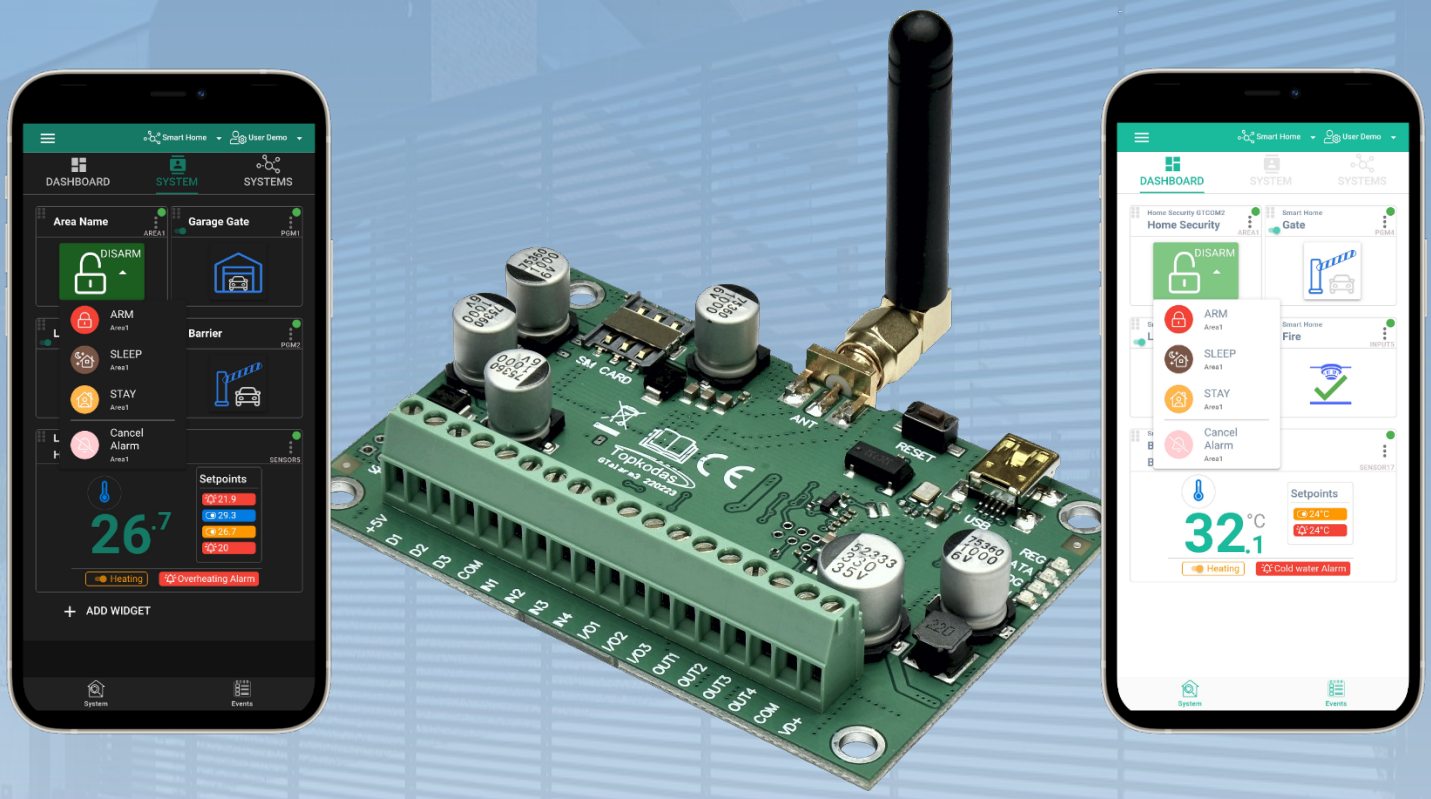
TOPKODAS

GTalarm3

Installation & Programming Manual



Security and automation system

Multifunctional device: access control + security + home automation

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

DESCRIPTION

Introducing GTalarm3, a powerful and flexible hybrid GSM smart home alarm system and automation solution, designed to secure and monitor various types of properties, including private boats, houses, cottages, village houses, garages, warehouses, and other buildings. GTalarm3 employs IoT Cloud GSM technology, allowing for remote monitoring and control of temperature and humidity, making it suitable for a wide range of applications.

FEATURES

- Reporting:
  - 8 cellular numbers through SMS
  - 8 cellular numbers Alarm calls
  - Android / iOS **SERANOVA** app push notifications.
  - Reporting system events to a central monitoring station using Internet Protocol Event Reporting with event type Contact ID. IP communication data is sent using the SIA IP DC09 standard protocol, which supports Ping supervision, AES128 Encoding, TCP/IP or UDP/IP via GSM GPRS. The supported versions of SIA DC09 standards:
    - ANSI/SIA DC-09-2007
    - ANSI/SIA DC-09-2012
    - ANSI/SIA DC-09-2013.
- Support for up to 32 wired zones for various security applications.
- Compatibility with 2-Wire or 4-Wire sensors for fire alarm systems.
- Built-in access control features. Access control for gates, doors, barriers, and more.
- 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
  - CALL for easy device management
  - Web app compatible with standard web browsers for increased accessibility
- Six ways to control PGM outputs and ARM/DISARM security system: Call, App, SMS, RFID, iButton, or Code.
- Up to 8 users can receive information about the protected object via SMS or DIAL short call.
- Remote configuration and monitoring via cloud service.
- 4 PGM outputs 24V/1000mA. Open Drain.
- 3 Input/Output Configurable. Analog inputs 0-30V / 4-20mA
- Up to 32 precision temperature and relative humidity sensors.
- Support for up to 32 sensor monitoring and control points with multi-point thermostat functionality
- Thermostat and automation support for up to 32 digital sensors, ideal for various temperature-sensitive environments.
- Controls heating or cooling equipment as well as humidifiers or dehumidifiers.
- Adjustable temperature set levels, relative humidity levels, and the differential between high and low set points.
- Ability to calibrate sensors.
- Custom units for sensor values.
- Sensors keep constant track of temperature and humidity levels.
- Programmable sensor hysteresis, control, alarm, restore values, and time delay.
- Remote configuration and control via GPRS connection, USB with SERA2 software, or the free **SERANOVA** app
- In-field firmware upgrade via USB and SERA2 software.
- Built-in access control features.
- Events log buffer. 3072 events.
- Built-in real-time clock backup battery.

GTalarm3 can be programmed remotely via GPRS connection or via USB using SERA2 upload/download software or the free app SERANOVA. This system is designed for ease of use and offers installers labor-saving features such as the ability to save configurations and transfer them to other modules when needed.

The GTalarm3 system is a comprehensive solution for installers looking to address security, access control, and home automation needs.

APPLICATIONS

The GTalarm3 system offers a wide range of applications across various sectors, ensuring the security, comfort, and efficient management of different environments. Here are some key applications:

- **Residential Security**: GTalarm3 can be used to secure homes, apartments, cottages, and village houses. It provides a comprehensive security solution with up to 32 wired zones, access control, and remote monitoring through the SERANOVA app.
- **Boat Security**: GTalarm3 can be adapted to secure private boats, yachts, and other marine vessels, providing protection against theft, fire, and unauthorized access.
- **Commercial Security**: GTalarm3 is suitable for securing commercial spaces such as offices, retail stores, and warehouses. Its access control features can help manage employee access and track entry/exit events.
- **Temperature and Humidity Control**: GTalarm3 can be used for managing the temperature and humidity in various environments, including greenhouses, server rooms, and storage facilities for temperature-sensitive goods like food, medicines, and agricultural crops.
- **Fire Alarm Systems**: GTalarm3 supports 2-Wire or 4-Wire sensors, making it an ideal choice for fire alarm systems in both residential and commercial settings.
- **Access Control**: GTalarm3 can be used for managing access to gates, doors, and barriers in residential, commercial, and industrial environments, ensuring only authorized individuals can enter.
- **HVAC Management**: The system's thermostat and automation capabilities make it suitable for managing heating, ventilation, and air conditioning (HVAC) systems in homes, small offices, and holiday houses.
- **Cold Storage Monitoring**: GTalarm3 can be used to monitor and control temperature and humidity in cold storage facilities for food, meat, medicines, and vaccines, ensuring optimal conditions are maintained.
- **Agricultural Applications**: The system is ideal for monitoring and controlling temperature and humidity levels in various agricultural settings, such as greenhouses, crop storage facilities, and growing tents.
- **Remote Control and Monitoring**: GTalarm3 allows users to remotely control and monitor various devices through its app, SMS, DIAL, and web internet capabilities, providing convenience and peace of mind.

These are just a few of the many possible applications of the GTalarm3 system. Its flexibility and adaptability make it a valuable solution for a wide range of security, access control, and environmental monitoring needs.

DOWNLOAD SERANOVA APP
by Scanning the QR Code

GET IT ON Google Play

Download on the App Store

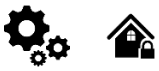
The meaning of icons in the manual:

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

Contents

1 General information about the module GTalarm3

1.1 Specifications



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

Outputs (PGM) OUT1-OUT4:
max current – (-V) 1000 mA;
All outputs can be controlled via short call DIAL or via SMS message. This feature may be used for gate opening.
Output alarm parameters may be programmed;
Programmable algorithms for outputs operation: CTRL/SMS/DIAL, SIREN, BUZER, ARM state, Zones OK, Light ; Flash, inverting, pulse mode

IN1 - IN4 inputs:
Custom SMS text for input alarm and restore;
Burglary alarm zones. Input type NC/NO/EOL/EOL+TAMPER 2.2K + 2.2K;
10K pull up resistor;
Analog input 0-30V;
Algorithm for zones operation: delay, interior, instant, 24 hours, silent, fire;
Response time;
Time of repeatable Alarm/Restore;
Commutation of selected output;

Inputs/outputs I/O1, I/O2, I/O3:
Programmable input or output;
Burglary alarm zones. Input type: Input type NC/NO/EOL/EOL+TAMPER 2.2K + 2.2K;
Analog 0-30V/0-20mA/4-20mA;
Current loop 2-wire smoke detector mode.

Digital inputs/ outputs D1-D3:
Dallas 1-Wire Bus, DS18b20, DS1990A;
Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321;
Wiegand interface DATA0/ DATA1, RFID reader, Keyboard;
The total length of the bus from 10 to 100m.

Expansion modules or programmable input/output:
Expandable inputs up to 32
Expandable outputs up to 32

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

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

Noce resistant MIC and Speaker (Optional feature)

Power supply voltage:
DC 8-30 V / 300mA max
Max. Allowed ripple voltage 100mV.

Consumption current:
In standby mode less than 50 mA.
In dialing or SMS/GPRS sending mode less than 300 mA.

Events Log:
Nonvolatile flash events log 3072 events

4.5V power source output for external modules:
Voltage 4.5V
Current limit 100mA

Environmental parameters:
Storage temperature range from -40 to +85 °C / -40 to 185 °F
Operational temperature range from -30 to +75 °C / from -22 to 167 °F
Max relative humidity under +40 °C / 104 °F 95%

Package weight 90g
Module weight: 43g
Overall dimensions of the module: 84x66x18mm

1.2 Used definitions and terms


Term	Description
Alarm Log	Records of active alarms or alarms that were raised and resolved, useful for problem analysis.
Arming/Disarming	The process to activate or deactivate the system's security.
Authorized user	A person with a mobile number registered in the GTalarm3 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	The identification of the caller.
COM	Negative power supply terminal.
Configuration	Setting the operational parameters of an item, like phone numbers, input names, and more.
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 for analysis. 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 updates like date, status, signal strength, and more.
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.
CMS	Central monitoring station
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

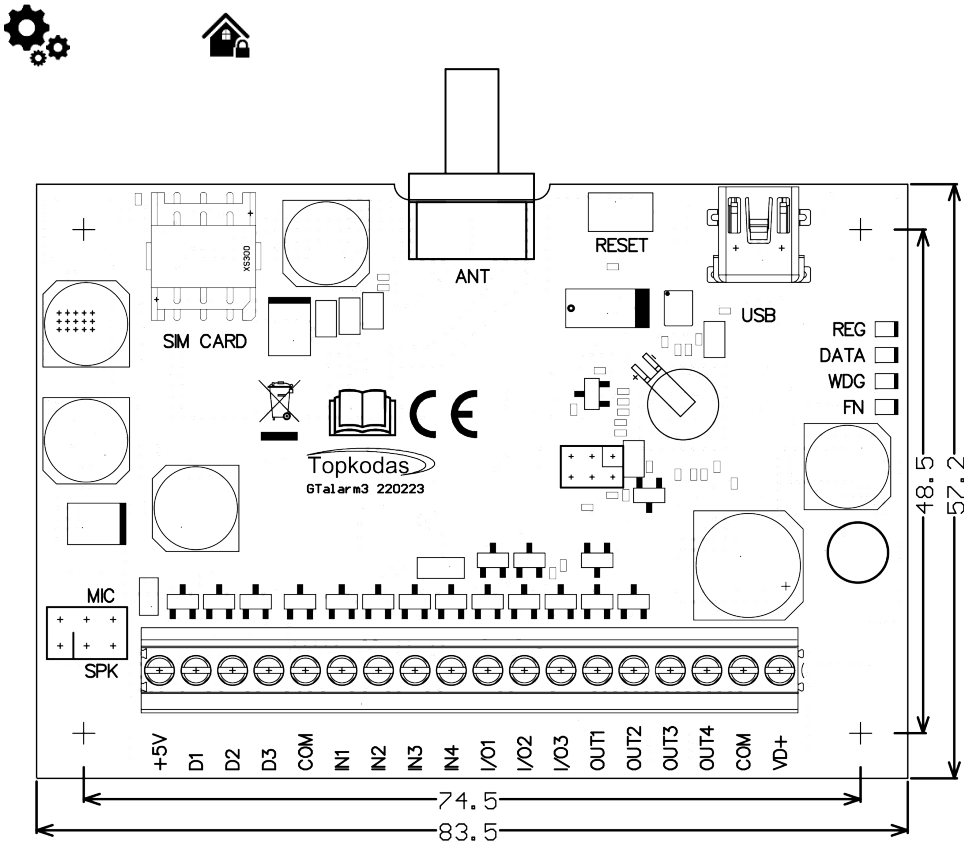
	
GTalarm3 module – 1 pcs	Shipping Package - 1 pcs

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

Table 2 Additional, under request package content

			
Mini USB cable	Plug-in type Switching Power Supply 12V/1A AC/DC	TPS12 13.7V/1.8A AC/DC Mini UPS Switching Power Supply with backup battery charging	Din Rail mounting adapter
			
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		Wiegand keypad & RFID reader
			
2.2 kOhm resistors - 14pcs	Spaces for PCB installation - 4 pcs		External microphone with 1 m cable and connecto

1.4 General view of the module



1. Nano SIM card holder of “Push-Pull” type
2. GSM antenna connector
3. RESET button
4. Mini USB programming connector
5. REG (yellow) see table 3
6. DATA (red) see table 3
7. WDG (green) see table 3
8. FN (BLUE) see table 3
9. Power supply and input/output connector
10. External microphone connector (optional)

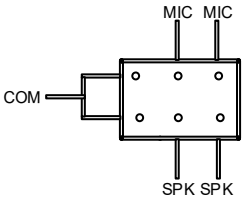


Figure 1 GTalarm3 PCB Layout

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

1.5 Meaning of LEDs and contacts

Table 3 Meaning of LEDs

Name	Indication variations	Meaning
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 reports has been send.
FN	Function LED	The programmable FN LED indicates functions like Input/Output status or system state.

Table 4 Terminal block. Contacts.

Contact No	Name	Max. voltage (V)	Optional functions and Description	
1	VD+	30	Positive supply contact	
			Power supply voltage	DC 8-30 V / 300mA max, Max. Allowed ripple voltage 100mV.
			Current in standby mode	<50mA
			Current when sending data	<300mA
2	COM		Negative supply terminal for keyboard(s), indicators and sensors.	
3 … 6	OUT1 ... OUT4	30	Programmable Output PGM1 - PGM4. Drain type. When state is ON, connects internally to COM	
			Max available current	1000mA
			Max available voltage	30V
7…9	I/O1-I/O3	30	Programmable functions	The zone for security system NC/NO/EOL/EOL+Tamper
				Output 20mA
				Analog current input 0-20mA
				Analog voltage input 0-30V
			Max available voltage	30V
10…13	IN1 … IN4	30	Programmable functions	Input with 10K resistor to the VD+ (Pull UP)
				Zone: NC, NO , EOL=2.2kΩ , EOL+ Tamper = 2.2K+2.2K
				Analog input 0-30V
			Max available voltage	30V
14	COM		Negative supply terminal for keyboard(s), indicators and sensors.	
15	D3	3.3	Programmable functions	Digital output
				Digital input
				Dallas 1-Wire bus. DS18b20, DS1990A
				Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
				Wiegand (1) interface DATA1 , RFID reader, keypad
			Max available voltage	3.3V
			Max available current	20mA
16	D2	3.3	Programmable functions	Digital output
				Digital input
				Dallas 1-Wire bus. DS18b20, DS1990A
				Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
				Wiegand (1) interface DATA0 , RFID reader, keypad
			Max available voltage	3.3V
			Max available current	20mA
17	D1	3.3	Programmable functions	Digital output
				Digital input
				Dallas 1-Wire bus. DS18b20, DS1990A
				Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
			Max available voltage	3.3V
			Max available current	20mA
18	+5V	4,5	Power supply for external temperature, humidity sensors	
			Max available voltage	4,5V
			Max available current	100mA

2 QUICK START: Initial Steps for GTalarm3 and SERA2 Software Preparation

YouTube LT QUICK START https://youtu.be/NR35lbFdi8A

2.1 Preparation

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

2.2 Control with free short call

The first one to call the controller will become the system administrator/owner. The controller automatically rejects the call and will be the only one who can administer and control the controller with free short call, SMS commands. When calling GTalarm3 for the first time, the phone number is stored in the module memory automatically. This means that it will be possible to control the first output OUT1 and ARM/DISARM the system with a short, free call. If this is enough, GTalarm3 can be installed without additional configuration.

CALL THE MODULE FROM YOUR MOBILE PHONE, AND YOU WILL RECEIVE AN SMS FROM THE MODULE.

2.3 Configuration methods

It is possible to configure device in following methods:

- **SERA2** software via **USB**
- **SERA2 remote** connection over internet Cloud service
- **SERANOVA app**

SMS text commands. For more details, see: *6.1 The table of installers SMS commands*Error: Reference source not found

In order to configure and control the device by SMS text message, send the text command to the GTalarm3 SIM card from one of the listed administrator phone numbers.

2.3.1 SERA2 software

SERA2 software is intended for GTalarm3 configuration locally via USB port or remotely via 'SERA Cloud Service' internet GPRS/LTE 2G/3G/4G network. This software simplifies system configuration process. SERA2 software is free, which you can download from our website: www.topkodas.lt

2.3.1.1 SE

RA2 Software Installation:

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

2.3.1.2 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]

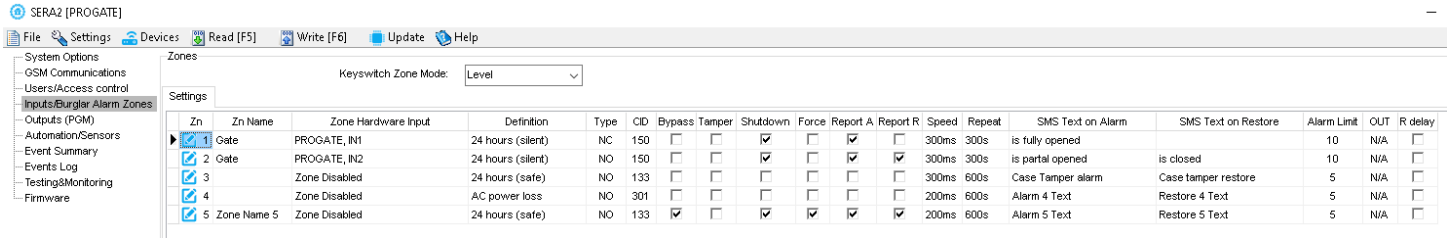


Figure 2SERA2> Inputs/ Burglar Alarm Zones

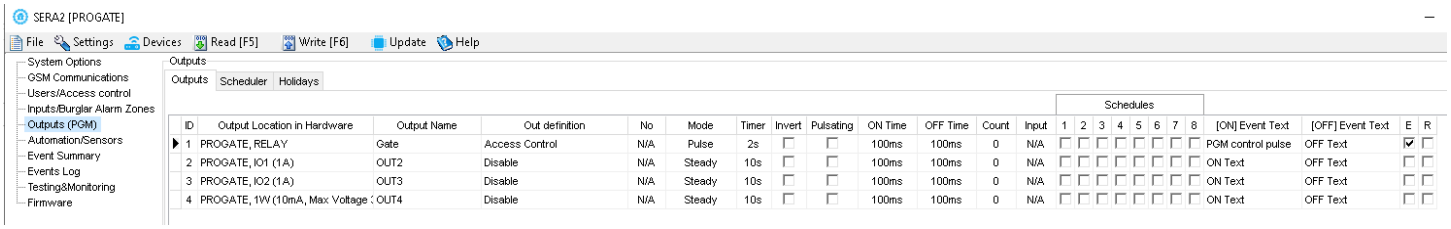


Figure 3SERA2> Outputs (PGM)

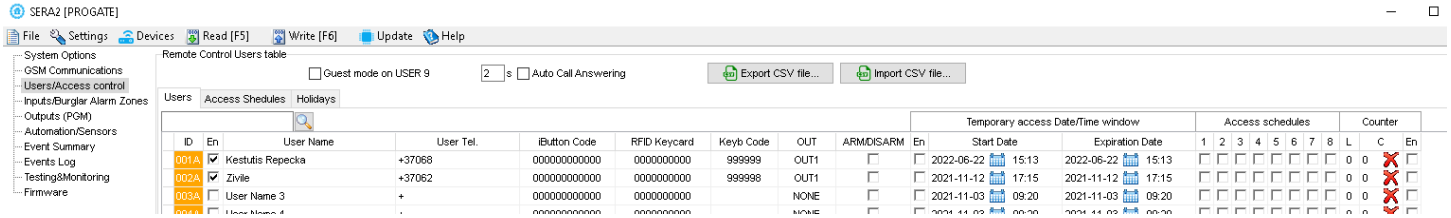


Figure 4SERA2> Users/ Access control

2.4 SERA2/SERANOVA APP Remote connection to module via internet using [SERA could service]

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.*

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
  - Full Hardware Monitoring system status, input voltages including temperature sensors, GSM network parameters level.
  - Update the module's firmware.
  - Read log

How does it works?

- **Connection Protocol**: A GPRS/LTE-backed TCP/IP protocol.
- **Connecting Platform**: The GSM module links through GPRS/LTE to the SERA cloud server.
- UID (IMEI) used when connecting: the SERA2 tool establishes the connection using the unique IMEI of the module.
- **Communication Pathways:**
  - GTalarm3 ↔ [SERA Cloud Service] ↔ SERA2
  - GTalarm3 ↔ [SERA Cloud Service] ↔ SERANOVA app (compatible across Android, iOS, and standard web browsers like Firefox, Chrome, etc.)
- **SERA Cloud Server's Role**: Forms a tunnel between GTalarm3 and either SERA2 or the designated app, enabling mutual communication via TCP protocol.

Note: Ensure the GPRS service is activated on the SIM card used in the GSM module. Typically, this service is automatically activated. If not, contact your GSM service provider to initiate it. It's recommended to use a SIM card that has a mobile data plan. On average, the module consumes between 10-50MB of mobile data monthly.

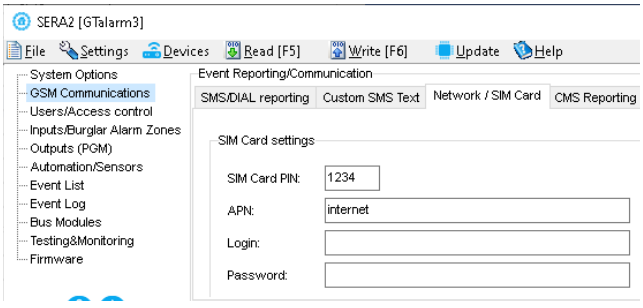
GPRS Service Specifications:

- Activation is mandatory for the GSM module's SIM card.
- Typically, GPRS service activates by default. If not, contact the GSM service provider for activation procedures.
- Employ a SIM card with a data plan enabled.
- Data Consumption Estimation: Between 10 to 50MB monthly.

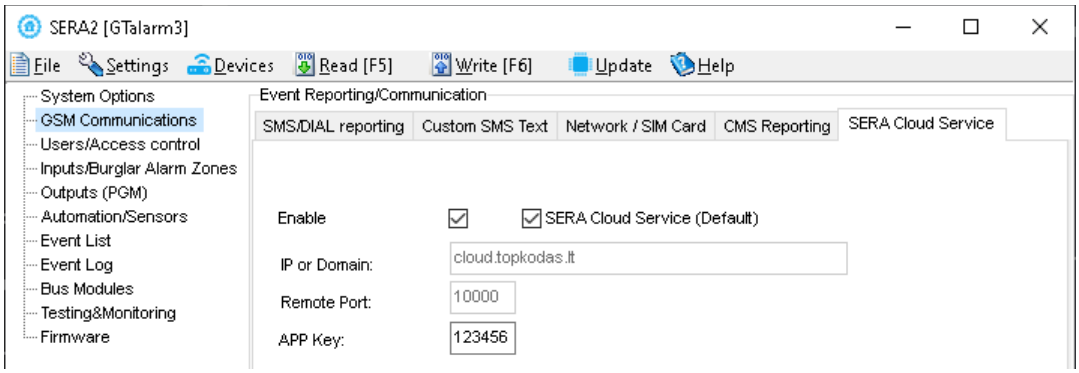
Setting up Remote Control over the Internet:

- Install SERA2 software.
- Navigate to SERA2>GSM Communications>Network/SIM Card tab.
- Configure APN, Login, Password (information from network provider).
- Access SERA2>GSM Communications>SERA Cloud Service tab. Activate [SERA Cloud Service] with default settings.

Sync the updated configuration to the module via the [Write] option.



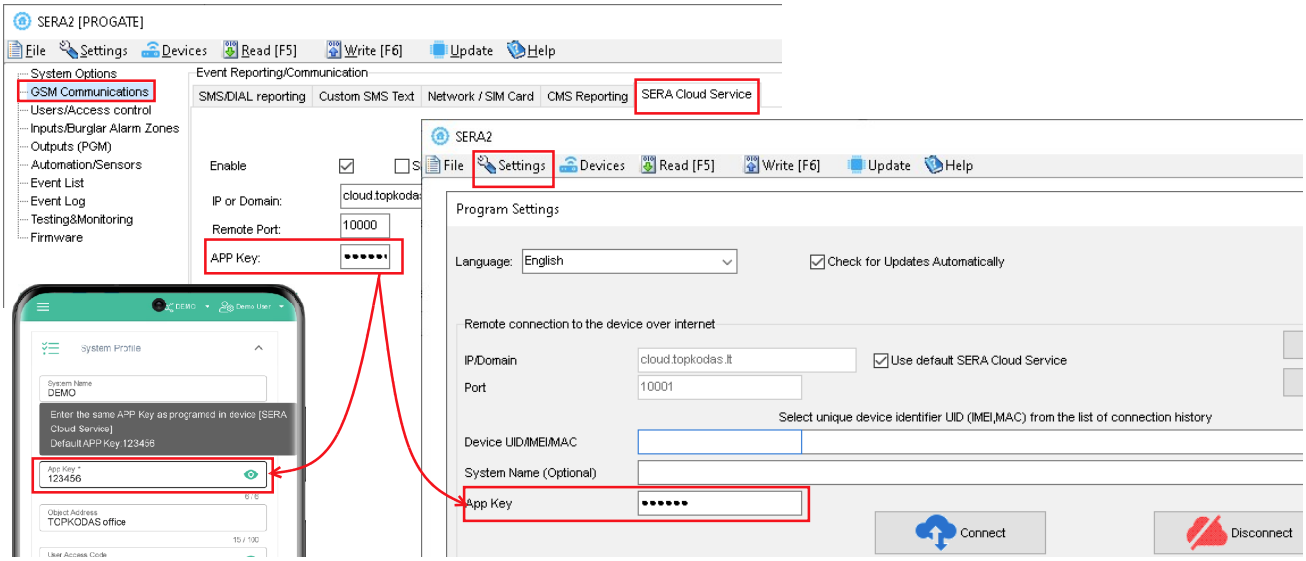
Ensure the APN is accurately set. An incorrect APN may disrupt data and VoLTE services. Consult your network provider for the correct APN details.



Enable	Toggle to 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	Default port is 10000; ensure no firewall interference.
Encryption 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.
- Use the same AppKey (default: 123456) across the module and SERA2 app.
- **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.
- To connect, use the module's UID (IMEI) and AppKey (default: 123456).
- Confirm matching App Key on the device with 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

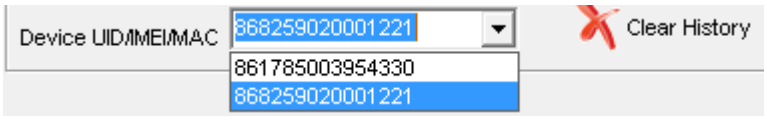
INST000000_008_APN#LOGIN#PSW#

- **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 (range: 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”.

2.5 Control with SERANOVA (Android/iOS) app

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

2.5.1 Steps to get started with SERANOVA

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

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

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

Launch As Web App

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

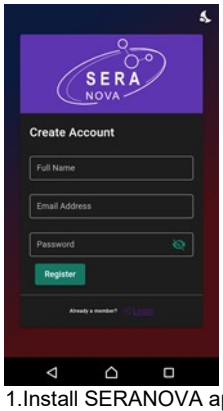
Download on the App Store

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

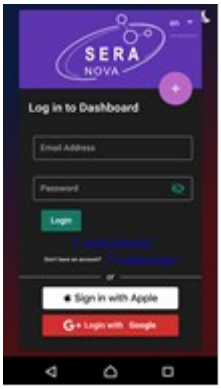
2. **Register** or sign in to your account.
3. **How Get IMEI**: To add a system, the device's IMEI is required. Obtain the IMEI by:
   - Making the initial call to the device. The first caller becomes the owner and administrator and receives an SMS with the IMEI from GTalarm3. Copy the IMEI, which serves 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

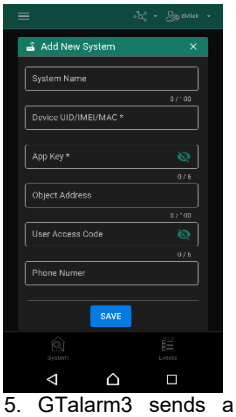
Enter a valid email address of a user who already has a SERANOVA account. The system will be automatically added to the user's account. If the user is added without a valid SERANOVA account email. The user can create a SERANOVA account later and add the system manually.



1.Install SERANOVA app
2.Create account

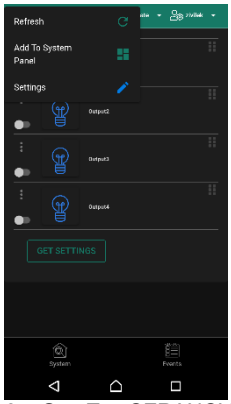


3.Log In
4. The first person to call the GTalarm3 SIM card number becomes the owner and administrator.

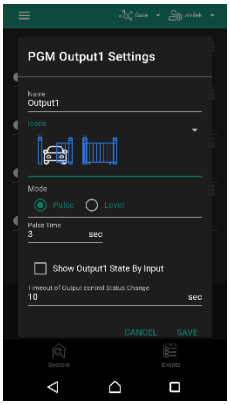


5. GTalarm3 sends a message with the IMEI
6. Enter the IMEI and App Key (Default 123456), **Enter User access code (Default 123456)**

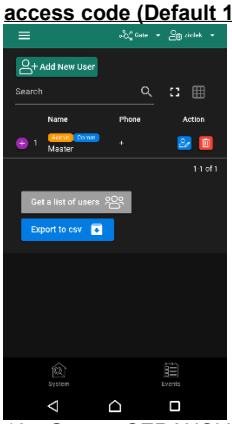
7. The system is now manageable



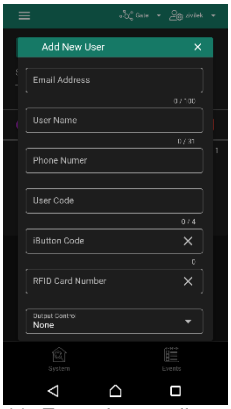
8. Go To SERANOVA> Menu> Outputs. Edit settings



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*

2.6 Control with SMS messages

Control the RELAY output with this SMS command:
Activate or deactivate selected output
USER123456␣021␣N#ST
021= command code
(Activate or deactivate selected output N)
N = output number
ST= output mode:
0 – deactivated output, 1- activated output
E.g. send SMS: USER123456␣021␣1#1 to activate OUT1.

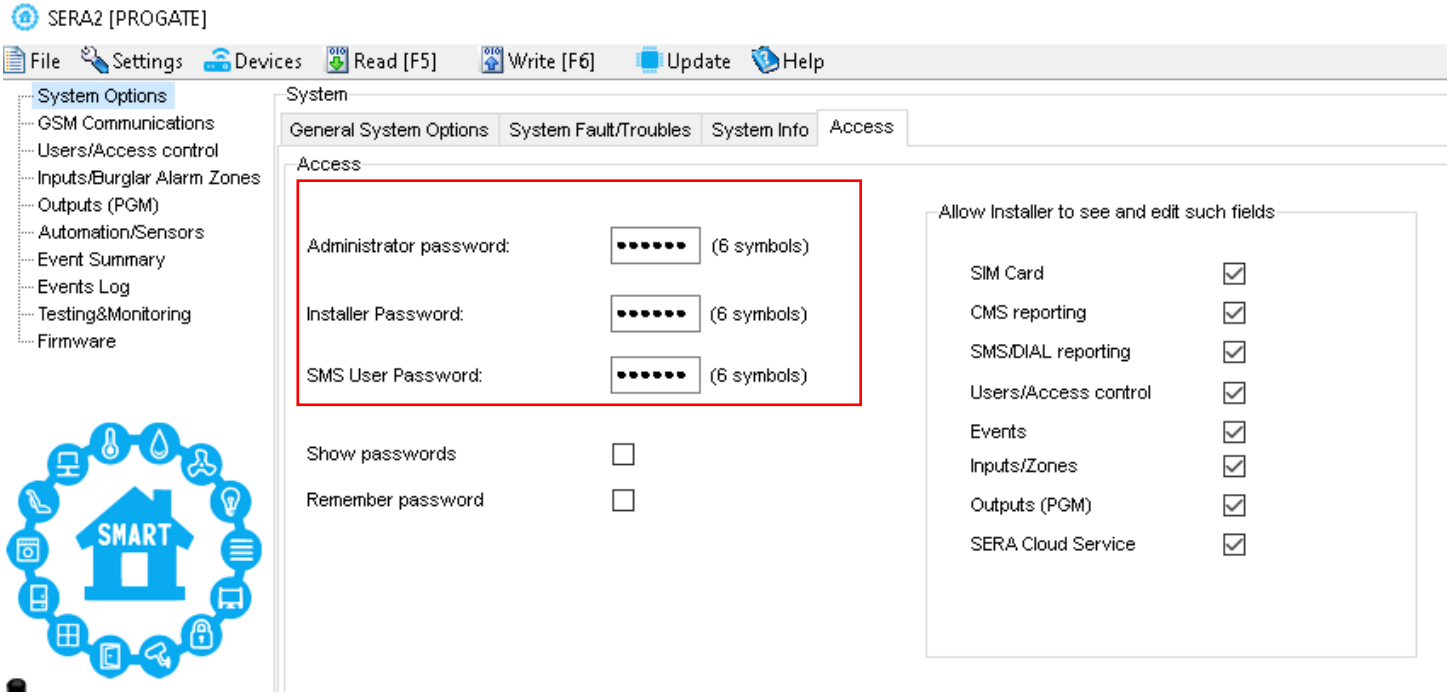
Output pulse activation for the time interval
USER123456␣022␣N#TIME#
022= command code,
N = output number 1-32;
TIME = 0-999999 Time interval in seconds for the output activation.
e.g. USER123456␣022␣2#5# Activate OUT2 for 5 seconds

3 System Access: Codes, Passwords, and Permissions

3.1 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 *6.1* 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 *6.2* 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



3.2 User codes for access control via keypad and SERANOVA app

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

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

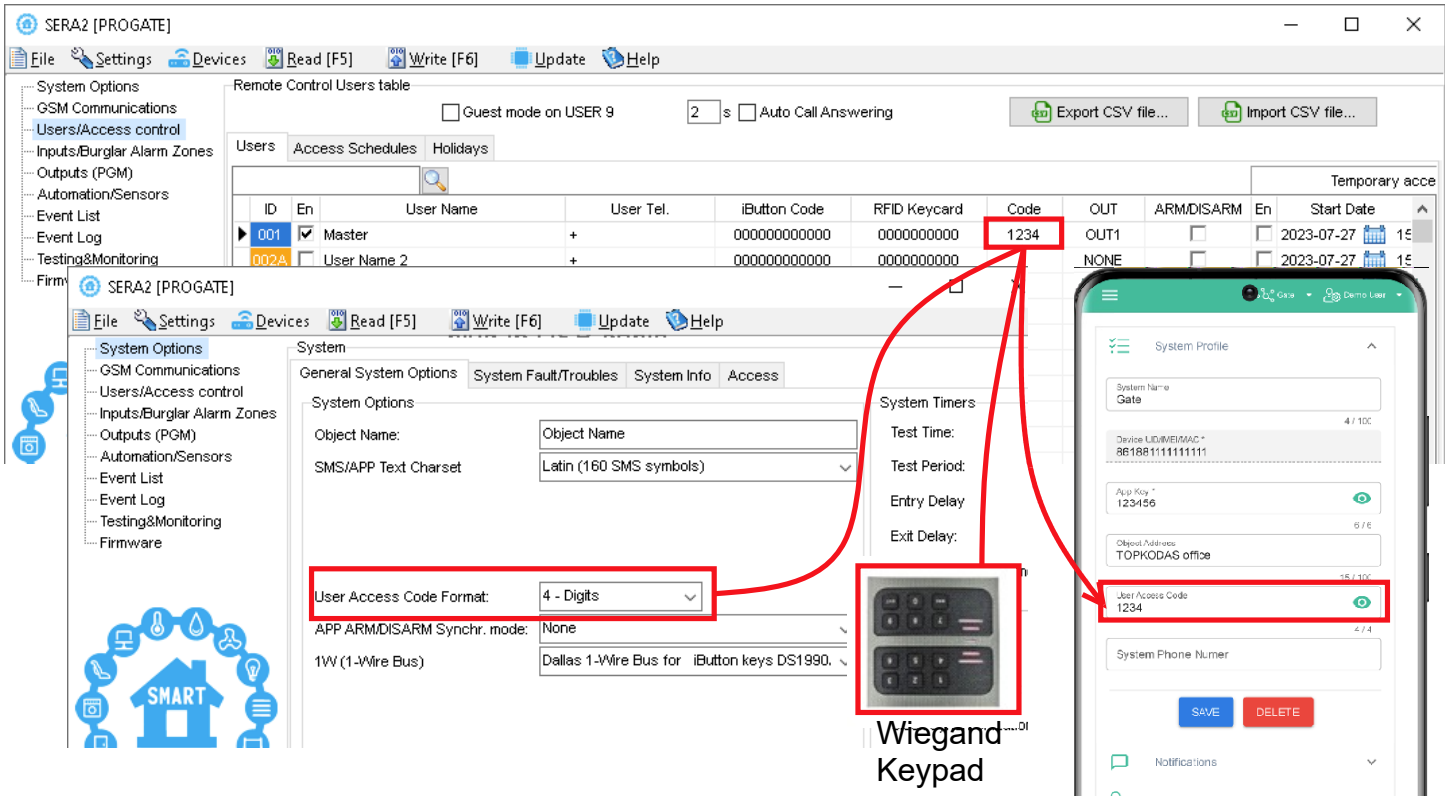


Figure 5User/ Access control and System Options> General System Options

3.3 Access control. Arming/Disarming methods

Arming Process:

- **Ready State**: The system will arm if there are no violated zones or tampers.
- **Unready State**: If any zones are violated or tampers are detected, the system won't arm. Instead, it will notify the user of the infringements either through an SMS to their phone or a push notification in the SERANOVA app. To proceed:
  - Restore all violated zones and tampers.
  - Or, bypass or disable the violated zones, enable the Force attribute, and disable any tampers.

Once set, the system starts an exit delay countdown, giving the user a window to vacate the secured area.

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

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

YouTube LT Access control: schedules, temporary access https://youtu.be/W5FSvN-Uitl

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

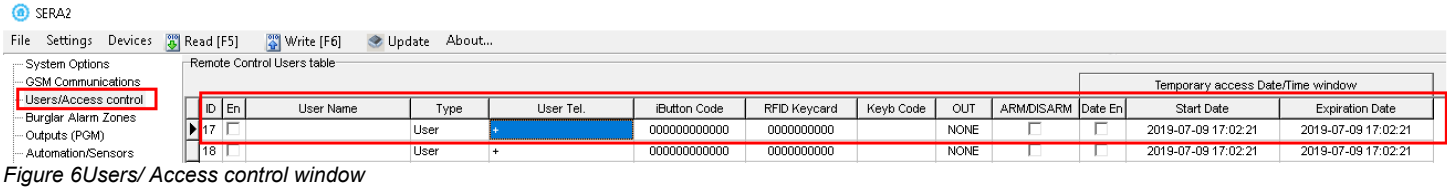
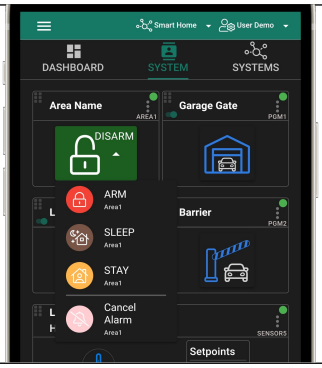


Figure 6Users/ Access control window



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.

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.

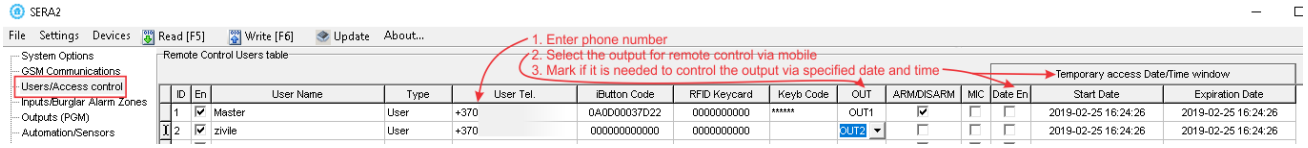


Figure 7 ARM/ DISARM by call settings

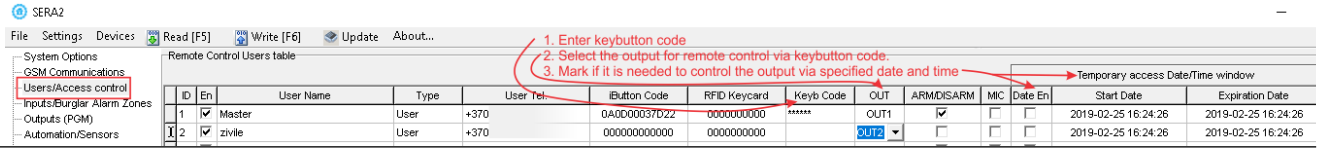
Arm/Disarm via SMS

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

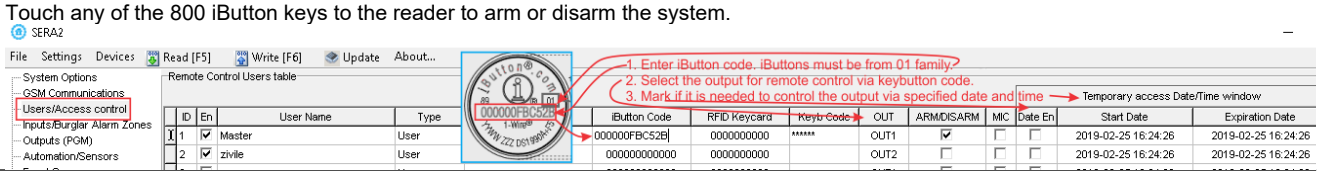
Arm/Disarm by Wiegand keypad

- 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.



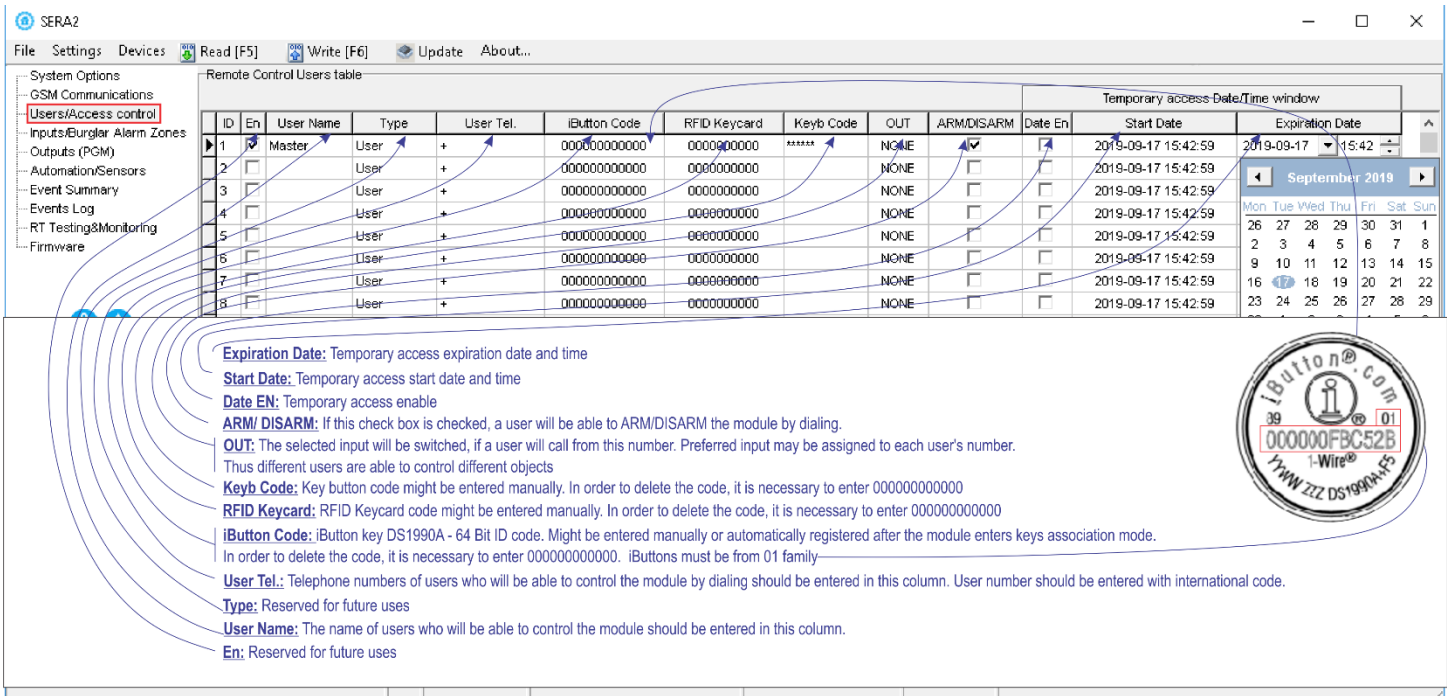
Arm/Disarm by RFID key card, keyfob

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,
You have to read it press [Read]
Edit settings
Write edited configuration press [Write]

More information about how to configure Arming/ Disarming:

3.4 Users & Access Control programming details.



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

The GTalarm3 module has User Access Schedules for controlling access. Inputs, outputs, readers, and cards are all set up with schedules that dictate their activation or deactivation times. For example, a user could be granted access to control a specific output from 12:00 a.m. to 6:00 a.m. daily. This time frame, from 12:00 a.m. to 6:00 a.m., Monday through Sunday, is defined as a schedule during which the user can open the Gate. These schedules can be configured under the Users> Access Schedules tab to view User Schedules, click on the "Access Schedules" tab.

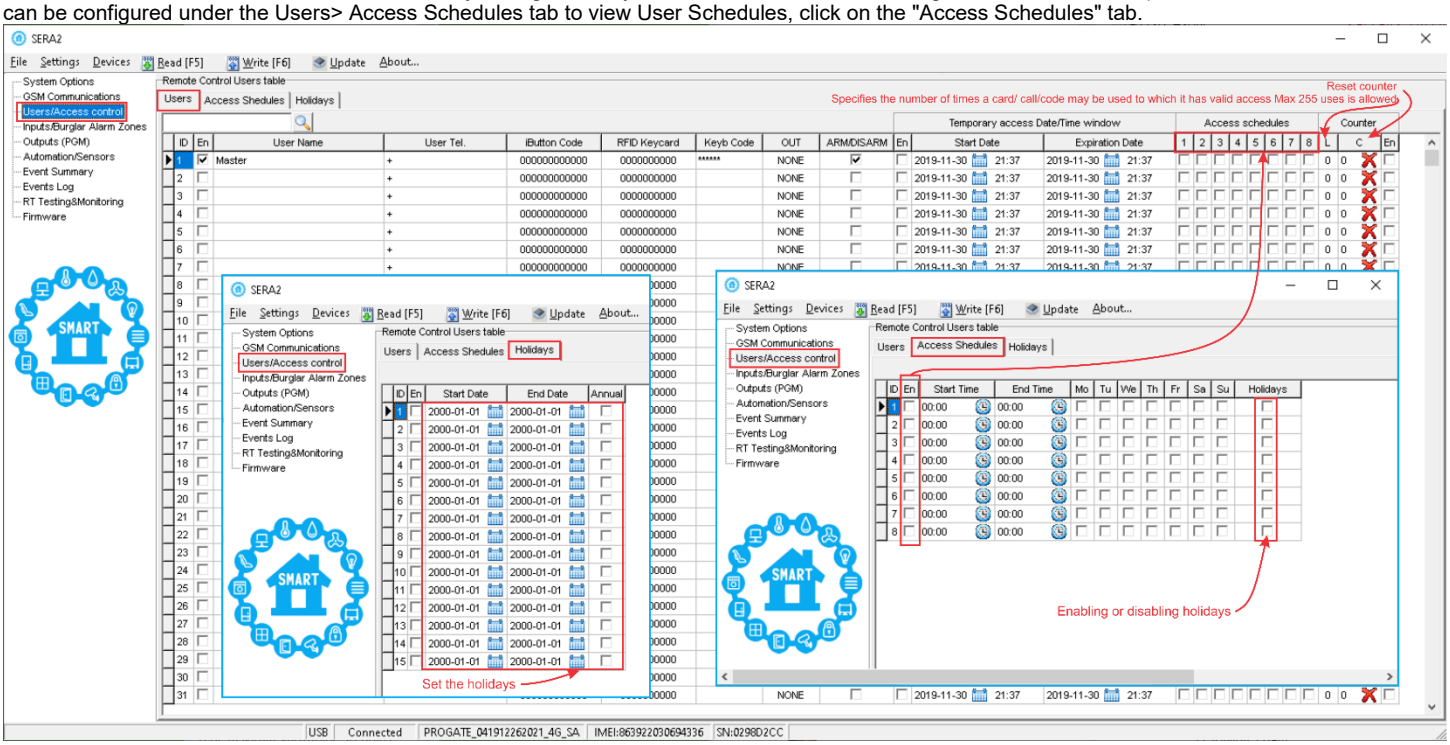


Figure 8 Users/ Access Control > Users, Users Access Control> Access Schedules and Users/ Access Control> Holidays window

Set time:

- Navigate to: Sera2 > System Options > General System Options.
- Set your desired time zone and synchronize the clock.
- Press [Write].

Wiegand keypad Configuration:

- Navigate to: Sera2 > System Options > Digital I/O Settings. Configure the following:
  - Digital I/O D2: Wiegand interface DATA0.
  - Digital I/O D3: Wiegand interface DATA1.
- Press [Write].

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 RFID keycard, iButton codes, and phone number should appear in the list.
- 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

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.

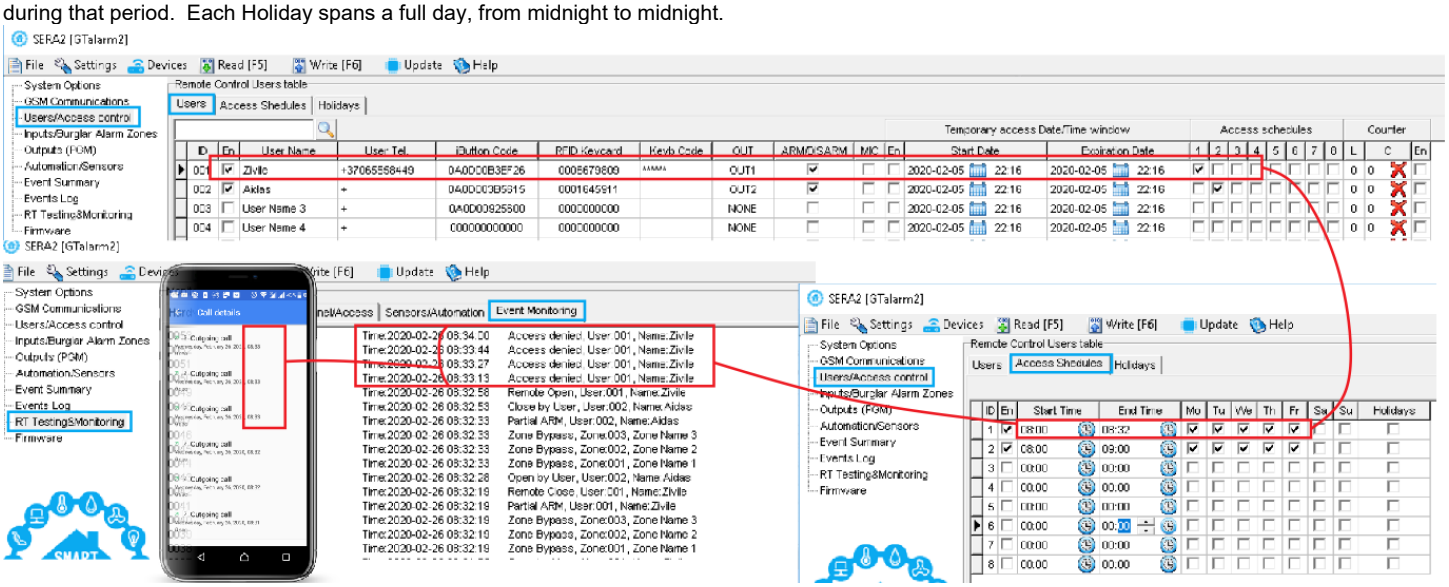


Figure 9 the example of schedule

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

3.5 Wiegand Keypad & RFID Card Reader, iButton Probe Wiring

Wiegand keypad specifications:

- Wiegand Terminals: **D0 / D1**
- 26bit Wiegand (Default);
- Keypad Operation: 8-Bit Burst Output. Each single key press as 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

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

The First iButton key 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).

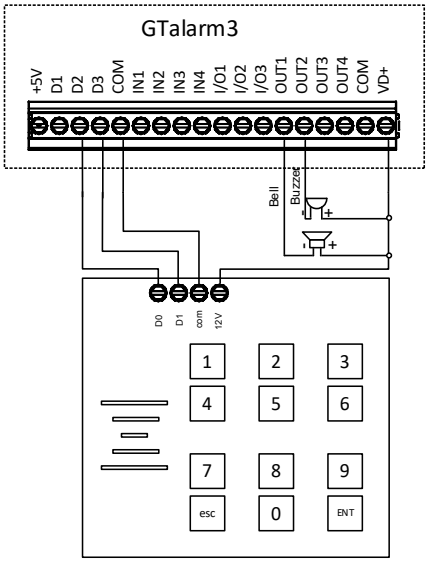


Figure 10 Wiegand keypad wiring

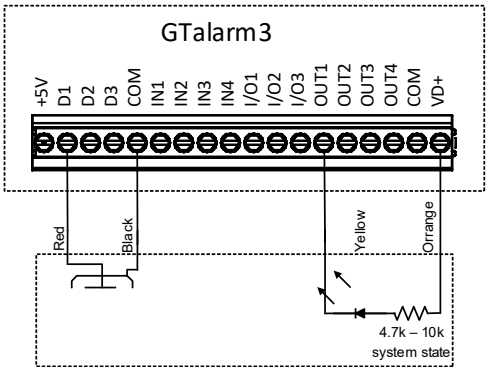


Figure 11iButton connecting diagram

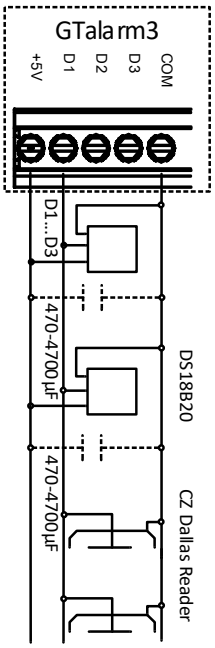


Figure 12 iButton connection diagram

The total length of the bus from 10 to 100 m. Depending of cable quality, and environment noise.
If LED is without resistor. External 4.7k – 10k resistor required.

3.6 Add iButton keys, RFID cards, Phone numbers to the memory of the module

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

Configurations methods:
- Start automatic learning mode via mini USB cable (Sera2 software).
- Start automatic learning mode via SMS command INST000000 063 1
- Enter Keycard numbers manually via mini USB cable (Sera2 software).
- Start automatic learning mode remotely via Sera2 software.

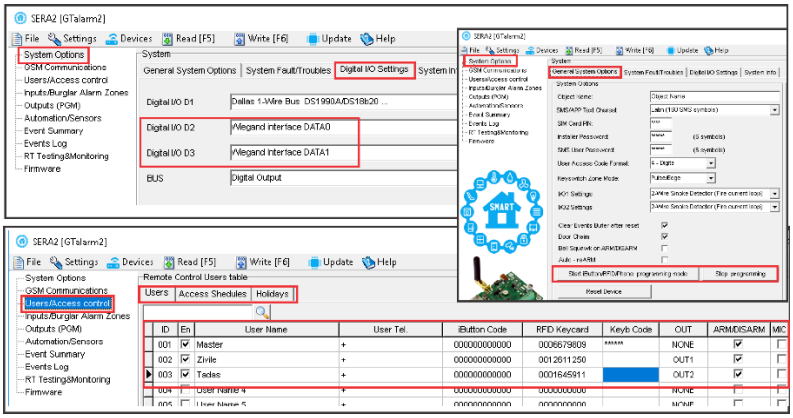
YouTube LT Enter iButton RFID codes to the memory *https://youtu.be/80yWW_j9pJk*

YouTube LT Activate RFID learning mode remotely *https://youtu.be/4MnPfxH7F04*

YouTube LT Access control: schedules, temporary access *https://youtu.be/W5FSvN-Uitl*

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

Go to Sea2> System Options> Digital I/O settings
Set Digital I/O D2 to “Wiegand Interface DATA0”
Set Digital I/O D3 to “Wiegand Interface DATA1”
Press [Write]
Go to Sera2> System Options> General system Options.
Press "Start iButton/ RFID/ Phone programming mode.
Go to Sera2> Users/ Access control window.
Touch RFID keycards to the reader.
RFID keycard number will appear in the list.
Go to System Options> General system Options and
Press "Stop programming" or wait until it will stop automatically.
Edit setting in the Users/ Access control window.
Press "Write"
Go to RT Testing & Monitoring> Hardware.
Press "Start Monitoring"
Go to RT Testing & Monitoring> Security Alarm Panel/ Access



Start automatic learning mode via SMS command INST000000 063 1

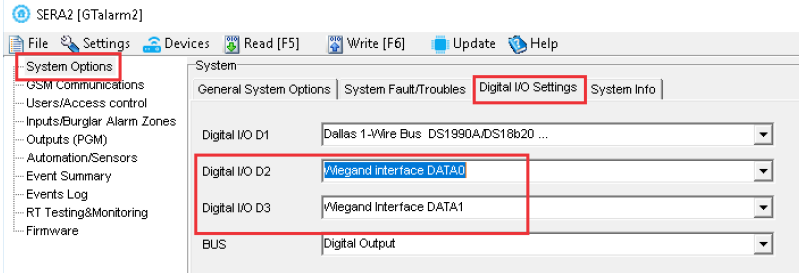
Send SMS message: INST000000 063 1
You will receive the message: iButton/RFID/Caller ID
Learning Mode is Switched ON
Touch RFID keycards to the RFID reader.
Sent the message: INST000000 063 0
You will receive the message: iButton/RFID/Caller ID
Learning Mode Stopped

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

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

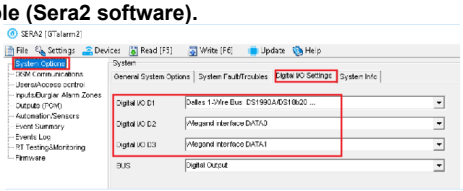
! Before activating the RFID learning mode via SMS, the module must have the appropriate System Options> Digital I/O Settings

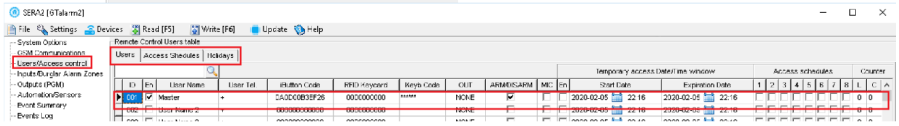
- For Wiegand keypad: “Wiegand interface DATA0 and Wiegand interface DATA1 must be set.
- For iButton probe Dallas 1-Wire Bus must be set



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

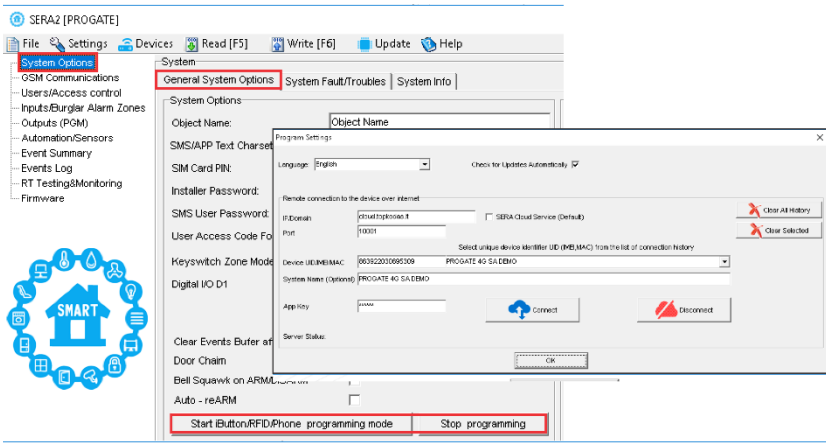
Go to Sea2> System Options> Digital I/O settings
Set Digital I/O D2 to “Wiegand Interface DATA0”
Set Digital I/O D3 to “Wiegand Interface DATA1”
Press [Write]
Go to Sera2> Users/ Access control.
Enter RFID keycard number
Edit other settings
Press "Write"
Go to RT Testing & Monitoring> Hardware
Press "Start Monitoring"
Go to Security Alarm Panel/ Access"
Touch the keycard to the RFID keypad.

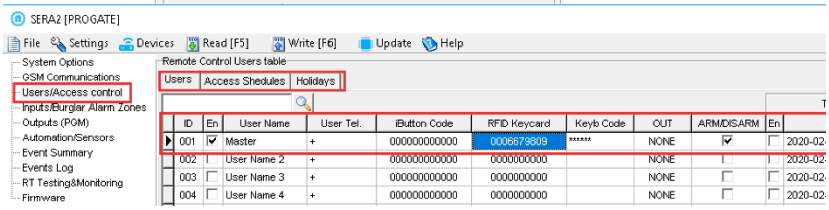




Remote Activation of Automatic RFID, iButton keys Learning Mode via Sera2 Software

- Launch the Sera2 software.
- Click [Connect remotely].
- Enter the necessary parameters: IMEI, App Key (default: 123456).
- Click [Connect].
- **Pre-activation Settings** go to *SERA2>System Options>Digital IO settings* tab:
    - For the Wiegand keypad: Set both
        - D2: "Wiegand interface DATA 0"
        - D3: "Wiegand interface DATA 1"
    - For the iButton probe: Select
        - D1: "Dallas 1-Wire Bus".
- Click [Write].
- Navigate to: Sera2 > System Options > General System Options.
- Click [iButton/RFID/Caller ID Learning Mode].
- Touch each RFID keycard to the Wiegand keypad or touch each iButton to the reader. A beep from the buzzer will confirm each added card or key.
- To exit, click [Stop programming] or simply wait for the learning mode to conclude on its own.





4 WIRING & INSTALLATION

This Installation & Programming manual provides the basic installation, wiring and programming information required to program the module GTalarm3 and connect all third party devices to the module.

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

- USB Mini-B type cable for configuration.
- Cable consisting of at least 4 wires for connecting the controller.
- Flat-head 2.5 mm screwdriver.
- External GSM antenna if reception is weak in the area.
- Activated nano-SIM card (can have turn off PIN code requests).

Order the necessary components separately from your local retailer

find wiring diagrams in the
Power supply, Battery Wiring Humidity sensors , AM2302/DHT22/AM2305/AM2306/AM2320/AM2321, Analog inputs 0-30V, 0-20mA, 4-20mA, Wiring Dallas 1-wire DS18b20, Burglar Alarm sensor zones wiring EOL NO NC, [4-Wire] Smoke detector Wiring, [2-Wire] Smoke Detector Wiring to I/O Inputs, Output PGM wiring. Bell, Relay, Led Wiring, Wiegand Keypad & RFID Card Reader Wiring, iButton keys.
You can find detailed explanation about every field in SERA2 software here: Programming

4.1 Power supply, Battery Wiring

To power the security system, use a stabilized power supply rated between 10-30 V and at least 1A. Ensure the maximum current of the power supply is calculated for optimal functionality. For convenience, consider our UPS power supply, TPS12, designed for security systems. This allows for a backup lead battery connection and AC loss event detection. Users will always be notified of system AC loss.

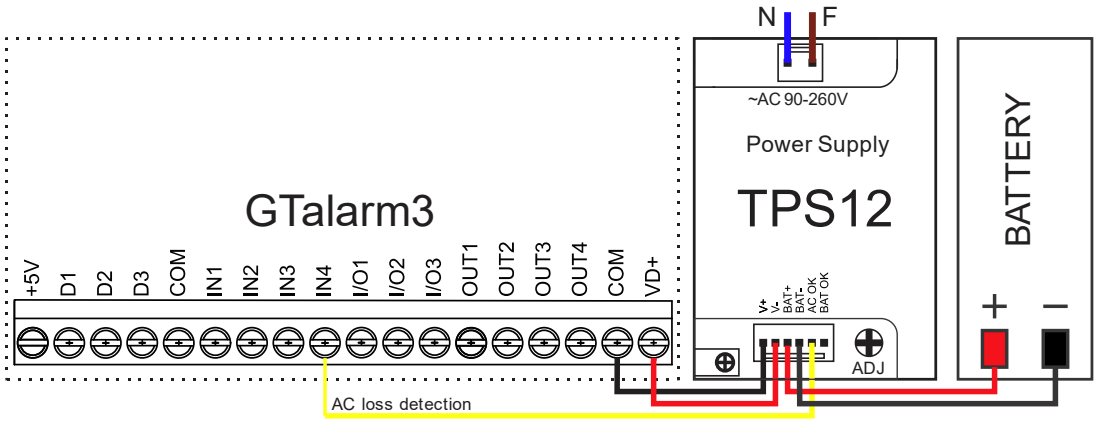


Figure 13 TPS12 Power supply connection to GTalarm3

The example how to configure the module GTalarm3 for AC failure, restore function

Go to “Burglar Alarm Zones” window in the SERA2 software. Double click on the 4th row and enter the required parameters. Press [OK]

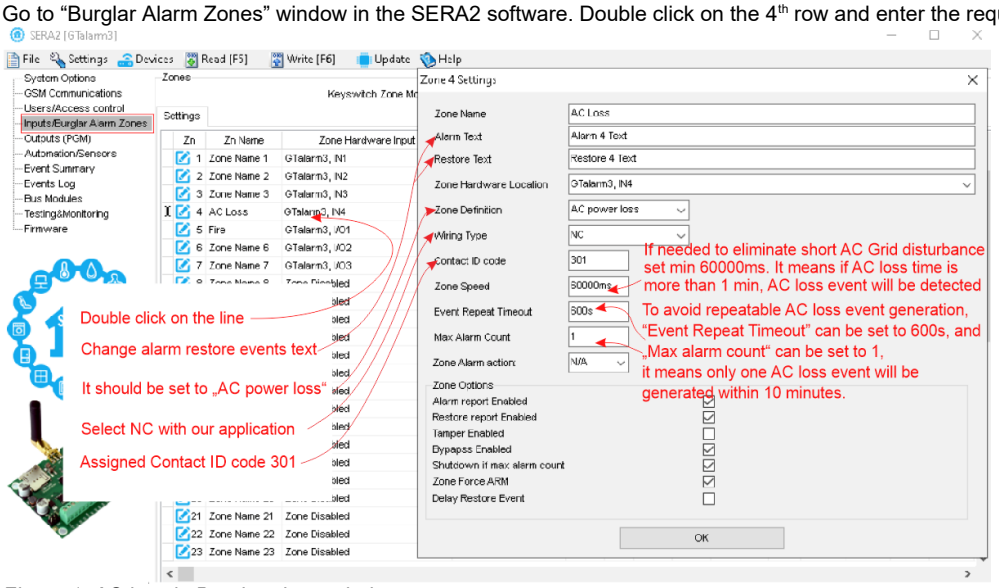


Figure 14AC loss in Burglar alarm window

Double click on Zone/Input the line
[Alarm Text]/ [Restore Text] - change alarm/ restore text
[Zone Definition]- Should be set to “AC power loss”
[Wiring Type]- Select NC with our application
[Contact ID code]- Assigned Contact ID code 301 as “AC power loss”
[Zone Speed]- If needed to eliminate short AC Grid disturbance set min 60000ms. It means if AC loss time is more than 1 min, AC loss event will be detected

[Event Repeat Timeout]- To avoid repeatable AC loss event generation, Event Repeat Timeout can be set to 600s, and Max Alarm Count can be set to 1, it means only one AC loss event will be generated within 10 minutes.

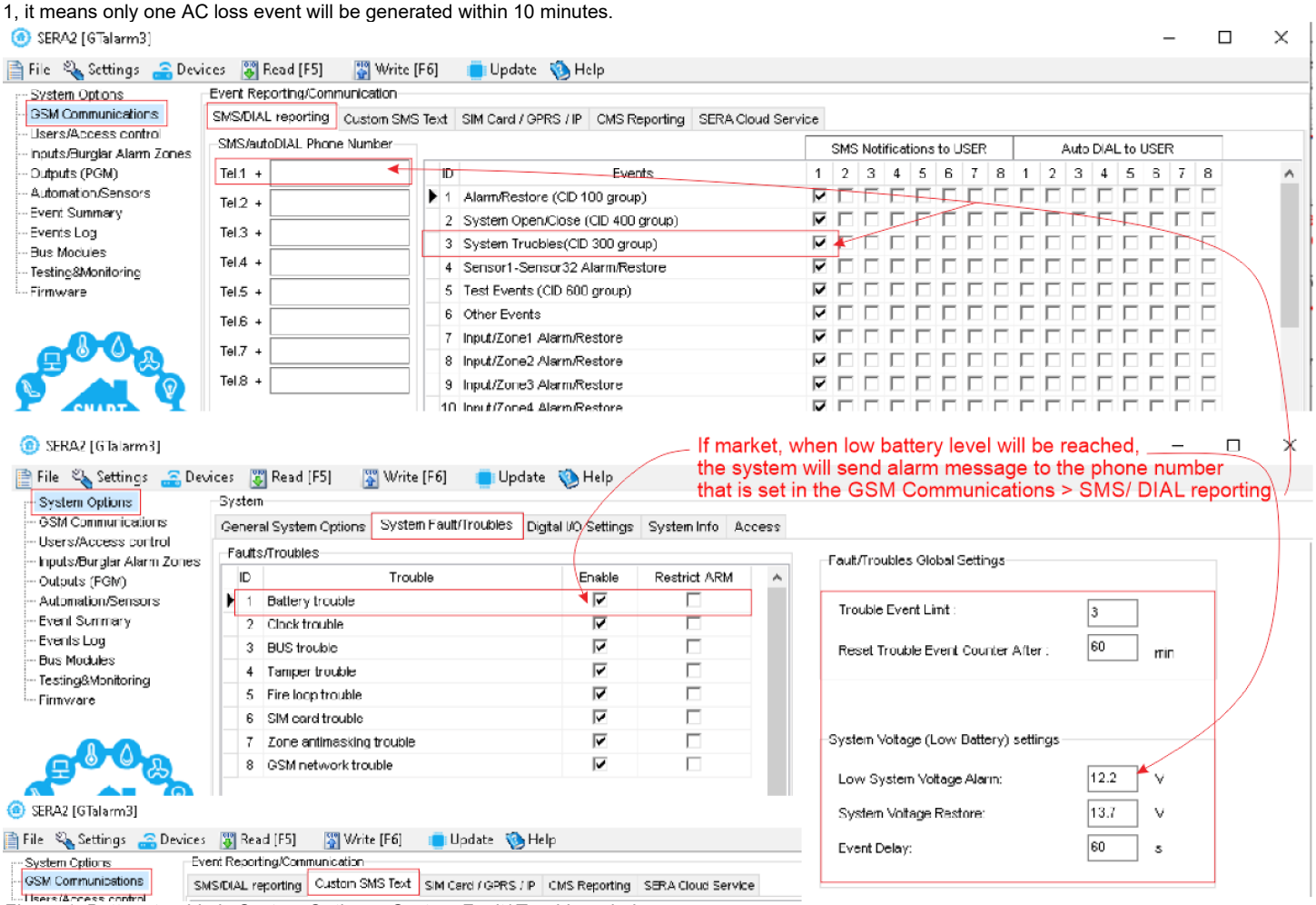


Figure 15Battery trouble in System Options> System Fault/ Troubles window

If [Battery trouble] event marked, it means when low battery level will be reached, the system will send alarm message to the phone number that is set in the GSM Communications> SMS/ DIAL reporting
GSM Communication> Custom SMS Text. It is possible to edit text

Power supply TPS12 installation manual: https://topkodas.lt/Downloads/TPS12_UM_EN.pdf
Power supply TPS12 : https://topkodas.lt/Downloads/GTalarm3_TPS12_AN_EN.pdf

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

4.2 Inputs

The module GTalarm3 has:

- **4 analog inputs (In1...In4 (0-30V))** for analog sensors connection. Or can be used as security system‘s zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- **3 programmable selectable analog inputs (I/O1, I/O2, I/O3 (0-30V/0-20mA),2-wire fire)** for analog sensors control or using as security system‘s zone with selectable type: NC/NO/EOL/EOL+TAMPER
- **3 programmable digital inputs (D1...D3(Max voltage 3.3V))** used for:
  - **Dallas 1-Wire Bus.** To connect temperature sensors DS18b20 or iButton key DS1990A, I/O expansion module 1WIO8
  - **Aosong 1-Wire bus Humidity Sensor** AM2302, DHT22, AM2320, AM2305, AM2306,
  - **Wiegand interface** DATA0/ DATA1, RFID reader, Keyboard.

4.3 Sensors. Security.

4.3.1 Burglar Alarm sensor zones wiring EOL NO NC

Connector terminal Input Ports:

- In1 to In4: These can be configured as security system zones with selectable types such as NC/NO/EOL/EOL+TAMPER.
- I/O1, I/O2, & I/O3: Options for configuration include NC/NO/EOL/EOL+TAMPER/2-Wire fire.

Zones:

- The system comes with 7 onboard wired burglary zones.
- These can be expanded to a total of 32 zones by using the **1WIO8 expansion module** connected via the 1-Wire bus.

Sensor Recommendations:

- Standard motion, fire, and glass break sensors are recommended.
- For powering these sensors, it's advised to use a standard 6-8 wire cable, specifically designed for security system installations.

Connection & Configuration:

- Connect the security system's sensors to the module as depicted in the subsequent connection diagrams.
- Adjust and set the necessary parameters for your setup.
- Finalize your configuration by pressing the [Write] icon.

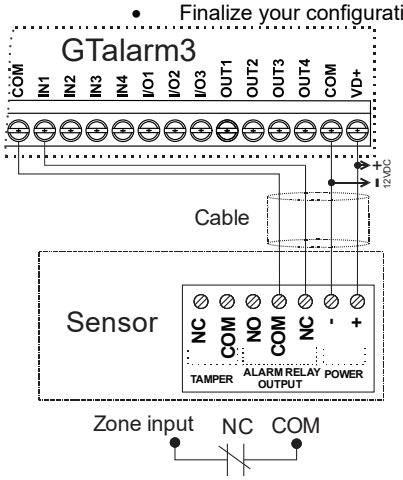


Figure 16NC Contacts, No EOL

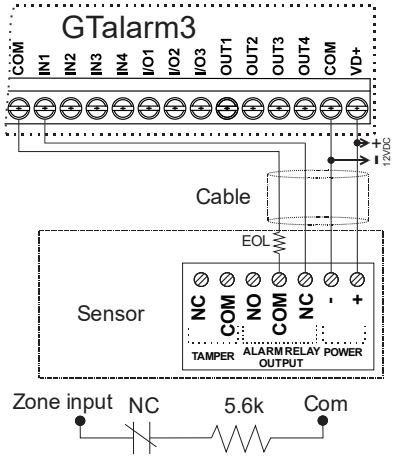


Figure 17 NC, With EOL

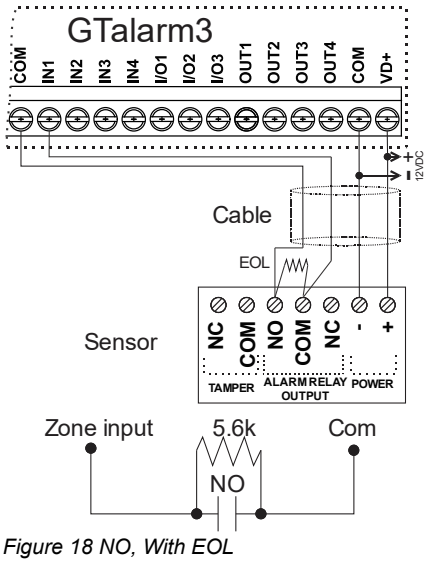


Figure 18 NO, With EOL

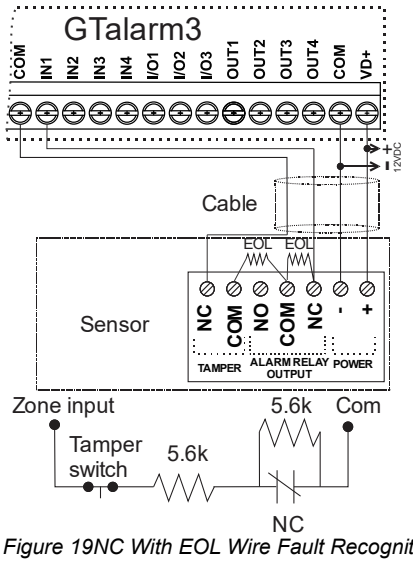


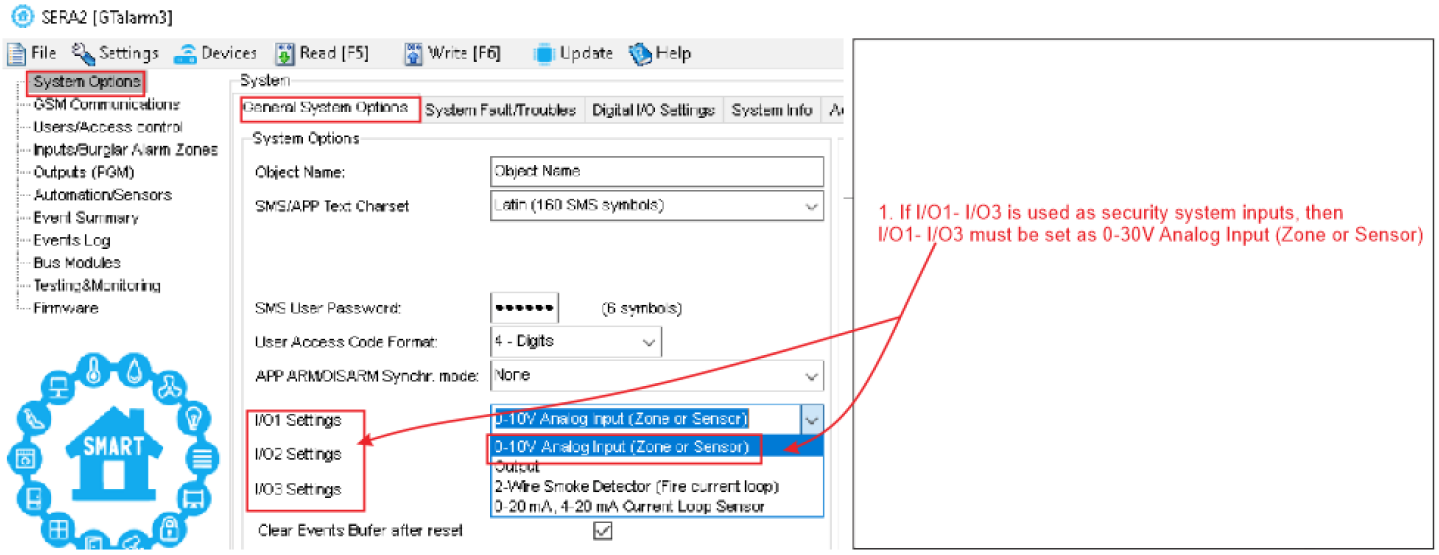
Figure 19NC With EOL Wire Fault Recognition

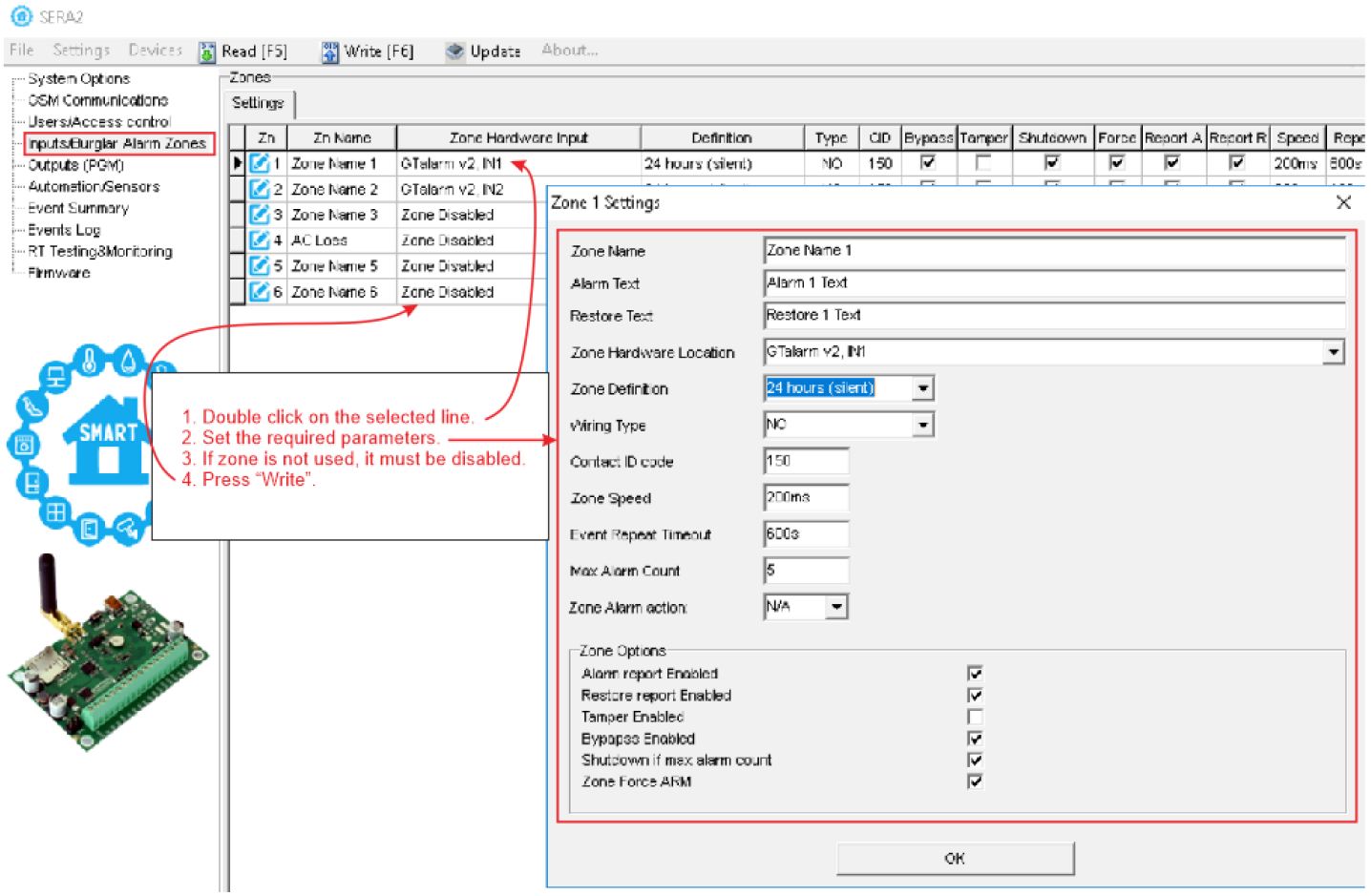
If I/O1- I/O3 is used as security system inputs, the I/O1- I/O3 must be set as 0-30V Analog Input (Zone or sensor)

- Double click on the selected line.
- Set the required parameters.
- If zone is not used, it must be disabled.
- Press [Write]

If you want to edit existing configuration,
You have to read it press [Read]
Edit settings
Write edited configuration press [Write]

More information about how to configure the zones:





4.3.2 Fire alarm and Smoke sensors

4.3.2.1 Guidelines for Locating Smoke Detectors and CO Detectors

Smoke Detectors:
Studies show that most house fires produce smoke before heat. Thus, it's advised to:

- Install smoke alarms outside sleeping areas and on every floor.
- Consider additional units in basements, bedrooms (especially where smokers sleep), dining rooms, furnace rooms, and other hallways.
- Space detectors 9.1m (30 feet) apart on smooth ceilings. Adjust spacing based on ceiling height, air flow, joists, and other factors.

Avoid:

- Installing at the top of peaked or gabled ceilings to prevent ineffective detection due to dead air spaces.
- Areas with turbulent air flow, like near doors, fans, or windows.
- Humid areas.
- Places where temperature exceeds 38ºC (100oF) or drops below 5ºC (41oF).

Legal requirements often dictate smoke alarm placement. Common mandates include installation in:

- All bedrooms and guest rooms.
- Areas outside sleeping zones within 6.4 m (21 ft) of bedroom doors.
- Every level, including basements.
- All floors of a residential care facility, excluding attics and crawl spaces.
- Living spaces of guest suites and residential care facilities.

CO Detectors:
Carbon monoxide (CO) is especially dangerous during sleep. Therefore, install CO alarms outside sleeping areas or on every home level. These alarms detect CO concentration and alert users before reaching harmful levels.
Avoid placing CO alarms:

- Where temperatures might drop below -10ºC or exceed 40 ºC.
- Near sources of paint thinner fumes.
- Within 1.5 meters of open-flame devices like furnaces or stoves.
- Near gas engine exhausts or chimneys.
- Close to car exhausts.

GTalarm3 Installation:
Begin by mounting additional modules inside the provided cabinet using the stand-offs. Place the cabinet in a dry, sheltered spot with access to uninterrupted AC power. Follow the installation sequence as described in the subsequent sections. Important: Don't power the system until after installation is complete.

4.3.2.2 [4-Wire] Smoke detector Wiring

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

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

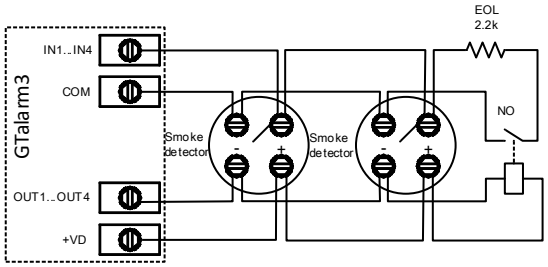
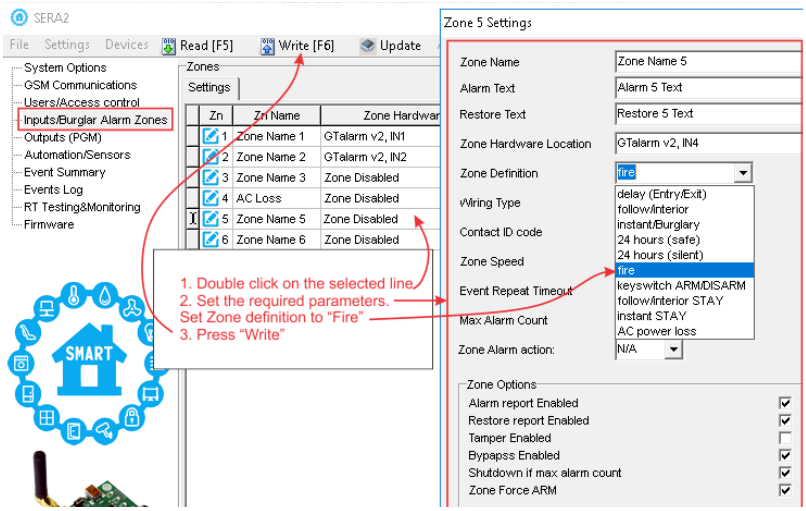


Figure 20 4-Wire Smoke Detector Installation

If you want to edit existing configuration,

- You have to read it press [Read]
- Edit settings
- Double click on the selected line
- Set the required parameters
- Set zone definition to "Fire"
- Press [Write]



4.3.2.3 [2-Wire] Smoke Detector Wiring to I/O Inputs

2-Wire Smoke Zone Overview:

- The 2-wire Smoke zone on the module is unique, designed solely for 2-wire smoke detectors as Fire Alarm initiating devices.
- It's an end-of-line (EOL) 2.2K resistor type zone.
- It can support up to 30 compatible 2-wire smoke detectors.
- This zone is permanently set as a 2-wire smoke zone.
- It functions as a trouble-supervised zone.
- The wiring of this zone is supervised by the control panel.

Zone Parameters:

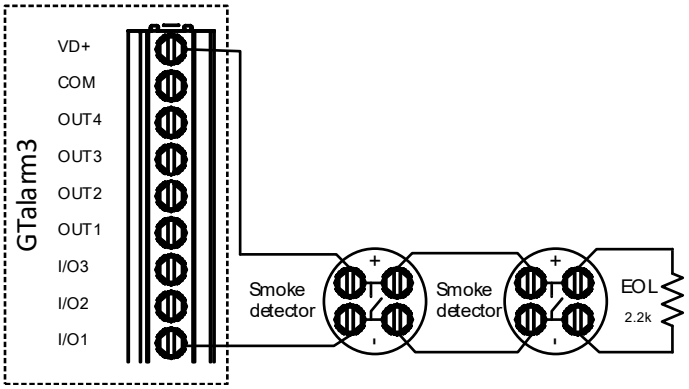
- The parameters must be specified as a “Fire Zone”.
- I/O1 to I/O3 can be set as a 2-wire smoke detector input.

System Responses:

- If there's a line short or the smoke detector is triggered, the control panel will generate an alarm, regardless of the system's armed status.
- An open line prompts the “Zone Fault” report. This report can be sent to the monitoring station or the user, based on programming.

Connect 2-Wire detector:

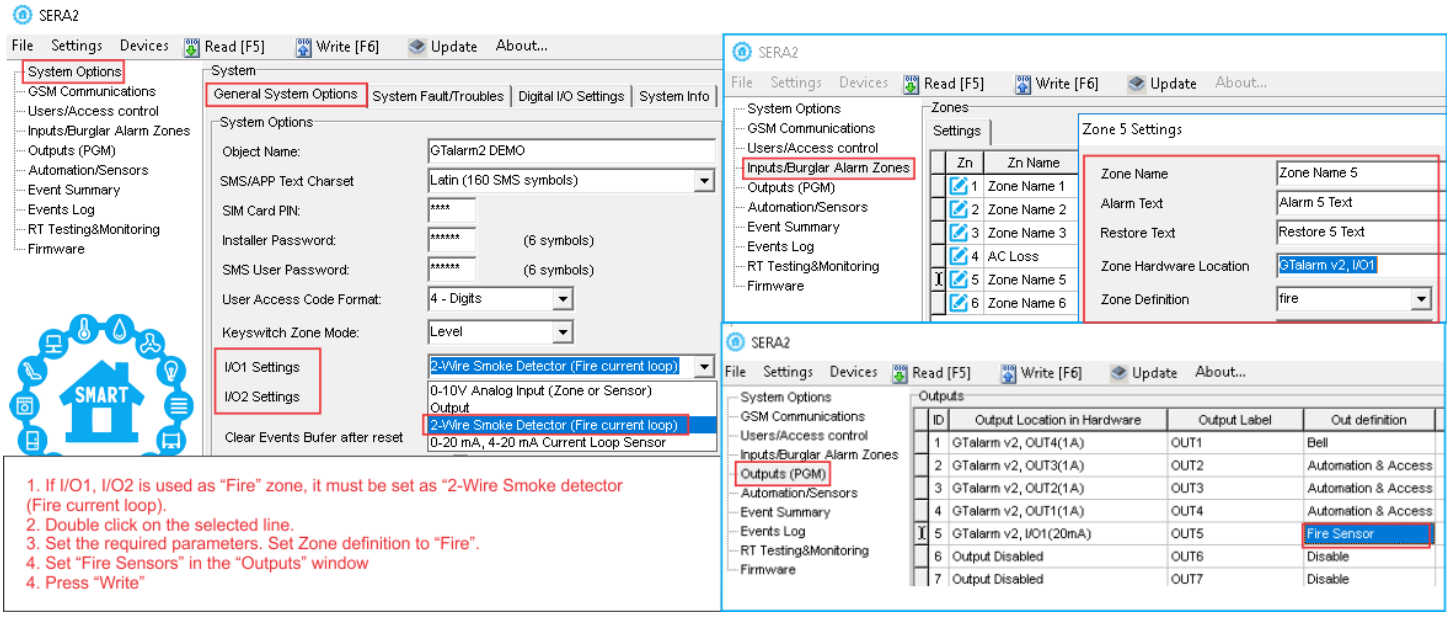
- Connect the [2-wire] smoke detector (current sensor) to the I/O1-I/O3 inputs as in the wiring diagram.
- Connect the power supply.
- Go to SERA2>*System Options*> *General System Options* from the menu and select 2-Wire Smoke Detector (Fire current loop)
- In the Zone table set I/O1 definition to “Fire”
- If I/O1, I/O2, I/O3 is used as “Fire” zone, it must be set as “2 wire smoke detector (fire current loop)
- Double click on the selected line
- Set the required parameters. Set zone definition to “Fire”
- Set “Fire Sensors” in the Output window
- Press [Write]



Edit existing configuration,

- You have to read it press [Read]
- Edit settings
- Write edited configuration press [Write]

More information about how to configure 2-Wire Smoke detectors:



4.4 Outputs

The module GTalarm3 has:

- Up to 32 outputs can be expanded with 1WIO8 I/O expansion module
- **4 open drain (1A) outputs:** OUT1 (1A)… OUT4 (1A). The outputs can be used for siren, relay, gate or other equipment. These outputs can be controlled via short call or SMS. Output operation algorithms: Automation /CTRL, Siren, Buzzer, ARM state, Zones OK, Light Flash, inverting, pulse mode
- **3 open drain (20mA) outputs:** I/O1 (20mA)… I/O3 (20mA). These outputs can be used for solid state relays, LED, to control devices up to 20mA.
- **3 outputs: D1 (10mA, Max Voltage 3,3V)** for LED, solid state relays control. ! Max voltage 3,3V
- **OUT1… OUT4 max current – (-V) 1000 mA.**
- All outputs can be controlled via short call DIAL or via SMS message. This feature may be used for gate opening
- Output alarm parameters may be programmed.
- Programmable algorithms for outputs operation: **CTRL/SMS/DIAL, SIREN, BUZER, ARM state, Zones OK, Light Flash, inverting, pulse mode**

A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system. Normally, **PGM outputs can be used to open/ close garage doors, activate lights, heating, watering and much more.** When a PGM output turns ON, the system triggers any device or relay connected to it.

4.4.1 Output PGM wiring. Bell, Relay, Led Wiring

Powering the Module:

- A standard AC/DC adapter with a voltage range of 10V-14V and current >=1A is recommended.

Connecting the Output Switch:

- The output switch grounds when activated from the module.
- Connect the positive side of the device to the VD+ terminal.
- Link the negative terminal to the selected output.
- In order to control big power alternating current equipment, it is comfortable to use solid state relays.

Sound Signaling bell Recommendations:

- We advise using a siren DC 12V, up to 1500mA.
- It's optimal to connect the siren with a 2 x 0.75 sq. mm cable.

Auxiliary Buzzer:

- Ideally, install the auxiliary buzzer indoors, close to the entrance.
- It operates in tandem with the main siren, notably during exit and entry delays.
- A suitable buzzer would be hit point PB12N23P12Q or a similar 12V DC, 150mA max piezoelectric buzzer.

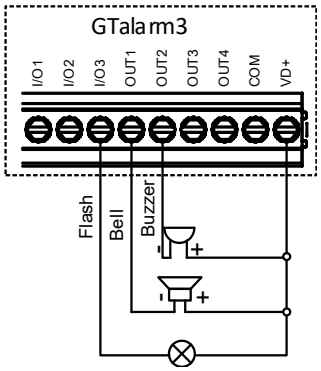


Fig. 1 OUT1-OUT4 Open drain 1000 mA connection

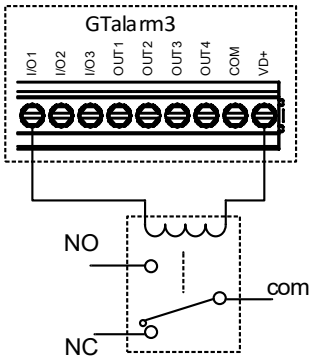


Fig. 2 Relay connection to OUT1-OUT4, I/O1, I/O2 20mA

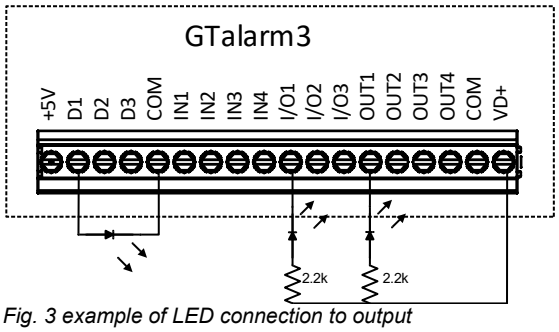


Fig. 3 example of LED connection to output

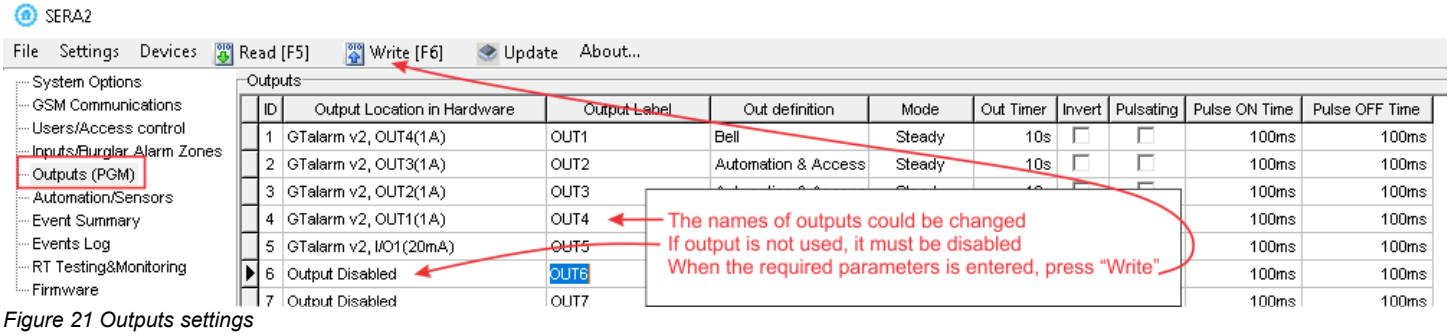


Figure 21 Outputs settings

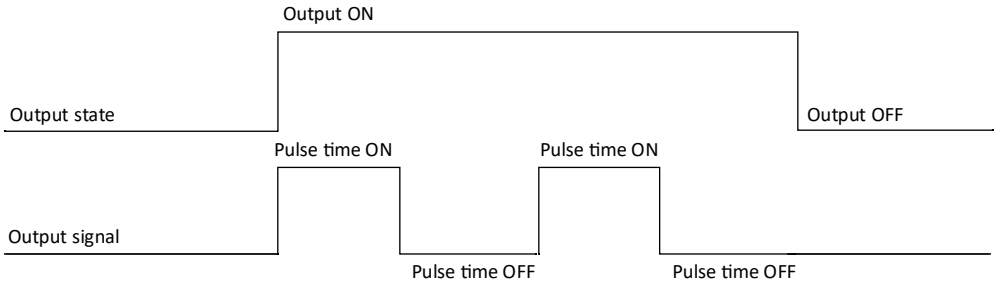
1. The names of outputs could be changed
2. If output is not used, it must be disabled
3. When the required parameters is entered, press [Write]

If you want to edit existing configuration,
You have to read it press [Read]

Edit settings
Write edited configuration press [Write]

Outputs can be set as timers.

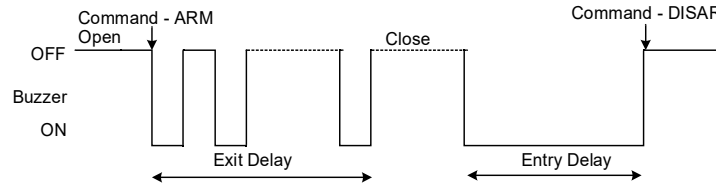
1. When output is activated for “Out Timer” time interval,
2. Relay contact start changing state from ON (pulse time ON) to OFF (Pulse time Off)
3. This cycle will repeat until output is deactivated.



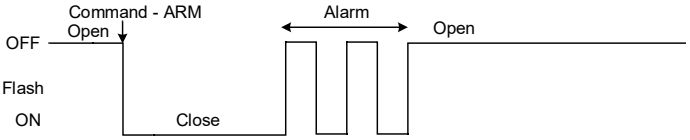
Bell: Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.

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

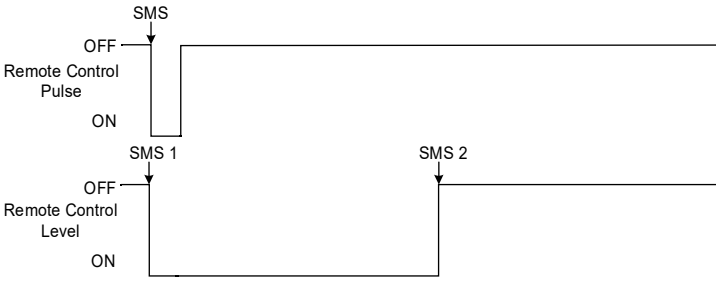
Buzzer: Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.



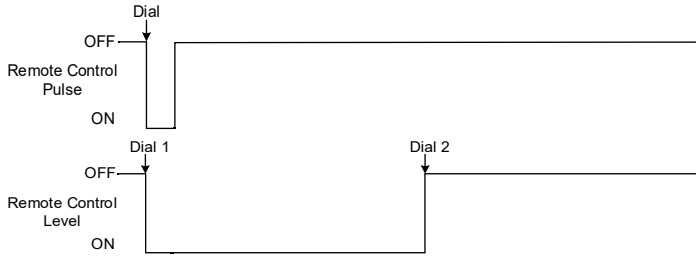
Flash: Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



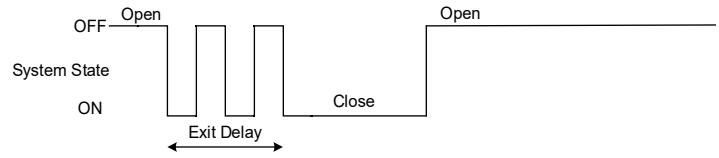
Remote Control: Output designed for connection of electrical devices which will be controlled by SMS message or phone call a) control by SMS message



Remote Control b) control by phone call

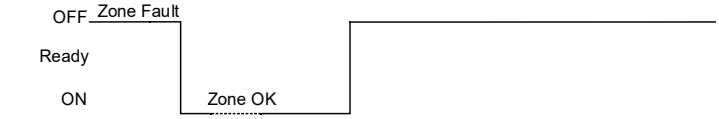


System State: Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.

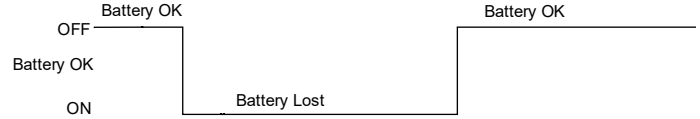


AC OK: Output for connection of indicator about control panel supply from alternating current

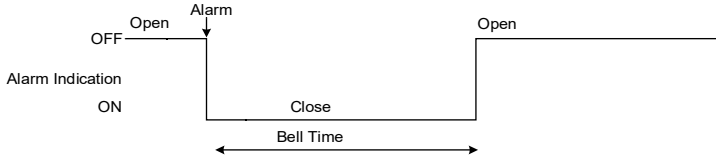
Ready: Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.



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



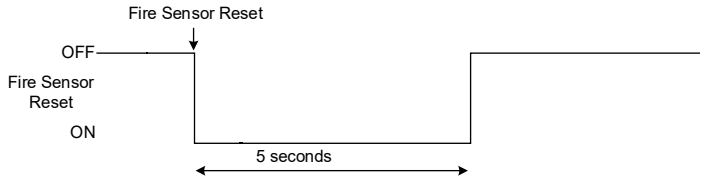
Alarm indication: Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.

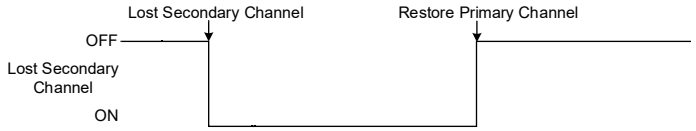


Lost Primary Channel: Output where a continuous signal is generated when communication with primary channel was lost.

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

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





4.4.2 Access control output with logging

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

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

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

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

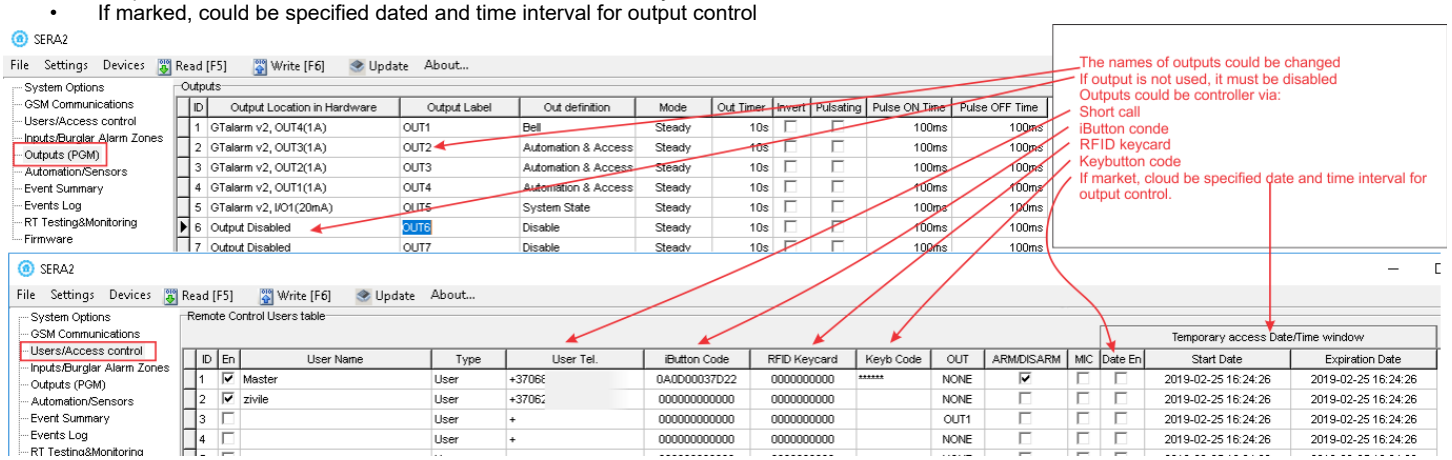
- Users with the right to ARM/DISARM the system always have access to control this output.
- Users without the right to ARM/DISARM the system (indicated by an unmarked field near ARM/DISARM in window *SERA2> User/ Access control*) can only access this output when the system is disarmed.
- When a user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

Event log e.g.

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

Quick start outputs:

- Install SERA2 software. For more information look at *Error: Reference source not found*
- Connect the module to the computer via mini USB cable.
- The names of outputs could be changed
- If output is not used, it must be disabled
- Output could be controlled via: short call, iButton, RFID, Keybutton code.
- If marked, could be specified dated and time interval for output control



4.5 Sensors. Automation

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

The module is compatible with the following Aosong 1-Wire bus Humidity Sensor Series AM23xx, such as: 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 lists values taken from datasheets. The Aosong data sheets do not specify maximum tolerances for most parameters, just 'typical' values. It would therefore seem that any particular device is not guaranteed to meet these specifications. For all the other devices the numbers above are the maximum tolerances and most also offer better 'typical' specifications.

Each AM23xx sensor connects on separate bus line to digital inputs (D1, D2, and D3). Total up to 3 AM23xx Aosong (Guangzhou) humidity sensors can be connected to GTalarm3

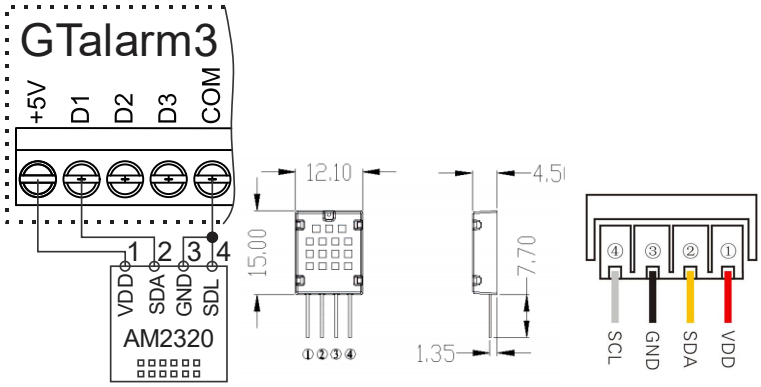


Figure 17 AM2320 and AM2320B connecting diagram

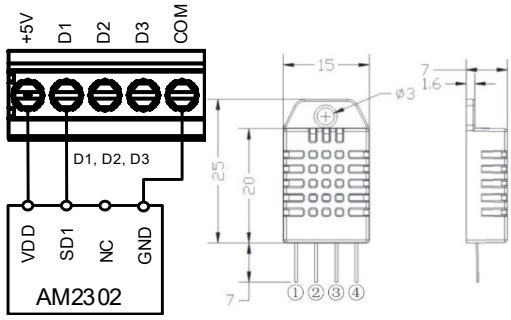


Figure 18 AM2302 connecting diagram

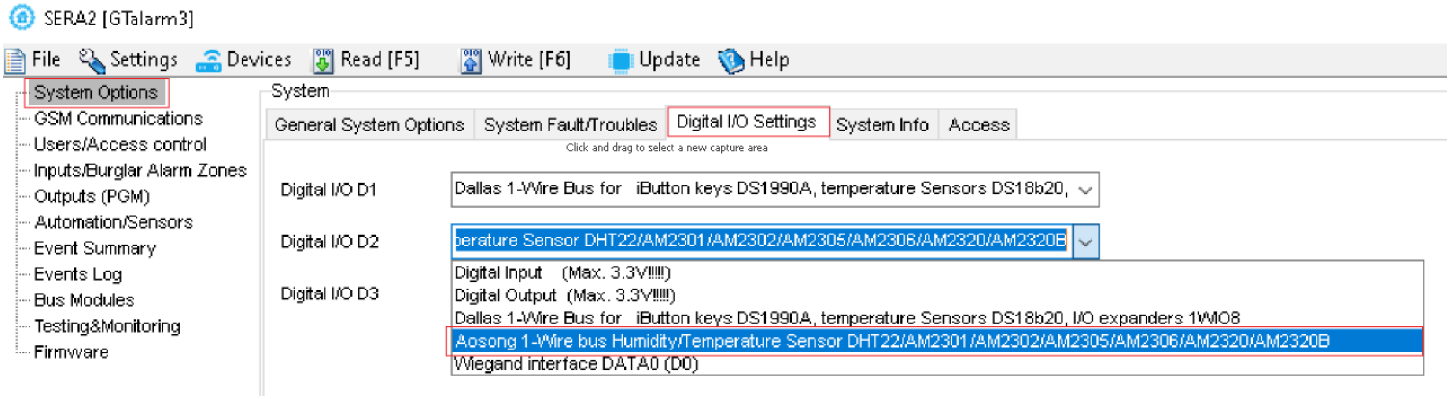


Figure 22 System Options> Digital I/O Settings

Steps to start AM23xx, AM2320, AM2305 sensors:

- Connect the sensor to D1, D2, or D3 according to the connection diagram.
- Navigate to SERA2>System Options>Digital I/O Settings and set the sensor type for D1, D2, and D3 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].

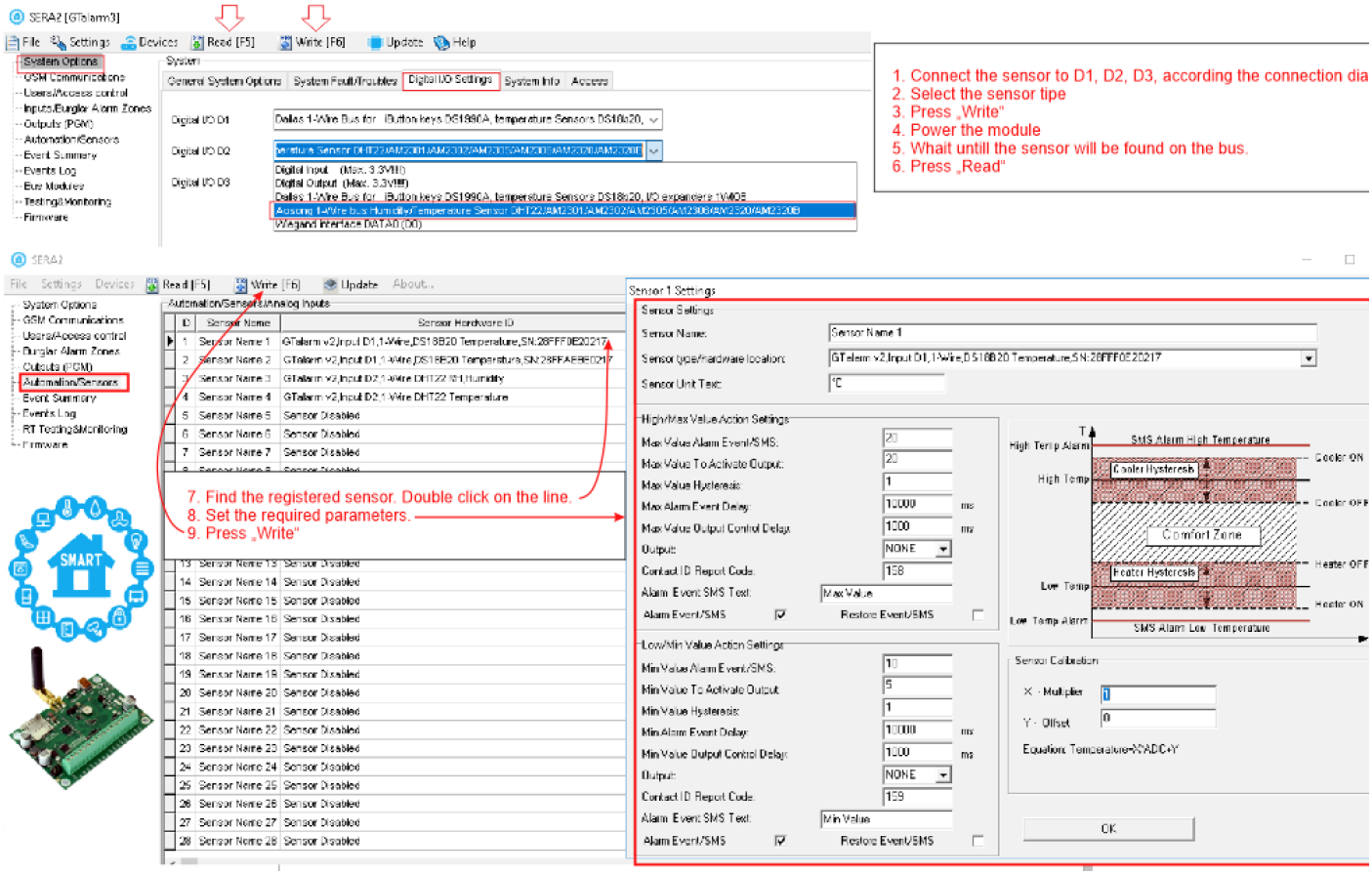


Figure 23Steps to start AM2320 and AM2302 sensors:

4.5.2 Analog inputs 0-30V, 0-20mA, 4-20mA

Steps to start analog sensors:

- Connect analog voltage sensors to In1-In4 and connect analog current sensors to I/O1- I/O3 according connection diagram.
- Set the I/O1- I/O3 to analog input
- If the input is not used, it must be disabled.
- Set the required parameters.
- Sensors could be calibrated.
- Press [Write]

If you want to edit existing configuration,
You have to read it press [Read]
Edit settings
Write edited configuration press [Write]

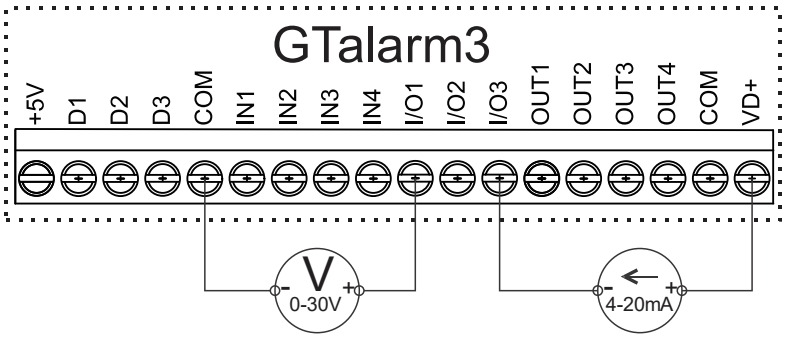


Figure 24Analog sensors connection diagram

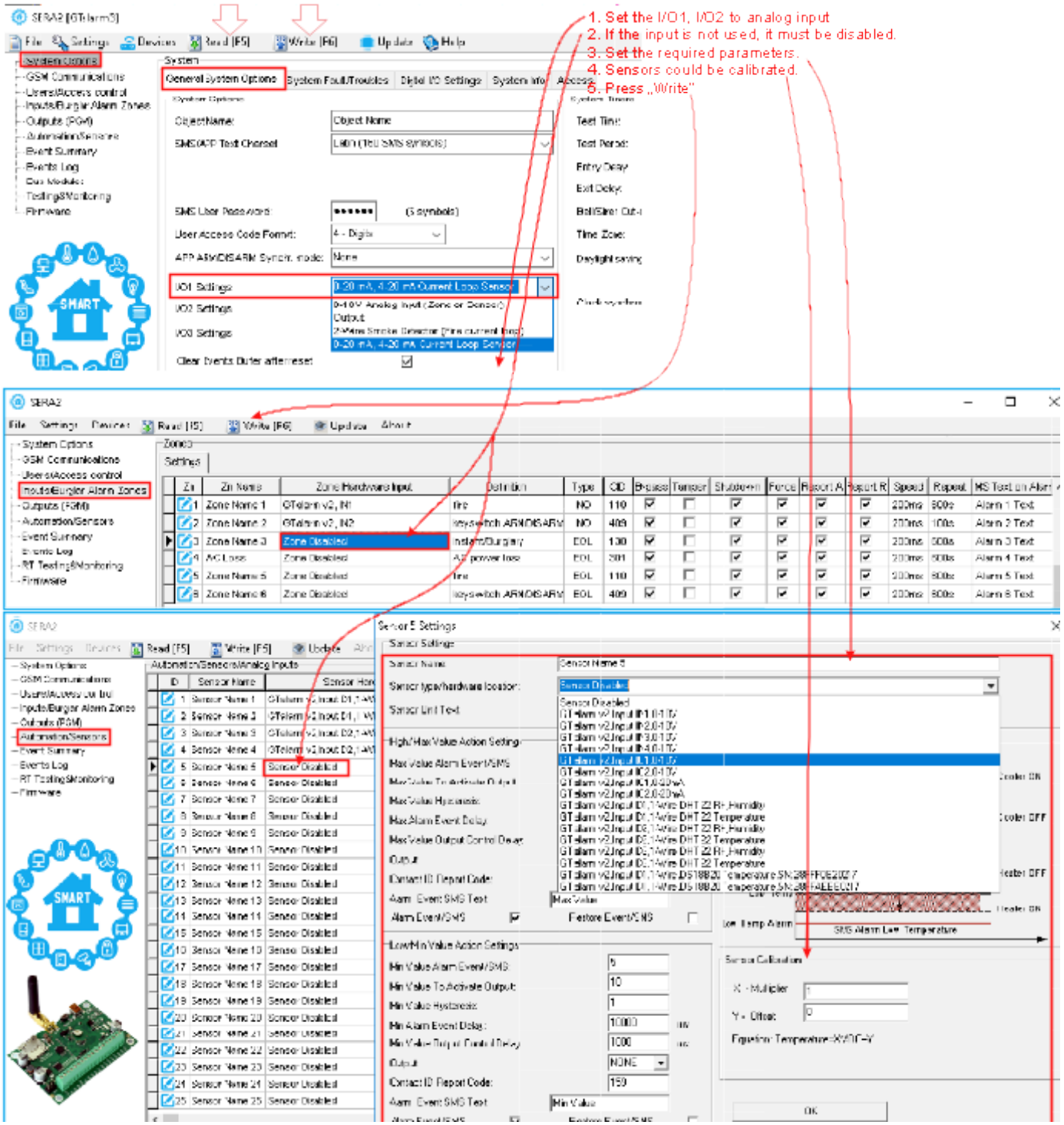


Figure 25Analog sensors settings

Any automation voltage analog sensors with a 0-30V range can be connected to IN1-IN4 (note: they have an internal 10K pull-up resistor).

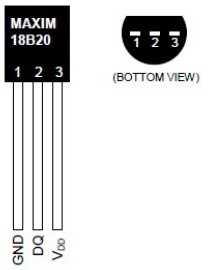
0-20mA, 4-20mA analogue sensors can be connected to I/O1…I/O3

Monitoring of sensors:

- For real-time hardware status, navigate to: RT Testing & Monitoring > Hardware, then press “Start Monitoring.”
- To access the list of alarm events with time and date stamps, go to: RT Testing & Monitoring > Event Monitoring.
- For more information, refer to:

4.5.3 Temperature sensors Dallas 1-wire DS18b20 installation & recommendations

The DS18B20 digital thermometer provides 12-bit Celsius temperature measurements. The DS18B20 communicates over a 1-Wire **Each DS18B20 has a unique 64-bit serial code, which allows multiple DS18B20s to function on the same 1-Wire bus.** Thus, it is simple 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.



to

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.

4.5.3.1 Wiring Dallas 1-wire DS18b20

1. Connect 1-Wire sensors DS18b20 to D1, D2, D3 according connection diagram.

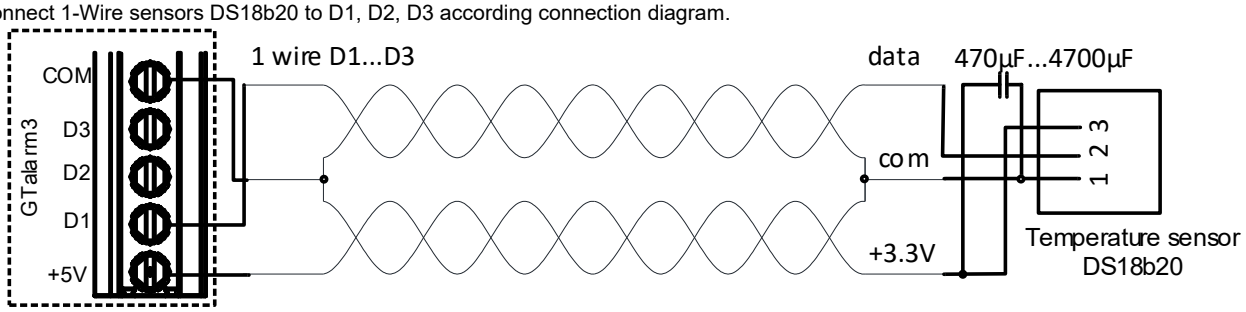


Figure 26 DS18b20 connection with long distance UTP or FTP cable

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

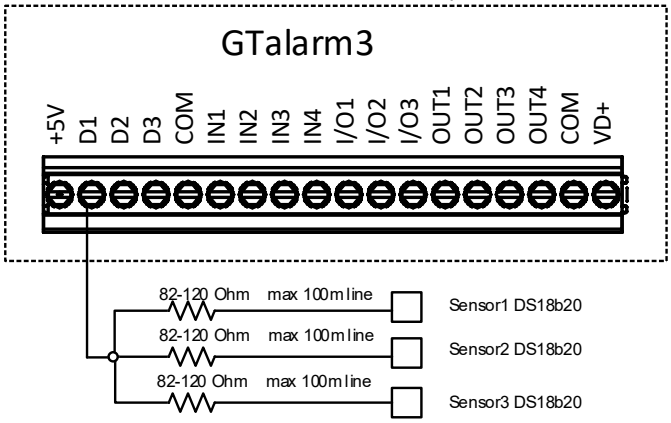


Figure 27 Star connection

The bus line impedance resistor must be as close as possible to the contacts of the module GTalarm3.

Cable Choice: Dallas recommends using an unshielded Cat 5 cable for the 1-Wire bus. An unshielded Cat 5 cable aids in maintaining a robust 1-Wire network, especially as you expand and add more sensors. Avoid shielded cables; the increased capacitance can disrupt the network.

Wiring Considerations:

- Utilize one twisted pair from the Cat 5 cable for data and ground, such as blue/blue-white. Another wire from a different pair should be used for the 3.3-volt supply.
- Avoid doubling up wires; this won't necessarily lower resistance. Instead, it can change the network's impedance and degrade reliability.
- All unused wires within the Cat 5 cable should remain unconnected; do not ground them.

Network Design for Larger Setups:

- For optimal performance, especially with a larger 1-Wire network, adhere to a daisy chain configuration. This means connecting each sensor to a single continuous cable that loops from one sensor to the next, minimizing miss-reads from cable reflections.
- Limit the cable length connecting each sensor to the main network to 50mm (2").
- While the daisy chain method is efficient, adding more than 10-15 sensors can still cause data bus loading problems. To counteract this, integrate a 100-120Ω resistor in series with the data line of each sensor before its network connection.
- The entire length of the bus can range from 10 to 100m, depending on the quality of the cable, number of sensors on the bus, and environmental noise. However, it's possible to connect up to 32 devices in certain conditions.

4.5.3.2 Temperature sensors Dallas 1-wire DS18b20 Configuration

Step by step to start DS18b20 sensors:

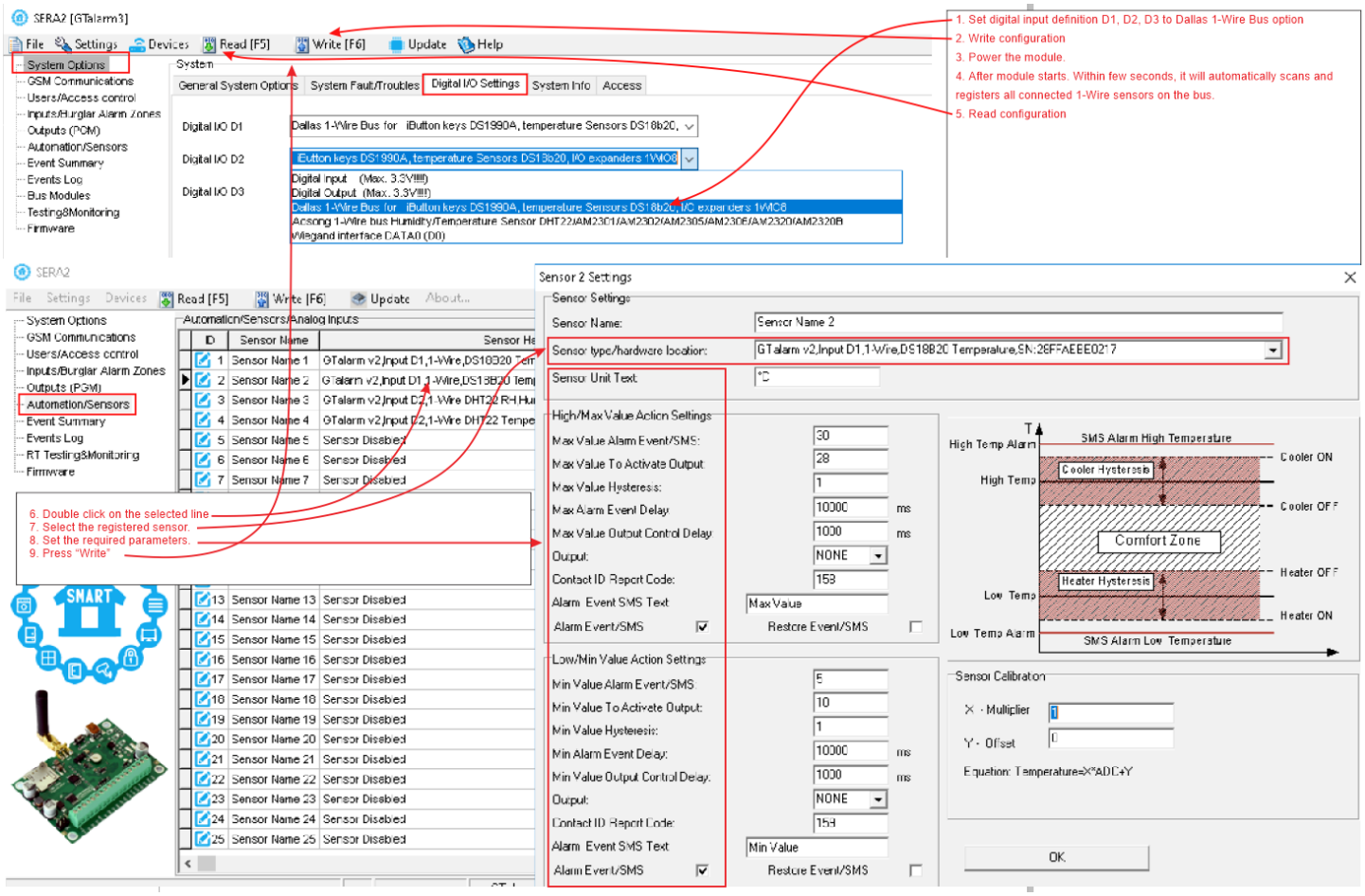
- Connect 1-Wire sensors DS18b20 to D1, D2, or D3 according to the connection diagram. If you need to connect more sensors to the same input, connect them in star or series.
- Set the digital input definitions for D1, D2, and D3 to the [Dallas 1-Wire Bus …] option.
- Write the configuration. Press [Write].
- Power on the module.
- After the module starts, it will automatically scan and register all connected 1-Wire sensors on the bus within a few seconds.
- Read the configuration.
- Double-click on the selected line.
- Select the registered sensor.
- Set the required parameters.
- Press [Write]

Edit existing configuration:

- You have to read it press [Read]
- Edit settings
- Write edited configuration press [Write]

Real time diagnostic and monitoring:

- Real time hardware status: *RT Testing & Monitoring> Hardware*. Press [Start Monitoring]
- The list of alarm events with time and date stamp: *RT Testing & Monitoring> Event Monitoring*
- It is possible to receive alarm SMS to the mobile phone: *GSM Communication> SMS/ Dial reporting*
- Real time sensor values and states: *RT Testing & Monitoring> Sensors/ Automation.*
- Write configuration. Press [Write].



4.5.3.3 How to change temperature scale from Celsius to Fahrenheit

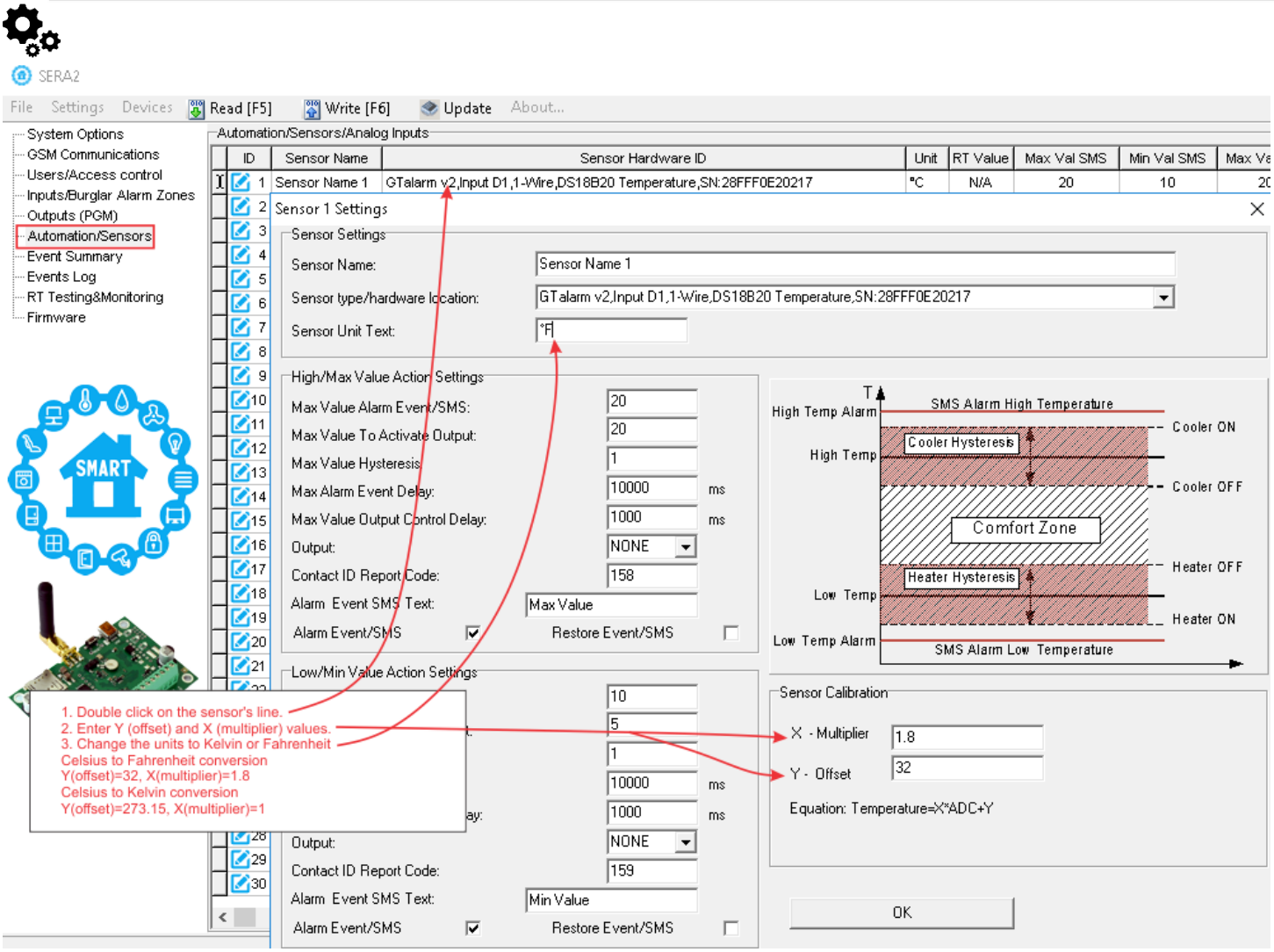


Figure 28 How to change temperature scale from Celsius to Fahrenheits and Kelvins

1. Double click on the sensor's line
2. Enter Y (offset) and X (multiplier) values
3. 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

If you want to edit existing configuration,
You have to read it press [Read]
Edit settings
Write edited configuration press [Write]

4.5.4 Step by Step: Checking Real-time Hardware and Sensor Status, Receiving Alarms, and Locating Event Lists

- 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: Access RT Testing & Monitoring > Sensors/Automation.
- To save the configuration, press [Write].

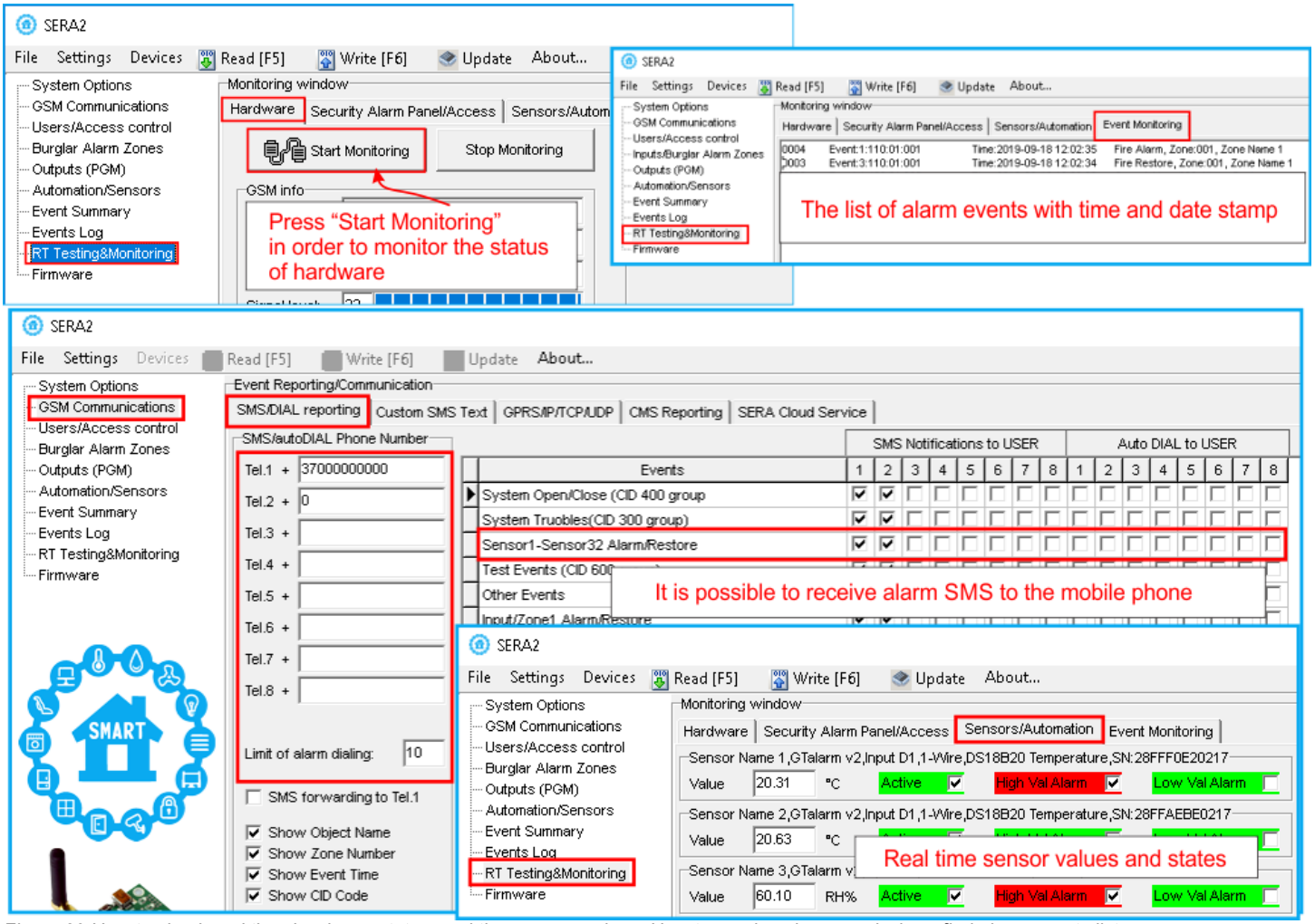


Figure 29 How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list

5 SERA2 configuration software

The SERA2 software is a configuration tool for the GTalarm3 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 GTalarm3 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".

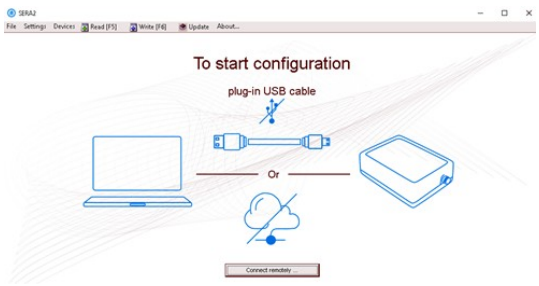


Figure 30Sera2 software

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 > GTalarm3

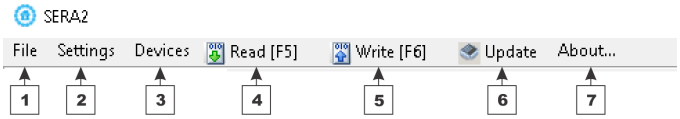


Figure 31 Command line

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

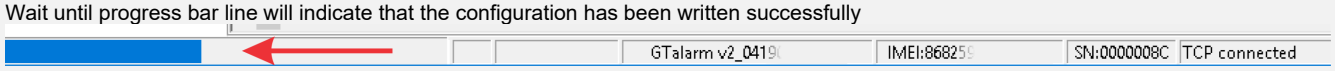


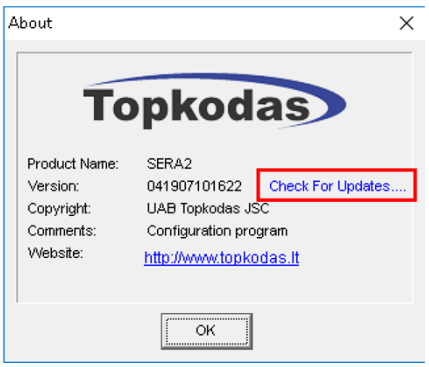
Figure 32 Progress bar

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 GTalarm3 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.

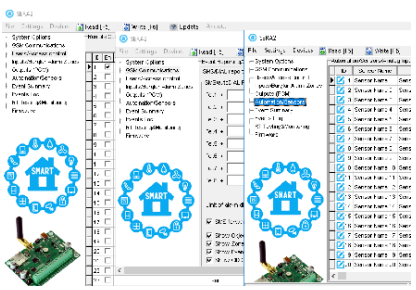
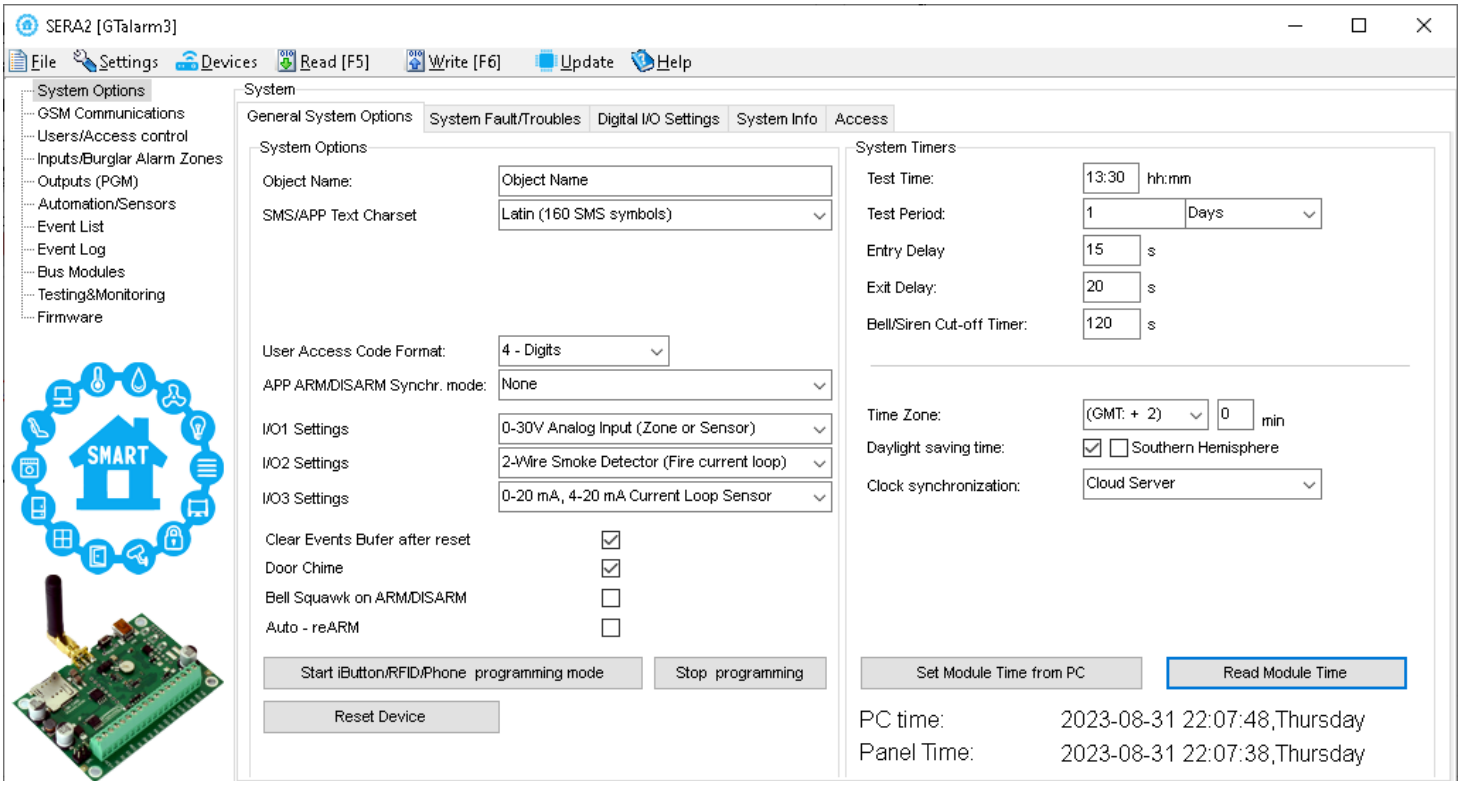


Figure 33configuration at the same time. Unlimited number of modules

5.1 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: The name and address of the object
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
Keyswitch Zone Mode: Select pulse or level. The module is arming by shortening zone to COM. Arm by output activation.
I/O1... I/O3 Settings: Set the programmable input or output to:

- 0-30V analog input
- Output
- 2- wire smoke detector or
- 0-20 mA, 4-20mA current loop sensor

Clear Events Buffer after reset: The memory of unsent reports will be deleted after the reset of the module
Door Chaim: Violations of delay zones when the alarm turned off will be accompanied by keyboard audible (Buzzer) signal
Bell Squack on ARM/ DISARM: 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
Auto- reARM: Arm the module if there is no activity in the area after the system disarming.
Stop iButton/ RFID programming: To finish entering iButton keys or RFID cards, click Stop programming button.
Start iButton/FRID programming mode: All added iButton keys or RFID cards will be registered in the order of sequence by clicking “Start programming”.
Reset Device: Reset the module.
Test Time: Auto Test report time of day
Test Period: Auto Test report period
Entry Delay: Time to enter the armed premises and enter your code to disarm your system before the alarm is triggered.
Exit Delay: Provide with enough time to exit the protected area before the system is armed.
Bell/ Siren Cut- off Timer: Duration of audible signal 0-9999s (sirens, Bell) after the alarm system activated.
Clock Synchronization: automatically time synchronization with: GSM Modem, Cloud Server or disable it.
Set Module Time from PC: Set module time from PC, which instantly provides the exact PC time.

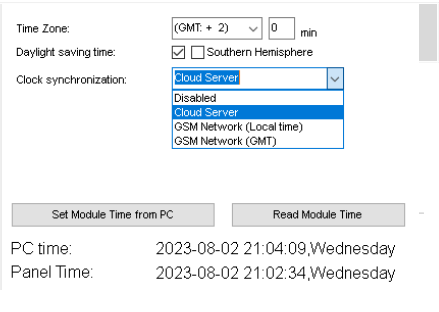
The system comes equipped with internal real-time clock (RTC) with battery that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly. SERA2 software provides the ability to select the Time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

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

5.2 Real-time clock Time Zone and Synchronization

The SERA2 software allows setting the GTalarm3 real time clock 'Time Zone' and automatic 'Daylight Saving'. Correct settings are crucial for modules using automatic schedules, as incorrect time zones can lead to erroneous schedule activation times.

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



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

Available time synchronization options: GSM Modem, Cloud Server, or disabling it.

! For accurate scheduling and event timing, it's essential to set the correct 'Time Zone' and choose the appropriate 'Clock Synchronization' method. Proper configuration is vital for modules that rely on automatic schedules. Inaccurate time zone settings can cause schedules to activate at the wrong times

! 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.

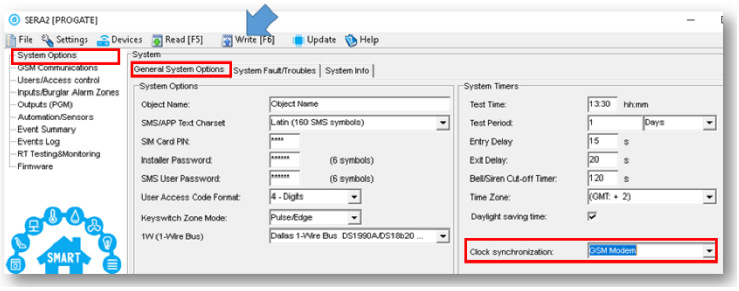


Figure 34SERA2> System Options> General System Options

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

Clock synchronization via GSM modem

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

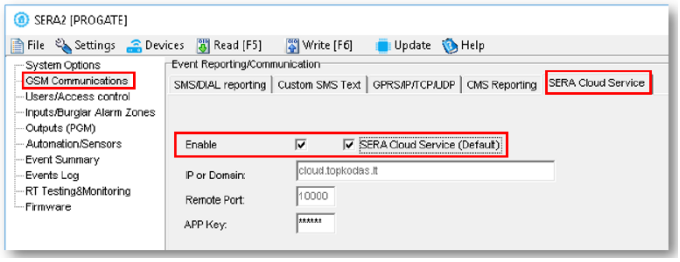


Figure 35 SERA2> GSM Communication> SERA Cloud Service

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

Clock synchronization via Cloud server

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

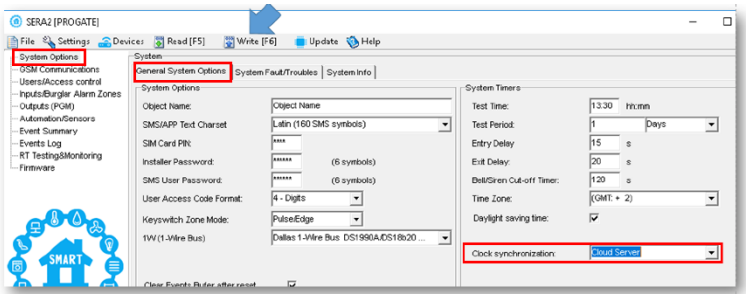


Figure 36 SERA2> System Options> General System Options

5.3 System Fault/ Troubles Programming

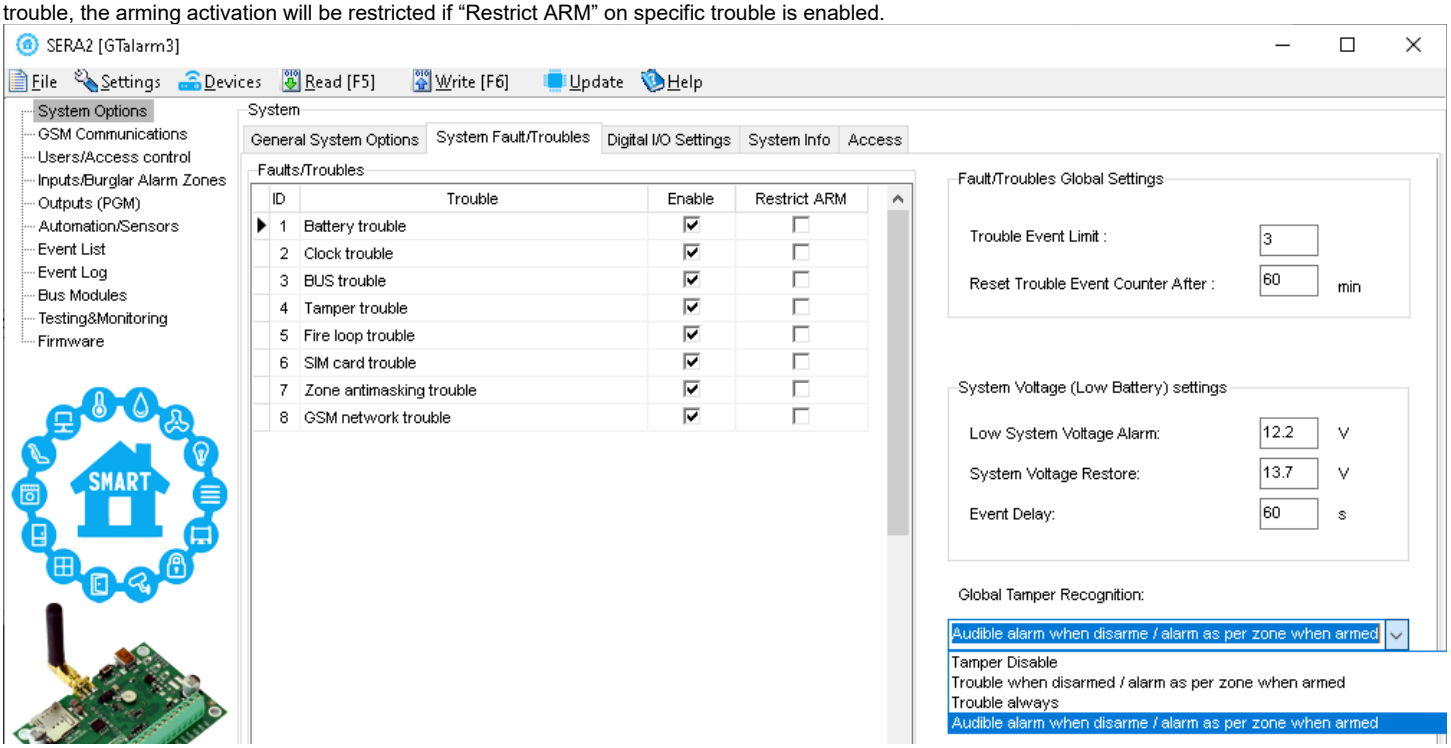
System Options > System Fault/ Troubles

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

In this window System trouble settings could be configured
The system can be armed in one of four modes DISARM, ARM, SLEEP, STAY.
By default, it is allowed to arm the system while the following system faults are present:

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

If needed, restrict arm, when such trouble occur, check near such trouble in the System options> System Fault/Troubles window. And in case of such trouble, the arming activation will be restricted if “Restrict ARM” on specific trouble is enabled.



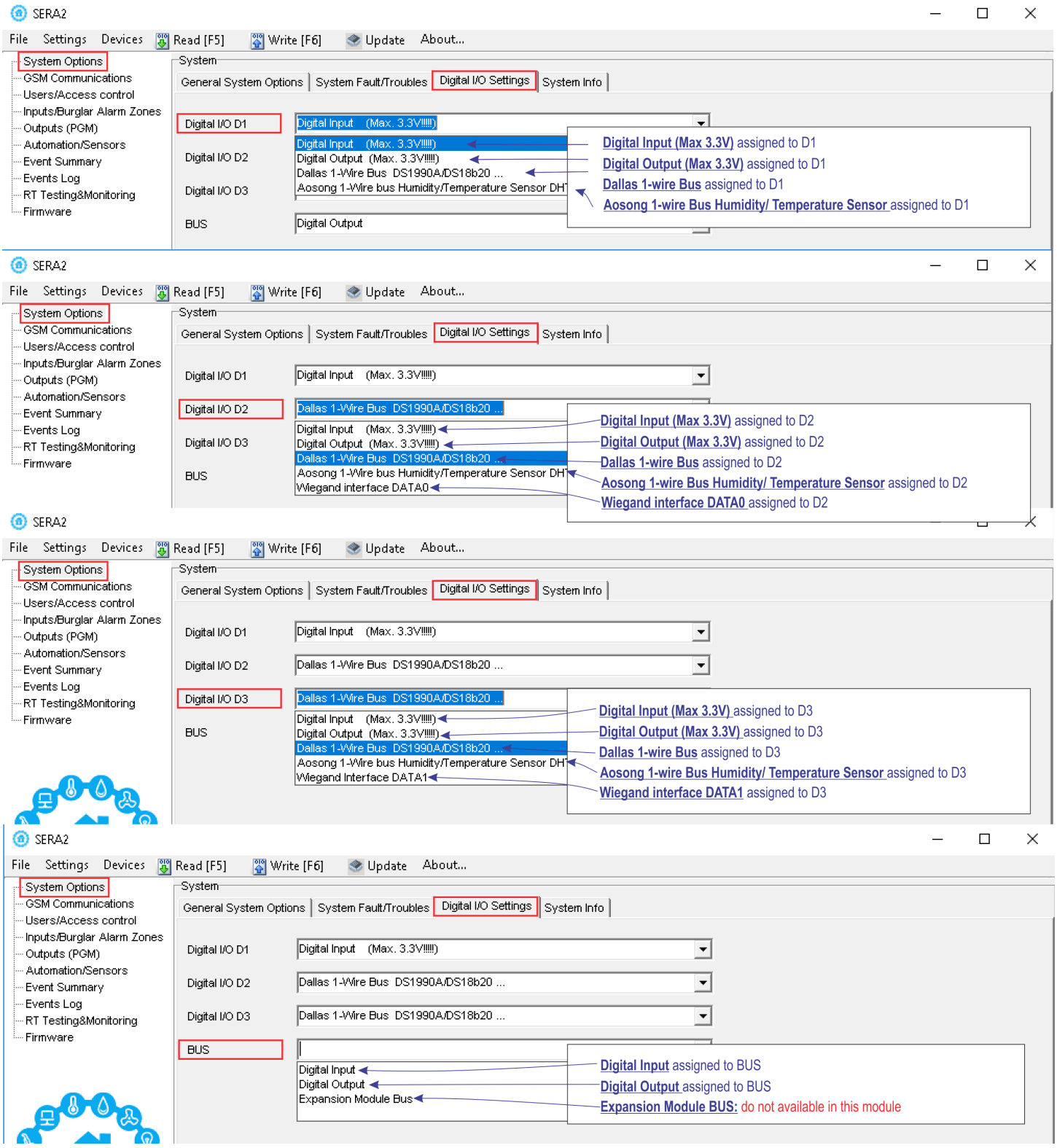
Trouble	This column lists potential system troubles
Enable	The system will detect a marked trouble
Restrict ARM	In case of such trouble, the arming activation will be restricted.
Battery trouble	Low system voltage. Power supply or backup battery voltage is low, needs to be recharged, or replaced.
Clock trouble	The time and date has not been set.
BUS trouble	The expansion device is no longer communicating with the module.
Tamper trouble	The zone(s) that was tampered
Fire loop trouble	The trouble is occurring with your smoke detectors.
SIM card trouble	Not available or impossible to read SIM card.
Zone ant masking trouble	Do not available in this module
GSM network trouble	SIM card is not registered with the GSM network provider
Low System Voltage Alarm	The module has detected a low voltage. This means that your system is running on the backup battery and voltage is dropped below allowed value.
System Voltage Restore	The module has detected that the system voltage has been restored.
Event Delay	System low voltage trouble event report delay.
Trouble Shutdown	Setting of the allowable number of the same trouble event, where in case of excess of such number the trouble reporting will be off. The number of such events is counted until the arming mode is changed (On/Off).
Fault/Troubles Global Settings	This setting determines the limit for repeated trouble alarms. Additionally, a timeout for such repeated alarms can be set.
System Voltage (Low battery)	When the system or battery voltage drops, the module can trigger a voltage alarm and initiate restore events once the voltage returns to the normal level. Both the alarm and restore voltage levels can be set manually. Additionally, a timeout for repeated alarms can be set [Event delay]

Global Tamper Recognition	Defines the control panel's response after detecting a tamper event.
	• **Tamper Disable**: The module will not trigger any alarm or trouble report.
	• **Trouble when disarmed / Alarm based on zone when armed**:
	  ○ Disarmed: Only trouble is generated. The module sends the specific report code.
	  ○ Armed: Module behavior is determined by the specific Zone Alarm Type.
	• **Trouble always**: Trouble is always generated, regardless of whether the system is armed or disarmed.
	• **Audible alarm when disarmed / Alarm based on zone when armed**:
	  ○ Disarmed: An audible alarm is produced. The module transmits the associated report code.
	  ○ Armed: Module behavior follows the specific Zone Alarm Type.

5.4 Digital Inputs/ Outputs programming

System Options > Digital I/O Settings

The Digital I/O Settings let you set digital input/ output parameters



5.5 GSM Communication

5.5.1 Event Notifications via SMS & DIAL

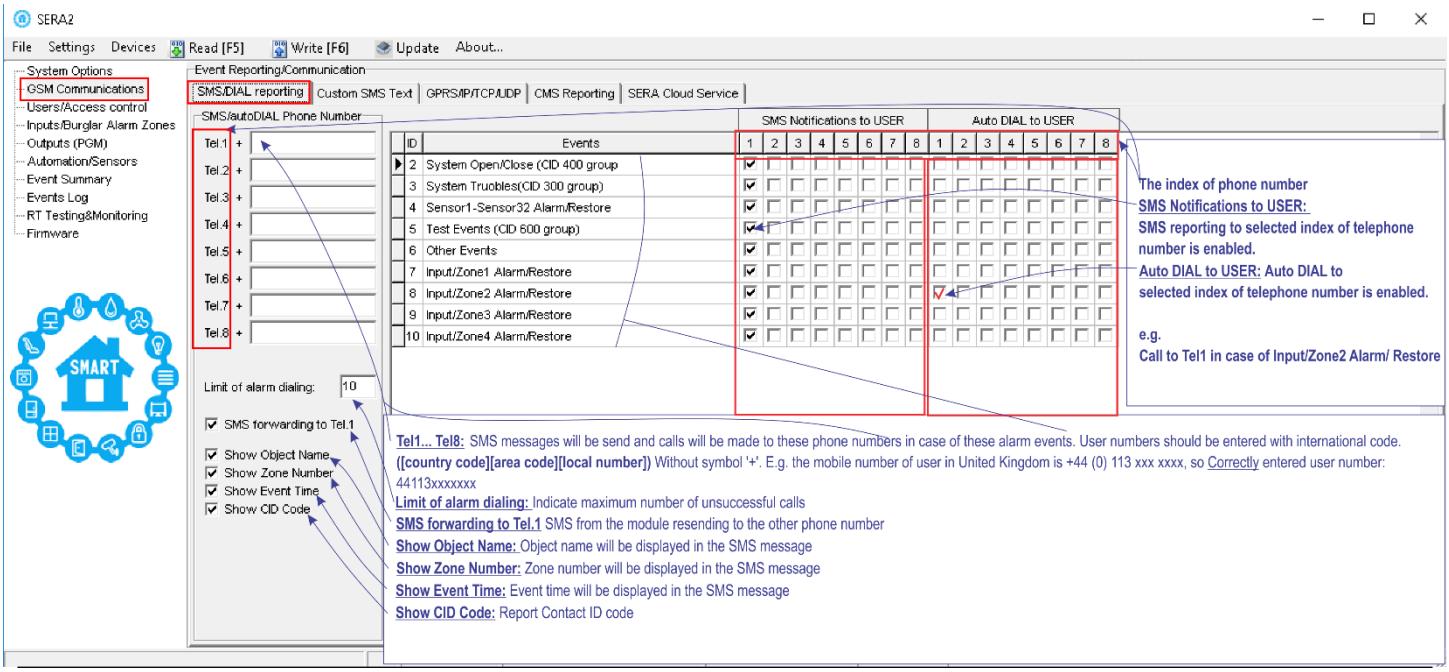
GSM Communications > SMS DIAL Reporting

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

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

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

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

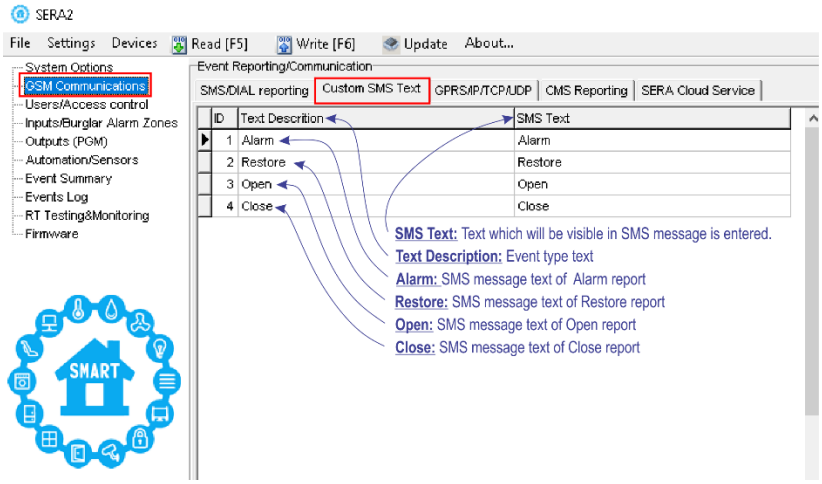


The SMS/auto DIAL Phone Numbers	Enter up to 8 user phone numbers for SMS and auto-dialing, using the international format **[Country code][Area code][Local number]** without the '+' symbol. For example, a UK number +44 (0) 113 xxx xxxx should be entered as 44113xxxxxxx. Incorrect formats would be 440113xxxxxxx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

5.5.2 Custom SMS Text

GSM Communication > Custom SMS Text

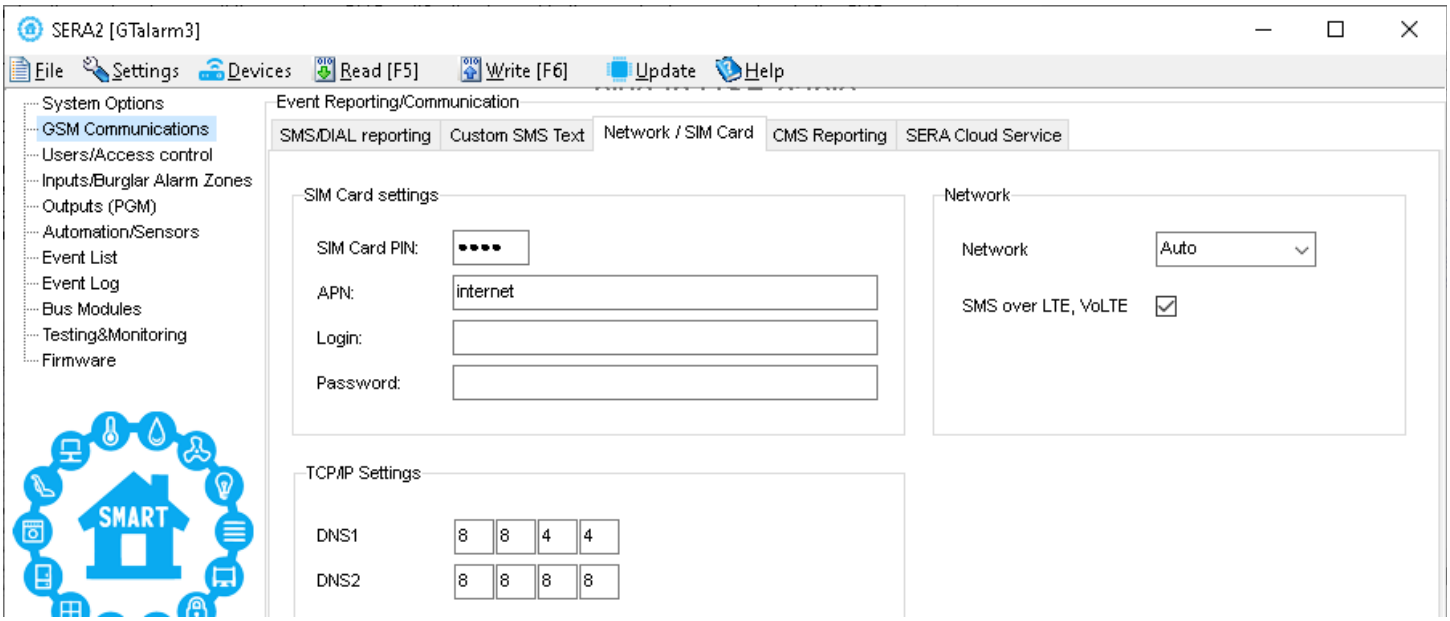
The Custom SMS Text options let you enter the text that will be send to the user in case if the alarm event occur.



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

5.5.3 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.

5.5.4 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).

The system is designed to report event notifications to the CMS by sending data messages. When CMS mode is enabled and set to GPRS, the system establishes a connection with the 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

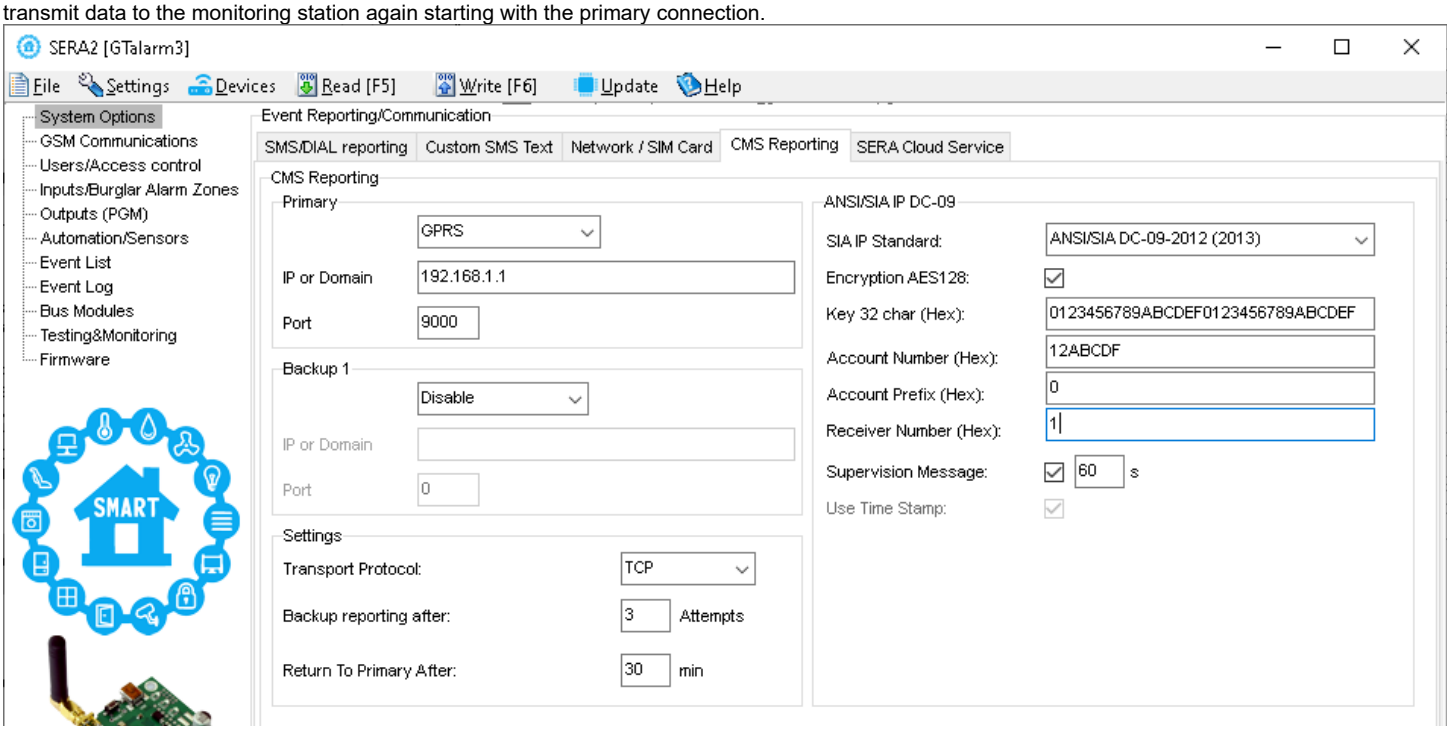
The system supports the following communication methods and protocols:

- 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.



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.

CMS Reporting	Primary central monitoring station settings
Backup 1	
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.

5.6 Zones programming

Connecting Detectors to GTalarm3:

- The GTalarm3 module has terminals for connecting detection devices such as motion detectors and door contacts.
- Once devices are connected to the module's zone terminals, you must configure the parameters for the corresponding zone.
- The module comes with 4 built-in wired zones and 2 programmable I/O inputs.
- If more connections are needed, the GTalarm3 can be expanded using an expansion module to accommodate up to 32 zones.

Zone Bypassing:

- Users have the option to "bypass" or deactivate a particular zone if it's been triggered. This allows the rest of the system to be armed without the need to reset the triggered zone.
- If a bypassed zone gets triggered during the exit/entry delay or while the system is active, it won't cause an alarm.

Stay Mode Features:

- "Stay mode" permits users to activate or deactivate the alarm system without having to exit the secured premises.
- If zones with the "Stay" feature are triggered when the system is in Stay mode, they won't set off an alarm. This is useful, for example, when you're at home and going to bed, and don't want certain zones (like inside motion detectors) to be active.
- The system will allow to enter Stay mode if:
  - A delay-type zone isn't triggered during the exit delay.
  - There's at least one zone with the Stay attribute enabled.
  - An arming method that includes an exit delay is used.

Difference between "Stay" and "Sleep" Zone Types:

- Zones with the "stay" type come with a delay zone timeout.
- Conversely, in the "sleep" zone type, what would typically be a delay zone becomes instant, meaning it triggers immediately.

Zone Reactions:

- If zones classified as "Instant" or "Silent" types are triggered, the system will NOT activate the siren or the keypad buzzer.
- For any zone designated as the "Delay" type:
  - When the system is in "Stay" mode, this zone behaves like an "Instant" zone, triggering immediately.
  - However, when the system is fully armed, the "Delay" zone operates with its typical delay.

Tampering:

- The tamper circuit is a continuous loop; any interruption triggers an alarm, whether the system is armed or not. This alarm activates the siren, keypad buzzer, and sends an SMS to the user. The alarm is set off by opening enclosures like the detection device, siren, cabinet, or keypad. To receive tamper alerts, ensure the “Tamper Enabled” option is checked, enabling both tamper detection and SMS notifications.

Programming:

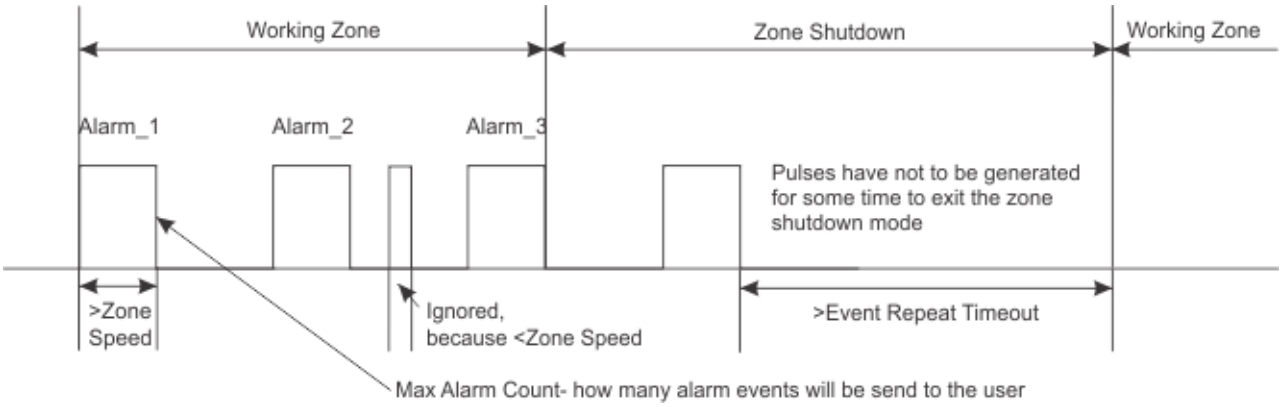
- Install SERA2 software.
- Connect the module to the computer via mini USB cable.
- Go to Zones window in the SERA2 software
- Set the required parameters
- Write configuration by pressing [Write] icon

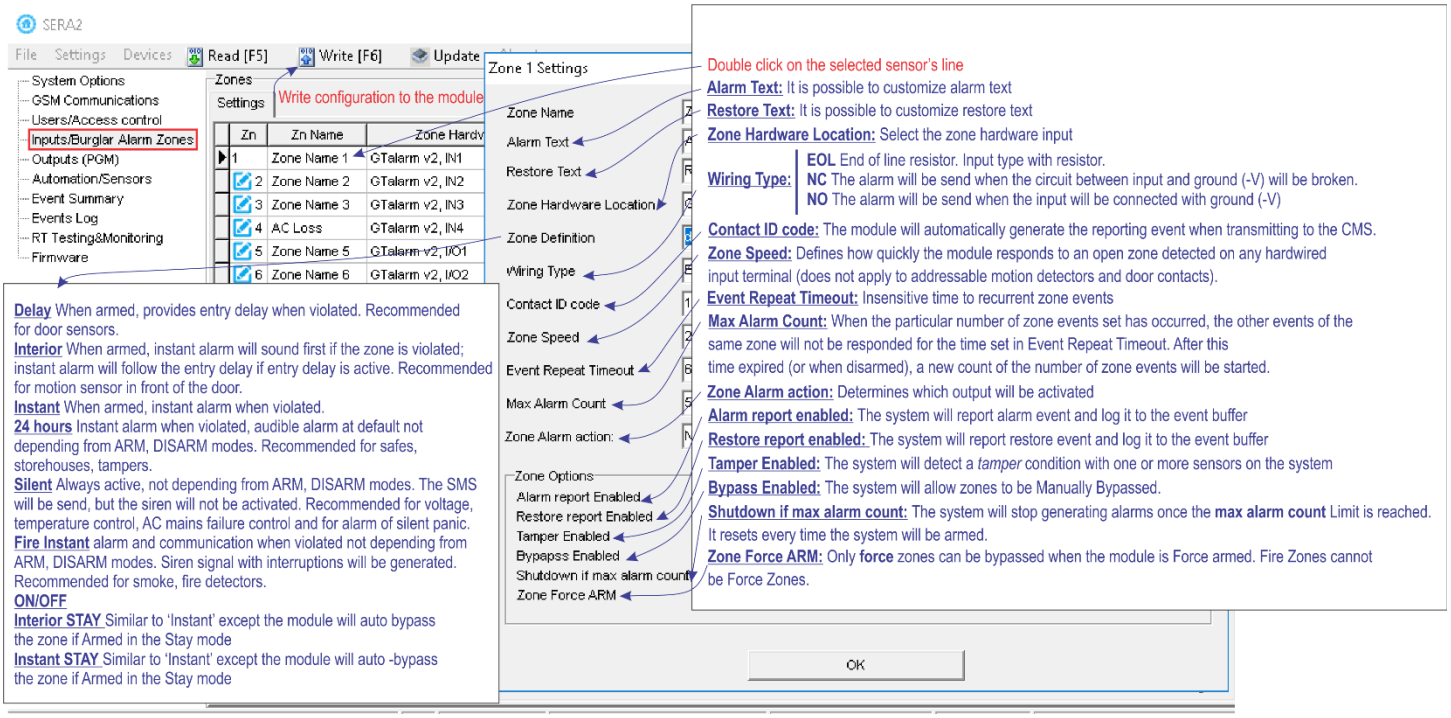
Note on Unused Zones: If any zone isn't in use, it must be disabled to avoid false triggers or alerts.

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

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

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



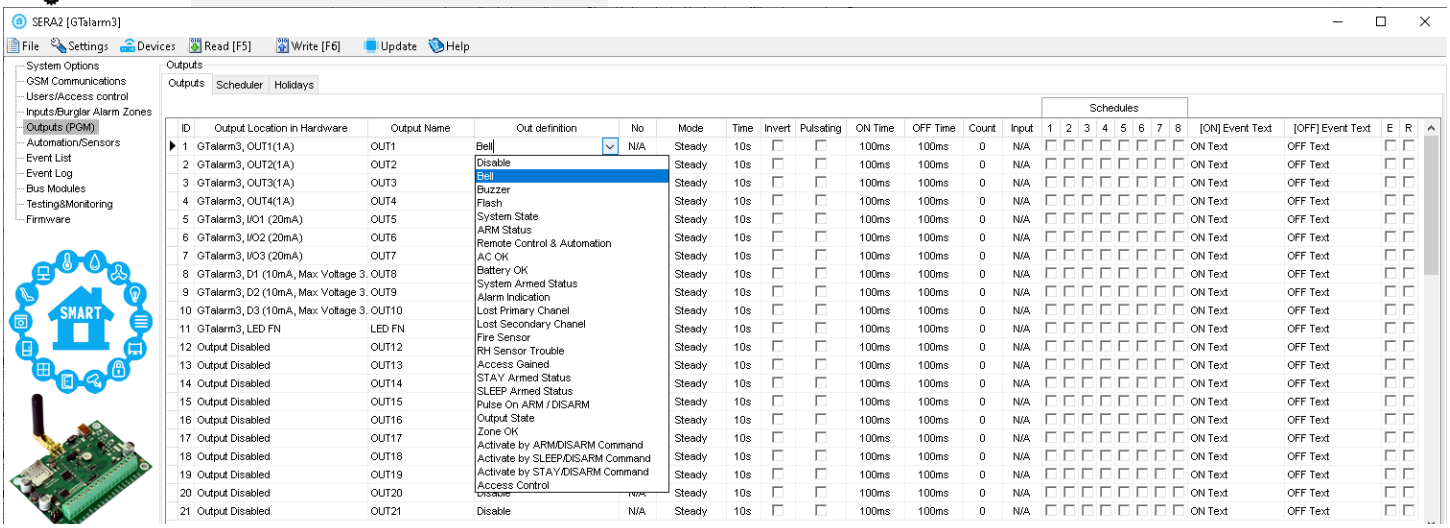


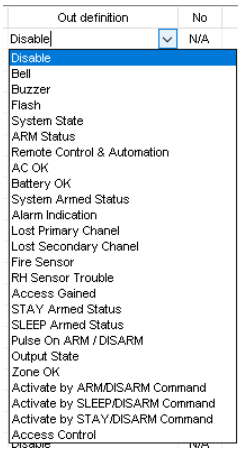
Alarm Text: It is possible to customize alarm text
Restore Text: It is possible to customize restore text
Zone Hardware Location: Select the zone hardware input
Wiring Type:
EOL End of line resistor. Input type with resistor.
NC The alarm will be send when the circuit between input and ground (-V) will 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
Instant STAY Similar to 'Instant' except the module will auto -bypass the zone if Armed in the Stay mode

5.7 Outputs. Bell & PGM programming

SERA2>Outputs (PGM)>[Outputs]



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.

5.8 Automation & Sensors Programming

SERA2> Automation /Sensors

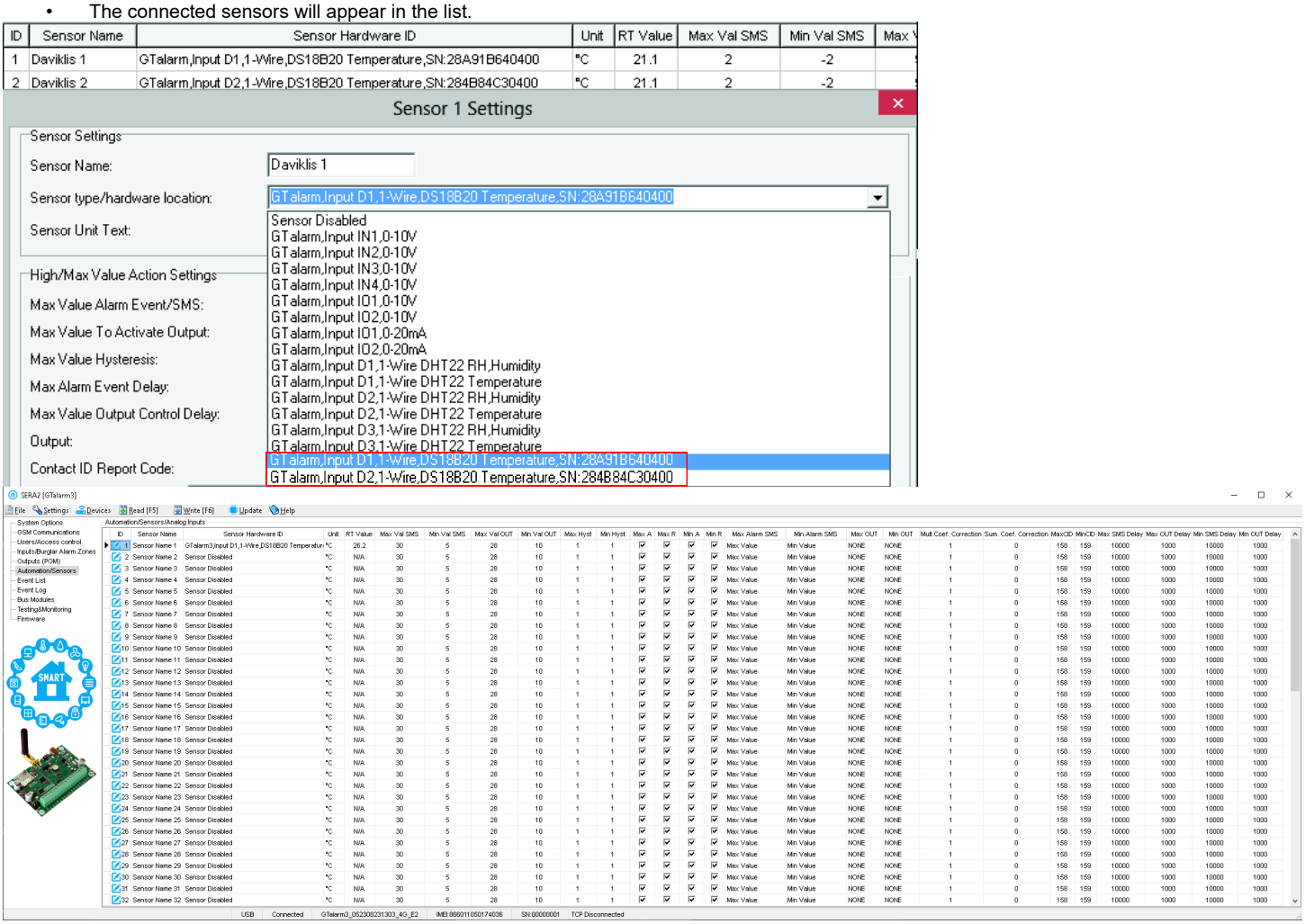
GTalarm3 Module Automation Insights:

- **Sensors:**
  - The GTalarm3 module interfaces with standard sensors that produce either an analog voltage/current (0-30V, 0-20mA) or digital data via the Maxim Dallas 1-Wire bus.
  - Sensor configurations and parameters are set using the SERA2 software.
- **Remote Configuration/Monitoring /Control/Access:**
  - Enables monitoring, controlling, and data logging from almost any global location through GSM GPRS/LTE networks.
  - Data is transmitted via GPRS/LTE, leveraging the TCP/IP protocol. Connection is made to the 'SERA Cloud service' which registers all devices. This connection is initialized by the SERA2 configuration tool using a unique identifier.
  - The SERA2 configuration tool sets up the connection using a unique ID, either IMEI or MAC.
  - The 'SERA Cloud service' facilitates efficient setup and configuration.
  - Ranges from basic data viewing to advanced features like receiving text alerts during alarms or transferring data logs remotely. Thanks to the GSM and GPRS/LTE capabilities, users can access this data whenever needed.
- **Testing & Monitoring:**
  - Monitoring of essential parameters like temperature, humidity, and potentially security, is crucial.
- **Localized Monitoring Systems:**
  - Adaptable for various environments, including but not limited to labs, museums, warehouses, computer rooms, food processing units, hospitals, and greenhouses.
  - Depending on specific needs, users can monitor ambient temperature, humidity, or utilize other processes like thermocouples. Sensors generating analog voltage/current or pulse outputs can broadcast this data universally.
- **Installation:**
  - Attach the GSM antenna and insert the SIM card with the PIN request deactivated.
  - Utilize a 10-30V/1A supply for power, and optionally connect the battery and the AC loss signal to IN4.
  - Connect the analog sensors (0-30V, 4-20mA) and digital sensors, like the DS18b20, following the GTalarm3's schematics.
- **Configuration:**
  - Start by setting up the SERA2 software.
  - Using a mini USB cable, link the module to a PC.
  - Initiate sensor parameters, PGM control outputs, and provide server reporting details.
  - Real-time monitoring offers insights on parameters like sensor inputs, voltages, current, and more.

5.8.1 Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software

Connecting Sensors to the Module:

- Double click on the selected sensor's line.
- Click on "Sensor type/ hardware location" and default sensor settings appear.
- Connect the sensors to the module. Connect the power supply.
  - Sensor's type should be select in the System Options> Digital I/O Settings window.
- Click [Read].
- The connected sensors will appear in the list.



Setting Sensor Parameters:

- Double-clicking on the desired sensor's line will open its configuration window.
  - For instance, double-clicking on the "Sensor Name 1" line will display the "Sensor 1 Settings" window.
- Within this window, you can adjust and set the required parameters for the chosen sensor.

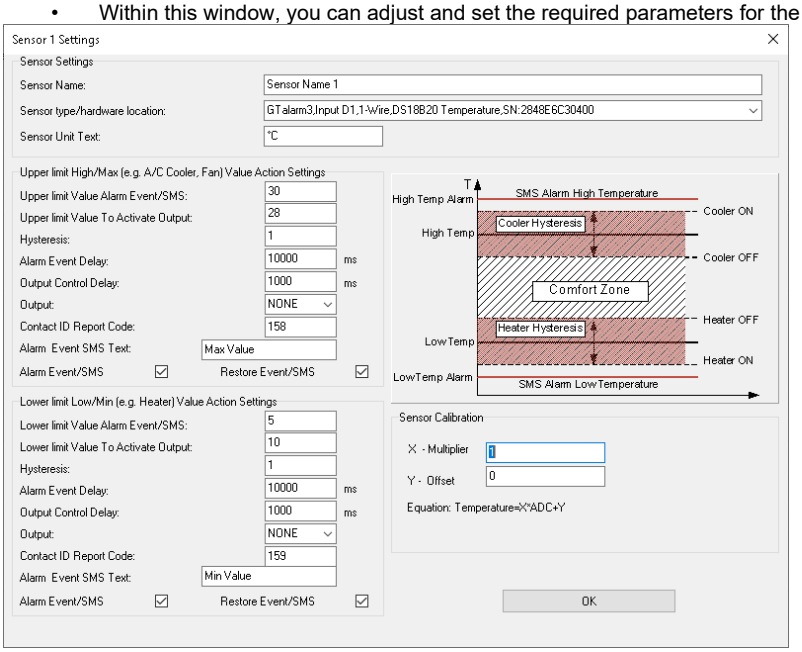


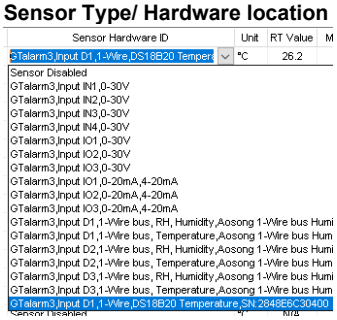
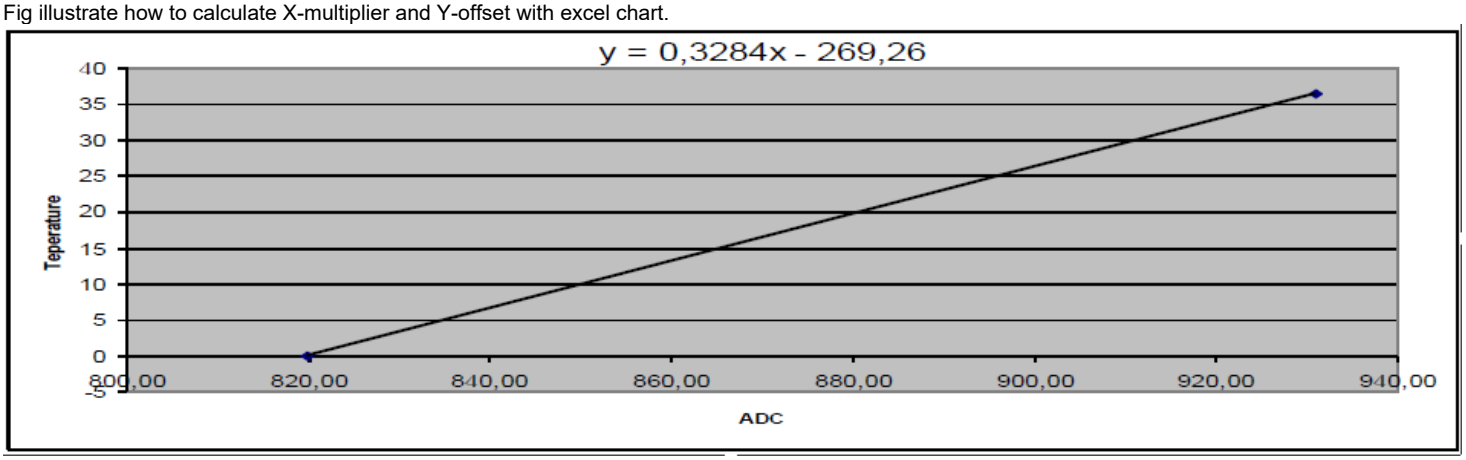
Table Column	Field name in Sensor Form	Column/Field Description
Sensor Name	**Sensor Name**	Sensor name
Sensor Hardware	**Sensor Type/ Hardware location** 	**Location of sensor connected to the module**: Specify which sensors are connected to the module. • **Sensor disabled**: Check if the sensor is deactivated. • **GTalarm, Input IN1…IN4, 0-30V**: Assign voltage input ranging from 0-30V to IN1…IN4. • **GTalarm, Input I/O1…I/O3, 0-30V**: Assign voltage input ranging from 0-30V to I/O1…I/O3. • **GTalarm, Input I/O1…I/O3, 0-20mA**: Assign current input for I/O1…I/O3 ranging from 0-20mA. • **GTalarm, Input D1…D3, 1-Wire DHT22 RH, Humidity**: Assign digital input D1…D3 for 1-Wire DHT22 RH Humidity sensor. • **GTalarm, Input D1…D3, 1-Wire DHT22 RH, Temperature**: Assign digital input D1…D3 for 1-Wire DHT22 RH Temperature sensor. • **1-Wire Temperature sensors**: Assign digital input D1…D3 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.
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.

Fig illustrate how to calculate X-multiplier and Y-offset with excel chart.



5.8.2 Recommendations for the user & installer

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

5.8.3 Realtime Testing & Monitoring > Sensors/ Automation

RT Testing & Monitoring > Sensors/ Automation

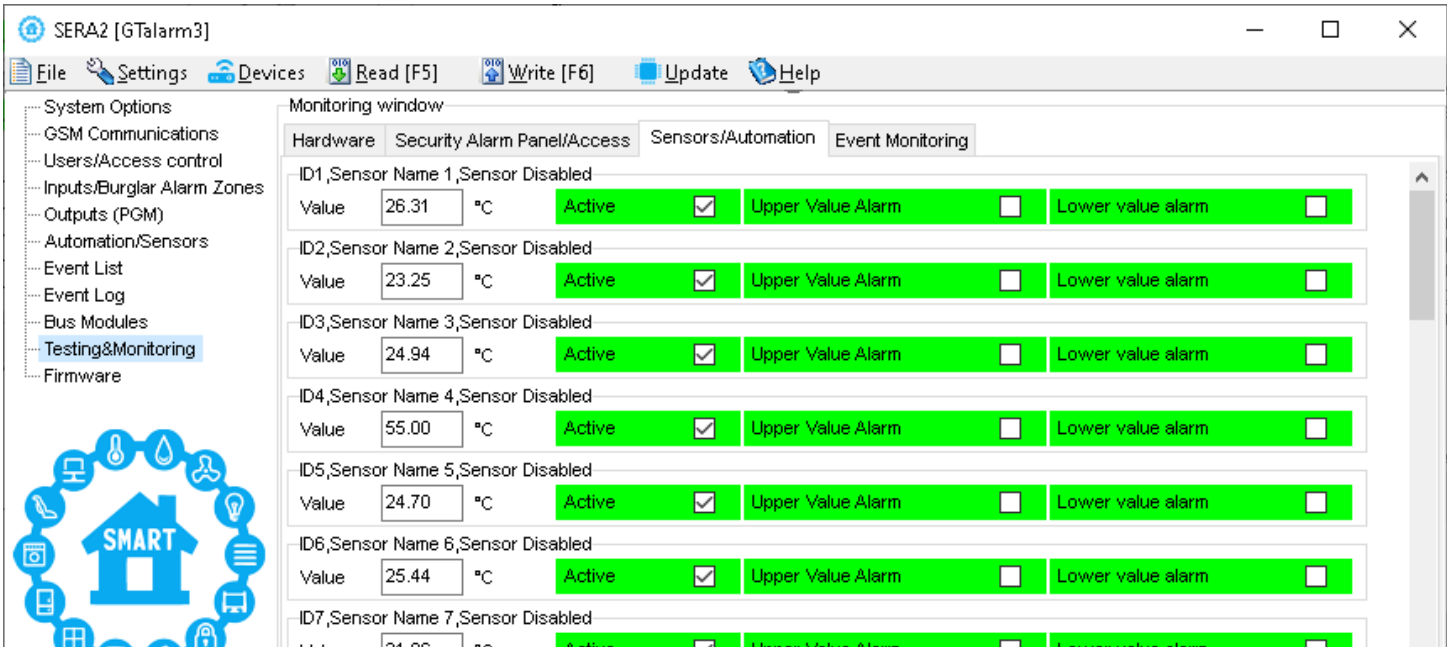
The Sensors/ Automation window let you see real time sensors states: is the sensor active, does it reaches high or low value alarm.

Recommendations for the user & installer

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



Sensor1…Sensor32	Sensor number
Value	The value of sensor's voltage
Active	If checked and the color is green, the sensor is active
High Val Alarm	If checked and the color is red, the high value alarm is generated
Low Val Alarm	If checked and the color is red, the low value alarm is generated

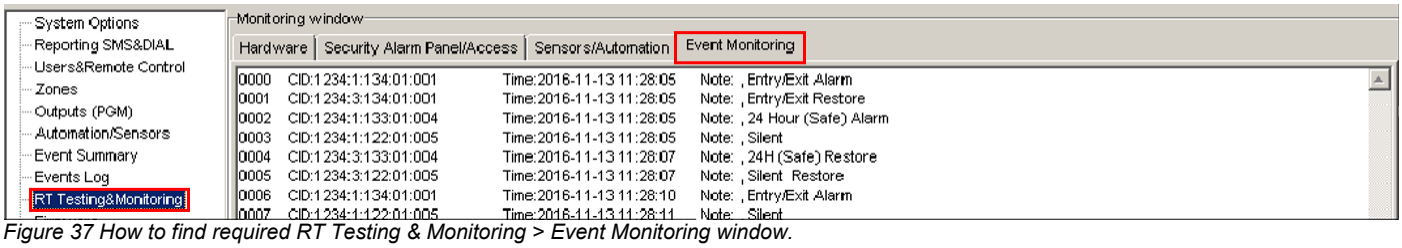


Figure 37 How to find required RT Testing & Monitoring > Event Monitoring window.

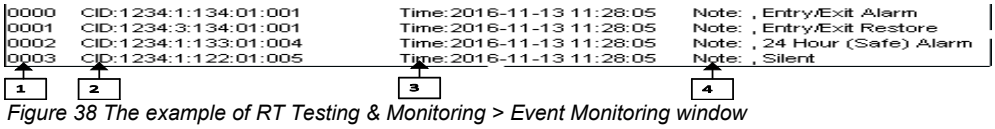


Figure 38 The example of RT Testing & Monitoring > Event Monitoring window

Table 7 Explanation of every field in "Event Monitoring" window

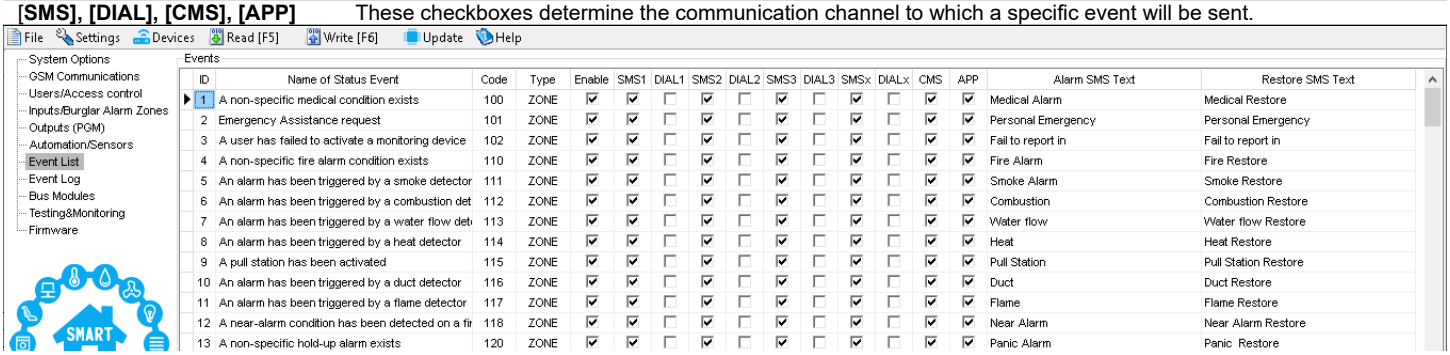
…	Event number
CID	Contact ID Code
Time	Event date and time
Note	Event report text which was indicated.

5.1 Event List

Event List

The Event List table illustrates Contact ID codes of the events and enable user to change the text that will be reported in case if the event occur.

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 USER — Refer to USER Report Options ZONE — Refer to Zone Report Options NUM — Refer to Numerical Report Options
[SMS], [DIAL], [CMS], [APP]	These checkboxes determine the communication channel to which a specific event will be sent.



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 detector	111	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Smoke Alarm	Smoke Restore
6	An alarm has been triggered by a combustion det	112	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Combustion	Combustion Restore
7	An alarm has been triggered by a water flow det	113	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Water flow	Water flow Restore
8	An alarm has been triggered by a heat detector	114	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Heat	Heat Restore
9	A pull station has been activated	115	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Pull Station	Pull Station Restore
10	An alarm has been triggered by a duct detector	116	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Duct	Duct Restore
11	An alarm has been triggered by a flame detector	117	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Flame	Flame Restore
12	A near-alarm condition has been detected on a fi	118	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Near Alarm	Near Alarm Restore
13	A non-specific hold-up alarm exists	120	ZONE	☑	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	Panic Alarm	Panic Restore

5.2 Events Log

Events Log

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

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

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

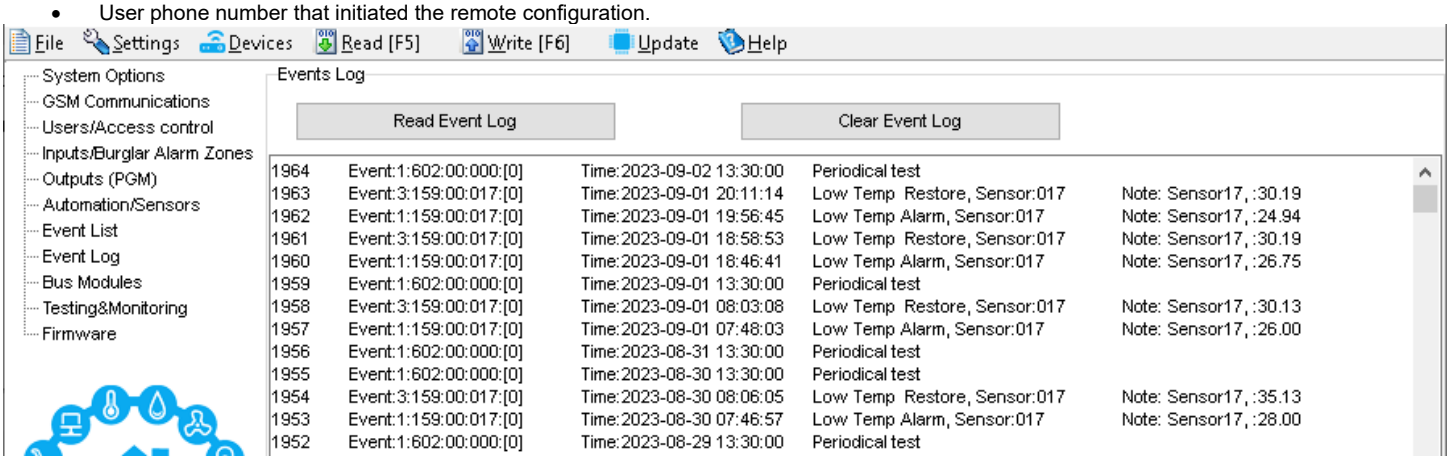


Table 8 Explanation of every field in "Events Log" window

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.

5.1 Real-Time Testing & Monitoring of Hardware

RT Testing & Monitoring > Hardware

Real-time monitoring of the system hardware can be achieved via USB or TCP Cloud connection. The Hardware Monitoring window offers real-time insights into the states of inputs and outputs, system state, voltages, sensor functionality, and GSM network registration information.

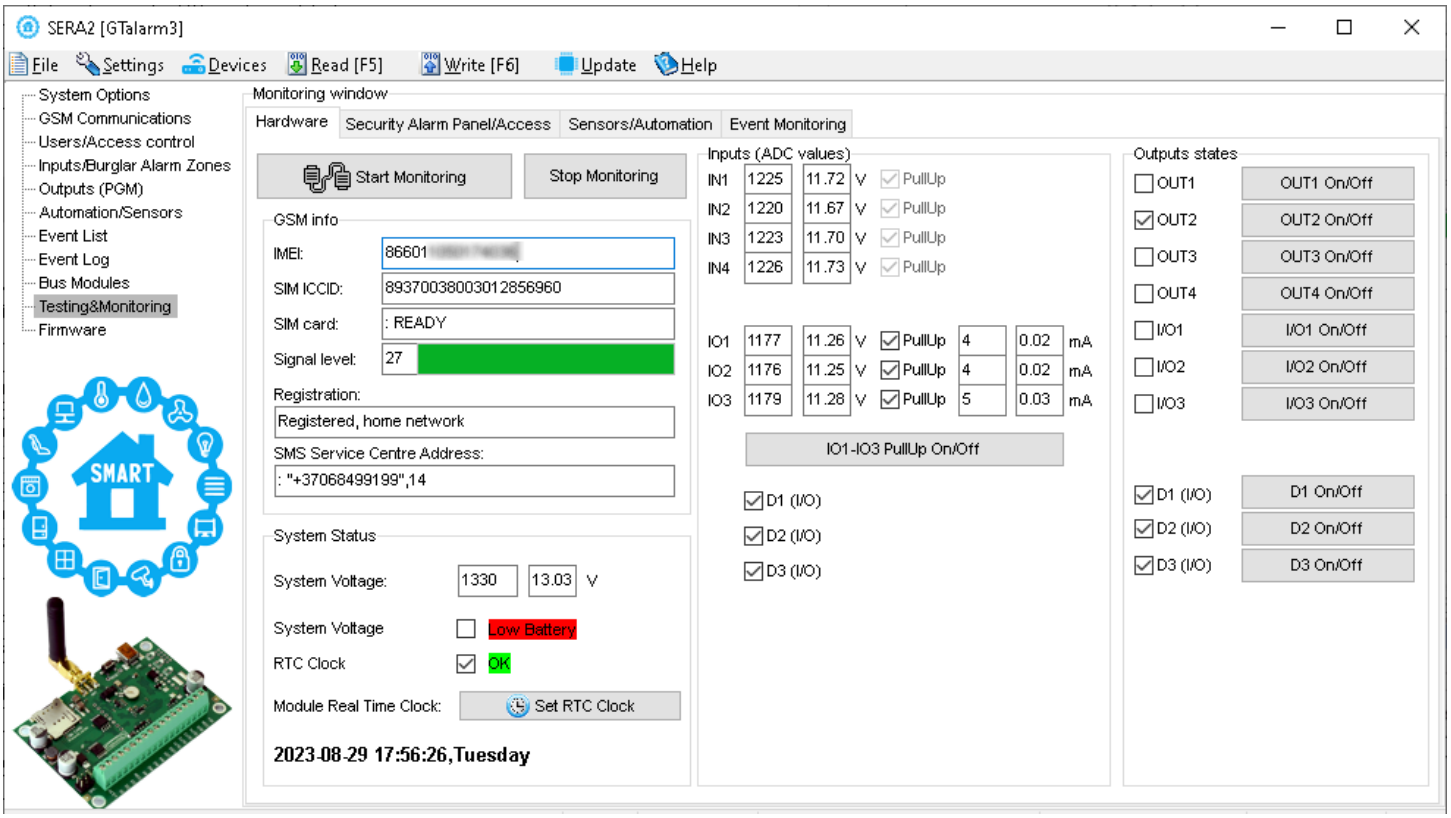
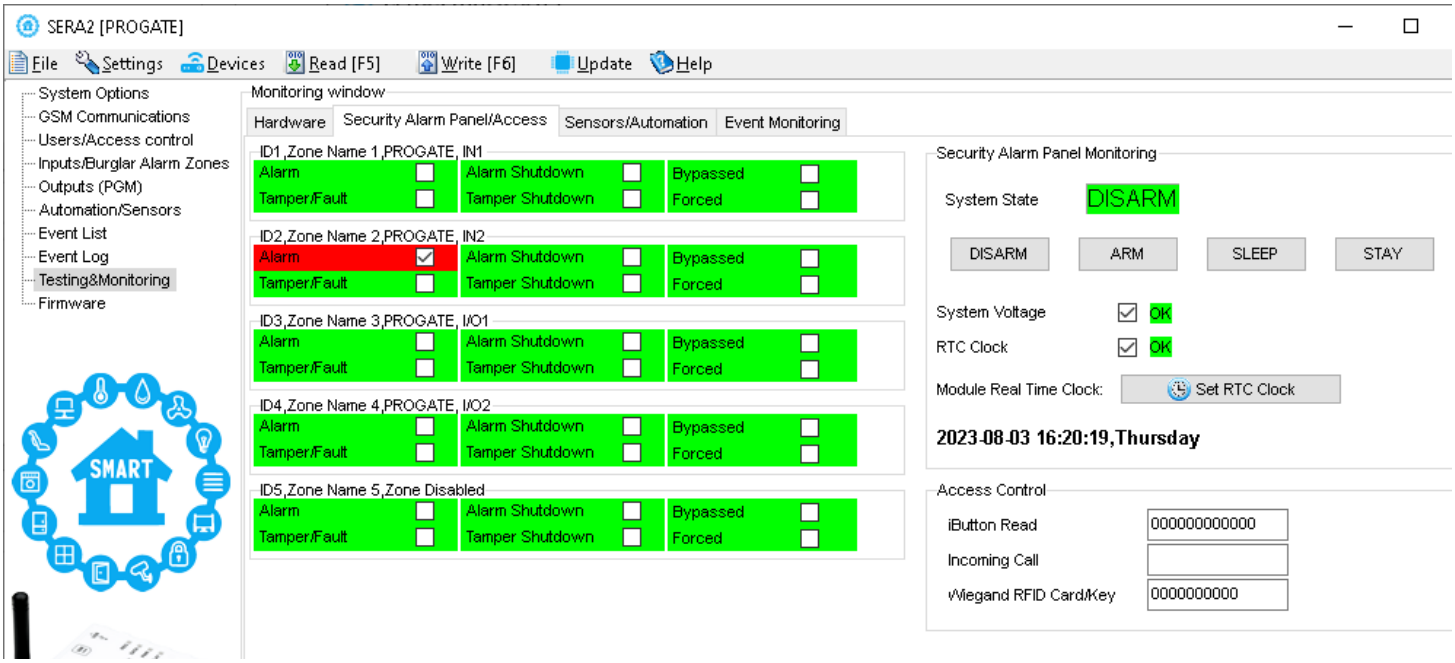


Figure 39 The example of RT Testing & Monitoring > Hardware window

Start Monitoring	Pressing **Start Monitoring** button starts the monitoring of the module.
Stop Monitoring	Pressing **Stop Monitoring** button stops the monitoring of the module.
IMEI	IMEI number of GSM modem available in the module
SIM ICCID	**ICCID (Integrated Circuit Card Identifier)** - A SIM card contains its unique serial number (ICCID). ICCIDs are stored in the SIM cards and are also printed on the SIM card.
SIM Card	If note READY is visible, it means that SIM card is fully functioning. Otherwise, check whether PIN code request is off or replace SIM card.
Signal level	Signal strength of GSM communication
Registration	State of GSM modem registration to GSM network.
SMS Service Centre Address	SMS center number. This number should be checked if it is correct. If this number is incorrect. SMS messaging may be impossible. This number may be changed after inserting SIM card into any mobile phone.
System Voltage	Power supply voltage. Nearby number is value of ADC voltage. When multiplying this number by the coefficient Fig. 32, voltage value (V) will be achieved.
System Voltage	System voltage OK/Trouble
RTC Clock	Real time clock OK/Trouble
Module Real Time Clock	Indicates the time of the module RTC
Set RTC Clock	By pressing this button real time clock of the module will be set.
Inputs In1…In4	In1…In4 is the indicated input ADC and voltage value V.
I/O1…I/O3	I/O1…I/O2 is the indicated voltage ADC value and current ADC value mA.
Out1…Out4 On/Off	Checked box nearby the appropriate output **Out1…Out4** means that this output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button
I/O1…I/O3 On/Off	Checked box nearby the appropriate input/output **I/O1…I/O3** means that this input/output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button
D1…D3 (I/O) On/Off	Checked check box nearby the digital outputs **D1…D3 (I/O)** means that the output currently has ‘0’ or ‘1’ state.

5.1.1 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.

6 SMS Commands for remote control and configuration

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

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

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

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

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

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

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

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

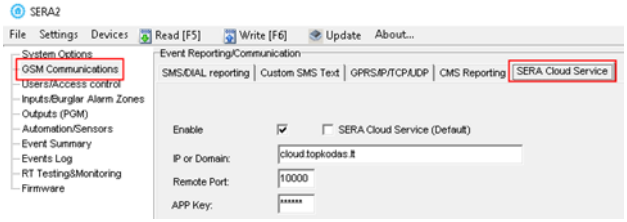
In this guide, we use the symbol "␣" to represent a single space. Each "␣" you see should be replaced with one space in your actual SMS text. Please avoid any extra spaces or characters before and after your message. Remember: For SMS, "␣" = Space. We use "␣" in examples for better clarity.

6.1 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 9 the table of installers commands

INST000000␣001␣ID#TEL#SMS#DIAL# e.g. INST000000␣001␣1#37066666666#11111111#10000000#	**To add admin user phone numbers for SMS and Call notifications upon an event, use the following format:** 001 = Code for adding admin user's phone numbers ID = User index (1-8) TEL = User's phone number (max 16 digits), without (+), including country and operator's code. End with '#' SMS = Notification event filter. 1 sends the event, 0 doesn't. Events are ordered (1.2.3...n), e.g., 001000 DIAL = Dial event filter. 1 dials if the event occurs, 0 doesn't. Events are ordered (1.2.3...n), e.g., 101000 #= delimiter **Example: INST000000 001 1#37066666666#0001000000#0000011111#** The event filter order is as follows, with 0 indicating disabled and 1 enabled: 1. Alarm/Restore (CID 100 group) 2. System Open/Close (CID 400 group) 3. System Troubles (CID 300 group) 4. Sensor1-Sensor32 Alarm/Restore 5. Test Events (CID 600 group) 6. Other Events 7. Input/Zone1 Alarm/Restore 8. Input/Zone2 Alarm/Restore 9. And so on.
INST000000␣002␣ID e.g. Delete admin User1 at index 1 INST000000␣002␣1	**To delete an admin user's phone number (used for SMS notifications), use the command '002' followed by the user ID index (1-8)**. 002 = Command code for deletion ID = User index (1 to 8)
INST000000␣003	**Delete all users in database.** 003 = Command code
INST00000 0␣004␣ID#TEL#OUT#OPT#NAME# e.g. Add user at index 1 , phone-37066666666, out1 INST000000␣004␣1#37066666666#1#10#Jon#	**To enter user‘s telephone number for remote control via short call** **USER NAME-only Latin characters is allowed inside SMS** 004= command code (enter user‘s telephone number for remote control via short call) ID = user ID number 001-800 TEL = user‘s telephone number (max 16 digits) without (+) comprised of country code, operator‘s code and user‘s telephone number. the end symbol #; OUT= output number, that will be controlled, 1-32. 0-Disabled, 1=OUT1=RELAY,2-OUT2,… OPT = 0 – disabled 1 – enabled, Sequence from the left to the right 1. User Enabled 2. Enable Arm/Disarm system by call NAME = User Name up to 31 characters.
INST000000␣005␣TEL# e.g. delete user associated with phone 37061611111 INST000000␣005␣37061611111	**To delete a user's remote control access according phone number, use:** 005 = Command code for deletion. TEL = User's phone number (16 digits max, without '+'), including country and operator codes. The number must match the one in the module's memory."
INST000000␣006␣ID e.g. delete user at index 200 INST000000␣006␣200	**Delete user's phone number by index.** 006= command code ID = Enter the user's index number from 001 to 800 to delete all data associated with the user.
INST000000␣007␣P#PER#HH:mm# e.g. INST000000␣007␣1#7#18:30#	**Automatic periodical test settings** 007= command code (Automatic periodical test) P= 0-test disabled, 1- test period by 24 hours, 2- period by hours PER= automatic test sending period from 1 to 99999 days or hours HH-hours 0-23 , mm- minutes 0-59 e.g. INST000000 007 2#1#14:50# The test will be send every 1 hour

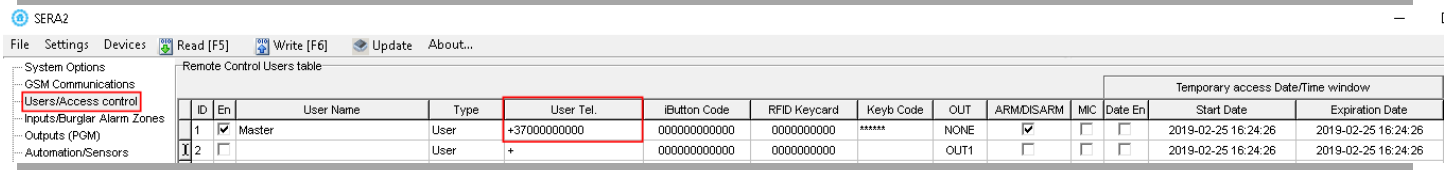
INST000000␣008␣APN#LOGIN#PSW# e.g. INST000000␣008␣internet### Apn="internet and no login and password.	**DATA/GPRS/LTE network settings** 008= command code (network settings) APN=31 symbols LOGIN=31 symbols PSW=31 symbols
INST000000␣009␣ADDR#PORT#PING#KEY# e.g. INST000000 009 cloud.topkodas.lt#1000#600#123456#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

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

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

6.2 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.

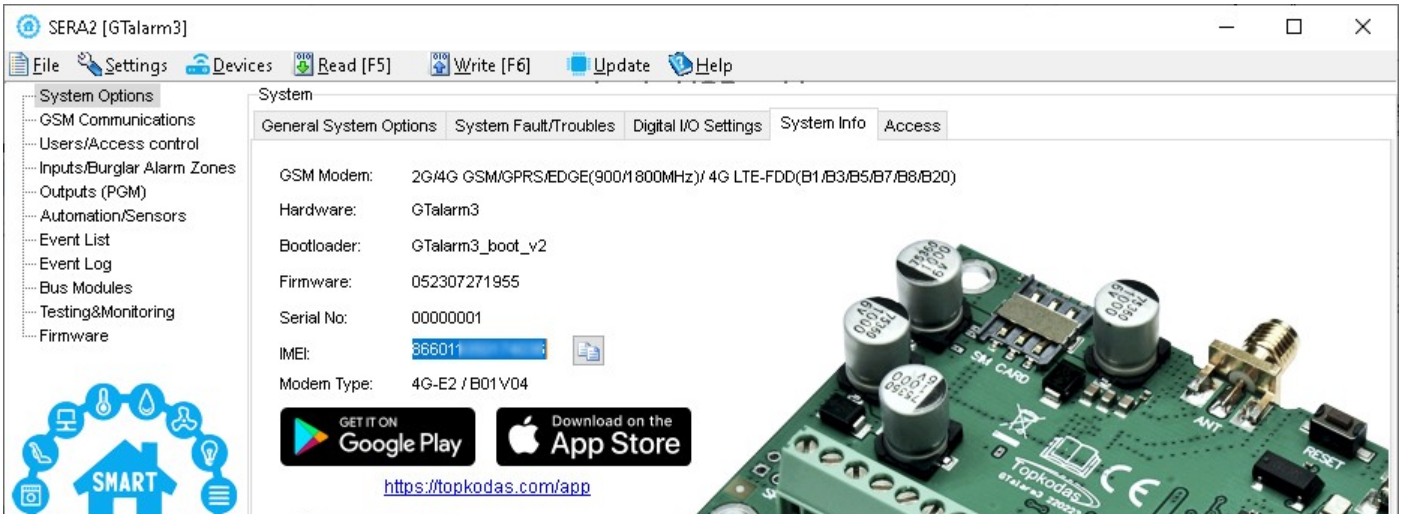
Table 10 the table of user's commands

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).

7 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.

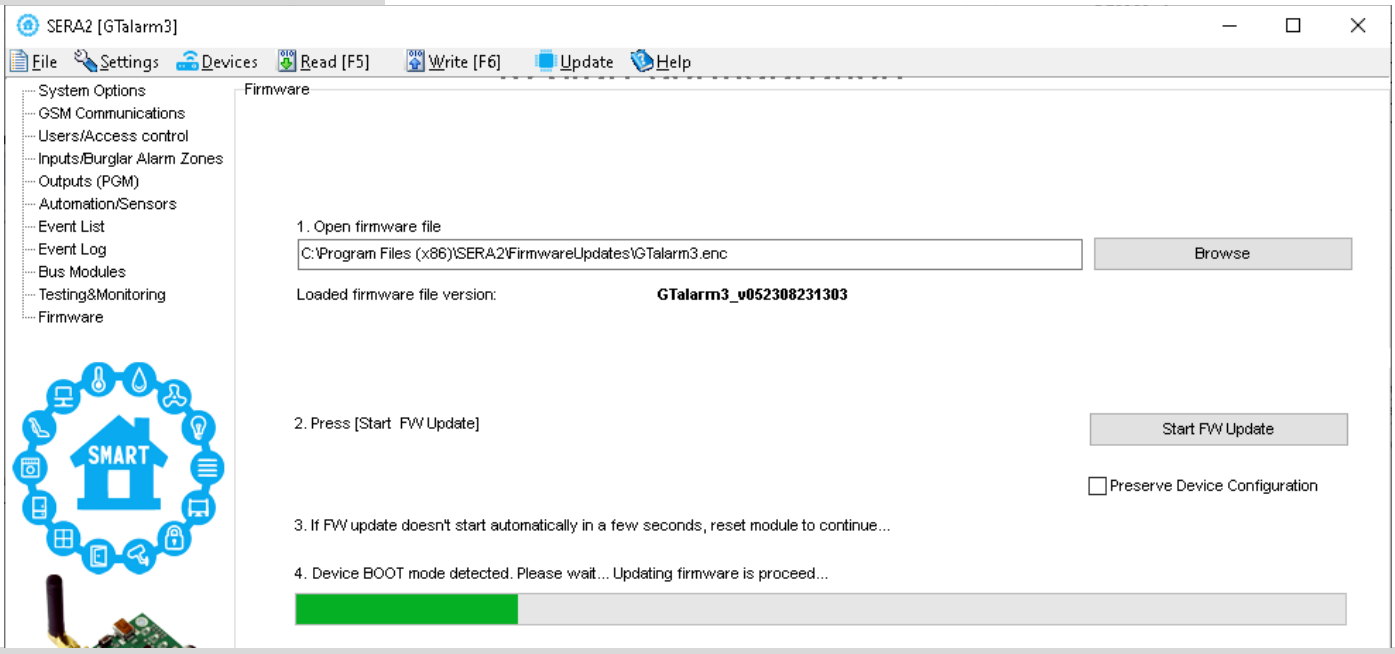


GSM Modem	Modem type and supported bands
Hardware	Device type
Bootloader	Bootloader version
Firmware	Configuration software
Serial No	Module registration number
IMEI	GSM modem IMEI address.

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.

8 Warranty Terms and Conditions

SAFETY INSTRUCTIONS FOR SERVICE PERSONS
Use the following list as a guide to find a suitable place for GTalarm3 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 GTalarm3 is not a substitute for property or life insurance. The module GTalarm3 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.