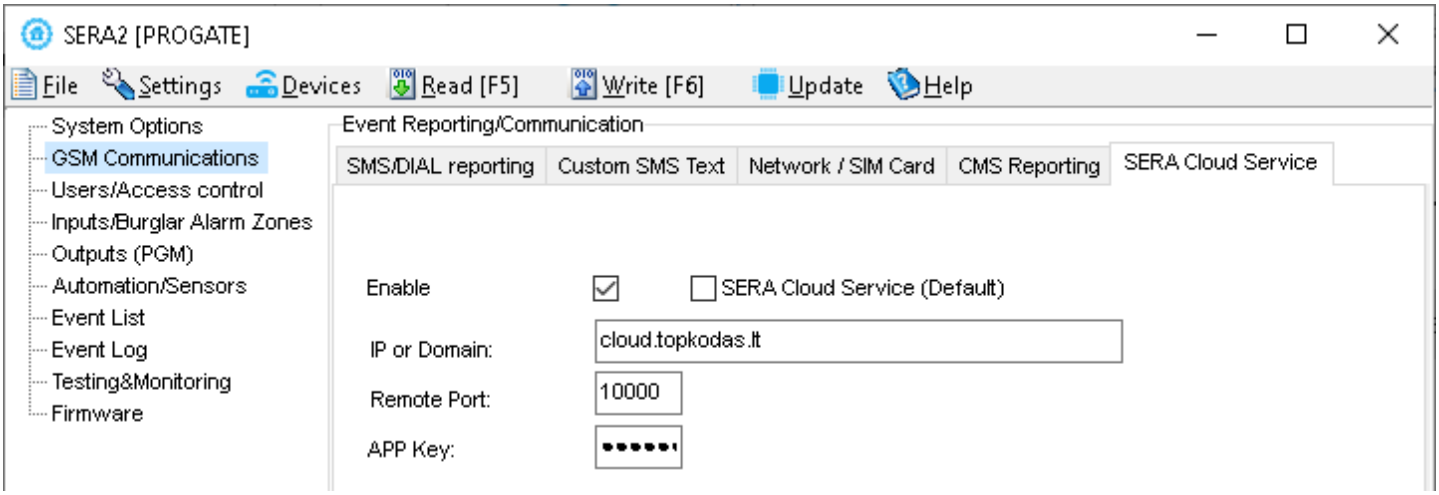
Ensure the SIM card has GPRS/LTE mobile data service activated by the network provider. Usually, this service is enabled by default. If not, reach out to the GSM service provider for activation.

Steps to activate Remote control over internet:

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

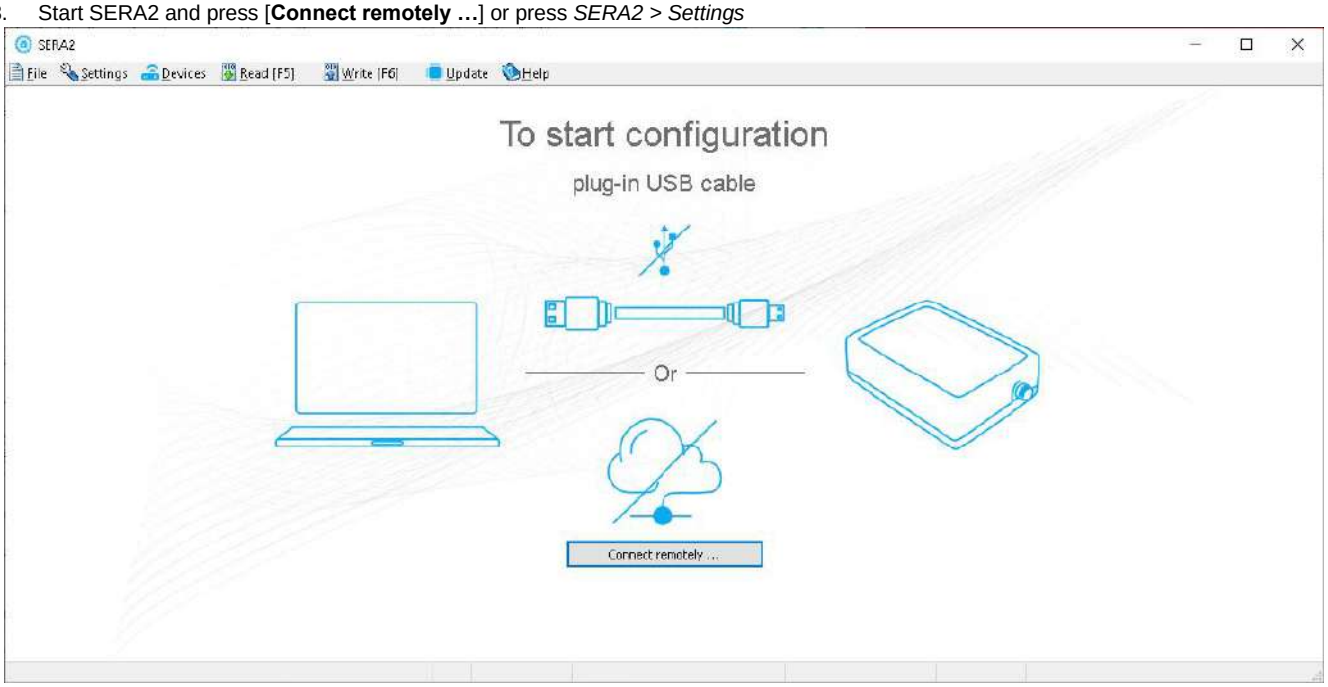


3. If needed, APN/Password/Login/IP/Domain/ Port /PING time /KEY can be set by SMS commands
   INST000000,008,APN#LOGIN#PSW#
   008= command code (GPRS network settings); APN=31 symbols; LOGIN=31 symbols; PSW=31 symbols
   e.g.
   INST000000,008,internet### - Apn="internet and no login and password.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

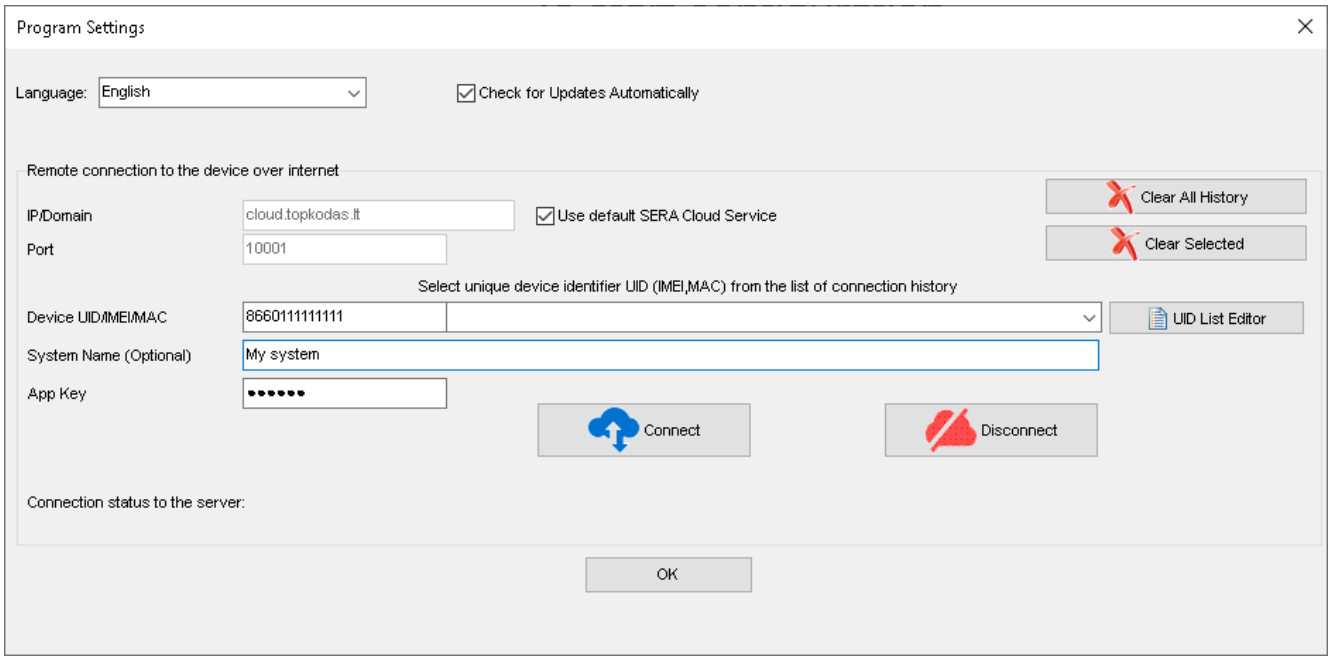


5. Write the configuration into the module by pressing [**Write**]
6. Ready the module by inserting the SIM card, attaching the antenna, and connecting the 12V/1A VDC power supply.
7. Wait for the module to register to the network and connect to the '*SERA Cloud service*'

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



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



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

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

9 SMS Commands for remote control and configuration

List of user SMS commands:

- Control outputs
- Set the system mode: Arm/Disarm/Stay/Sleep
- Bypass zones
- Set the time of the module
- Request zone test and system state
- Forward messages to other number

List of installer SMS commands:

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

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

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

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

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

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

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

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

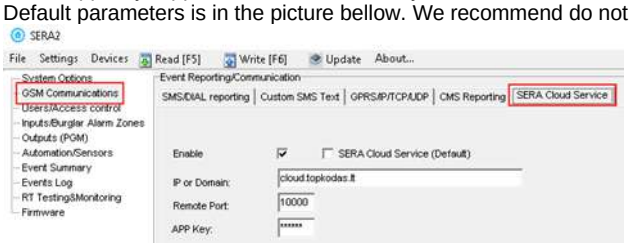
Very important!!! In this guide, '␣' symbolizes a space in SMS commands and examples. Replace '␣' with a space in your SMS texts, avoiding extra spaces or characters. '␣' is used for clarity in examples

9.1 The table of installers SMS commands

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

Table 7 the table of installers commands

INST000000␣001␣ID#TEL#SMS#DIAL# e.g. INST000000␣001␣1#37066666666#11111111#10000000#	**To add admin user phone numbers for SMS and Call notifications upon an event, use the following format:** 001 = Code for adding admin user's phone numbers ID = User index (1-8) TEL = User's phone number (max 16 digits), without (+), including country and operator's code. End with '#' SMS = Notification event filter. 1 sends the event, 0 doesn't. Events are ordered (1.2.3...n), e.g., 001000 DIAL = Dial event filter. 1 dials if the event occurs, 0 doesn't. Events are ordered (1.2.3...n), e.g., 101000 #= delimiter **Example: INST000000 001 1#37066666666#0001000000#0000011111#** The event filter order is as follows, with 0 indicating disabled and 1 enabled: 1. Alarm/Restore (CID 100 group) 2. System Open/Close (CID 400 group) 3. System Troubles (CID 300 group) 4. Sensor1-Sensor32 Alarm/Restore 5. Test Events (CID 600 group) 6. Other Events 7. Input/Zone1 Alarm/Restore 8. Input/Zone2 Alarm/Restore 9. And so on.
INST000000␣002␣ID e.g. Delete admin User1 at index 1 INST000000␣002␣1	**To delete an admin user's phone number (used for SMS notifications), use the command '002' followed by the user ID index (1-8)**. 002 = Command code for deletion ID = User index (1 to 8)
INST000000␣003	**Delete all users in database.** 003 = Command code
INST000000␣004␣ID#TEL#OUT#OPT#NAME# e.g. Add user at index 1 , phone-37066666666, out1 INST000000␣004␣1#37066666666#1#10#Jon#	**To enter user‘s telephone number for remote control via short call** **USER NAME-only Latin characters is allowed inside SMS** 004= command code (enter user‘s telephone number for remote control via short call) ID = user ID number 001-800 TEL = user‘s telephone number (max 16 digits) without (+) comprised of country code, operator‘s code and user‘s telephone number. the end symbol #; OUT= output number, that will be controlled, 1-32. 0-Disabled, 1=OUT1=RELAY,2-OUT2, … OPT = 0 – disabled 1 – enabled, Sequence from the left to the right 1. User Enabled 2. Enable Arm/Disarm system by call NAME = User Name up to 31 characters.
INST000000␣005␣TEL# e.g. delete user associated with phone 37061611111 INST000000␣005␣37061611111	**To delete a user's remote control access according phone number, use:** 005 = Command code for deletion. TEL = User's phone number (16 digits max, without '+'), including country and operator codes. The number must match the one in the module's memory."
INST000000␣006␣ID e.g. delete user at index 200 INST000000␣006␣200	**Delete user's phone number by index.** 006= command code ID = Enter the user's index number from 001 to 800 to delete all data associated with the user.
INST000000␣007␣P#PER#HH:mm# e.g. INST000000␣007␣1#7#18:30#	**Automatic periodical test settings** 007= command code (Automatic periodical test) P= 0-test disabled, 1- test period by 24 hours, 2- period by hours PER= automatic test sending period from 1 to 99999 days or hours HH-hours 0-23, mm- minutes 0-59 e.g. INST000000 007 2#1#14:50# The test will be send every 1 hour
INST000000␣008␣APN#LOGIN#PSW#	**DATA/GPRS/LTE network settings**

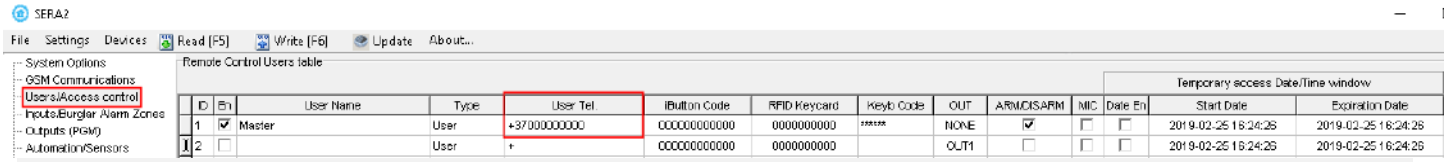
e.g. INST000000␣008␣internet### Apn="internet and no login and password.	008= command code (network settings) APN=31 symbols LOGIN=31 symbols PSW=31 symbols
INST000000␣009␣ADDR#PORT#PING#KEY# e.g. INST000000 009 cloud.topkodas.lt#1000#600#123456#	**SERA cloud Service Parameters** 009= command code (Remote control of the module over the Internet) ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain text length of up to 47 characters) PORT= TCP port number .Default:10000 PING= 600 default. KEY= App Key. App and remote service key. Default:"123456" Default parameters is in the picture bellow. We recommend do not change these parameters. 
INST000000␣010␣E e.g. deactivate cloud service INST000000␣010␣0 e.g. activate cloud service INST000000␣010␣1	**Enable or disable the 'SERA Cloud service' for APP and remote device connection.** 010= command code (To activate the connection to the remote control server). E= 1- (enabled) or 0 - (disabled).
INST000000␣011␣E e.g. INST000000␣011␣1 - Enable GUEST mode e.g. INST000000␣011␣0 - Disable GUEST mode e.g. Dual command 011 and 004 set USER9 INST000000␣011␣1␣004␣9##1#10#Unauthorized# Enable Guest mode on USER9, set control OUT1 Username: 'Guest'	**Enable/Disable GUEST (unauthorized call) mode on USER 9. APP and remote connection to device.** 011= command code (activate GUEST mode on USER 9). Enable incoming call guest mode on USER 9 settings. Module will accept all unauthorized calls and do selected action (e.g. to control an output, gate) on USER 9. E= 1-enabled, 0-disabled
INST000000␣012␣TEL#OUT#OPT#NAME# e.g. INST000000␣012␣37066666666#1#10#Jon#	**Enter the user's telephone number for remote control via a short call without an index.** **USER NAME-only Latin characters is allowed inside SMS** 012= Command code (enter the user's telephone number in the free space for remote control via a short call) TEL = The user's telephone number (max 16 digits) without the (+) sign, consisting of the country code, operator's code, and the user's telephone number. Use the end symbol #. OUT = Output number for remote control that will be controlled value= (0-32). 0 = Disabled, 1=OUT1(RELAY), 2=OUT2… and so on. OPT = 0 – Disabled, 1 – Enabled (Sequence from left to right): 1. User Enabled 2. Enable Arm/Disarm alarm system by call NAME = User Name up to 31 characters.
INST000000␣013␣TEL # NAME# e.g. INST000000␣013␣37066666666#Jon#	**Add the user's telephone number for remote control via a short call to the free space of memory. Enable the user and assign control of RELAY (OUT1).** **i** Note: To assign a user to a specific index or enable user control for other outputs, utilize the commands 004 or 012. 013= Command code TEL = The user's telephone number (max 16 digits) without the (+) sign, consisting of the country code, operator's code, and the user's telephone number. Use the end symbol #. NAME: User Name (optional, up to 31 characters).
INST000000␣018	**View user phone numbers from the user database using:** 018= Command code The response SMS will appear as: **[Enabled],[ID],[Phone],[Output]** Where: User Enabled (0 for disabled, 1 for enabled) ID= User index Phone= User phone number Output= Chosen output number for remote control.
INST000000␣019␣N#P	**To change the operation algorithm of the output**

e.g. INST000000,019,1#24 Set OUT1 as [Access Control]	019= command code (To change the operation algorithm of the output) N = output number from 1 to 32 P = output operation algorithm. Set 0 to 24 0. Disable 1. Bell 2. Buzzer 3. Flash 4. System State 5. ARM Status 6. Remote Control & Automation 7. AC OK 8. Battery OK 9. System Armed Status 10. Alarm Indication 11. Lost Primary Chanel 12. Lost Secondary Chanel 13. Fire Sensor 14. RH Sensor Trouble 15. Access Gained 16. STAY Armed Status 17. SLEEP Armed Status 18. Pulse On ARM / DISARM 19. Output State 20. Zone OK 21. Activate by ARM/DISARM Command 22. Activate by SLEEP/DISARM Command 23. Activate by STAY/DISARM Command 24. Access Control
INST000000,020,N	**Invert output state** 020= command code (outputs inversion) N = output number from 1 to 32.
INST000000,021,N#ST	**Output activation or deactivation** 021= command code (Output activation or deactivation) N = output number 1-32 ST = output mode 0 – OFF, 1- ON
INST000000,022,N#TIME#	**Output activation for the time interval** 022= command code (Output activation for the time interval) N = output number 1-32 TIME = 0-999999 Time interval in seconds for the output activation.
INST000000,030,ST	**Change security system's mode (ARM/DISARM/STAY/SLEEP)** 030= command code (Change security system's mode) ST = 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP
INST000000,031,ZN#BYP	**Zone bypassing by sms command** 031= command code (Zone bypassing) ZN = zone number from 1 to 32 BYP= 1 – zone bypass 0- zone active.
INST000000,063,S	**iButton keys learning/deleting mode** 063= command code (iButton keys learning/deleting mode) S=iButton keys entering/deletion mode. 0-Disable iButton/RFID keys learning mode 1-Enable iButton/RFID keys learning mode 2-iButton/RFID keys deleting mode. To delete these keys from memory, which will be touched to the reader
INST000000,070,N#VALUE # e.g. INST000000,070,1#23.5#	**Programming of max sensors value upon reaching, the SMS message with „High Alarm" text will be sent** 070= command code (max sensors value upon reaching which, the SMS message with „High Alarm" text will be sent) N = sensor number VALUE= Format 0000.00 High Alarm Value
INST000000,071,N#VALUE #	**Programming of minimal sensors value upon reaching the SMS message with „Low Alarm" text will be sent** 071= command code (min sensors value upon reaching which, the SMS message with „Low Alarm" text will be sent) N = sensor number VALUE = Format 0000.00 Low Alarm Value
INST000000,072,N#VALUE#	**Programming of sensor max value upon reaching the selected output will be activated.** For example, cooling equipment 072= command code (sensor max value upon reaching the selected output will be activated.) N = sensor number VALUE= Format 0000.00 sensor max value upon reaching, the selected output will be activated.
INST000000,073,N#VALUE#	**Programming of sensor min value upon reaching the selected output will be activated.** For example, heating equipment 073= command code (sensor min value upon reaching the selected output will be activated.) N = sensor number VALUE= Format 0000.00 Sensor min value upon reaching which, the output will be activated.
INST000000,090,NewInstPsw	**Change installer's password** (Installers password should be changed before exploitation of the

	module) 090= command code (Change of installer‘s password) NewInstPsw = New Installer‘s password.
INST000000␣091␣NewUserPsw e.g. INST000000␣091␣654321	**Change user‘s password** (User‘s password should be changed before exploitation of the module) 091= command code (Change user‘s password) NewUserPsw = New user‘s password.
INST000000␣092	**Remote reset of the module via SMS messages** 092= command code (Remote reset of the module via SMS messages)
INST000000␣093␣yyyy/MM/dd#HH:mm#	**Time of the module setting via SMS message.** The time is usually synchronized via a server or mobile network. However, if synchronization is disabled, it can be set manually via SMS. 093= command code (Time of the module setting via SMS message) Time format of the module: yyyy/MM/dd#HH:mm# yyyy -year MM-month 1-12 dd - day of the month 1-31 HH-hours 0-23 mm- minutes 0-59
INST000000␣094␣TEL#SMS e.g. INST000000␣094␣+370616111111#Hello	**SMS from the module forwarding to the other phone number** 094= command code (SMS from the module resending to the other phone number) TEL = phone number to which will be forwarded sms text SMS = sms text that will be send to the referred number. TEL=861611111111 local number or international format e.g. +370616111111 **SMS text =Latin Charset** After this command could not be other commands like: 094 SMS 030 1 because all messages will be forwarded to other numer "SMS 030 1"
INST 000000␣095␣E	**Zone Walk Test request** 095= command code (Zone Test request) E = 1- test request activated, 0- test request deactivated When zone is activated, the bell generates the sound, ARM/DISARM system automatically turn off this function
INST 000000␣096	**Fire sensors reset.**
INST000000␣100␣N	**System state request:** 100= command code (System state request) N = System state request type 1- System test request, Request information about the module (: IMEI, FW, LEVEL etc.) 2- the values of active sensors request 3 -Request about active zone states 4 -Request about output states 5 - System state request. The module will send information on input/output states and system state (ARM/DISARM/STAY).

9.2 The table of users SMS commands

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



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

Table 8 the table of user's commands

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

10 System Info of device and Firmware Updates

System Options > System Info

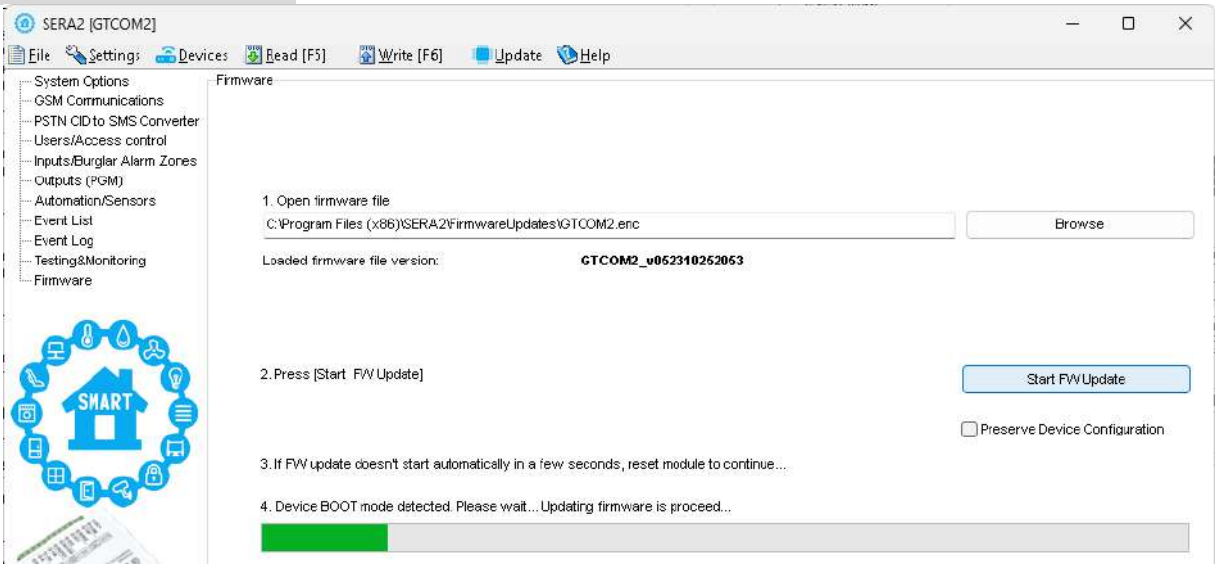
The System Info window let you take a look to the main hardware, boot loader, firmware, serial no, IMEI, GSM Modem information.

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

Firmware Update:

SERA2 > Firmware

This window let you update the firmware of the module.



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

Firmware Update Steps:

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

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

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

11 Warranty Terms and Conditions

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

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

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

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

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

Items Not Covered by Warranty

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

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

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

Disclaimer of Warranties

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

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

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

WARNING - READ CAREFULLY

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

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

• Inadequate Installation
The module must be installed properly in order to provide adequate protection.
• Criminal Knowledge
This system contains security features which were known to be effective at the time of manufacture. It is possible for persons
With criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.
• Access by Intruders
Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.
• Power Failure
Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.
• Failure of Replaceable Batteries
Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.
• Compromise of GSM network
Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent signal interference.
• System Users
A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the module and that they know how to respond when the system indicates an alarm
• Smoke Detectors
Smoke detectors may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.
Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fire is equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, and improper storage of flammable materials, overloaded electrical circuits, and children playing with matches or arson.
Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.
• Motion Detectors
Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.
Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.
• Warning Devices
Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.
• GSM network
If GSM network are used to transmit alarms, it may be out of service for certain periods of time.
• Insufficient Time
There may be circumstances when the system will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.
• Component Failure
Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.
• Inadequate Testing
Most problems that would prevent the module from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an accident, or any kind of construction activity inside or outside the premises.
•Security and Insurance
Regardless of its capabilities, the module PROGATE is not a substitute for property or life insurance. The module PROGATE also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation.