



GTalarm2

Installation & Programming Manual



Security, monitoring and automation system



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

The module GTalarm2 is a security, automation and access control system with 6 zone inputs. It is possible to connect up to 32 sensors to these inputs.

The module GTalarm2 has:

6 analog inputs 0-10 V,
2 analog inputs 0-20 mA,
4 outputs 24 V /1000 mA open drain.
3 digital input/outputs.

The zones can be used to automate PGM activations.

The module GTalarm2 features up to 800 users for remote control purpose and up to 8 users for remote monitoring via SMS purpose.

This system is designed to be easy to use, and provides installers with labor-saving features. It is possible to save the configuration to the file and upload to the other module if needed.

Once installed, all bus modules, including motion detectors, can be programmed remotely via GPRS connection or via USB using SERA2 upload/download software.

The module GTalarm2 is a logical solution to every installer's security, access control and home automation installation needs.

Features of the module GTalarm2

- Communication via SIA IP DC09 protocol
- 2G or 3G modem
- 4 Analog inputs (pull up 5.1K) 0-10V
- 2 Analog Input/ Output , 0-10V , 0-20mA
- 3 Digital Inputs/Outputs 3.3V , 20mA,
- Wiegand interface, Dallas 1-Wire Bus
- 4 PGM outputs 24V/1000mA. Open Drain.
- Up to 32 sensors, temperature, humidity etc.
- Digital expansion module BUS.
- Built-in access control features
- In-field firmware upgradeable via USB and SERA2 software
- Events log buffer. 2048 events
- Program remote controls using the master or installer codes
- Up to 800 users remote controls with mob phone,
- Up to 800 users remote controls with iButton or RFID keycard
- Up to 800 user code. To control with Wiegand keyboard.
- Built-in-real-time clock backup battery
- Unlimited control via SMS.
- Push button software reset

The meaning of icons in the manual:



Automation part



Security system's part



Very important



Important



About the manual

Contents

1	General information about the module GTalarm2	4
1.1	Specifications	4
1.2	Used definitions and terms	4
1.3	Package content	5
1.4	General view of the module	6
1.5	Meaning of LEDs and contacts	7
1.6	System Access codes. Default passwords	8
2	QUICK START First steps to prepare GTalarm2 and SERA2 software	9
3	Installation	10
3.1	Power supply, Battery Wiring	10
3.2	Inputs	11
3.3	Sensors. Automation	11
3.3.1	Humidity sensors AM2302/DHT22/AM2305/AM2306/AM2320/AM2321	11
3.3.2	Analog inputs 0-10V, 0-20mA, 4-20mA	13
3.3.3	Temperature sensors Dallas 1-wire DS18B20 installation & recommendations	15
3.3.3.1	Wiring Dallas 1-wire DS18B20	15
3.3.3.2	Temperature sensors Dallas 1-wire DS18B20 Configuration	16
3.3.3.3	How to change temperature scale from Celsius to Fahrenheit	17
3.3.4	Step by step: How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list?	17
3.4	Sensors. Security	18
3.4.1	Burglar Alarm sensor zones wiring EOL NO NC	18
3.4.2	Fire alarm and Smoke sensors	21
3.4.2.1	Guidelines for Locating Smoke Detectors and CO Detectors	21
3.4.2.2	[4-Wire] Smoke detector Wiring	21
3.4.2.3	[2-Wire] Smoke Detector Wiring to I/O Inputs	22
3.5	Outputs	23
3.5.1	Output PGM wiring. Bell, Relay, Led Wiring	25
3.5.2	Access control output with logging	25
3.5.3	Quick start outputs	26
3.6	Access control. Arming/Disarming methods	26
3.6.1	Wiegand Keypad & RFID Card Reader, iButton Probe Wiring	29
3.6.2	Enter iButton, RFID, Phone numbers to the memory of the module	30
3.7	How to set clock synchronization?	31
5	Programming	33
5.1	SERA2 Uploading/Downloading Software	33
5.2	General system options programming	34
5.3	System Fault/ Troubles Programming	36
5.4	Digital Inputs/ Outputs programming	37
5.5	Zones programming	38
5.6	Outputs. Bell & PGM programming	40
5.7	Users & Access Control programming details	41
5.8	DISARM /ARM/SLEEP/STAY the security system	44
5.9	Reporting SMS&Dial in Case of Alarm Events	46
5.9.1	Reporting to the user's mobile phone	47
5.9.2	Custom SMS Text	47
5.10	Reporting to the Central Monitoring Station	48
5.10.1	GPRS/ IP/ TCP/ UDP details programming	48
5.10.2	Central Monitoring Station details programming	49
5.11	Event Summary (Events)	50
5.11.1	RT Testing & Monitoring. Hardware	51
5.12	RT Testing & Monitoring Security Alarm Panel/ Access	52
5.13	Automation & Sensors Programming	53
5.13.1	Automation/Sensors (Automation/Sensors/Analog Inputs) Programming in SERA2 Software	53
5.14	Data Transmitting to Server & Remote Control	56
5.14.1	TCP/ IP Remote Control	56
5.15	Events Log	57
5.16	Remote Monitoring, Control, Configuration, FW update over the internet	57
5.17	Testing & Monitoring Automation	59
5.17.1	Realtime Testing & Monitoring > Sensors/ Automation	59
5.17.2	Realtime Testing & Monitoring > Event Monitoring	60
6	Info: Hardware, Firmware, Bootloader, Serial No & Updates	61
6.1	Firmware Update	62
7	Recommendations for the user & installer	62
8	Remote control and configuration using SMS Commands	62
9	The table of installers commands	63
10	The table of users commands	66
11	APP configuration	66
12	Warranty Terms and Conditions	67

1 General information about the module GTalarm2

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 max current – (-V) 1000 mA.
- OUT2 max current – (-V) 1000 mA.
- OUT3 max current – (-V) 1000 mA.
- 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:

- SMS text for input alarm and restore
- Available to control until 32 sensors
- Programmable enabling or disabling of inputs;
- Burglary alarm zones. Input type NC/NO/EOL/EOL+TAMPER 2.2K + 2.2K
- 5.1K pull up resistor.
- Analog input 0-10V
- Algorithm for zones operation: delay, interior, instant, 24 hours, silent, fire
- Response time;
- Time of additional response;
- Commutation of selected output
- Control of analog sensors

Inputs/outputs I/O1-I/O2:

- Programmable input or output
- Burglary alarm zones. Input type: NC/NO/EOL/EOL+TAMPER
- Analog 0-10V/0-20mA/4-20mA
- Control of analog sensors

Digital inputs/ outputs D1-D3:

- Programmable optional digital input or output
- Max. Voltage 3.3V
- Dallas 1-Wire Bus, DS18B20, DS1990A
- Aosong 1-Wire bus Humidity Sensor AM2302 DHT22 AM2305 AM2306 AM2320 AM2321
- Wiegand interface DATA0/ DATA1, RFID reader, Keyboard.
- The total length of the bus from 10 to 100m.

Module control:

ARM/DISARM of the security system via:

- „Key switch” input level or pulse mode.
- SMS message 800 users
- short call DIAL 800 users
- Maxim-Dallas iButton key (iButton DS1990A – 64 Bit ID)) 800 users.
- Wiegand keypad code or RFID keycard or key fob 800 users

3.3V power source output for external modules:

- Voltage 3.3V
- Current limit 100mA

BUS expansion modules or programmable input/output:

- Voltage 8-15V
- Current 20mA

Automatic periodical test:

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

Power supply voltage:

- Nominal power supply voltage – 12.6 V
- Power supply voltage range 8 – 15 V
- 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 2048 events

Environmental parameters:

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

Package weight 90g

Module weight: 43g

Overall dimensions of the module: 84x66x18mm

1.2 Used definitions and terms



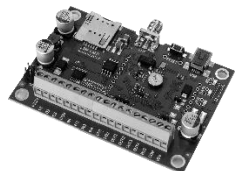
Term	Description
Alarm Log	Contains information about alarms that are currently active on the system or information about alarms that have been raised and then resolved on the system. This log can be useful in analyzing problems and trends in the system.
Arming/Disarming	A process of enabling/disabling system's security.
Authorized user	It is a person whose mobile phone's number is entered in GTalarm2 module. Several authorized users with the same rights may be entered into the module.
Backup battery	The secondary power source of the system. In case of a main power failure, the backup battery will take over.
Bell squawk	If enabled, the siren/bell indicates the completed system arming and disarming process (except the arming in STAY mode). After the system is successfully armed, the siren/bell will emit 2 short beeps and 1 long beep after the system is disarmed. By default, the parameter is disabled.
Bypass/Activate Zone	Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. The zone will remain bypassed until the system is disarmed. Zones can only be bypassed and activated when the system is not armed.
Caller ID	Caller's identification
COM	Negative power supply terminal.
Configuration	Programming of the settings, which will define the operation of the item. For example, user's telephone numbers, set-up of periodicity for sending SMS message, input names etc.
CMS	Central monitoring station
DIAL	The system makes a call to the number specified.
Diagnostic Tool	When using Configuration tool software, you may monitor system inputs/ outputs, view changes of peripheral devices, instantly configure necessary options, for example, enabling/disabling PGM outputs, etc.
Entry Delay	The system initiates the entry delay countdown if a Delay type zone is violated. The countdown is indicated by short beeps emitted by keypad buzzer and by steady beep emitted by system's buzzer. The indication is intended to advise the user that the system should be disarmed. If the system is disarmed before the entry delay expires, no alarm will be caused.
EOL	(End of line resistor) input type with resistor.

Event	The information that the user receives.
Event Log	A list of system events that is uploaded from the device's memory to the configuration software for further analysis. The system logs all information about system configuration, system actions and info messages.
Exit Delay	A period of time intended for user to leave the secured area. The system begins the countdown after the arming process initiation.
Fault	A specific problem or error that prevents the system from working properly. The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault and send SMS text message notification to the listed user phone number.
iButton key	A unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. The module supports up to 800 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.
Installer	a person provided with INST (installer's) password
Master/User Code	Allows to carry out system arming/ disarming as well as minor system configuration and control
Normally closed (NC)	It is a switch that passes current until actuated.
Normally open (NO)	It is a switch that must be actuated to pass current.
Periodic Test Event	Provides the following information on alarm system: date & time, status (armed/disarmed), GSM signal strength, mains power supply status, temperature value measured by primary and secondary temperature sensors (if any).
Pull-up resistor	Is that it weakly "pulls" the voltage of the wire it is connected to towards +V (or whatever voltage represents a logic "high").
PGM output	A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system or if the user has initiated the PGM output state change manually.
Ping period	Sets period of time defining how often the module sends ping data packet to the server.
Service messages	ARM/DISARM, test, resetting of the system.
SSR	Solid State Relay
SMS forward	System can re-sent all incoming SMS messages to the specified users. It is useful if the GSM operator of the inserted SIM card sends some useful information (SIM card validation or payment account status and etc.) or it is necessary to monitor all incoming SMS messages by specified user.
User	It is a person being aware USER password.
Zone	Detection devices such as motion detectors and door contacts are connected to the alarm system's zone terminals.
Zone state/status	Zone status is a position of a certain zone being enabled or disabled. Meanwhile, zone state points out the condition of a certain zone, which can either be violated (i.e. In case of alarm) or restored.
+V	Positive power supply terminal.

1.3 Package content



Table 1 Standard package content



GTalarm2 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



2.2 kOhm resistors - 12 pcs
5.1 kOhm resistors – 2 pcs



Spaces for PCB installation - 4 pcs



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



GSM antenna



External microphone with 1
m cable and connector



iButton probe with LED indicator



GSM antenna with cable



Mini USB cable

			
iButton DS1990A-F5+ key	Water Proof DS18B20 Temperature Probe with 1m cable	Temperature sensor DS18B20	Humidity sensor AM2320
			
Humidity sensor DHT22 (AM2302)	Humidity sensor AM2305	Wiegand keypad & RFID reader	Mini CD - 1 pcs: • User's guide in PDF • Program SERA2

1.4 General view of the module

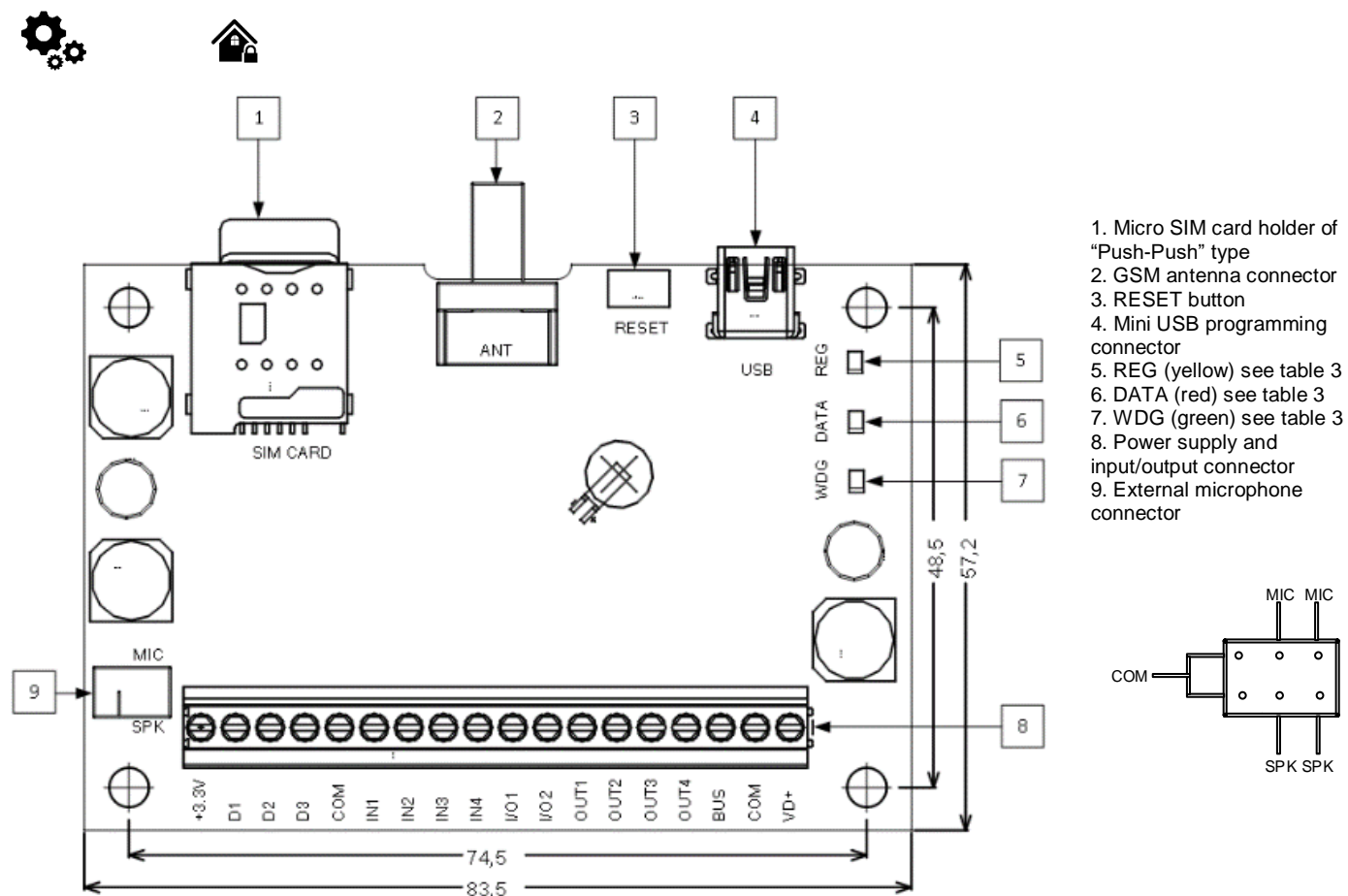


Figure 1 GTalarm2 PCB Layout



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.

Table 4 Terminal block. Contacts.

Contact No	Name	Max. voltage (V)	Optional functions and Description	
1	VD+	15	Positive supply contact	
			Power supply voltage	8-15V
			Current in standby mode	<50mA
			Current when sending data	<300mA
2	COM		Negative supply terminal for keyboard(s), indicators and sensors.	
3	BUS	15	Programmable functions	Expansion module data BUS
				Output, 20mA
			Max available voltage	15V
4 ... 7	OUT1 ... OUT4	24	Programmable Output PGM1 - PGM4. Drain type. When state is ON, connects internally to COM	
			Max available current	1000mA
			Max available voltage	24V
8, 9	I/O1-I/O2	15	Programmable functions	The zone for security system NC/NO/EOL/EOL+Tamper ⁽¹⁾
				Output 20mA
				Analog current input 0-20mA
			Max available voltage	15V
10 ... 13	IN1 ... IN4	15	Programmable functions	Input with 5.1K resistor to the VD+ (Pull UP)
				The zone for security system NC/NO/EOL/EOL+Tamper
			Max available voltage	15V
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
16	D2	3.3	Programmable functions	Max available current
				20mA
				Digital output
				Digital input
				Dallas 1-Wire bus. DS18B20, DS1990A
				Aosong 1-Wire bus. Humidity Sensor AM2302, DHT22, AM2305, AM2306
17	D1	3.3	Programmable functions	Wiegand (1) interface DATA0, RFID reader, keypad
				Max available voltage
				3.3V
				Max available current
				20mA
				Digital output
18	3.3V	3.3	Power supply for external temperature, humidity sensors	

		Max available voltage	3.3V
		Max available current	100mA

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

1.6 System Access codes. Default passwords.

Table 5 Default passwords and explanation

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

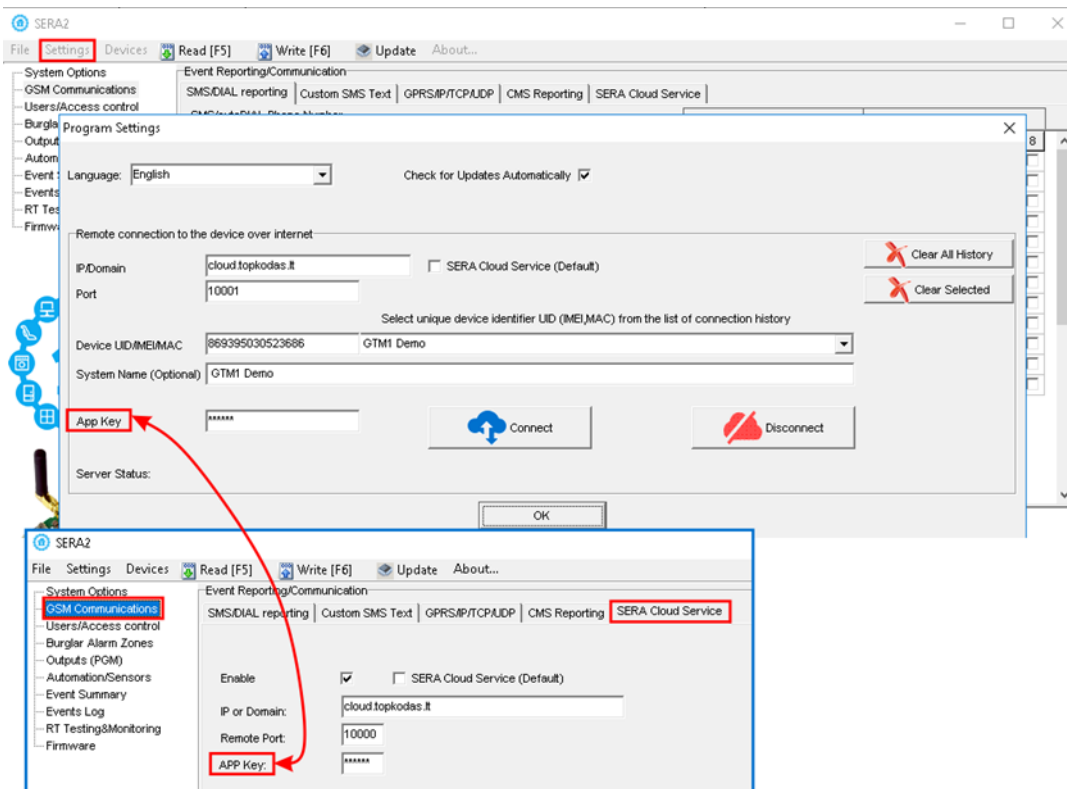


Figure 2 App key must be the same in all configuration fields



APP Key: 123456 used with the App and for connecting to the module remotely. "APP Key" in module must be same in: Sera2> Settings (in the command line) and Sera2> GSM Communications> Sera Cloud Service

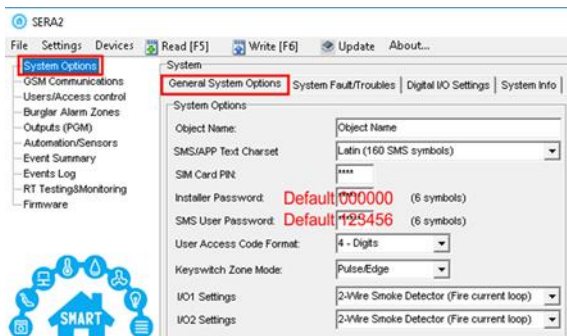


Figure 3 Default Installer and SMS User passwords



SMS user password could be used only with the phone numbers that has been included in Users/ Access control list. If the phone number is not in this list, it could not be used with SMS user password.



SMS user password is the same for all phone numbers from Users/ Access control list.



Installer password could be used with any phone number. It is critical to keep in secret this password. It is possible to change the configuration of the module with installer password.

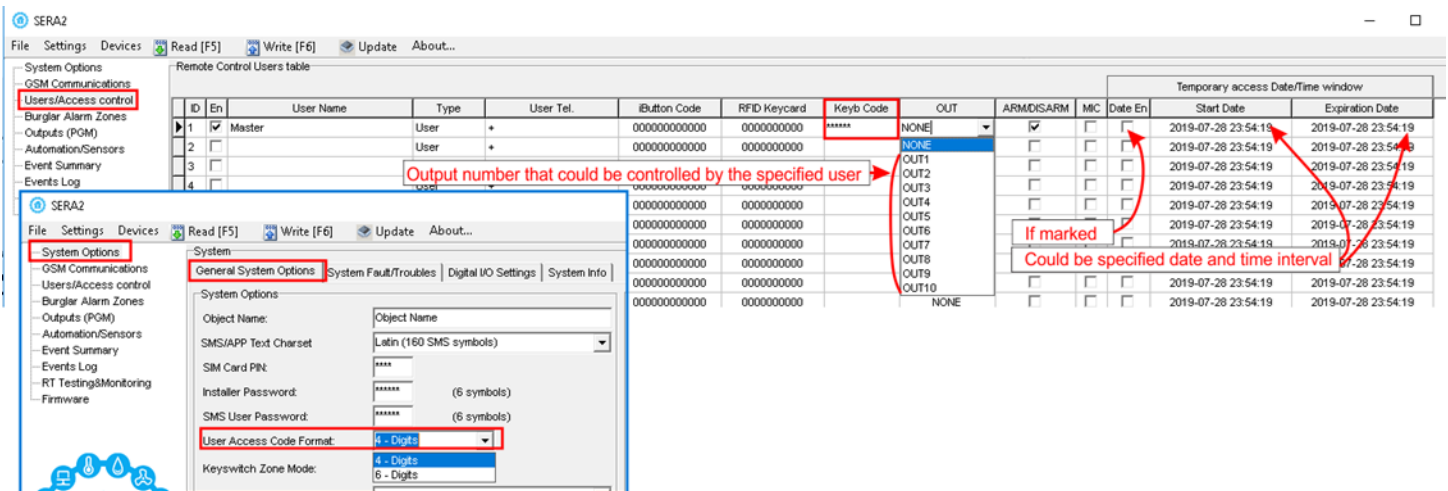


Figure 4 Figure 5 Master code SERA2> Users/ Access control



Master Code: 1234 or 123456 system control if selected 6 digits in the SERA2> System Options> General System Options> User Access Code Format

2 QUICK START First steps to prepare GTalarm2 and SERA2 software.



QUICK START

<https://youtu.be/NR35IbFdi8A>

Preparation procedure of the module GTalarm2.

- Connect the GSM antenna to the antenna connector.
- Insert the SIM card in the SIM card holder. Ensure that PIN request function is disabled.
- Connect the module to the computer via mini USB cable.
- Connect power supply

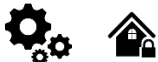


CALL TO THE MODULE FROM YOUR MOBILE
YOU WILL RECEIVE SMS FROM THE MODULE

Install configuration software SERA2.

- Go to the <http://topkodos.lt/> website and download SERA2 software.
- Open the folder containing installation of the software SERA2. Click the file „SERA2 setup.exe“
- If installation directory of the software is OK, press [Next]. If you would like to install the software in the other directory press [Change], specify other installation directory and then press “next”.
- Check if the correct data are entered and press Install
- After successful installation of the software SERA2, press [Finish]

3 Installation



This Installation & Programming manual provides the basic installation, wiring and programming information required to program the module GTalarm2 and connect all third party devices to the module.

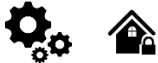


find wiring diagrams in the

[Power supply](#), [Battery Wiring](#), [Humidity sensors](#), [AM2302/DHT22/AM2305/AM2306/AM2320/AM2321](#), [Analog inputs 0-10V, 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](#)

3.1 Power supply, Battery Wiring



It is possible to supply the security system from stabilized power supply source 10-15 V and not less than 1,5A. It is necessary to calculate max current of power supply. The current of the alarm system is the current used by sensors, relays, siren and other devices. It is most convenient to use power supply source applied for power supply of security systems with the option to connect backup lead battery. It is recommended to mount remote control relays into sockets. Sockets may be easily fixed in metal box. It is necessary to select relays according to preferred voltage and current.

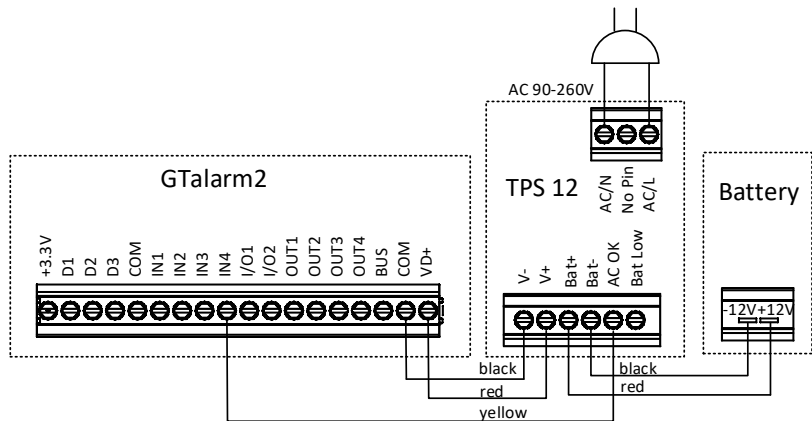


Figure 5 Power supply connection

The example how to configure the module GTalarm2 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 "save" icon.

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

Zone 4 Settings

Zn	Zn Name	Zone Hardware Input	Definition	Typ
1	Zone Name 1	GTalarm v2, IN1	delay (Entry/Exit)	Ex
2	Zone Name 2	GTalarm v2, IN2	follow/interior	Ex
3	Zone Name 3	GTalarm v2, IN3	instant/Burglary	Ex
4	AC Loss	GTalarm v2, IN4	AC power loss	N
5	Zone Name 5	GTalarm v2, I/O1	fire	Ex
6	Zone Name 6	GTalarm v2, I/O2	keyswitch ARM/DISARM	Ex

Zone 4 Settings

Zone Name: AC Loss

Alarm Text: Alarm 4 Text

Restore Text: Restore 4 Text

Zone Hardware Location: GTalarm v2, IN4

Zone Definition: AC power loss

Wiring Type: NC

Contact ID code: 301

Zone Speed: 60000ms

Event Repeat Timeout: 600s

Max Alarm Count: 1

Zone Alarm action: N/A

Zone Options

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

Annotations:

- Double click on the line
- Change alarm restore events text
- It should be set to „AC power loss“
- Select NC with our application
- Assigned Contact ID code 301
- 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
- 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 6 AC loss in Burglar alarm window

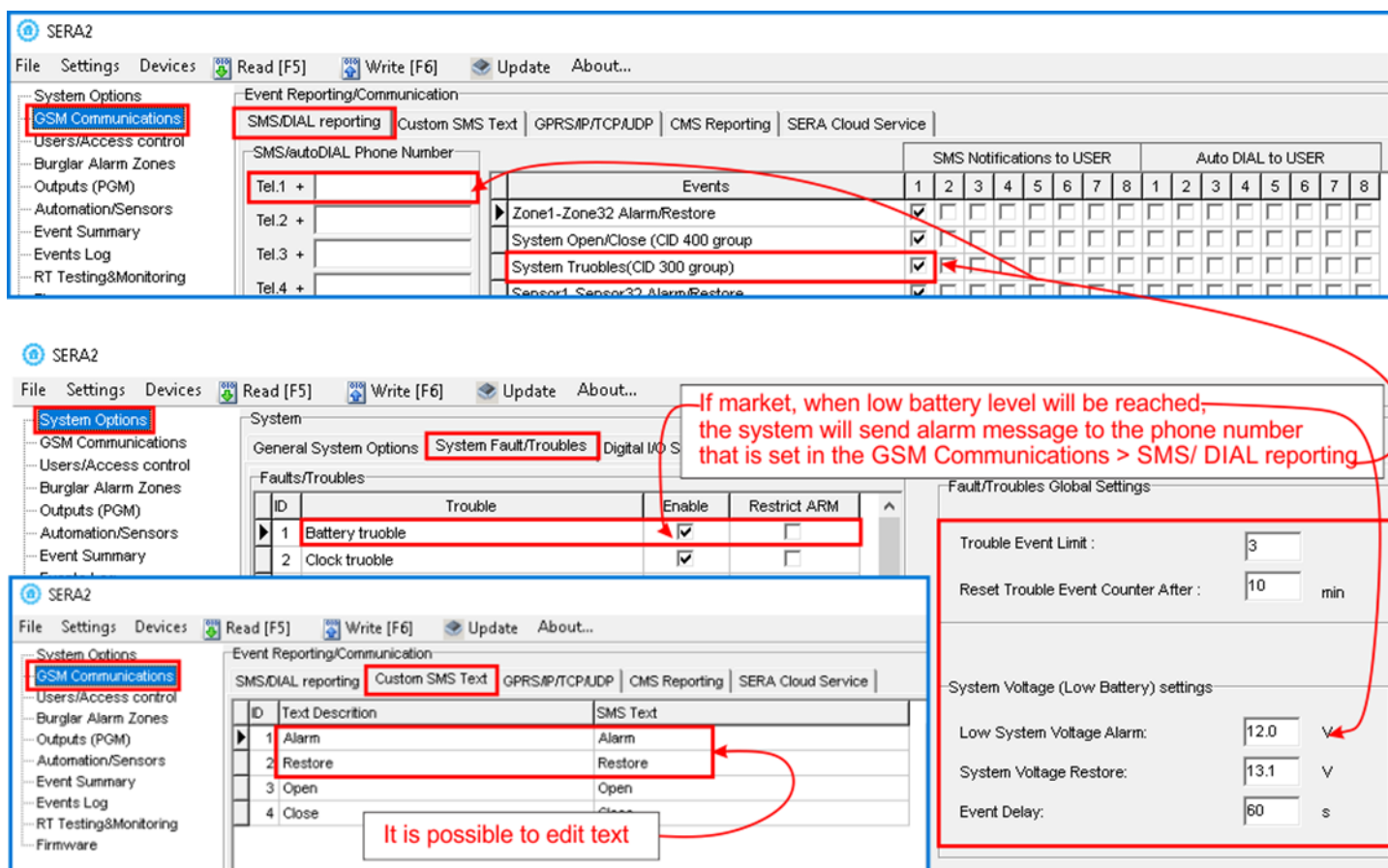


Figure 7 Battery trouble in System Options > System Fault/ Troubles window



Power supply TPS12 installation manual: https://topkondas.lt/Downloads/TPS12_UM_EN.pdf
Power supply TPS12 : https://topkondas.lt/Downloads/GTAlarm2_TPS12_AN_EN.pdf



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

3.2 Inputs

The module GTAlarm2 has:

- **6 burglary zones.** Can be expanded up to 32.
- **4 analog inputs (In1...In4 (0-10V))** for analog sensors connection. Or can be used as security system's zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- **2 programmable analog inputs (I/O1, I/O2(0-10V/0-20mA))** 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,
 - **Aosong 1-Wire bus Humidity Sensor** AM2302, DHT22, AM2305, AM2306,
 - **Wiegand interface** DATA0/ DATA1, RFID reader, Keyboard.

3.3 Sensors. Automation

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



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

Table 6 Sensors AM2302, AM2320/AM2321 specification

Manufacturers' Specification

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

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

Each AM2302 sensor connects on separate bus line to digital inputs (D1, D2, and D3). Total up to 3 AM2302 Aosong (Guangzhou) humidity sensors can be connected to GTalarm2

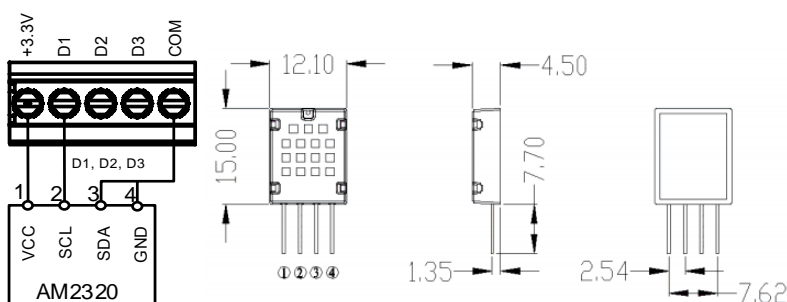


Figure 17 AM2320 connecting diagram

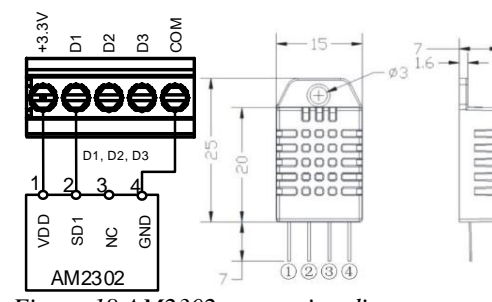


Figure 18 AM2302 connecting diagram

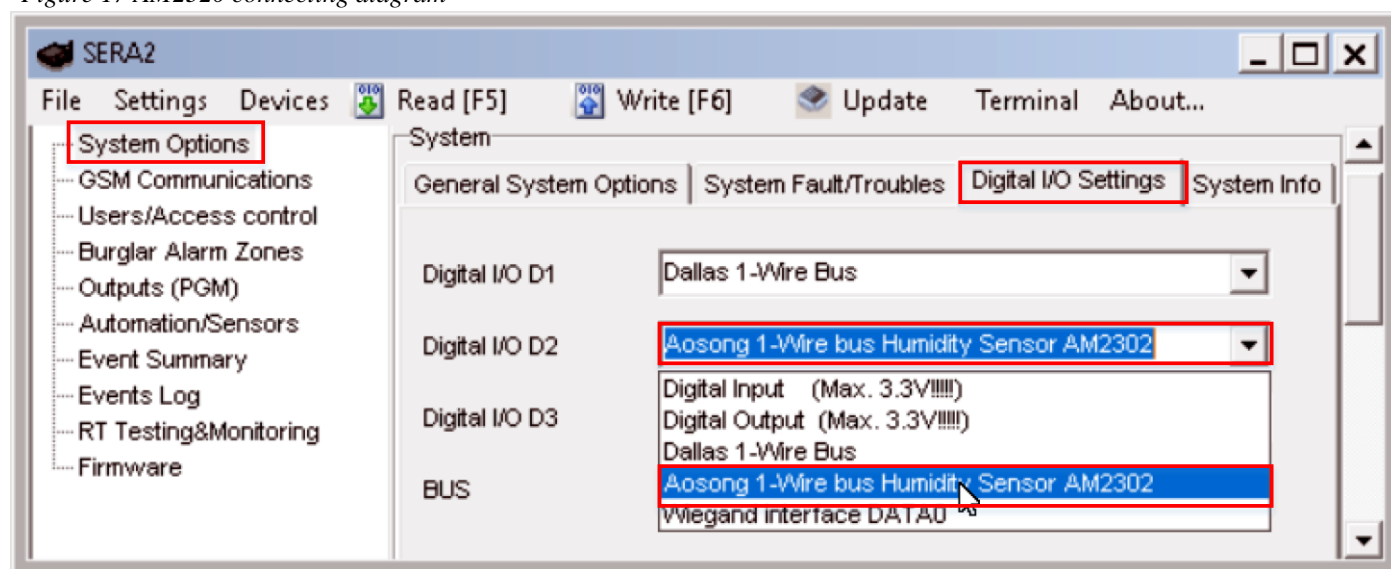


Figure 8 System Options> Digital I/O Settings

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

Steps to start AM2320 and AM2302 sensors:

1. Connect the sensor to D1, D2, D3, according the connection diagram
2. Select the sensor type
3. Press „Write“
4. Power the module
5. Wait until the sensor will be found on the bus.
6. Press „Read“
7. Find the registered sensor. Double click on the line.
8. Set the required parameters.
9. Press „Write“

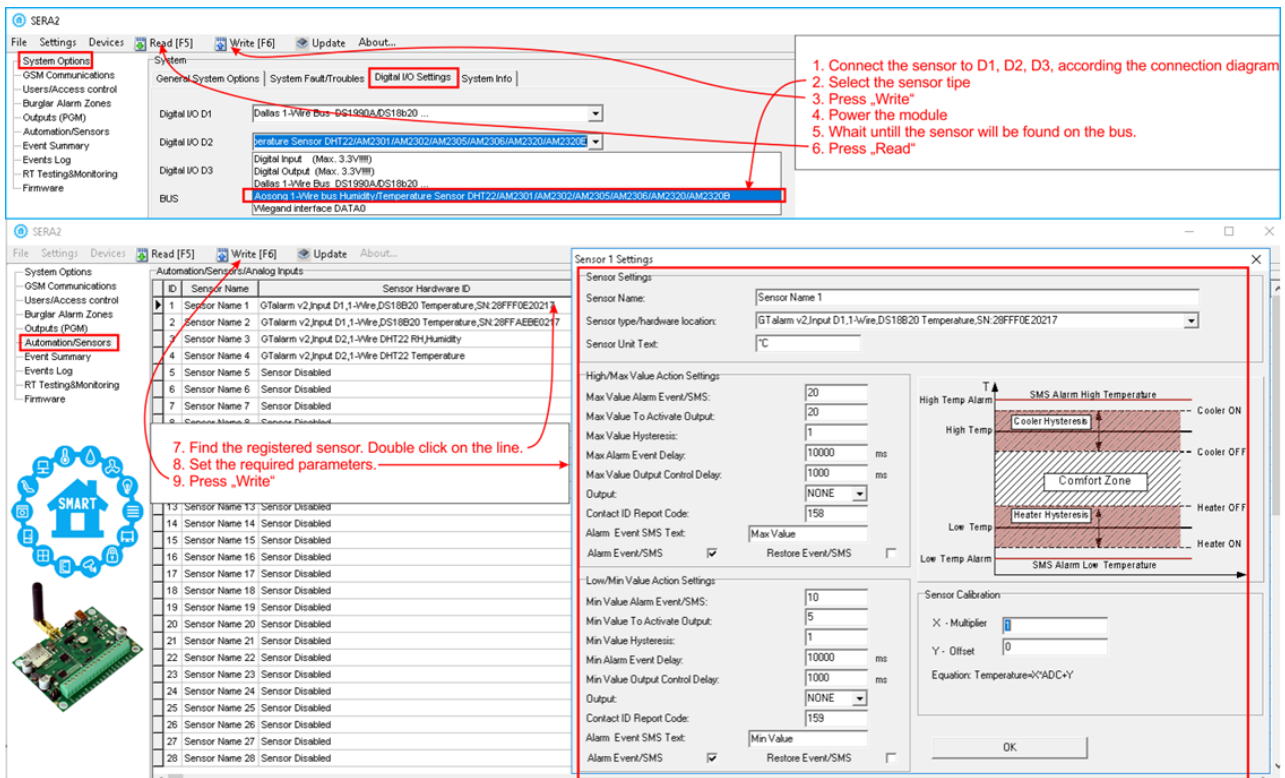


Figure 9 Steps to start AM2320 and AM2302 sensors:



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

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

3.3.2 Analog inputs 0-10V, 0-20mA, 4-20mA



Steps to start analog sensors:

1. Connect analog voltage sensors to In1, In2, In3 and connect analog current sensors to I/O1, I/O2 according connection diagram..
2. Set the I/O1, I/O2 to analog input
3. If the input is not used, it must be disabled.
4. Set the required parameters.
5. Sensors could be calibrated.
6. Press „Write“

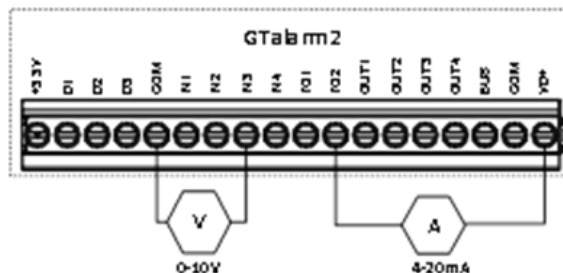


Figure 10 Analog sensors connection diagram

If you want to edit existing configuration,
 You have to read it (press "Read" in the command line)
 Edit settings
 Write edited configuration (press "Write" in the command line)

1. Set the I/O1, I/O2 to analog input
 2. If the input is not used, it must be disabled.
 3. Set the required parameters.
 4. Sensors could be calibrated.
 5. Press „Write“

General System Options

System Options

Object Name: GTalarm2 DEMO

SMS/APP Text Charset: Latin (160 SMS symbols)

SIM Card PIN: ****

Installer Password: ***** (6 symbols)

SMS User Password: ***** (6 symbols)

User Access Code Format: 4 - Digits

Keyswitch Zone Mode: Level

I/O1 Settings: 0-20 mA, 4-20 mA Current Loop Sensor

I/O2 Settings: 2-Wire Smoke Detector (Fire current loop)

Clear Events Buffer after reset: Output

Door Chain: 2-Wire Smoke Detector (Fire current loop)

Bell Squawk on ARM/DISARM: 0-20 mA, 4-20 mA Current Loop Sensor

Inputs/Burglar Alarm Zones

Zn	Zn Name	Zone Hardware Input	Definition	Type	CID	Bypass	Tamper	Shutdown	Force	Report A	Report R	Speed	Repeat	MS Text on Alarm
1	Zone Name 1	GTalarm v2, IN1	fire	NO	110	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s	Alarm 1 Text
2	Zone Name 2	GTalarm v2, IN2	keyswitch ARM/DISARM	NO	409	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	100s	Alarm 2 Text
3	Zone Name 3	Zone Disabled	instant/Burglary	EOL	130	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s	Alarm 3 Text
4	AC Loss	Zone Disabled	AC power loss	EOL	301	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s	Alarm 4 Text
5	Zone Name 5	Zone Disabled	fire	EOL	110	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s	Alarm 5 Text
6	Zone Name 6	Zone Disabled	keyswitch ARM/DISARM	EOL	409	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s	Alarm 6 Text

Sensor 5 Settings

Sensor Name: Sensor Name 5

Sensor type/hardware location: Sensor Disabled

Sensor Unit Text: Sensor Disabled

High/Max Value Action Settings:

Max Value Alarm Event/SMS: GTalarm v2.Input I01,0-10V

Max Value To Activate Output: GTalarm v2.Input I01,0-20mA

Max Value Hysteresis: GTalarm v2.Input I02,0-20mA

Max Alarm Event Delay: GTalarm v2.Input D1,1-Wire DHT22 RH, Humidity

Max Value Output Control Delay: GTalarm v2.Input D2,1-Wire DHT22 RH, Humidity

Output: GTalarm v2.Input D3,1-Wire DHT22 RH, Humidity

Contact ID Report Code: GTalarm v2.Input D1,1-Wire,DS18B20 Temperature,SN:28FF0E20217

Alarm Event SMS Text: GTalarm v2.Input D1,1-Wire,DS18B20 Temperature,SN:28FAEBE0217

Low Temp Alarm: SMS Alarm Low Temperature

Low/Min Value Action Settings:

Min Value Alarm Event/SMS: 5

Min Value To Activate Output: 10

Min Value Hysteresis: 1

Min Alarm Event Delay: 10000 ms

Min Value Output Control Delay: 1000 ms

Output: NONE

Contact ID Report Code: 159

Alarm Event SMS Text: Min Value

Alarm Event/SMS: ☒ Restore Event/SMS: ☐

Sensor Calibration:

X - Multiplier: 1

Y - Offset: 0

Equation: Temperature=X*ADC+Y

OK

Figure 11 Analog sensors settings



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



Current measure analogue sensors can be connected to I/O1 and I/O2 0-20mA, 4-20mA



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

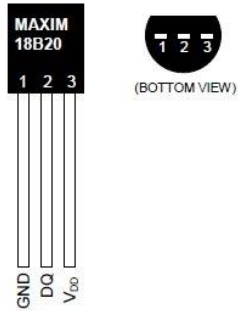
7. Real time hardware status: RT Testing & Monitoring> Hardware. Press "Start Monitoring"
8. The list of alarm events with time and date stamp: RT Testing & Monitoring> Event Monitoring
9. It is possible to receive alarm SMS to the mobile phone: GSM Communication> SMS/ Dial reporting
10. Real time sensor values and states: RT Testing & Monitoring> Sensors/ Automation.

11. Write configuration. Press write.

3.3.3 Temperature sensors Dallas 1-wire DS18B20 installation & recommendations



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



Applications/Uses

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

Key Features

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

3.3.3.1 Wiring Dallas 1-wire DS18B20

1. Connect 1-Wire sensors DS18B20 to D1, D2, D3 according connection diagram.

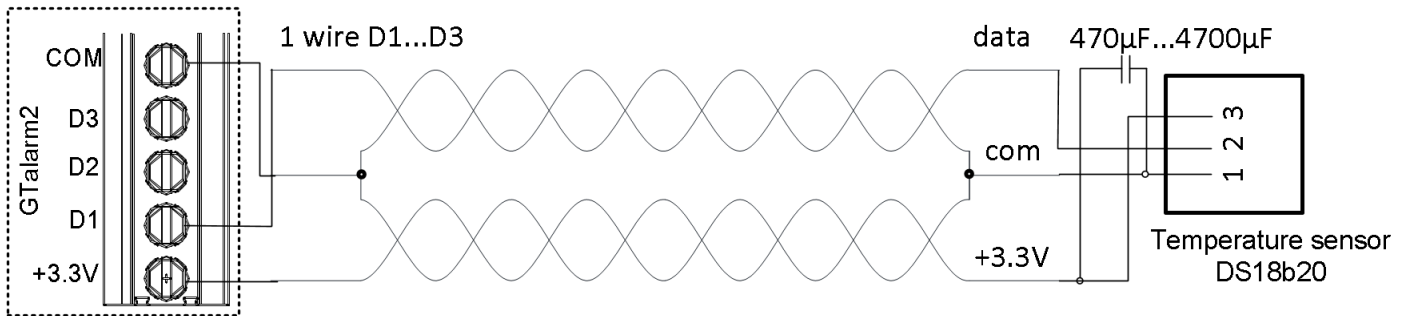


Figure 12 DS18b20 connection with long distance UTP or FTP cable

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

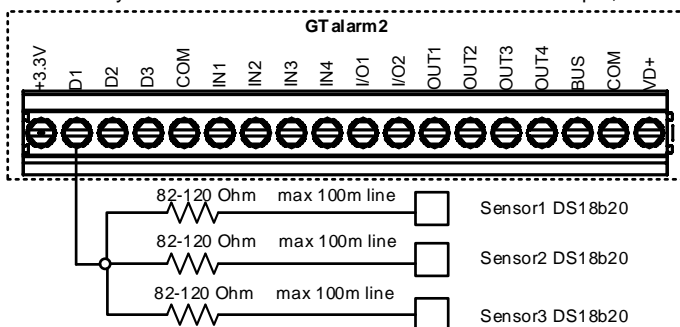


Figure 13 Star connection



The resistor must be as close as possible to the contacts of the module GTalarm2.

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

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

If you intend to have a large 1-Wire network, it is important that you design the network correctly, otherwise you will have problems with timing/reflection issues and loss of data. You must connect each sensor to a single continuous cable which loops from sensor to sensor in turn (daisy chain). This will reduce potential miss-reads due to reflections in the cable. Each sensor should have a maximum of 50mm (2") of cable connected off this main network. Even when using this method, connecting more than 10-15 sensors will still cause problems due to loading of the data bus. To minimize

this effect, place a 100-120Ω resistor in series in the data line of each sensor before connecting to the network. The total length of the bus from 10 to 100m. Depending of cable quality sensors number on bus, and environment noise. There is possibility to connect up to 32 devices.

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

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

3.3.3.2 Temperature sensors Dallas 1-wire DS18B20 Configuration



Step by step to start DS18B20 sensors:

1. Connect 1-Wire sensors DS18B20 to D1 or D2, D3 according connection diagram. If you need to connect more sensors to the same input, connect them as a star or serial.
2. Set digital input definition D1, D2, D3 to Dallas 1-Wire Bus option
3. Write configuration
4. Power the module.
5. After module starts. Within few seconds, it will automatically scans and registers all connected 1-Wire sensors on the bus.
6. Read configuration
7. Double click on the selected line
8. Select the registered sensor.
9. Set the required parameters.
10. Press "Write"

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

The screenshot displays the SERA2 software interface for configuring sensors. The main window shows 'Digital I/O Settings' with D1, D2, and D3 configured as 'Dallas 1-Wire Bus'. The 'Sensor 2 Settings' dialog box is open, showing 'Sensor Name 2' and 'Sensor type/hardware location: GTAlarm v2, Input D1, 1-Wire, DS18B20 Temperature, SN: 28FFAE8E0217'. The 'High/Max Value Action Settings' section is configured with various thresholds and delays. A diagram on the right illustrates the temperature control logic, showing 'SMS Alarm High Temperature' and 'SMS Alarm Low Temperature' thresholds, and a 'Comfort Zone' between 'Cooler Hysteresis' and 'Heater Hysteresis'.

Figure 14 sensors settings Dallas 1-Wire DS18B20

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

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

3.3.3.3 How to change temperature scale from Celsius to Fahrenheit

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

Figure 15 How to change temperature scale from Celsius to Fahrenheit and Kelvins

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

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

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

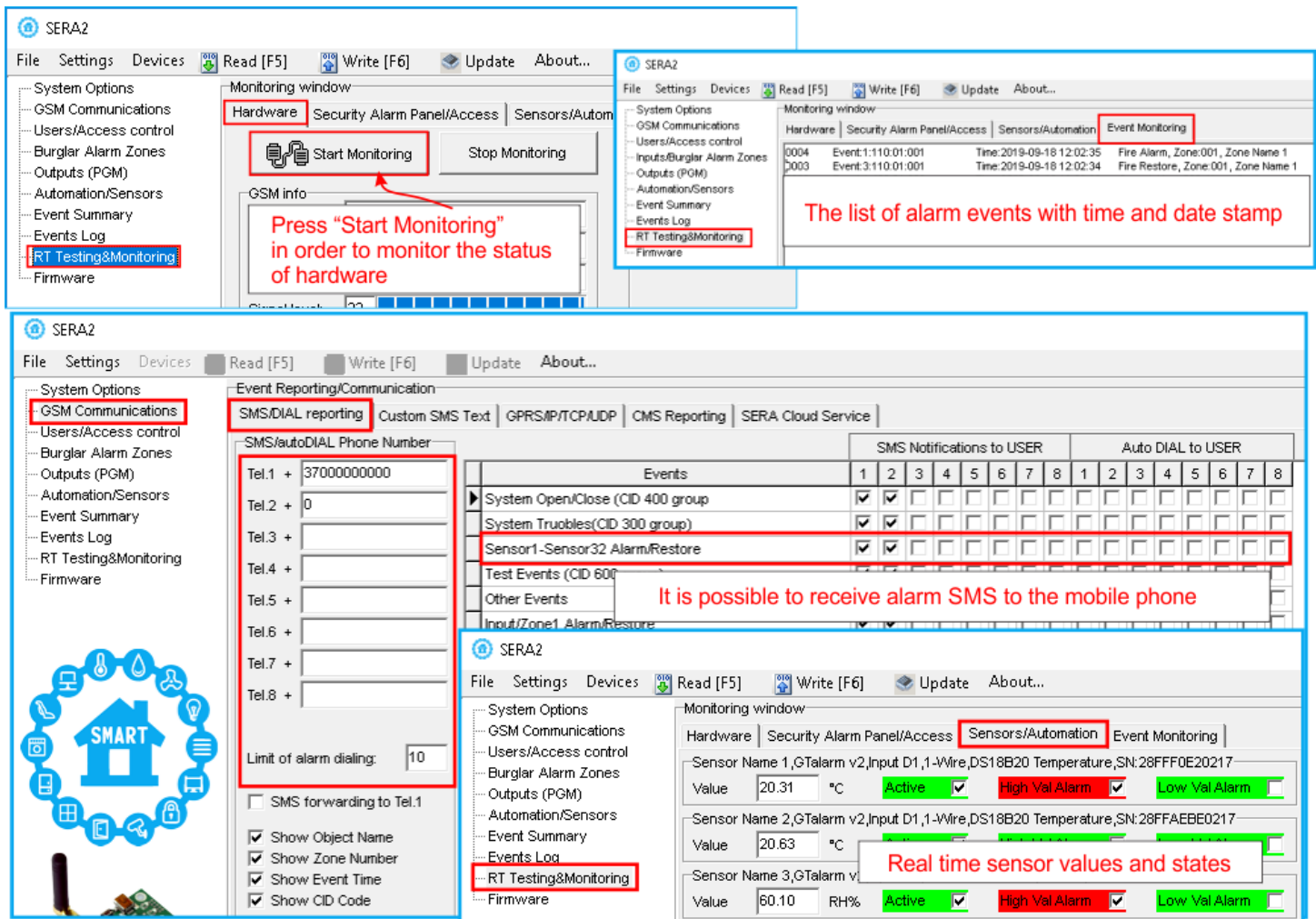


Figure 16 How to check real time hardware status, real time sensor values. How to receive alarms and where find alarm events list

3.4 Sensors. Security.

3.4.1 Burglar Alarm sensor zones wiring EOL NO NC



- In1...In4 Can be used or use it as security system's zones with selectable type: NC/NO/EOL/EOL+TAMPER.
- I/O1, I/O2 with selectable type: NC/NO/EOL/EOL+TAMPER. External pool-up resistor 5.1K is required.

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

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

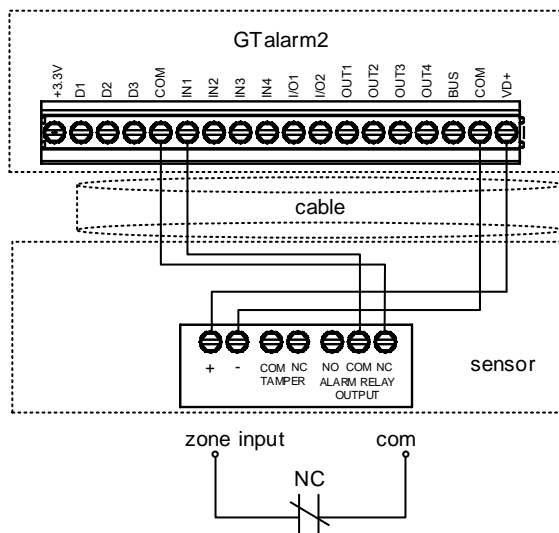


Figure 17 NC Contacts, No EOL

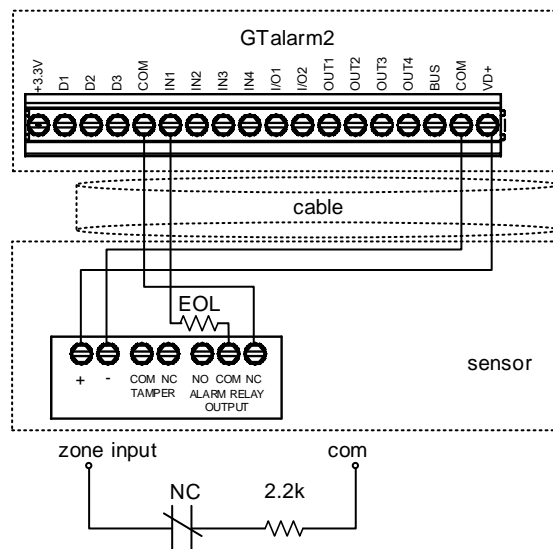


Figure 18 NC, With EOL

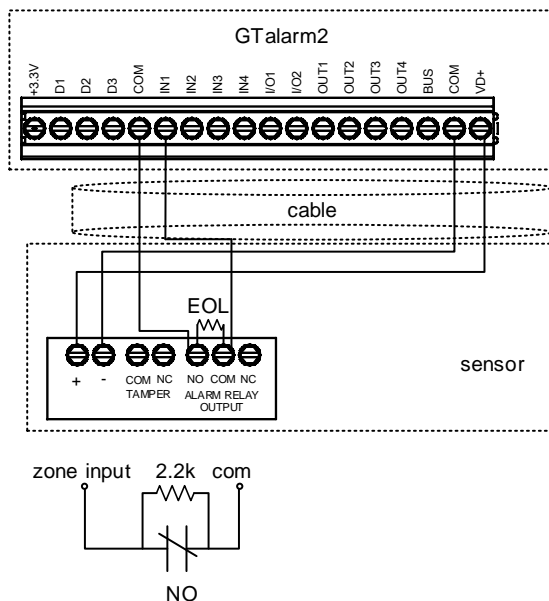


Figure 19 NO, With EOL

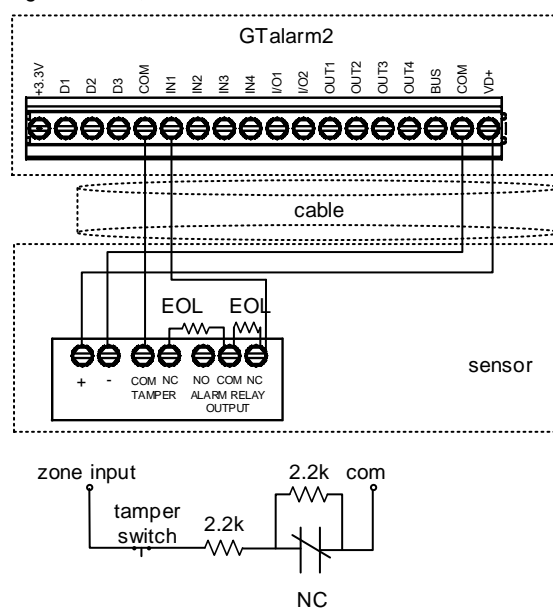


Figure 20 NC With EOL Wire Fault Recognition

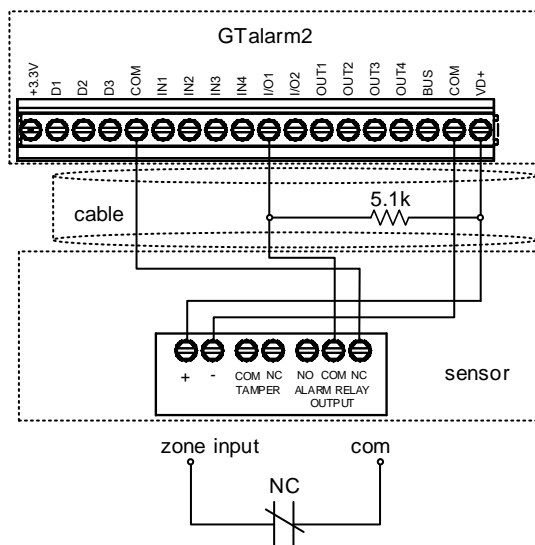


Figure 21 sensors connection to I/O1, I/O2

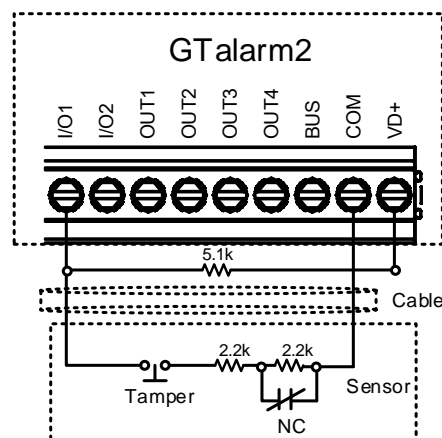


Figure 22 EOL+TAMPER sensors connection to I/O1, I/O2

The module has 2 I/O analogue input/ output circuits I/O1 and I/O2. They also can be used for burglary alarm zones. Input type: NC/NO/EOL/ EOL+TAMPER. I/O1, I/O2 do not have internal pull-up resistors unlike IN1-IN4. So if you want to use I/O as burglar zones to connect NO/NC/EOL sensors to I/O1 or I/O2 you have to connect external 5.1K resistor between I/O and +VD, as is shown in attached diagram.

! I/O1, I/O2 do not have internal pull-up resistors. So if you want to connect NO/NC sensors to I/O1 or I/O2 you have to connect 5.1K resistor between I/O and +VD

! Please note. If I/O1 set as 2-wire, you don't need 5.1k resistor.

1. If I/O1, I/O2 is used as security system inputs, then I/O1, I/O2 must be set as 0-10V Analog Input (Zone or Sensor)

1. Double click on the selected line.
2. Set the required parameters.
3. If zone is not used, it must be disabled.
4. Press "Write".

Zn	Zn Name	Zone Hardware Input	Definition	Type	CID	Bypass	Tamper	Shutdown	Force	Report A	Report R	Speed	Repe
1	Zone Name 1	GTalarm v2, IN1	24 hours (silent)	NO	150	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200ms	600s
2	Zone Name 2	GTalarm v2, IN2											
3	Zone Name 3	Zone Disabled											
4	AC Loss	Zone Disabled											
5	Zone Name 5	Zone Disabled											
6	Zone Name 6	Zone Disabled											

Zone 1 Settings

Zone Name: Zone Name 1

Alarm Text: Alarm 1 Text

Restore Text: Restore 1 Text

Zone Hardware Location: GTalarm v2, IN1

Zone Definition: 24 hours (silent)

Wiring Type: NO

Contact ID code: 150

Zone Speed: 200ms

Event Repeat Timeout: 600s

Max Alarm Count: 5

Zone Alarm action: N/A

Zone Options:

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

OK

Figure 23Burglar Alarm Zones settings

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)



More information about how to configure the zones: [Zones programming](#)

3.4.2 Fire alarm and Smoke sensors

3.4.2.1 Guidelines for Locating Smoke Detectors and CO Detectors



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

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

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

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

- Do not locate smoke detectors at the top of peaked or gabled ceilings; dead air space in these locations may prevent smoke detection.

- Avoid areas with turbulent air flow, such as near doors, fans or windows. Rapid air movement around the detector may prevent smoke from entering the unit.

- Do not locate detectors in areas of high humidity.

- Do not locate detectors in areas where the temperature rises above 38°C (100°F) or falls below 5°C (41°F).

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

- (1) In all sleeping rooms and guest rooms.

- (2) Outside of each separate dwelling unit sleeping area, within 6.4 m (21 ft) of any door to a sleeping room, the distance measured along a path of travel.

- (3) On every level of a dwelling unit, including basements.

- (4) On every level of a residential board and care occupancy (small facility), including basements and excluding crawl spaces and unfinished attics.

- (5) In the living area(s) of a guest suite.

- (6) In the living area(s) of a residential board and care occupancy (small facility).

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

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

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10°C or exceed 40 °C.

- Near paint thinner fumes.

- Within 5 feet (1.5 meters) of open flame appliances such as furnaces, stoves and fireplaces.

- In exhaust streams from gas engines, vents, flues or chimneys.

- In close proximity to an automobile exhaust pipe; this will damage the detector.

GTalarm2. Begin the installation by mounting additional modules in the cabinet using the stand-offs provided, then mount the cabinet in a dry, protected area with access to unswitched AC power. Install hardware in the sequence indicated in the following pages. Do NOT apply power until installation is complete.

3.4.2.2 [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.

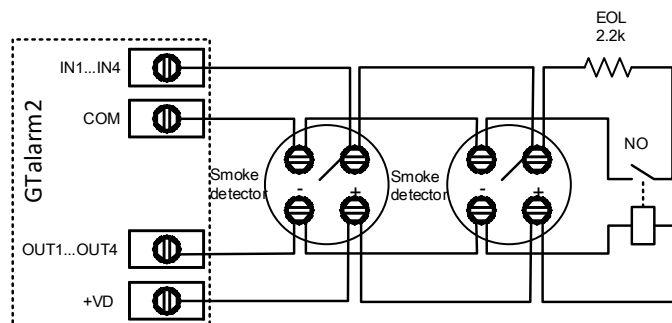


Figure 24 4-Wire Smoke Detector Installation

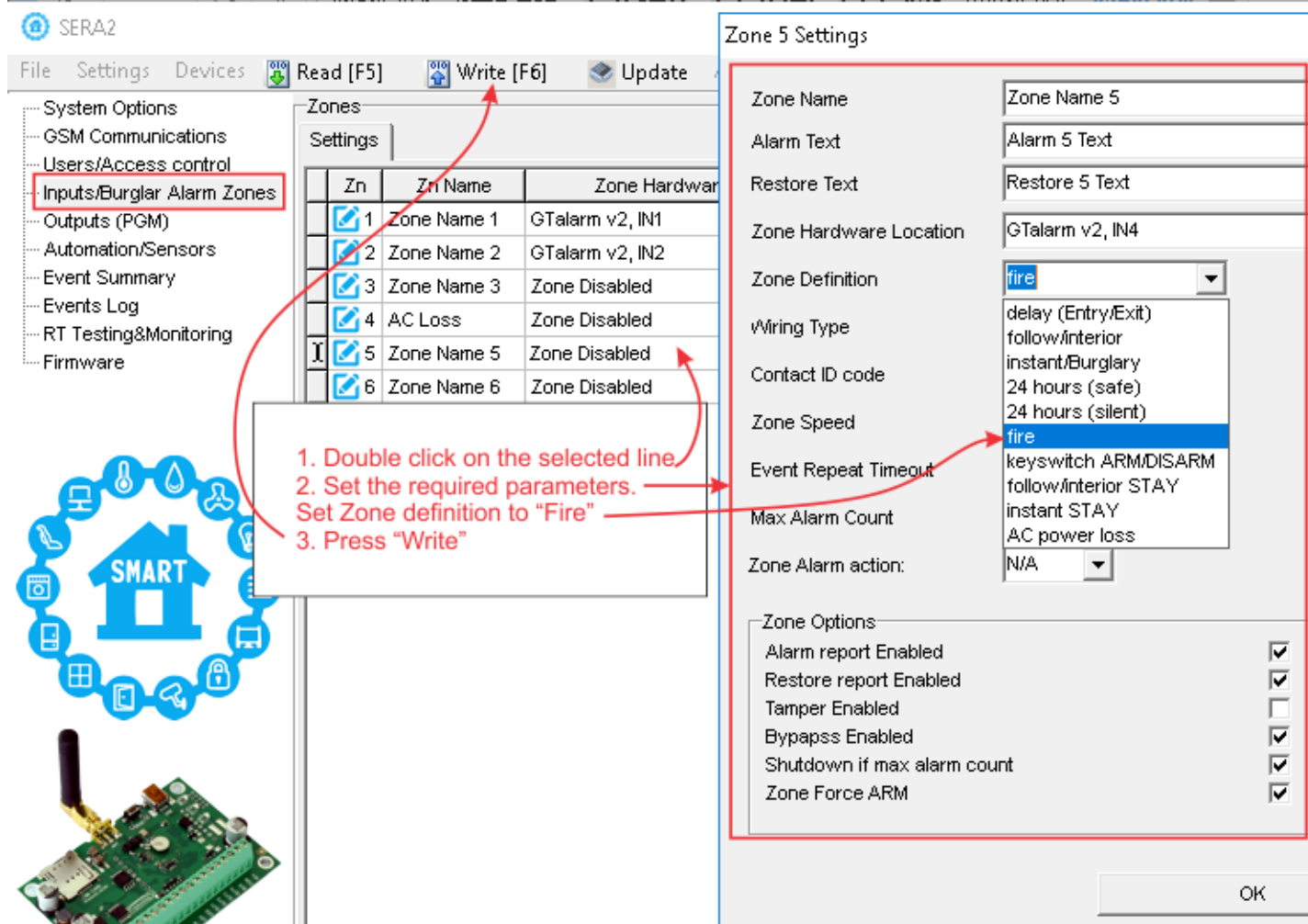


Figure 25[4-Wire] Smoke detector settings

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

3.4.2.3 [2-Wire] Smoke Detector Wiring to I/O Inputs



The 2-wire Smoke zone on the module is the only zone in the system that can have 2-wire smoke detectors as Fire Alarm initiating devices. This zone is an end-of-line EOL 2.2K resistor type and can accommodate up to 30 compatible 2-wire smoke detectors. The zone is fixed as a 2-wire smoke zone. I/O 2-wire smoke zone is trouble supervised zone. The zone wiring is supervised by the control panel.

The parameters of the zone should be defined as a "Fire Zone". I/O1 and I/O2 can be defined as a 2-wire smoke detector input 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.

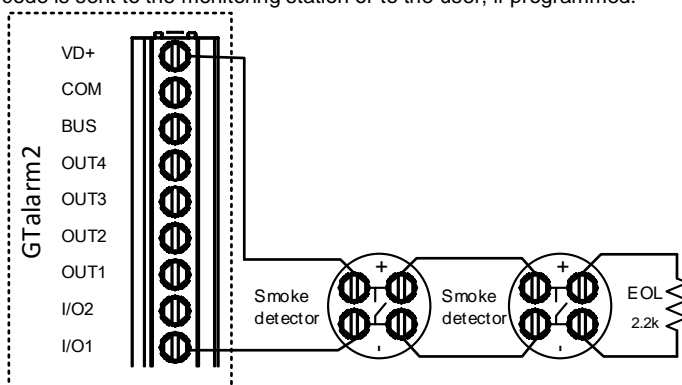


Figure 26 2-wire smoke detector wiring diagram

1. Connect the [2-wire] smoke detector (current sensor) to the I/O1, I/O2 inputs as in the wiring diagram.
2. Connect the power supply.
3. Install SERA2 software.
4. Go to "System Options> General System Options" from the menu and select 2-Wire Smoke Detector (Fire current loop)
5. In the Zone table set I/O1 definition to "Fire"

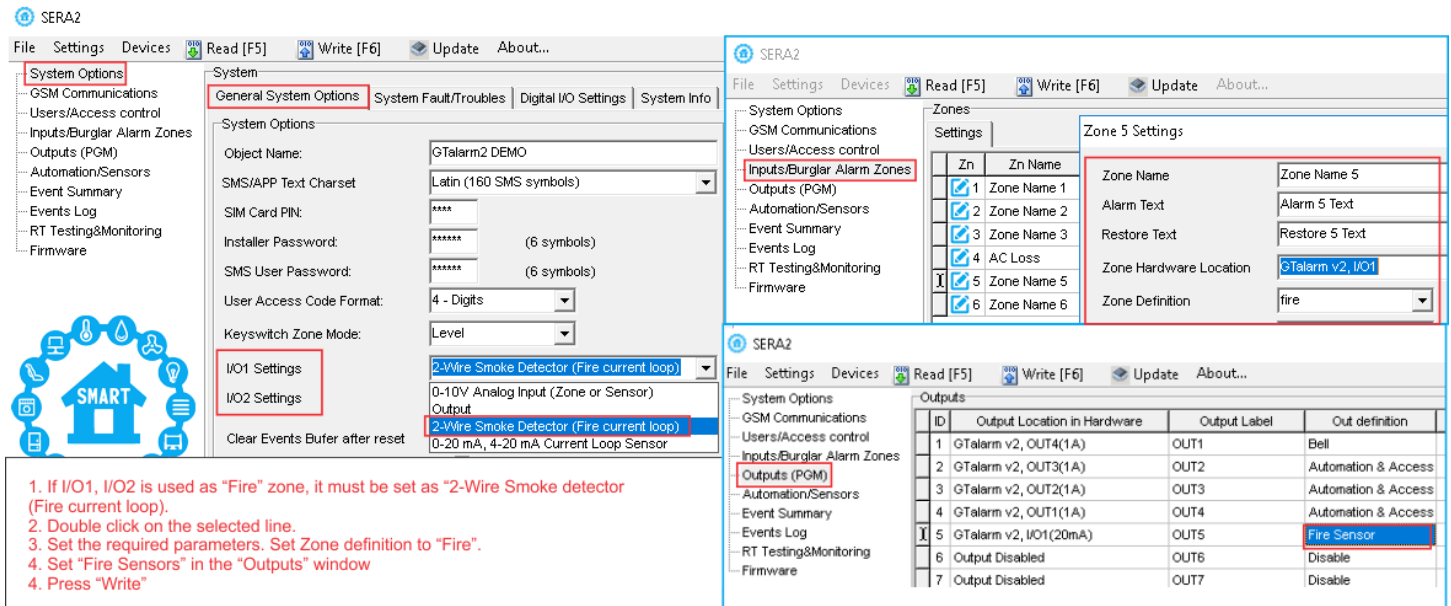


Figure 27 3.4.2.3 [2-Wire] Smoke Detector settings

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)



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



I/O1, I/O2 do not have internal pull-up resistors. So if you want to connect NO/NC sensors to I/O1 or I/O2 you have to connect 5.1K resistor between I/O and +VD



If I/O1 set as 2-wire, don't need connect 5.1k resistor to +VD.

3.5 Outputs



The module GTalarm2 has:

- **4 open drain (1A) outputs:** OUT1 (1A)... OUT4 (1A). The outputs can be used for siren, relay, lamp connection. 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
- **2 open drain (20mA) outputs:** I/O1 (20mA)... I/O2 (20mA). These outputs can be used for solid state relays, LED, to control devices up to 20mA.
- **3 outputs: D1 (10mA, Max Voltage 3,3V)** for LED, solid state relays control. ! Max voltage 3,3V
- **1 programmable output BUS.** Voltage 8-15V, Current 20mA
- **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.

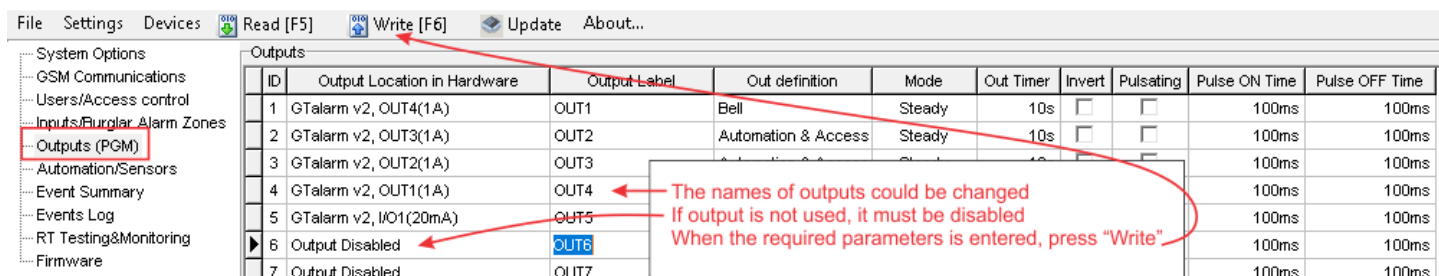


Figure 28 Outputs settings

If you want to edit existing configuration,

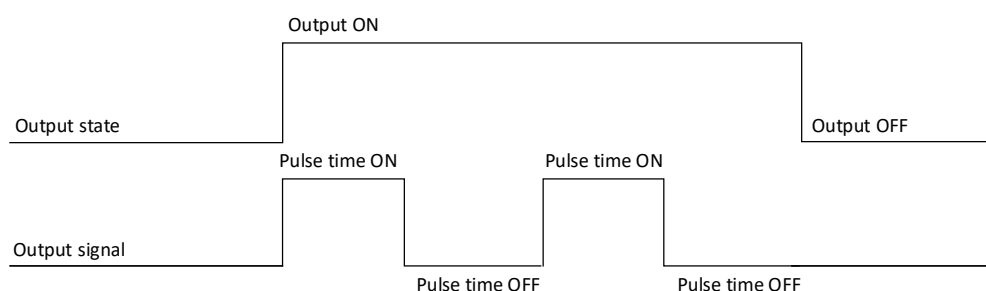
You have to read it (press "Read" in the command line)

Edit settings

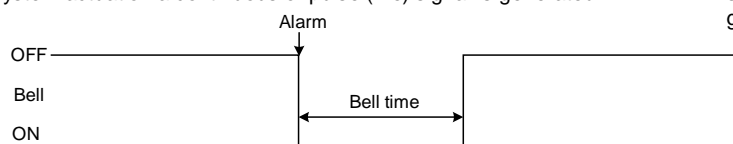
Write edited configuration (press "Write" in the command line)

Outputs can be set as timers.

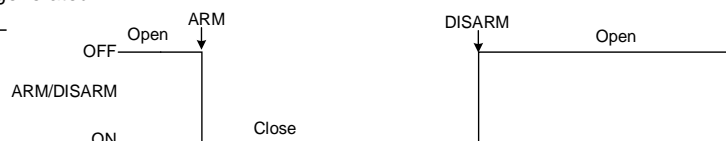
1. When output is activated for "Out Timer" time interval,
2. Relay contact start changing state from ON (pulse time ON) to OFF (Pulse time Off)
3. This cycle will repeat until output is deactivated.



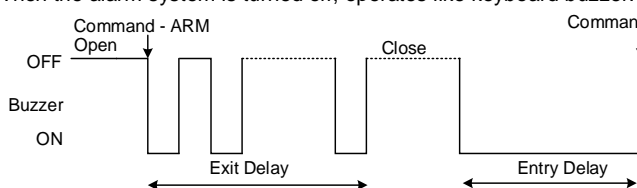
Bell: Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.



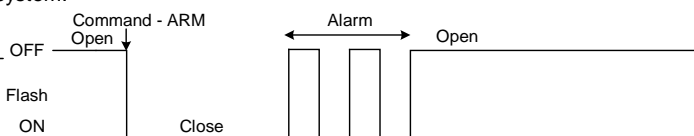
ARM/DISARM: Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.



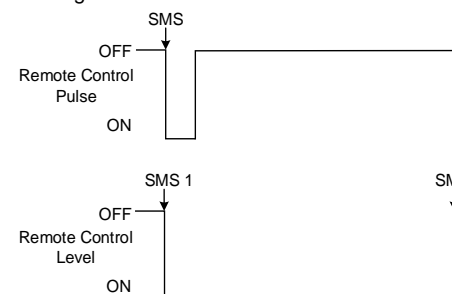
Buzzer: Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.



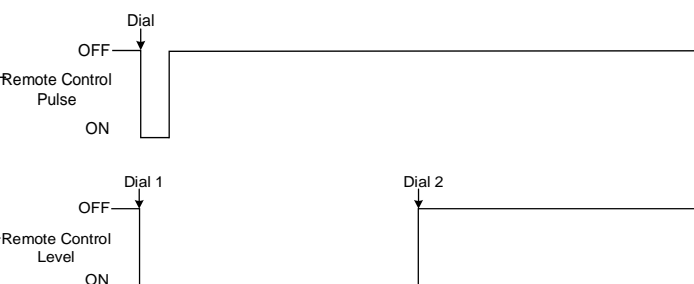
Flash: Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



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

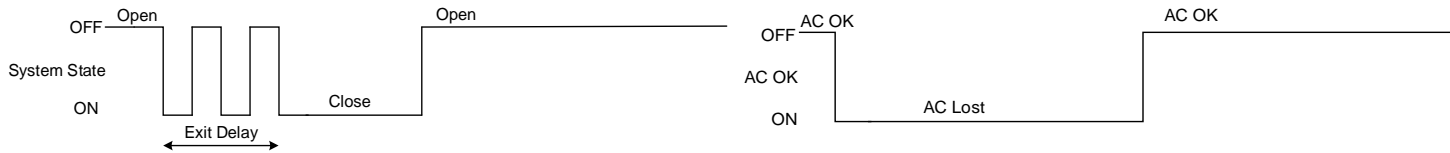


Remote Control b) control by phone call

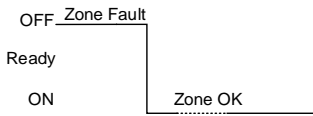


System State: Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.

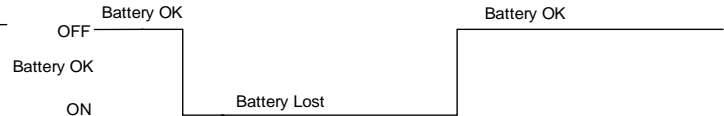
AC OK: Output for connection of indicator about control panel supply from alternating current



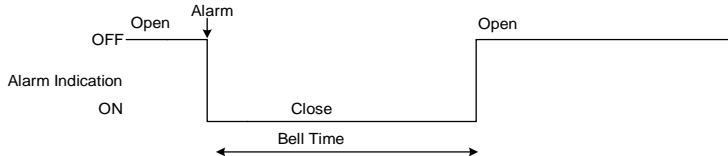
Ready: Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.



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



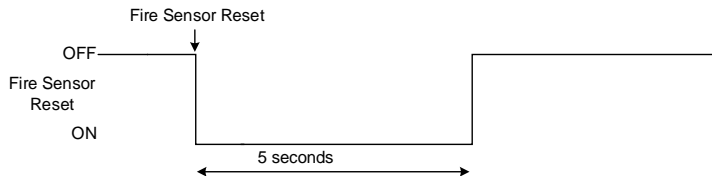
Alarm indication: Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.



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



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



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



3.5.1 Output PGM wiring. Bell, Relay, Led Wiring

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

1. Connect devices to the selected outputs as shown in the figures below. For sound signaling we recommend to use siren DC 12V up to 1500mA. It is recommended to connect the siren to the system by using 2 x 0,75 sq. mm double insulation cable. Auxiliary BUZZER is recommended to be installed inside the premises not far from the entrance. Buzzer operates together with the main siren also when the system starts calculating the time to leave the premises and the time till alarm response of the security system after entering the premises (see clause 7.1). It is possible to use buzzer of hit point PB12N23P12Q or similar modified piezoelectric 12V DC, 150mA max Buzzer. Standard AC/DC adapter with the voltage 10V-14V and current $\geq 1A$ might be used to powering the module

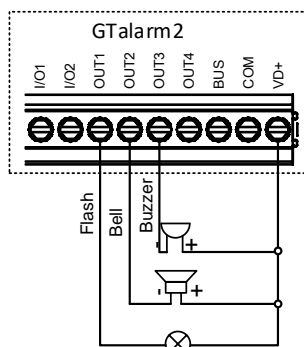


Fig. 1 OUT1-OUT4 Open drain 1000 mA connection

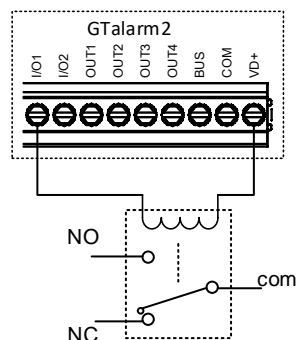


Fig. 2 Relay connection to OUT1-OUT4, I/O1, I/O2 20mA

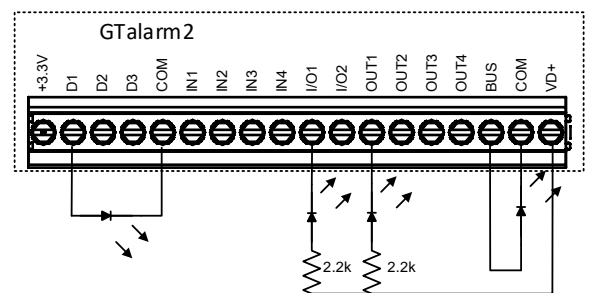


Fig. 3 example of LED connection to output

3.5.2 Access control output with logging

Set output definition to [Access Gained].

This output generates even if access device is granted by user who controls this output.

- If user has right to ARM/DISARM system, it always has access to this output.
- If ARM/DISARM flag is not set user can access this output only if system is Disarmed (Open).
- If access is granted by user, 421 event Access granted is stored into the log. If not Access denied event 422

- if output will have definition [Automation / CTRL] it also can be controlled by user in any ways but it will not generate 421 and 422 events, And will not care about ARM/DISARM

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

3.5.3 Quick start outputs

1. Install SERA2 software. For more information look at [SERA2 Uploading/Downloading Software](#)
2. Connect the module to the computer via mini USB cable.

The names of outputs could be changed
 If output is not used, it must be disabled
 Outputs could be controller via:
 Short call
 iButton code
 RFID keycard
 Keypunch code
 If market, could be specified date and time interval for output control.

ID	Output Location in Hardware	Output Label	Out definition	Mode	Out Timer	Invert	Pulsating	Pulse ON Time	Pulse OFF Time
1	GTalarm v2, OUT4(1A)	OUT1	Bell	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
2	GTalarm v2, OUT3(1A)	OUT2	Automation & Access	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
3	GTalarm v2, OUT2(1A)	OUT3	Automation & Access	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
4	GTalarm v2, OUT1(1A)	OUT4	Automation & Access	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
5	GTalarm v2, IO1(20mA)	OUT5	System State	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
6	Output Disabled	OUT6	Disable	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms
7	Output Disabled	OUT7	Disable	Steady	10s	<input type="checkbox"/>	<input type="checkbox"/>	100ms	100ms

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MIC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+3706E	0A0D00037D22	0000000000	*****	NONE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input checked="" type="checkbox"/>	zivil	User	+3706G	0000000000	0000000000		NONE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
3	<input type="checkbox"/>		User	+	0000000000	0000000000		OUT1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
4	<input type="checkbox"/>		User	+	0000000000	0000000000		NONE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Figure 29 Outputs settings

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)



Outputs can be controlled only in Automation/ CTRL mode.

- In order to control big power alternating current equipment, it is comfortable to use solid state relays.
- Standard AC/DC adapter with the voltage 10V-14V and current $\geq 1A$ might be used to powering the module.

3.6 Access control. Arming/Disarming methods



Arming process:

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



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



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



Access control: schedules, temporary access

<https://youtu.be/W5FSvN-UitI>

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

SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

GSM Communications

Users/Access control

Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

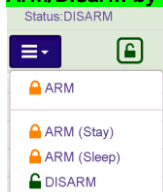
Remote Control Users table

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	Date En	Start Date	Expiration Date
17	<input type="checkbox"/>		User	+	000000000000	0000000000		NONE	<input type="checkbox"/>	<input type="checkbox"/>	2019-07-09 17:02:21	2019-07-09 17:02:21
18	<input type="checkbox"/>		User	+	000000000000	0000000000		NONE	<input type="checkbox"/>	<input type="checkbox"/>	2019-07-09 17:02:21	2019-07-09 17:02:21

Temporary access Date/Time window

Figure 30 Users/ Access control window

Arm/Disarm by mobile, web app



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

Arm/Disarm by call

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



SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

GSM Communications

Users/Access control

Inputs/Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

Remote Control Users table

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MIC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+370	0A0D00037D22	0000000000	*****	OUT1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input checked="" type="checkbox"/>	zivil	User	+370	000000000000	0000000000		OUT2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Temporary access Date/Time window

1. Enter phone number
2. Select the output for remote control via mobile
3. Mark if it is needed to control the output via specified date and time

Figure 31 ARM/ DISARM by call settings

Arm/Disarm via SMS

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

The system **rejects the SMS text messages containing wrong SMS password** even from a listed user phone number. To arm the system by SMS text message, send the following text to the system's phone number USER 123456_030_ST
030= command code (Change security system's mode (ARM/DISARM/STAY/SLEEP)
ST = Security system mode 0-DISARM, 1-ARM ,2-STAY ,3-SLEEP

Arm/Disarm by keypad

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

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

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



SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

GSM Communications

Users/Access control

Inputs/Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

Remote Control Users table

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MIC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+370	0A0D00037D22	0000000000	*****	OUT1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input checked="" type="checkbox"/>	zivil	User	+370	000000000000	0000000000		OUT2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Temporary access Date/Time window

1. Enter keybutton code
2. Select the output for remote control via keybutton code.
3. Mark if it is needed to control the output via specified date and time

Figure 32 ARM/DISARM by keypad settings

Arm/Disarm by iButton key

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



SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

GSM Communications

Users/Access control

Inputs/Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

Remote Control Users table

ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MIC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+370	000000FBC52E	0000000000	*****	OUT1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input checked="" type="checkbox"/>	zivil	User	+370	000000000000	0000000000		OUT2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Temporary access Date/Time window

1. Enter iButton code. iButtons must be from 01 family.
2. Select the output for remote control via keybutton code.
3. Mark if it is needed to control the output via specified date and time

Figure 33 ARM/DISARM by iButton code settings

Arm/Disarm by RFID key card, keyfob

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



If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)



More information about how to configure Arming/ Disarming:

SERA2
File Settings Devices Read [F5] Write [F6] Update About...

System Options
GSM Communications
Users/Access control
Inputs/Burglar Alarm Zones
Outputs (PGM)
Automation/Sensors
Event Summary
Events Log
RT Testing&Monitoring
Firmware

Remote Control Users table

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

Temporary access Date/Time window

September 2

26 27 28 29 30
2 3 4 5 6
9 10 11 12 13
16 17 18 19 20
23 24 25 26 27

Expiration Date: Temporary access expiration date and time
Start Date: Temporary access start date and time
Date EN: Temporary access enable
ARM/ DISARM: If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
OUT: The selected input will be switched, if a user will call from this number. Preferred input may be assigned to each user's number. Thus different users are able to control different objects
Keyb Code: Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
RFID Keycard: RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
iButton Code: iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family
User Tel.: Telephone numbers of users who will be able to control the module by dialing should be entered in this column. User number should be entered with international code.
Type: Reserved for future uses
User Name: The name of users who will be able to control the module should be entered in this column.
En: Reserved for future uses

En: Reserved for future uses

User Name: The name of users who will be able to control the module should be entered in this column.

Type: Reserved for future uses

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 key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family

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.

Date EN: Temporary access enable

Start Date: Temporary access start date and time

Expiration Date: Temporary access expiration date and time

The module GTalarm2 controls access by using schedules. Inputs, outputs, readers and cards through access levels are all configured with schedules by which they will be energized or de-energized, enabled or disabled. For example, you might assign an output to be energized from 12:00 a.m. to 6:00 a.m. every day. The 12:00 a.m. to 6:00 a.m., Monday through Sunday, time period is called a schedule. The "Access Schedules" tab enables you to create the schedule you will use to configure your GTM module. Click "Access Schedules" tab to display the Schedules screen:

SERA2
File Settings Devices Read [F5] Write [F6] Update About...

System Options
GSM Communications
Users/Access control
Inputs/Burglar Alarm Zones
Outputs (PGM)
Automation/Sensors
Event Summary
Events Log
RT Testing&Monitoring
Firmware

Remote Control Users table

Users Access Schedules Holidays

Specifies the number of times a card/ call/code may be used to which it has valid access Max 255 uses is all

ID	En	User Name	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	En	Start Date	End Time	Mo	Tu	We	Th	Fr	Sa	Su	Holidays
1	<input checked="" type="checkbox"/>	Master	+	000000000000	0000000000	*****	NONE	<input checked="" type="checkbox"/>		2019-11-30	21:37								
2	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
3	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
4	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
5	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
6	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
7	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								
8	<input type="checkbox"/>		+	000000000000	0000000000		NONE	<input type="checkbox"/>		2019-11-30	21:37								

Enabling or disabling holidays

Set the holidays

Go to Sera2> System Options> Digital I/O Settings
Set Digital I/O D1 to Dallas 1-Wire Bus.

Go to Sera2> System Options> General system Options.
Press "Start iButton/ RFID/ Phone programming mode.

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
Set time zone
Set clock synchronization
Press "Write"

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

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

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

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

Suppose you must create a Cleaning Crew schedule. The schedules are to be set up as follows: Monday-Friday 5 p.m.-1 a.m., Saturday and Sunday 8 a.m.-1 p.m., no holidays. This becomes three separate schedules, as follows.
2 Monday-Friday, 5 p.m.-11:59 p.m. (Remember, the time range cannot cross midnight, so 11:59 p.m. is the limit.)
3 Tuesday-Saturday, 12:00 a.m.-1:00 a.m.
4 Saturday-Sunday, 8:00 a.m.-1:00 p.m.

Note: Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, schedules that contain that specific Holiday type will work. The Holiday allows users to further customize how the panel works. For example, the user can block access to a building on that day, or grant special access during that day. Each Holiday added is considered a full day, extending from midnight to midnight. The options available when configuring a holiday are Annual, Type, Date and Year. While Annual is enabled, the date added as a Holiday will be a Holiday every year. This disables the Annual check box and allows a user to select a specific year, so that only during that date and year will the Holiday selection work.

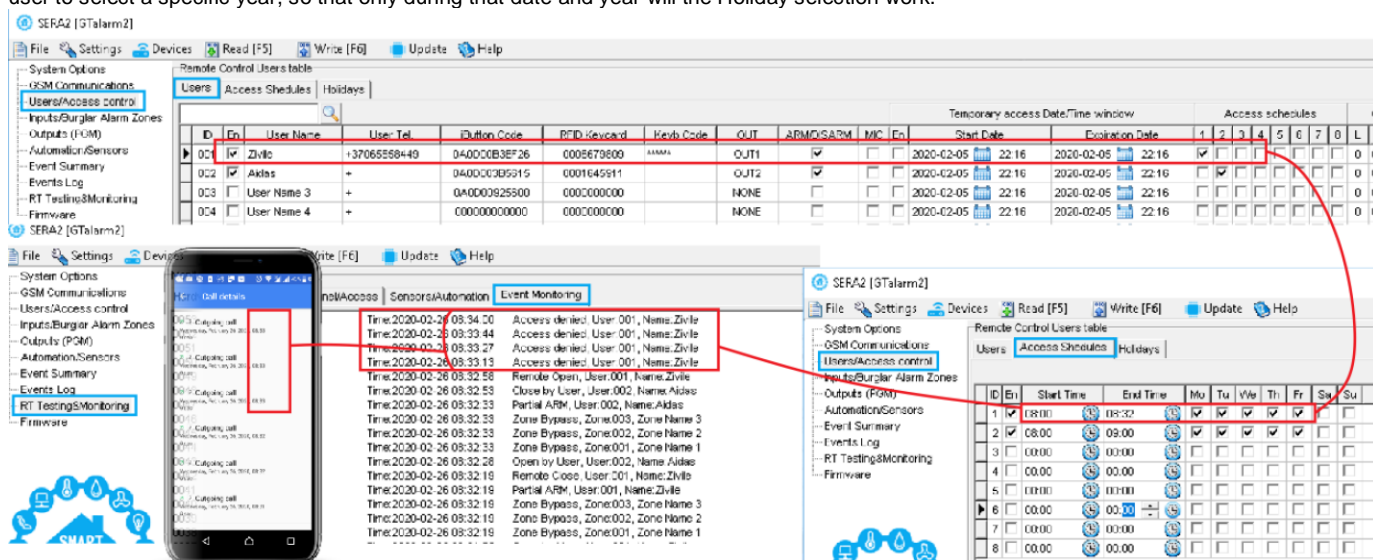


Figure 46 The example of schedule
DISARM /ARM/SLEEP/STAY

3.6.1 Wiegand Keypad & RFID Card Reader, iButton Probe Wiring



Wiegand keypad specifications:
26bit Wiegand (Default);
8bit key press code

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

i 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).

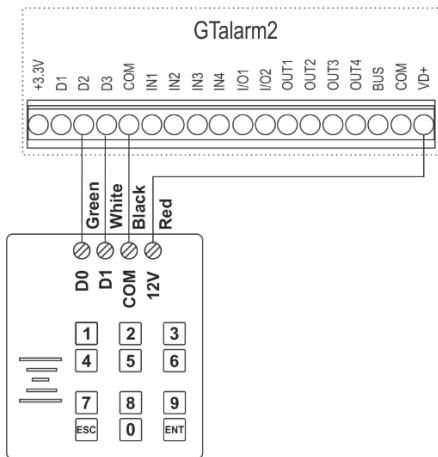


Figure 34 Wiegand keypad wiring

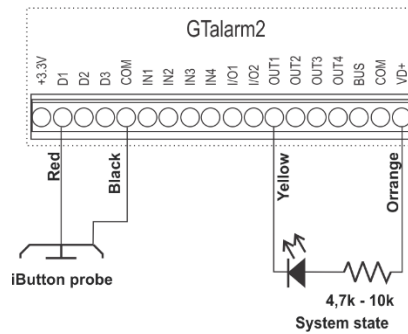


Figure 35 iButton connecting diagram

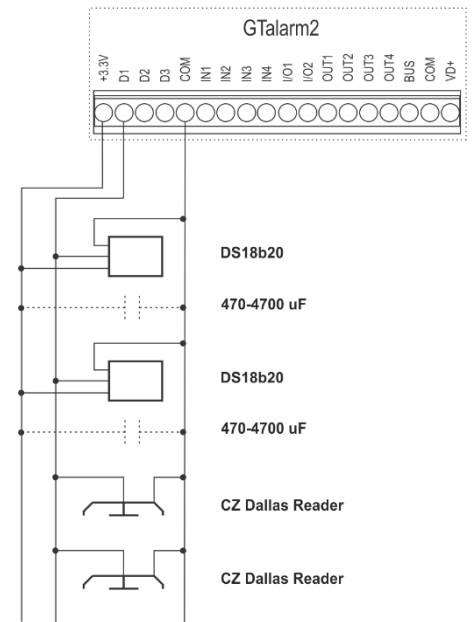


Figure 36 iButton connection diagram



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.

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

First steps:

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

Configurations methods:

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

If you want to edit existing configuration,

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

Write edited configuration (press "Write" in the command line)



YouTube

Enter iButton RFID codes to the memory

https://youtu.be/80yWW_j9pJk



YouTube

Activate RFID learning mode remotely

<https://youtu.be/4MnPfxH7F04>



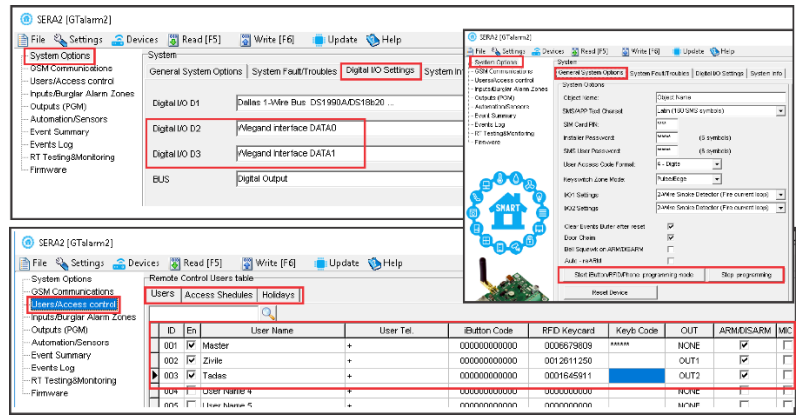
YouTube

Access control: schedules, temporary access

<https://youtu.be/W5FSvN-UitI>

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

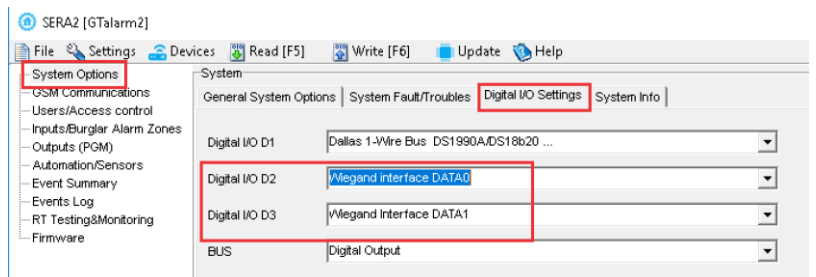
Send SMS message: INST000000 063 1
 You will receive the message: iButton/RFID/Caller ID
 Learning Mode is Switched ON
 Touch RFID keycards to the RFID reader.
 Sent the message: INST000000 063 0
 You will receive the message: iButton/RFID/Caller ID
 Learning Mode Stopped

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.

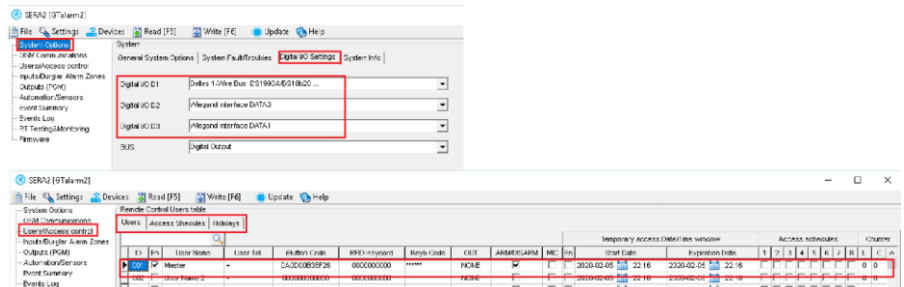
Before activating the RFID learning mode via SMS, the module must have the appropriate System Options> Digital I/O Settings

- 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.



Start automatic learning mode remotely via Sera2 software.

Start Sera2 software

Press "Connect remotely" button

Enter required parameter.

(Default App Key is 123456)

Press "Connect"

Go to Sera2> System Options> General System Options

Press "iButton/RFID/Caller ID Learning Mode"

Touch RFID keycards to the Wiegand keypad"

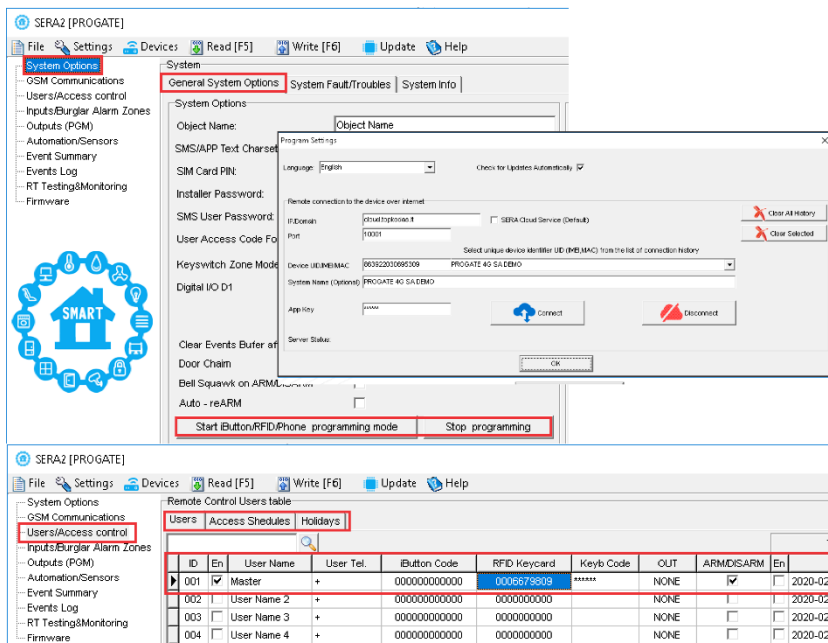
Press "Stop programming" button

Or wait until the learning mode will stop automatically



Before activating the RFID learning mode remotely, 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



Refer to: Users & Access Control programming details.

3.7 How to set clock synchronization?

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

You can select **clock synchronization** via:

GSM modem

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

Cloud Server

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

Or disable clock synchronization

Clock synchronization via GSM modem

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

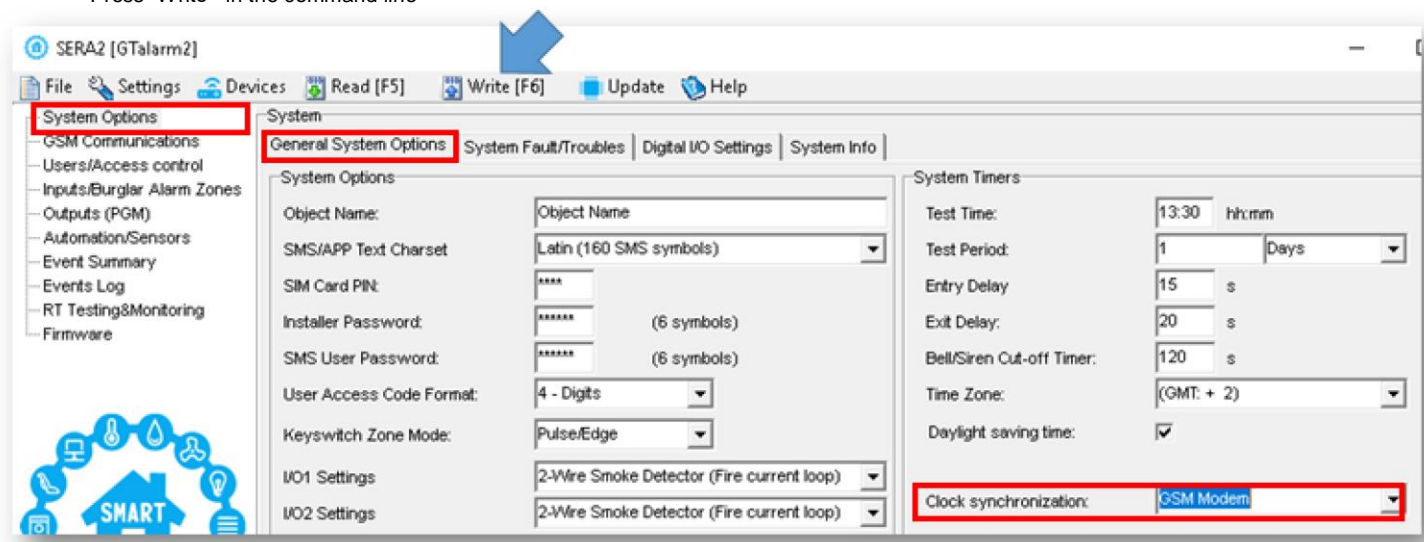


Figure 37 SERA2> System Options> General System Options

Clock synchronization via Cloud server

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

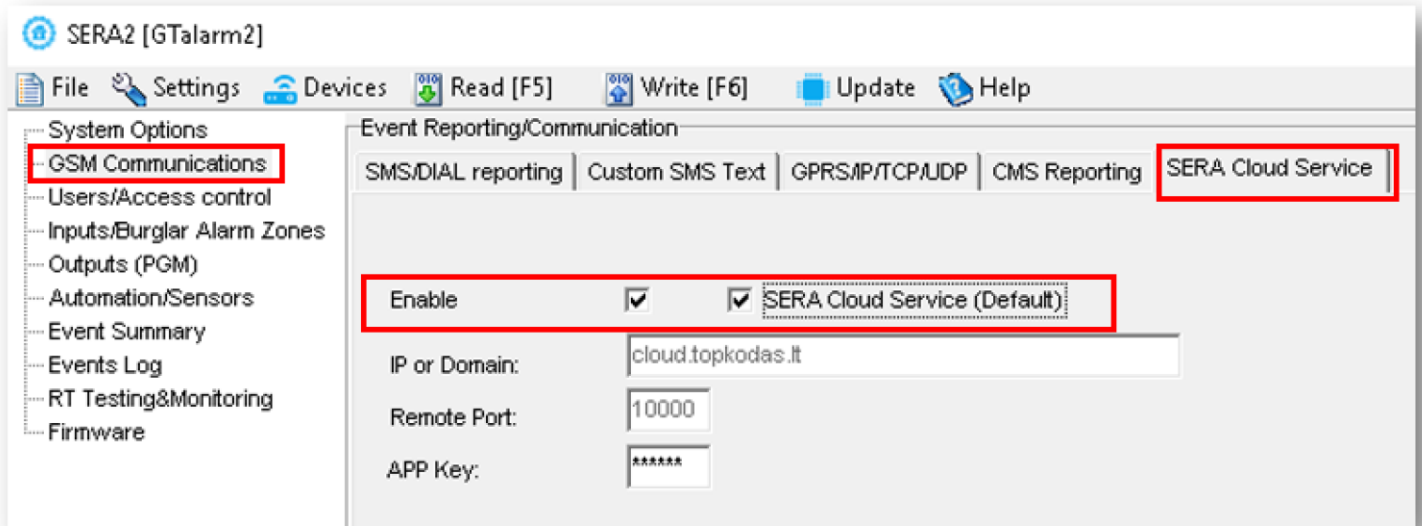
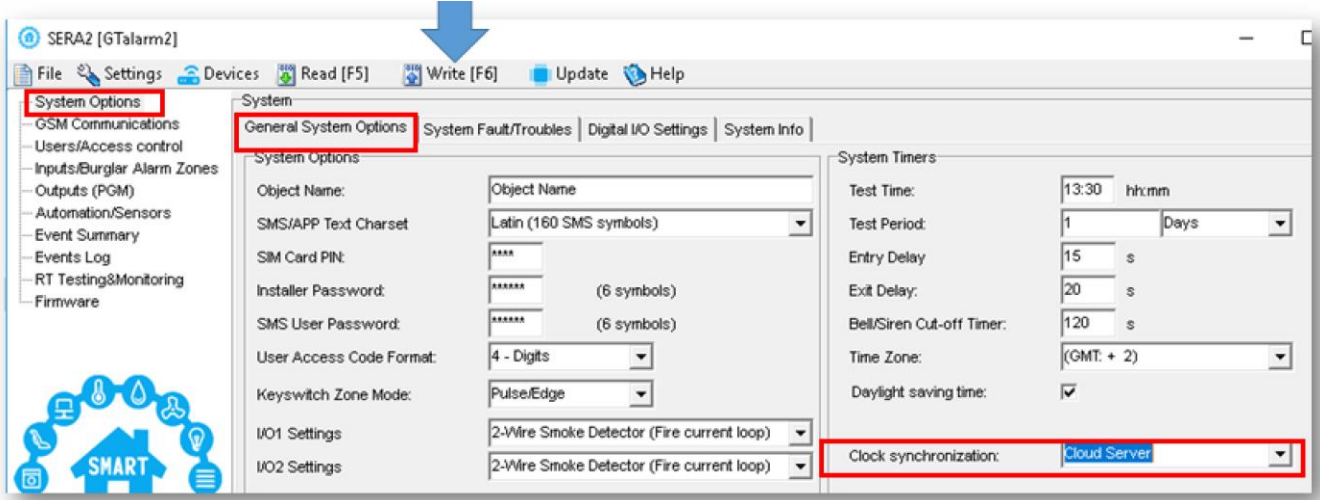


Figure 38 SERA2> GSM Communication> SERA Cloud Service

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



If you want to edit existing configuration,

Figure 39 SERA2> System Options> General System Options

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

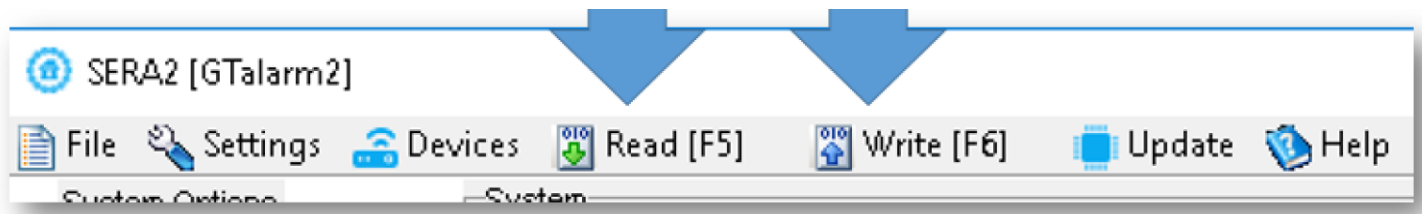


Figure 40 SERA2 Command line

4

5 Programming

In order to configure and control the system by SMS text message, send the text command to the GTalarm2 phone number from one of the listed user phone numbers. More

SERA2 software configuration tool is intended for the module GTalarm2 configuration locally via USB port or remotely via GPRS network. This software simplifies system configuration process by allowing to use a personal computer in the process.

5.1 SERA2 Uploading/Downloading Software



We recommend programming the module GTalarm2 with SERA2 software

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

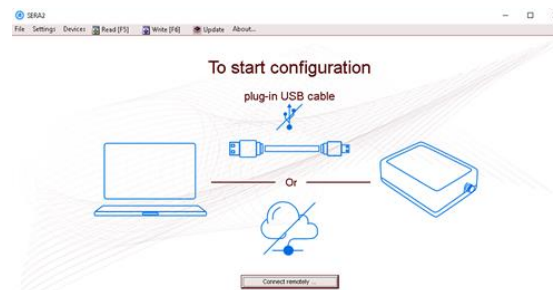


Figure 41 How to start configuration with Sera2 software

Connection of the module to your PC

! The module must be powered with (+12V >500 mA) voltage, it should have inserted SIM card (with replenished account and removed PIN CODE REQUEST). Module must be connected to the PC via mini USB cable

Work with the software SERA2

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

If you are sure that the module is fully connected to PC and power supply, please go to Devices > GTalarm v2

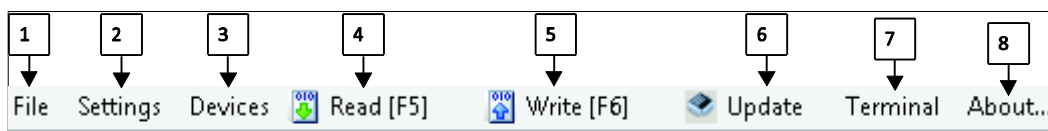


Figure 42 The meaning of icons

! 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

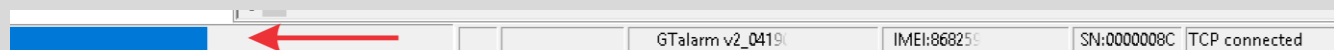


Figure 43 Progress bar

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

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

! If you want to receive software updates, go to Settings and mark “Check for Updates Automatically”. When new update will be available, the program will inform you, and you have to start the update. After that you have to connect the module to the computer via mini USB cable. You have to write this update to the module GTalarm2 by pressing “Update” in the bottom line in SERA2 software.

If you want to update the module manually, got to “About” and press “Check for updates”



Figure 44 How to update the module manually

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

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

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

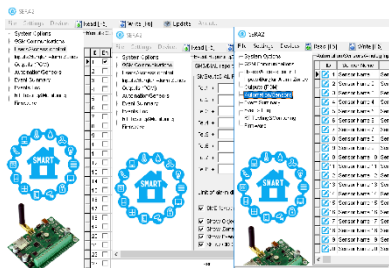


Figure 45 Unlimited number of modules configuration at the same time



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

If you want to edit existing configuration,

You have to read it (press "Read" in the command line)

Edit settings

Write edited configuration (press "Write" in the command line)

5.2 General system options programming



Time Zone: (GMT: + 2)

Daylight saving time: ☒

Clock synchronization: Cloud Server

Set Module Time from PC

Read Module Time

PC time: 2019-08-05 09:39:37, Monday

Panel 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.

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

[System Options](#) > General system Options

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

SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

General System Options

System Options

Object Name: The name and address of the object

SMS/APP Text Charset: Text charset: Latin, Eastern European, Baltic or Western European.

SIM Card PIN: Default 1234

Installer password: Default 000000 It allow to enter installer programming mode

SMS User Password: Default 123456 It allow utilize arming method and enter user programming mode

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/O2 Settings: Set the programmable input or output to:

0-10V analog input

Output

2- wire smoke detector or

0-20 mA, 4-20mA current loop sensor

Clear Events Buffer after reset: The memory of unsend reports will be deleted after the reset of the module

Door Chain: Violations of delay zones when the alarm turned off will be accompanied by keyboard audible (Buzzer) signal

Bell Squawk on ARM/ DISARM: Activate the bell output briefly causing the squawk to alert users that the module is being armed

Auto - reARM: Arm the module if there is no activity in the area after the system disarming.

Start iButton/RFID programming mode

Stop iButton/RFID programming

Panel Time:

Reset Device

Stop iButton/RFID programming: To finish entering iButton keys or RFID cards, click Stop programming button.

Start iButton/RFID 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.

Object name: The name and address of the object

SMS/APP Text Charset: Text charset: Latin, Eastern European, Baltic or Western European.

SIM Card PIN: Default 1234

Installer password: Default 000000 It allow to enter installer programming mode

SMS User Password: Default 123456 It allow utilize arming method and enter user programming mode

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/O2 Settings: Set the programmable input or output to:

0-10V 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 Chain: Violations of delay zones when the alarm turned off will be accompanied by keyboard audible (Buzzer) signal

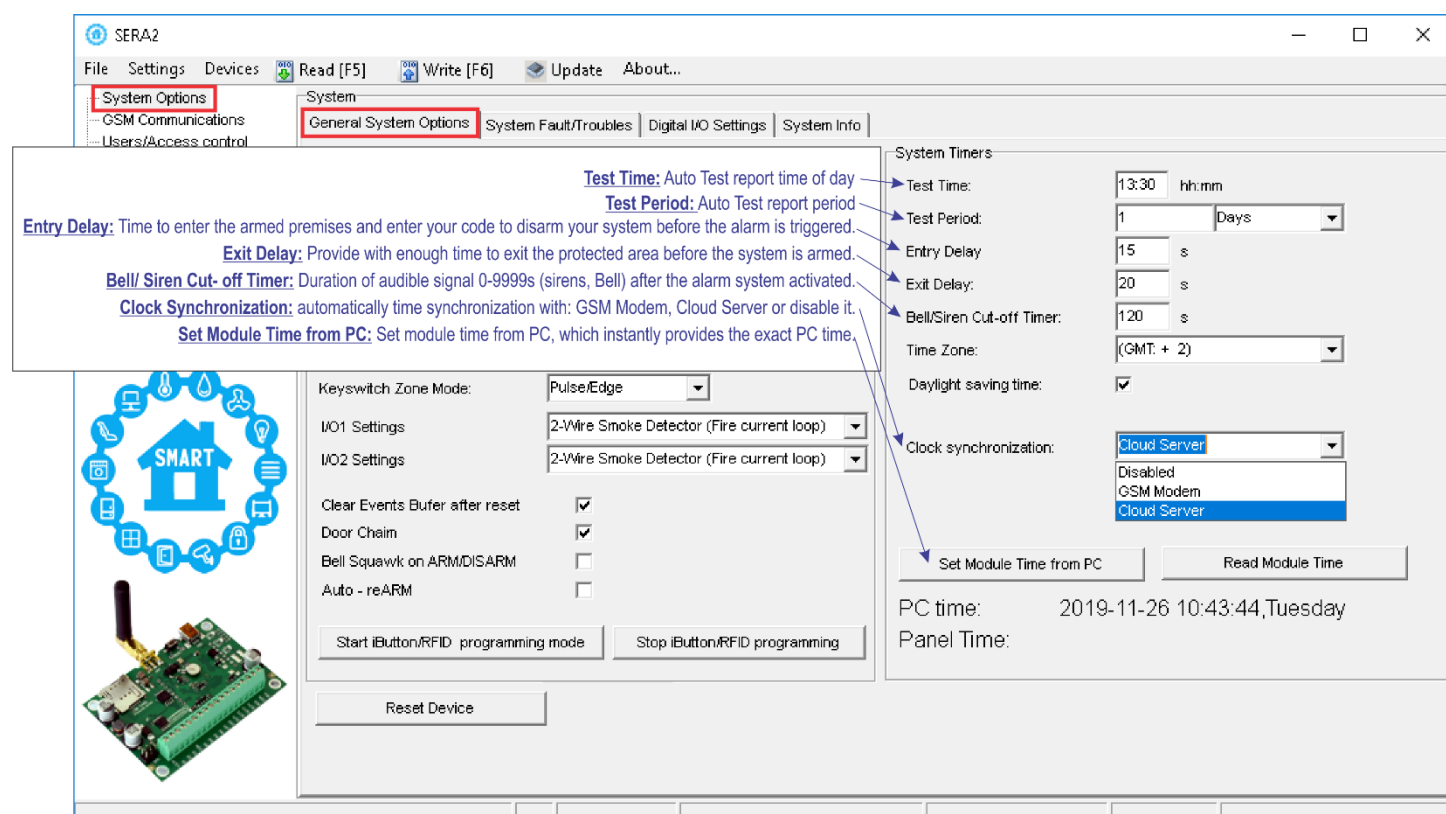
Bell Squawk on ARM/ DISARM: Activate the bell output briefly causing the squawk to alert users that the module is being armed, disarmed or that an Entry or Exit Delay was triggered

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/RFID 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.

5.3 System Fault/ Troubles Programming



[System Options](#) > System Fault/ Troubles

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

System Options

- GSM Communications
- Users/Access control
- Inputs/Burglar Alarm Zones
- Outputs (PGM)
- Automation/Sensors
- Event Summary
- Events Log
- RT Testing&Monitoring
- Firmware

System

General System Options | **System Fault/Troubles** | Digital I/O Settings | System Info

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

Fault/Troubles Global Settings

Trouble Event Limit :

Reset Trouble Event Counter After : min

System Voltage (Low Battery) settings

Low System Voltage Alarm: V

System Voltage Restore: V

Event Delay: s

Global Tamper Recognition:

Tamper Disable

Trouble when disarmed / alarm as per zone when armed

Trouble always

Enable: The system will detect a marked trouble

Restrict Arm: In case of such trouble, the arming activation will be restricted.

Trouble Event Limit: Allowable number of the same trouble event

Low System Voltage Alarm: The system is running on the backup battery and voltage is dropped below allowed value.

System Voltage Restore: The voltage has been restored and has been reached defined value.

Event Delay: System low voltage trouble event report delay.

GSM network trouble: SIM card is not registered with the GSM network provider

Zone antimasking trouble: Do not available in this module

SIM card trouble: Not available or impossible to read SIM card.

Fire loop trouble: The trouble is occurring with your smoke detectors.

Tamper trouble: The zone(s) that was tampered

BUS trouble: Do not available in this module.

Clock trouble: The time and date has not been set.

Battery trouble: Power supply or backup battery voltage is low, needs to be recharged, or replaced

Audible alarm when disarmed/ alarm as per zone when armed: When disarmed: Generates Audible Alarm. The module transmits the defined report code and generates an audible alarm. When armed: Follows Zone Alarm Type. The module follows the zone's alarm type.

Trouble always: Generates Trouble Only (when armed or disarmed).

Trouble when disarmed/ alarm as per zone when armed: When disarmed: Generates Trouble Only. The module transmits the defined report code. When armed: Follows Zone Alarm Type.

Tamper Disable: The module will not generate an alarm or trouble.

Enable: The system will detect a marked trouble

Restrict Arm: In case of such trouble, the arming activation will be restricted.

Battery trouble: 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: Do not available in this 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 anti masking trouble: Do not available in this module

GSM network trouble: SIM card is not registered with the GSM network provider

Trouble Event Limit: Allowable number of the same trouble event

Low System Voltage Alarm: The system is running on the backup battery and voltage is dropped below allowed value.

Event Delay: System low voltage trouble event report delay.

Audible alarm when disarmed/ alarm as per zone when armed: When disarmed: Generates Audible Alarm. The module transmits the defined report code and generates an audible alarm. When armed: Follows Zone Alarm Type. The module follows the zone's alarm type

Trouble always: Generates Trouble Only (when armed or disarmed)

Trouble when disarmed/ alarm as per zone when armed: When disarmed: Generates Trouble Only. The module transmits the defined report code. When armed: Follows Zone Alarm Type

Tamper Disable: The module will not generate an alarm or trouble

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

5.4 Digital Inputs/ Outputs programming



System Options > Digital I/O Settings

The Digital I/O Settings let you set digital input/ output parameters and expansion BUS options

The screenshots show the 'Digital I/O Settings' window in the SERA2 software. The left sidebar contains a tree view with 'System Options' selected. The main window has tabs for 'General System Options', 'System Fault/Troubles', 'Digital I/O Settings', and 'System Info'. The 'Digital I/O Settings' tab is active, showing configuration for Digital I/O D1, D2, D3, and the BUS. A list of available devices is shown on the right, with callouts indicating the assigned device for each I/O line.

- Digital I/O D1:** Digital Input (Max. 3.3V) assigned to D1, Digital Output (Max. 3.3V) assigned to D1, Dallas 1-wire Bus assigned to D1, Aosong 1-wire Bus Humidity/ Temperature Sensor assigned to D1.
- Digital I/O D2:** Digital Input (Max. 3.3V) assigned to D2, Digital Output (Max. 3.3V) assigned to D2, Dallas 1-wire Bus assigned to D2, Aosong 1-wire Bus Humidity/ Temperature Sensor assigned to D2, Wiegand interface DATA0 assigned to D2.
- Digital I/O D3:** Digital Input (Max. 3.3V) assigned to D3, Digital Output (Max. 3.3V) assigned to D3, Dallas 1-wire Bus assigned to D3, Aosong 1-wire Bus Humidity/ Temperature Sensor assigned to D3, Wiegand interface DATA1 assigned to D3.
- BUS:** Digital Input assigned to BUS, Digital Output assigned to BUS, Expansion Module BUS: do not available in this module.

5.5 Zones programming



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

GTalarm2 comes equipped with 4 on-board wired zones and 2 programmable I/O inputs. For additional detection device connection, the number of zones can be expanded. GTalarm2 zones can be expanded with expansion module up to 32.

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

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

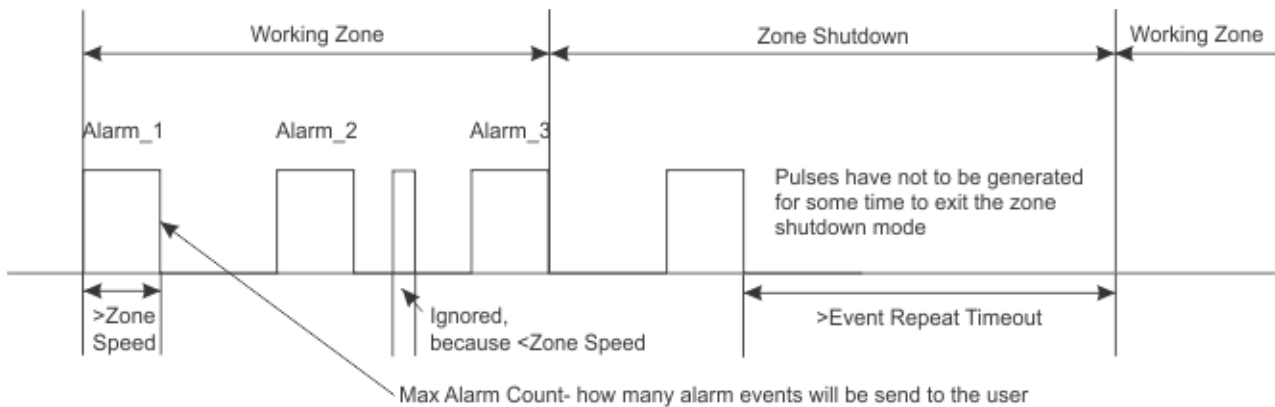
The system can be STAY-armed under the following conditions: If a Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exists, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must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

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

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

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

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



SERA2

File Settings Devices Read [F5] Write [F6] Update

System Options

GSM Communications

Users/Access control

Inputs/Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

Event Summary

Events Log

RT Testing&Monitoring

Firmware

Zones

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

Zone 1 Settings

Zone Name

Alarm Text

Restore Text

Zone Hardware Location

Zone Definition

Wiring Type

Contact ID code

Zone Speed

Event Repeat Timeout

Max Alarm Count

Zone Alarm action

Zone Options:

Alarm report Enabled

Restore report Enabled

Tamper Enabled

Bypass Enabled

Shutdown if max alarm count

Zone Force ARM

OK

Double click on the selected sensor's line

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.

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, tamperers.

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

5.6 Outputs. Bell & PGM programming



SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

- GSM Communications
- Users/Access control
- Inputs/Burglar Alarm Zones
- Outputs (PGM)**
- Automation/Sensors
- Event Summary
- Events Log
- RT Testing&Monitoring
- Firmware

Outputs

ID	Output Location in Hardware	Output Label	Out definition	Mode	Out Timer	Invert	Pulsating	Pulse ON Time	Pulse OFF Time
1	GTalarm v2, OUT1(1A)	OUT1	Disable	Steady	10s			100ms	100ms
2	GTalarm v2, OUT2(1A)	OUT2	Bell						
3	GTalarm v2, OUT3(1A)	OUT3	Buzzer						
4	GTalarm v2, OUT4(1A)	OUT4	Flash						
5	GTalarm v2, IO1(20mA)	OUT5	System State						
6	GTalarm v2, IO2(20mA)	OUT6	Ready						
7	GTalarm v2, D1 10mA, Max Voltage 3	OUT7	Automation & Access Control						
8	GTalarm v2, D2 10mA, Max Voltage 3	OUT8	AC OK						
9	GTalarm v2, D3 10mA, Max Voltage 3	OUT9	Battery OK						
10	GTalarm v2, BUS 20mA	OUT10	ARM/DISARM						

Mode: Steady: Steady ON/OFF mode
Timer: Output ON pulse mode

Out Timer: Pulse time duration can be from 1 to 999999 sec.

Invert: Inversion is activated

Pulsating: Pulsating mode is activated. Then output is activated. It will pulsate according pulse ON/OFF time.

Pulsating ON Time: Pulsating mode pulse ON duration.

Pulsating OFF Time: Pulsating mode pulse OFF duration.

Access Gained: If user has right to ARM/DISARM system, it always has access to this output. If ARM/DISARM flag is not set user can access this output only if system is Disarmed (Open)

RH Sensor Trouble: Output for RH Sensor trouble operation. In this mode output can automatically reset Humidity sensor if trouble occurs.

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

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

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

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

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

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

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

Automation & Access Control: Remote control by call mode is enabled. Output designed for connection of electrical devices which will be controlled by SMS message or phone call

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

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

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

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

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

Disable: Output disabled

Out definition:

Access Gained: If user has right to ARM/DISARM system, it always has access to this output. ? If ARM/DISARM flag is not set user can access this output only if system is Disarmed (Open).

RH Sensor Trouble: Output for RH Sensor trouble operation. In this mode output can automatically reset Humidity sensor if trouble occurs.

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

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

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

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

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

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

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

Automation & Access Control: Remote control by call mode is enabled. Output designed for connection of electrical devices which will be controlled by SMS message or phone call

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

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

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

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

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

Disable: Output disabled

Mode:

Steady: Steady ON/OFF mode

Timer: Output ON pulse mode

Out Timer: Pulse time duration can be from 1 to 999999 sec.

Invert: Inversion is activated

Pulsating: Pulsating mode is activated. Then output is activated. It will pulsate according pulse ON/OFF time.

Pulsating ON Time: Pulsating mode pulse ON duration.

Pulsating OFF Time: Pulsating mode pulse OFF duration.

5.7 Users & Access Control programming details.





Access control: schedules, temporary access

<https://youtu.be/W5FSvN-UitI>

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



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

SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options

- GSM Communications
- Users/Access control**
- Inputs/Burglar Alarm Zones
- Outputs (PGM)
- Automation/Sensors
- Event Summary
- Events Log
- RT Testing&Monitoring
- Firmware

Remote Control Users table

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

Temporary access Date/Time window

September 2019

Mon Tue Wed Thu Fri Sat Sun

26 27 28 29 30 31 1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

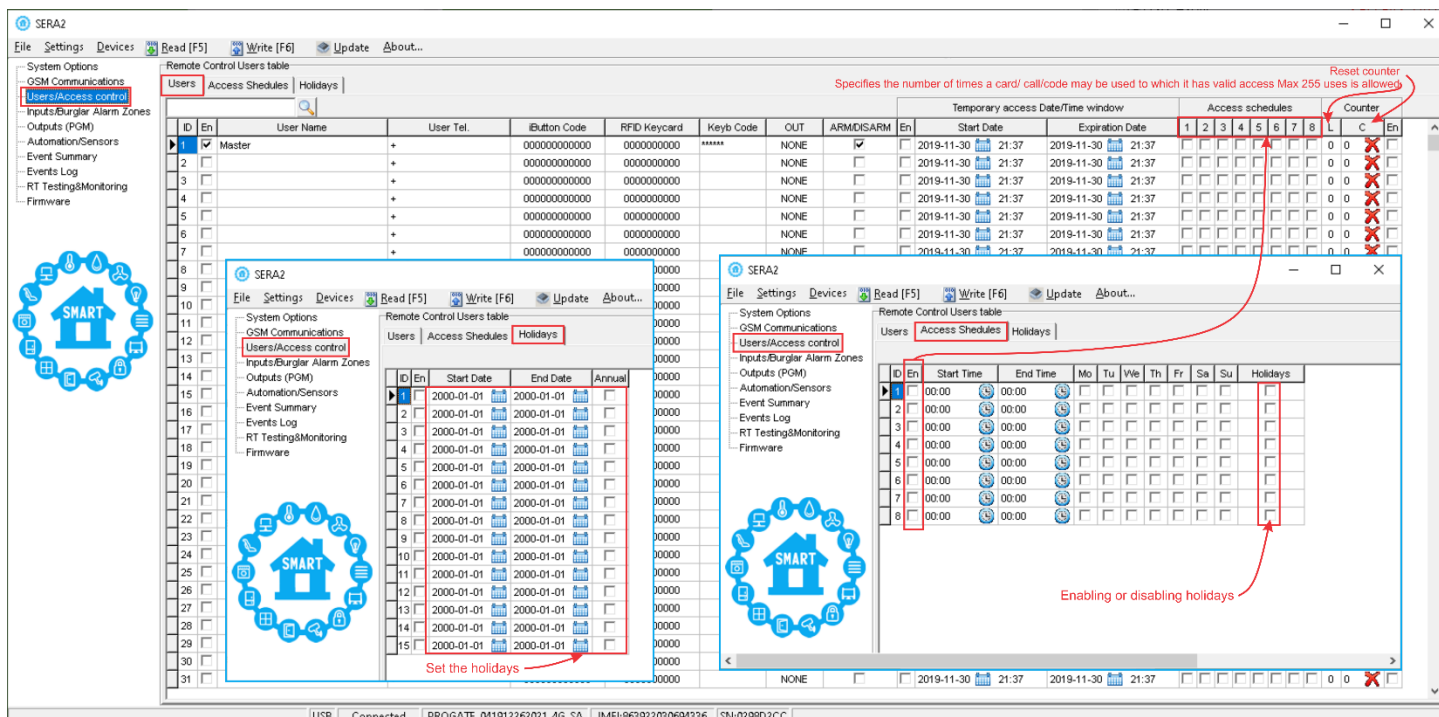
Expiration Date: Temporary access expiration date and time
 Start Date: Temporary access start date and time
 Date EN: Temporary access enable
 ARM/ DISARM: If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
 OUT: The selected input will be switched, if a user will call from this number. Preferred input may be assigned to each user's number.
 Thus different users are able to control different objects
 Keyb Code: Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
 RFID Keycard: RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
 iButton Code: iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode.
 In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family
 User Tel.: Telephone numbers of users who will be able to control the module by dialing should be entered in this column. User number should be entered with international code.
 Type: Reserved for future uses
 User Name: The name of users who will be able to control the module should be entered in this column.
 En: Reserved for future uses

En: Reserved for future uses**User Name:** The name of users who will be able to control the module should be entered in this column.**Type:** Reserved for future uses**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 key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family**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.**Date EN:** Temporary access enable**Start Date:** Temporary access start date and time**Expiration Date:** Temporary access expiration date and time

The module GTalarm2 controls access by using schedules. Inputs, outputs, readers and cards through access levels are all configured with schedules by which they will be energized or de-energized, enabled or disabled. For example, you might assign an output to be energized from 12:00 a.m. to 6:00 a.m. every day. The 12:00 a.m. to 6:00 a.m., Monday through Sunday, time period is called a schedule. The "Access Schedules" tab enables you to create the schedule you will use to configure your GTM module. Click "Access Schedules" tab to display the Schedules screen:



Go to Sera2> System Options> Digital I/O Settings
Set Digital I/O D1 to Dallas 1-Wire Bus.
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
Set time zone
Set clock synchronization
Press "Write"

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

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

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

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

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

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

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

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

Note: Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, schedules that contain that specific Holiday type will work. The Holiday allows users to further customize how the panel works. For example, the user can block access to a building on that day, or grant special access during that day. Each Holiday added is considered a full day, extending from midnight to midnight. The options available when configuring a holiday are Annual, Type, Date and Year. While Annual is enabled, the date added as a Holiday will be a Holiday every year. This disables the Annual check box and allows a user to select a specific year, so that only during that date and year will the Holiday selection work.

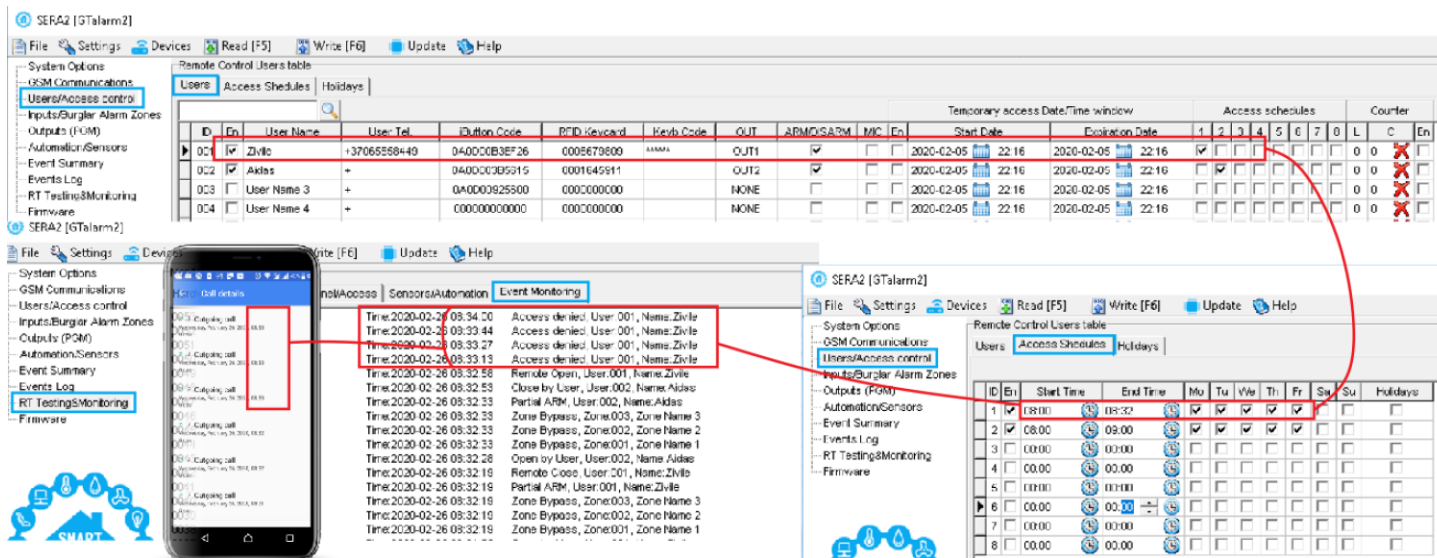


Figure 46 The example of schedule

5.8 DISARM /ARM/SLEEP/STAY the security system



System Options > System Fault/ Troubles

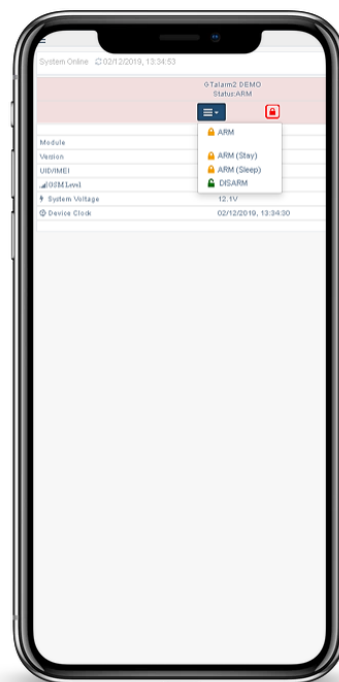
In this window System trouble settings could be configured

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.



SERA2

File Settings Devices Read [F5] Write [F6] Update About...

System Options
GSM Communications
Users/Access control
Inputs/Burglar Alarm Zones
Outputs (PCM)
Automation/Sensors
Event Summary
Events Log
RT Testing&Monitoring
Firmware

Remote Control Users table

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

Temporary access Date/Time window

September 2019

Mon Tue Wed Thu Fri Sat Sun

26 27 28 29 30 31 1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

Expiration Date: Temporary access expiration date and time
Start Date: Temporary access start date and time
Date EN: Temporary access enable
ARM/ DISARM: If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
OUT: The selected input will be switched, if a user will call from this number. Preferred input may be assigned to each user's number.
Thus different users are able to control different objects
Keyb Code: Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
RFID Keycard: RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
iButton Code: iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family—
User Tel.: Telephone numbers of users who will be able to control the module by dialing should be entered in this column. User number should be entered with international code.
Type: Reserved for future uses
User Name: The name of users who will be able to control the module should be entered in this column.
En: Reserved for future uses

iButton.com
000000FBC52B
1-Wire®
DS1990A-45

En: Reserved for future uses

User Name: The name of users who will be able to control the module should be entered in this column.

Type: Reserved for future uses

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 key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000. iButtons must be from 01 family

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.

Date EN: Temporary access enable

Start Date: Temporary access start date and time

Expiration Date: Temporary access expiration date and time

5.9 Reporting SMS&Dial in Case of Alarm Events



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

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

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

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

5.9.1 Reporting to the user's mobile phone



GSM Communications > SMS DIAL Reporting

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

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

1. The system activates the siren/bell. The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.
2. The system attempts to send an SMS text message (if programmed), containing the violated name. The system will send SMS text messages regarding each violated zone separately.
 - a) If the user phone number is unavailable, it will attempt to send the SMS text message to the next listed user phone number, assigned to the same zone as the previous one. The user phone number may be unavailable due to the following reasons: mobile phone was switched off or was out of GSM signal coverage.
 - b) By default, the system will continue sending the SMS text message to the next listed user phone numbers in the priority order. The system try to send the SMS text message as many times as programmed.
3. If programmed, the system attempts to ring the first user phone number via GSM. The system will dial regarding each violated zone separately. The system will dial the next listed user phone number, assigned to the same zone. The user can be unavailable due to the following reasons: Mobile phone was switched off, mobile phone was out of GSM signal coverage or provided "busy" signal.
- d) The system will continue dialing the next listed user phone numbers in the priority order. The system will dial again as many times as programmed and the same order as phone numbers listed in the memory if it end up with all unsuccessful attempts to dial to the user.



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

SMS/autodial Phone Number

ID	Events	SMS Notifications to USER								Auto DIAL to USER							
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
2	System Open/Close (CID 400 group)	✓															
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	Input/Zone3 Alarm/Restore	✓															
10	Input/Zone4 Alarm/Restore	✓															

Limit of alarm dialing: 10

☒ SMS forwarding to Tel.1

☒ Show Object Name

☒ Show Zone Number

☒ Show Event Time

☒ Show CID Code

Tel1... Tel8: SMS messages will be send and calls will be made to these phone numbers in case of these alarm events. User numbers should be entered with international code. ([country code][area code][local number]) Without symbol '+'. E.g. the mobile number of user in United Kingdom is +44 (0) 113 xxx xxxx, so Correctly entered user number: 44113xxxxxxx

Limit of alarm dialing: Indicate maximum number of unsuccessful calls

SMS forwarding to Tel.1 SMS from the module resending to the other phone number

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

The index of phone number SMS Notifications to USER: SMS reporting to selected index of telephone number is enabled.

Auto DIAL to USER: Auto DIAL to selected index of telephone number is enabled.

e.g. Call to Tel1 in case of Input/Zone2 Alarm/ Restore

SMS Notifications to USER: SMS reporting to selected index of telephone number is enabled.

Auto DIAL to USER: Auto DIAL to selected index of telephone number is enabled. e.g. Call to Tel1 in case of Input/Zone1 Alarm/ Restore

Tel1... Tel8: SMS messages will be send and calls will be made to these phone numbers in case of these alarm events. User numbers should be entered with international code. ([country code][area code][local number]) Without symbol '+'. E.g. the mobile number of user in United Kingdom is +44 (0) 113 xxx xxxx, so Correctly entered user number: 44113xxxxxxx

Limit of alarm dialing: Indicate maximum number of unsuccessful calls

SMS forwarding to Tel.1 SMS from the module resending to the other phone number

Show Object Name: Object name will be displayed in the SMS message

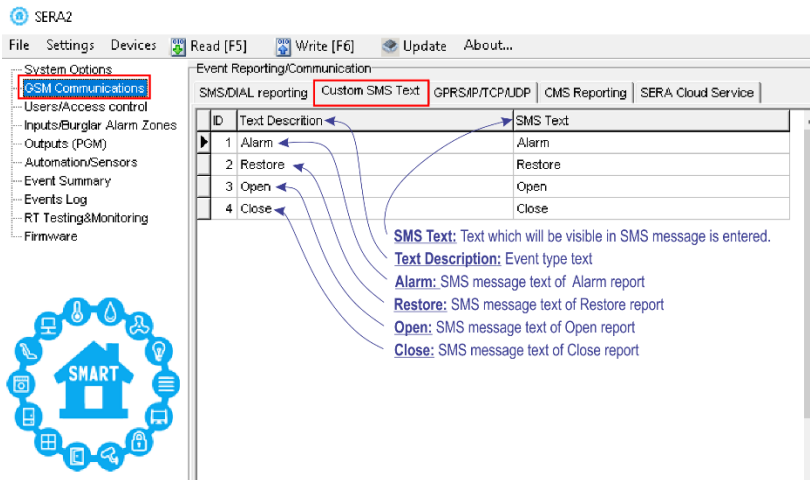
Show Zone Number: Zone number will be displayed in the SMS message

Show Event Time: Event time will be displayed in the SMS message

Show CID Code: Report Contact ID code

5.9.2 Custom SMS Text





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

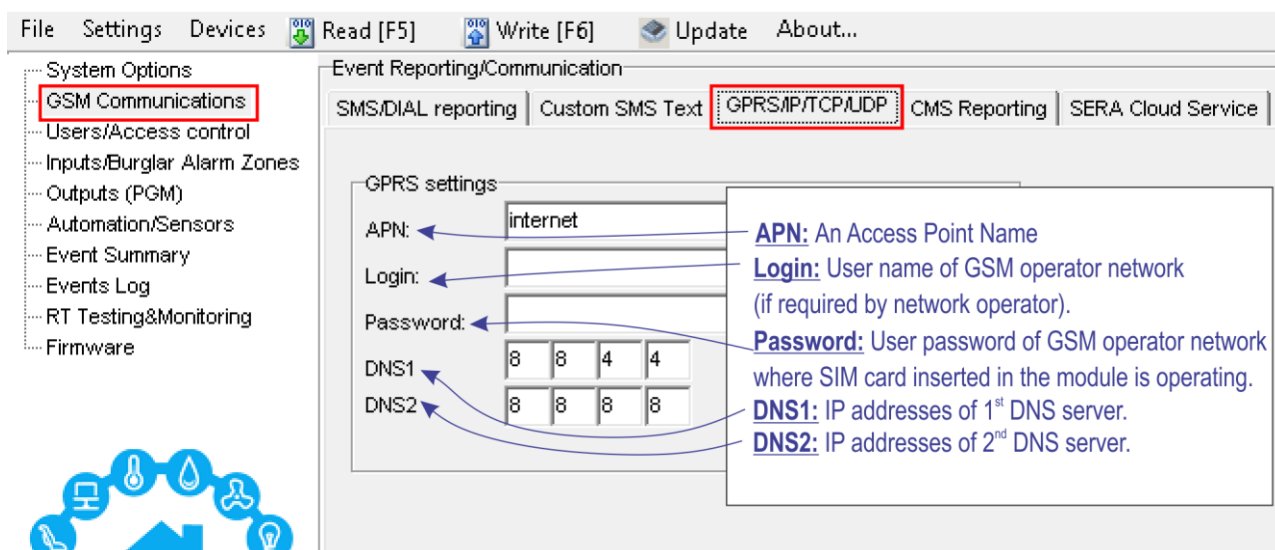
Close: SMS message text of Close report

5.10 Reporting to the Central Monitoring Station



5.10.1 GPRS/ IP/ TCP/ UDP details programming





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.

5.10.2 Central Monitoring Station details programming



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

GSM Communication > CMS Reporting

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

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

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

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

Data Messages – Events

The system supports the following communication methods and protocols:

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

SMS –SMS to User text format.

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

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

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

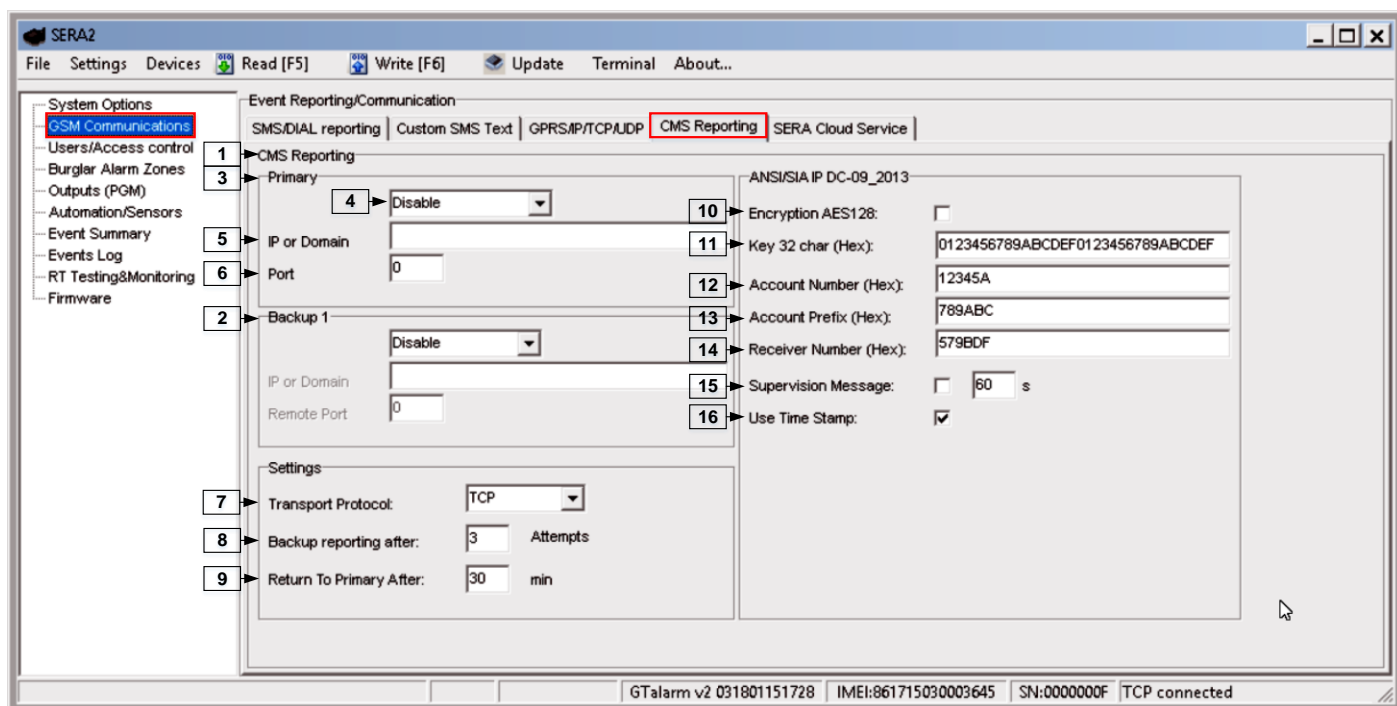


Figure 48 the example of GSM Communication > CMS Reporting window

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.

Table 7 Explanation of every field in "CMS Reporting" window

1	CMS Reporting	Primary central monitoring station settings
2	Backup 1	
3	Primary	Primary central monitoring station settings
4	GPRS or Disable	Data transmitting to the primary CMS via GPRS network or data transiting Disable
5	IP or Domain	The IP address xxx.xxx.xxx or domain name of the receiver station.
6	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.
2	Backup 1	Backup 1 central monitoring station settings
7	Transport Protocol (TCP or UDP)	The used link protocol: UDP (datagrams exchange without connection) or TCP (connected mode).
8	Backup reporting after n attempts	If communication with primary central monitoring station (CMS) is disable, switch to backup CMS after n attempts
9	Return To Primary After n min	Return To Primary After n min
10	Encryption AES128	The "Encryption" option validates the encryption of messages. If this option is enabled, the encryption key must be defined.
11	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.
12	Account Number (Hex)	mandatory, consists of 3-16 hexadecimal digits
13	Account Prefix (Hex)	Optional, consists of 6 hexadecimal digits maximum.
14	Receiver Number (Hex)	Optional, consists of 6 hexadecimal digits maximum.
15	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.
16	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.

5.11 Event Summary (Events)



Event Summary (Events)

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

1	2	3	4	5	6	7
ID	Name of Status Event	Code	Enable	Alarm SMS Text	Restore SMS Text	Type
1	A non-specific medical condition exists	100	<input checked="" type="checkbox"/>	Medical Alarm	Medical Restore	SER
2	Emergency Assistance request	101	<input checked="" type="checkbox"/>	Personal Emergency	Personal Emergency	NONE
3	A user has failed to activate a monitoring device	102	<input checked="" type="checkbox"/>	Fail to report in	Fail to report in	USER
4	A non-specific fire alarm condition exists	110	<input checked="" type="checkbox"/>	Fire Alarm	Fire Restore	ZONE
						NUM

Figure 49 the example Event Summary (Events) window

Table 8 Explanation of every field in "Event Summary" window

2	ID	Report sequence number												
3	Name of Status Event	Event (report) name												
4	Code	Report Contact ID code.												
5	Enable	The indicated report will be sent when it is checked.												
6	Alarm SMS Text	Alarm text which will be visible in SMS message is entered.												
7	Restore SMS Text	Restore text which will be visible in SMS message is entered.												
8	Type	<table> <tr> <td>9</td><td>None</td><td></td></tr> <tr> <td>10</td><td>USER</td><td>Refer to USER Report Options</td></tr> <tr> <td>11</td><td>ZONE</td><td>Refer to Zone Report Options</td></tr> <tr> <td>12</td><td>NUM</td><td>Refer to Numerical Report Options</td></tr> </table>	9	None		10	USER	Refer to USER Report Options	11	ZONE	Refer to Zone Report Options	12	NUM	Refer to Numerical Report Options
9	None													
10	USER	Refer to USER Report Options												
11	ZONE	Refer to Zone Report Options												
12	NUM	Refer to Numerical Report Options												

1.1. RT Testing & Monitoring. Hardware.



RT Testing & Monitoring > Hardware

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

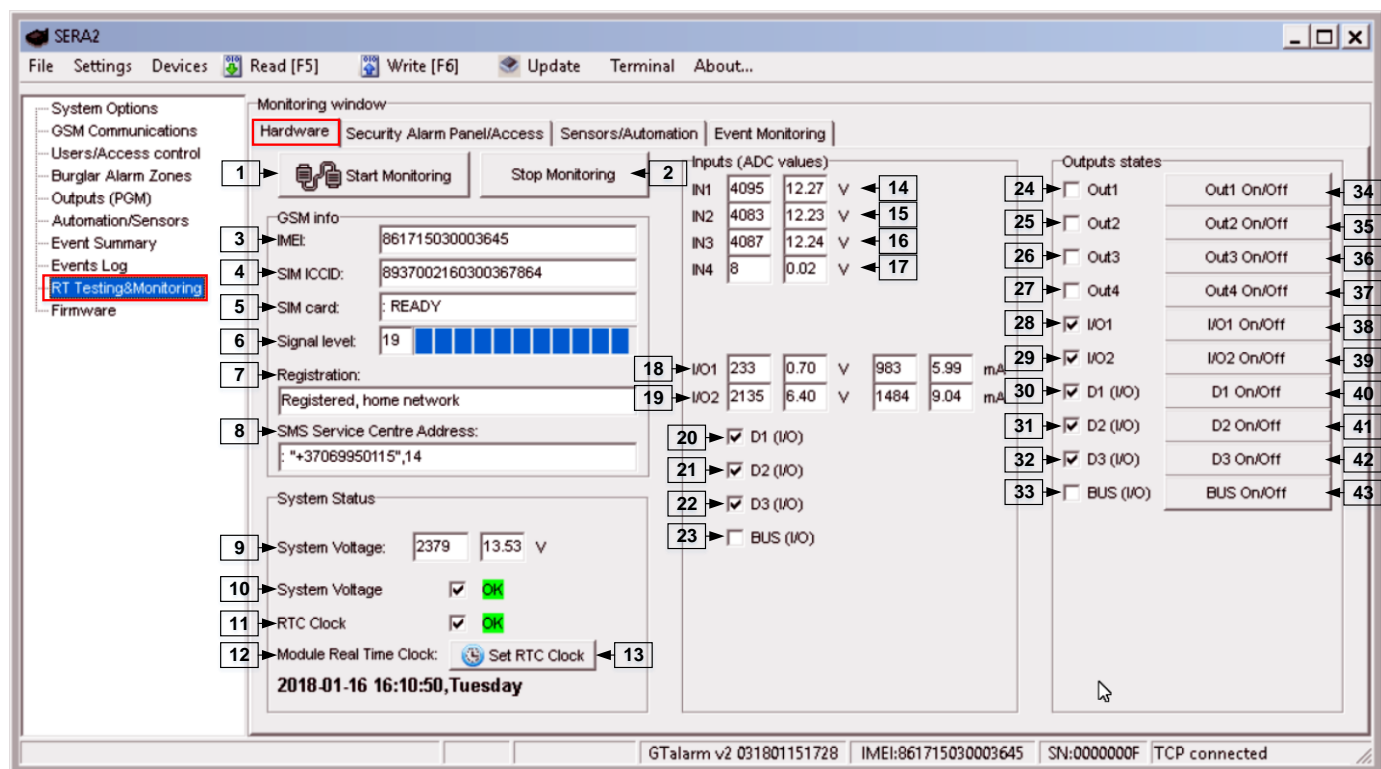


Figure 50 The example of RT Testing & Monitoring > Hardware window

Table 9 Explanation of every field in "Hardware" window

1	Start Monitoring	Pressing Start Monitoring button starts the monitoring of the module.
2	Stop Monitoring	Pressing Stop Monitoring button stops the monitoring of the module.
3	IMEI	IMEI number of GSM modem available in the module

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

5.12 RT Testing & Monitoring Security Alarm Panel/ Access



RT Testing & Monitoring > Security Alarm Panel/ Access

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

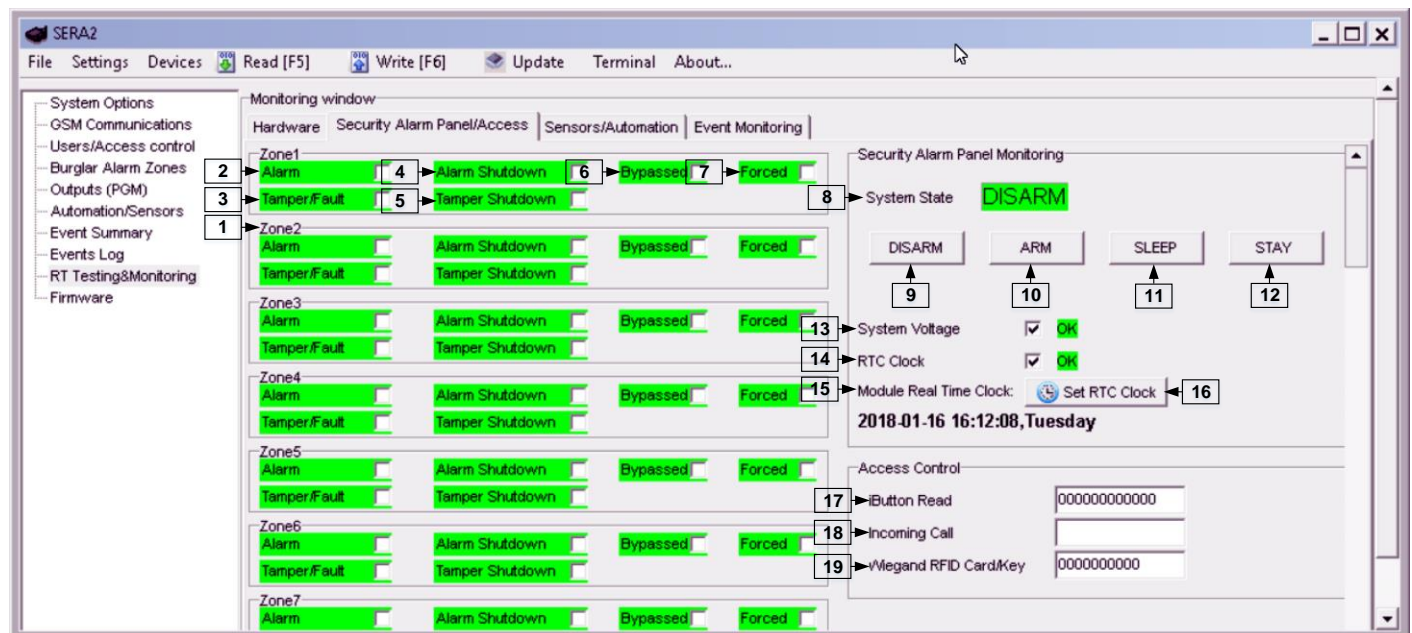


Figure 51 the example of RT Testing & Monitoring > Security Alarm Panel/ Access window

If the checkbox is checked and the color is red the trouble is indicating. If color is green, trouble is not indicated. The text nearby indicates the trouble.

Table 10 Explanation of every field in "Security Alarm Panel/ Access" window

1	Zone1...Zone32	Zone number
2	Alarm	If checked and the color is red the zone is alarmed
4	Alarm Shutdown	If checked and the color is red alarm shutdown for the zone is activated. Allowable number of the same alarm events is reached and the same events will not be reported.
6	Bypassed	If checked and the color is red, the zone is bypassed.
7	Forced	If checked and the color is red, the zone is forced
3	Tamper/Fault	If checked and the color is red, the zone is tampered.

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

5.13 Automation & Sensors Programming



The most important information due to automation with the module GTalarm2

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

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

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

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

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

Step by step to set the parameters of security system:

Installation:

- Install the module GTalarm2 and sensors (PIR, smoke detectors, door contacts
- Connect the GSM antenna to the antenna connector. Insert the SIM card in the SIM card holder. Ensure that PIN request function is disabled. Connect the battery
- Connect the power supply
- Connect the sensors (PIR, smoke detectors, door contacts) to the module GTalarm2, according connecting diagrams
- Connect Bell, Siren to the output of the GTalarm2, according connecting diagram
- Connect Wiegand keypad and RFID reader, according connecting diagram

Configuration:

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

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



How to connect sensor's to the module:

1. Double click on the selected sensor's line.
2. Click on "Sensor type/ hardware location" and default sensor settings appear.

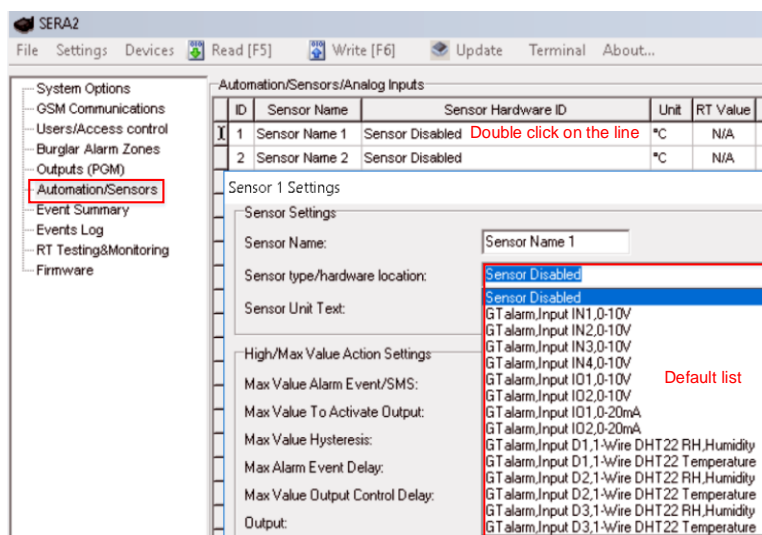


Figure 52 the example of Automation/Sensors (Automation/Sensors/Analog Inputs) window

3. 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.
4. Click "Read".

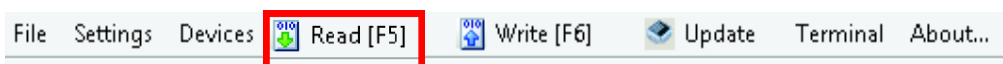


Figure 53 How to find required Read icon.

5. The connected sensors will appear in the list.

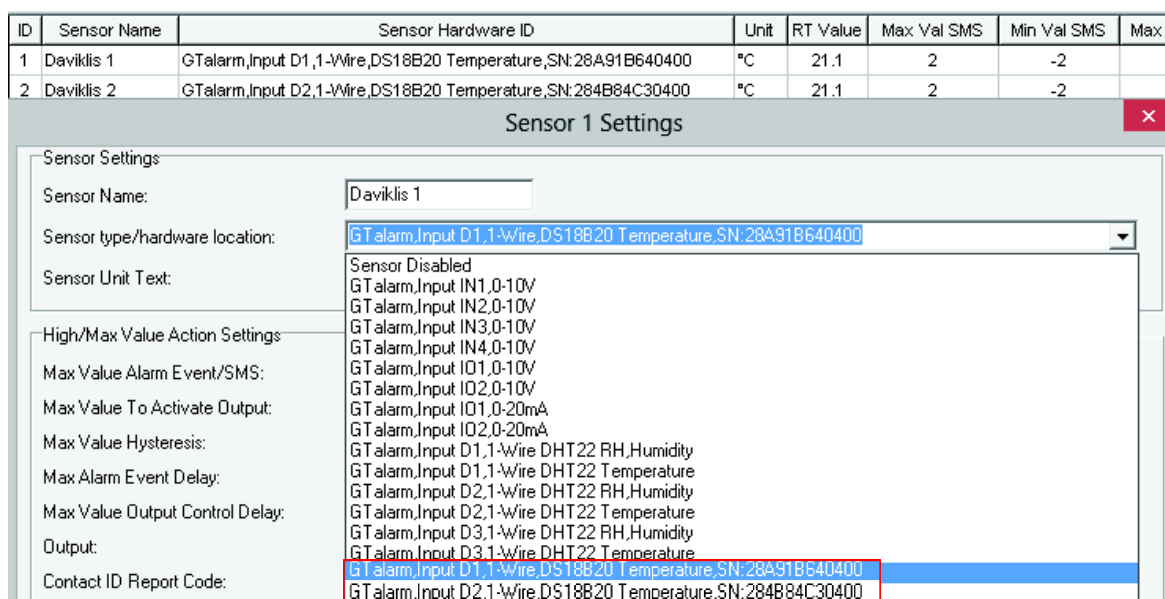


Figure 54 the example of Automation/Sensors (Automation/Sensors/Analog Inputs) window
How to set sensor's parameters:

Double click on the selected sensor's line will show selected sensor's configuration window.

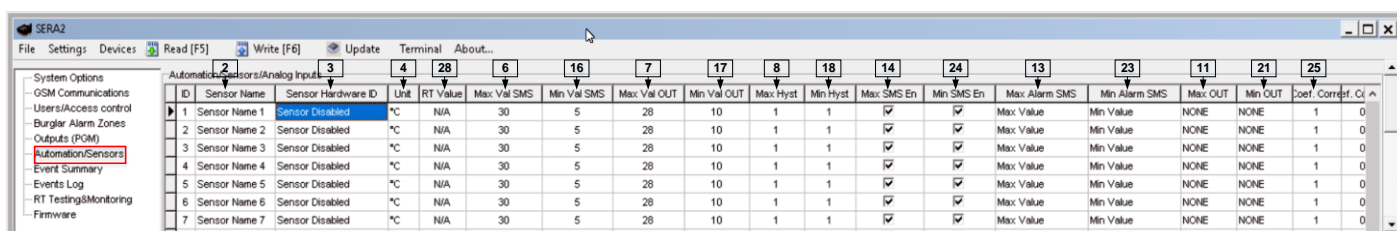


Figure 55 the example of Automation/Sensors (Automation/Sensors/Analog Inputs) window

For example double click on "Sensor Name 1" line will show "Sensor 1 Settings" window. The required parameters of the sensor 1 can be set in that window.

Sensor 1 Settings

1 Sensor Settings

2 Sensor Name: Sensor Name 1

3 Sensor type/hardware location: Sensor Disabled

4 Sensor Unit Text: °C

5 High/Max Value Action Settings

6 Max Value Alarm Event/SMS: 30

7 Max Value To Activate Output: 28

8 Max Value Hysteresis: 1

9 Max Alarm Event Delay: 10000 ms

10 Max Value Output Control Delay: 1000 ms

11 Output: NONE

12 Contact ID Report Code: 158

13 Alarm Event SMS Text: Max Value

14 Enable Alarm Event/SMS ☒

15 Low/Min Value Action Settings

16 Min Value Alarm Event/SMS: 5

17 Min Value To Activate Output: 10

18 Min Value Hysteresis: 1

19 Min Alarm Event Delay: 10000 ms

20 Min Value Output Control Delay: 1000 ms

21 Output: NONE

22 Contact ID Report Code: 159

23 Alarm Event SMS Text: Min Value

24 Enable Alarm Event/SMS ☒

25 X - Multiplier 1

26 Y - Offset 0

Equation: Temperature=X*ADC+Y

27 OK

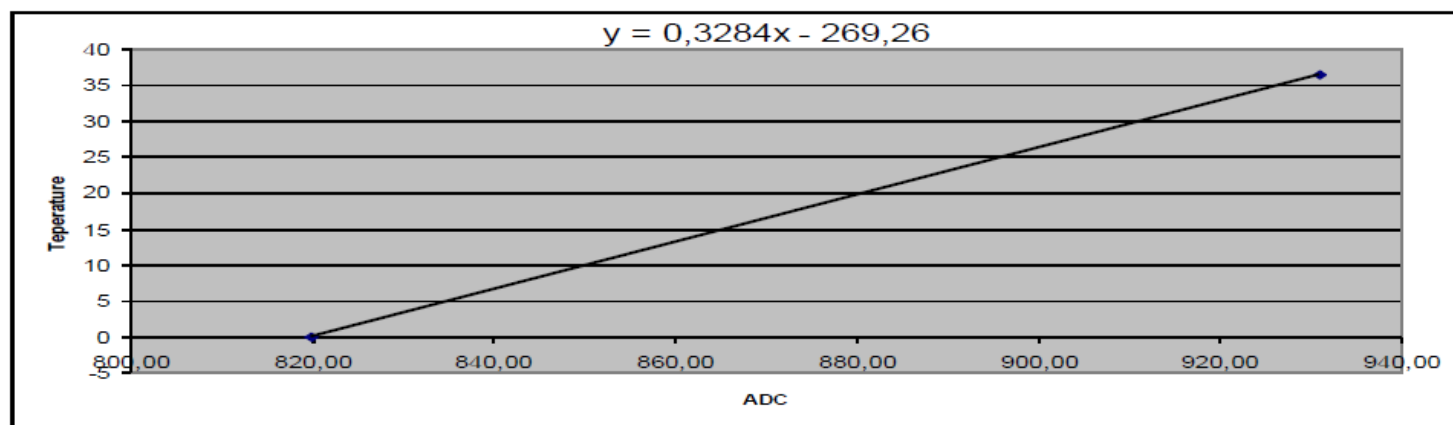
Figure 56 the example of Automation/Sensors (Automation/Sensors/Analog Inputs) window

Table 11 Explanation of every field in "Automation/ Sensors" window

2	Sensor Name	Sensor name
3	Sensor Type/ Hardware location= Sensor Hardware ID	Select the sensor type hardware location Location of sensor connected to the module. Select connected sensors Sensor disabled GTalarm, Input IN1...IN4, 0-10V Voltage input IN1... IN4, 0-10V assigned GTalarm, Input I/O1...I/O2, 0-10V Voltage input. I/O1...I/O2 0-10V assigned GTalarm, Input I/O1...I/O2, 0-20mA Current I/O1...I/O2 , 0-20mA assigned GTalarm, Input D1...D3, 1-Wire DHT22 RH, Humidity Humidity assigned GTalarm, Input D1...D3, 1-Wire DHT22 RH, Temperature Temperature assigned 1-Wire Temperature sensors Digital input D1...D3, 1-Wire DS18B20 Temperature sensor
4	Sensor Unit Text= Unit	Sensor Unit Text
6	Max Value Alarm Event/ SMS= Max Val SMS	Maximum allowable temperature value, which will be reported.
7	Max Value To Activate Output= Max Val OUT	Maximum allowable temperature value, which will activate the selected output
8	Max Value Hysteresis= Max Hyst	Temperature hysteresis value is indicated.
9	Max Alarm Event Delay= Max SMS Delay
10	Max Value output Control Delay= Max OUT Delay
11	Output= Max OUT	The output which will be activated, when the maximum allowable temperature value will be reached
12	Contact ID Report Code= Max CID	Report Contact ID code
13	Alarm Event SMS Text= Max Alarm SMS	Text, which will be visible in SMS message in case of set temperature excess, is entered.
14	Enable Alarm Event/ SMS= Max SMS en	The indicated report will be sent when it is checked.
16	Min Value Alarm Event/ SMS= Min Val SMS	Minimum allowable temperature value, which will be reported.
17	Min Value To Activate Output= Min Val OUT	Minimum allowable temperature value, which will activate the selected output.
18	Min Value Hysteresis= Min Hyst	Temperature hysteresis value is indicated.
19	Min Alarm Event Delay= Min SMS Delay
20	Min Value Output Control Delay= Min OUT Delay

21	Output= Min OUT	The output which will be activated, when the minimum allowable temperature value will be reached
22	Contact ID Report Code= Min CID	Report Contact ID code
23	Alarm Event SMS Text= Min Alarm SMS	Text, which will be visible in SMS message in case of set temperature excess, is entered.
24	Enable Alarm Event/ SMS= Min SMS en	The indicated report will be sent when it is checked.
25	X-multiplier= Mult Coef Correction	X-multiplier coefficient. Following the equation "Temperature=X*ADC+Y" to calculate X and Y coefficients. Measure temperature in two points at least.
26	Y-offset= Sum Coef Correction	Y-offset coefficient. Following the equation "Temperature=X*ADC+Y" to calculate X and Y coefficients. Measure temperature in two points at least.
	Temperature= X*ADC+Y	
12	Contact ID Report Code= Max CID	Max and Min Contact ID report codes. Report codes are the Ademco CID, SIA DC09 format. The module can automatically program a set of default report codes. The Contact ID Reporting Format can be modified and changed. Enter any of the desired text in the "Alarm SMS Text" field.
22	Contact ID Report Code= Min CID	
28	RT Value	After the connection to the module and after clicking on a read icon the real time value of the sensor will be displayed in this field.

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



5.14 Data Transmitting to Server & Remote Control



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

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

5.14.1 TCP/ IP Remote Control



GSM Communication > SERA Cloud Service

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

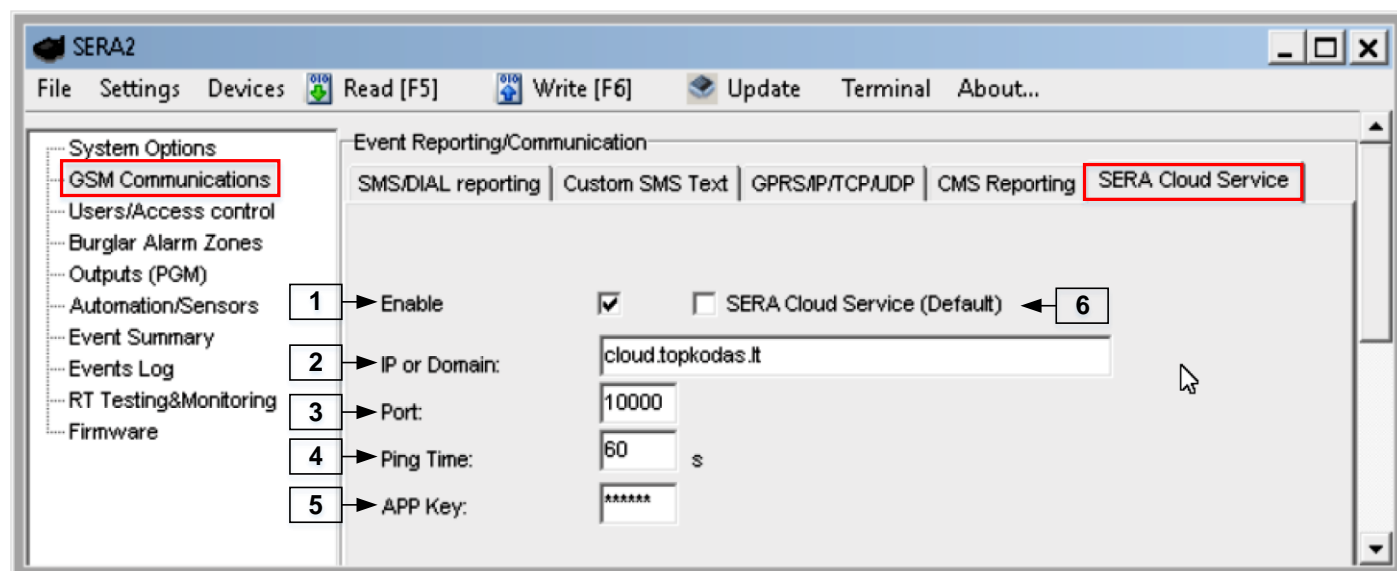


Table 5 explains every field in the of Reporting SMS & DIAL > TCP/ IP Remote Control window

Table 12 Explanation of every field in "TCP/ IP Remote Control" window

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

5.15 Events Log



Events Log

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

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

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

Communication with monitoring station status.

1		2	
Read Event Log		Clear Event Log	
1043	Event:1234:1:158:00:009	Time:2016-11-12 13:24:49	Note: Sensor9, :85.00, High Temp Alarm, Zone:009
1044	Event:1234:1:602:00:000	Time:2016-11-12 13:30:00	Note: , Periodical test
1045	Event:1234:1:660:00:006	Time:2016-11-12 13:30:00	Note: , GSM signal strength
1046	Event:1234:1:627:00:000	Time:2016-11-12 13:41:14	Note: , Program mode entry
1047	Event:1234:1:305:00:000	Time:2016-11-12 13:43:42	Note: , System Reset
1048	Event:1234:1:158:00:00C	Time:2016-11-12 13:43:49	Note: Sensor12, :85.00, High Temp Alarm, Zone:00C
1049	Event:1234:1:158:00:00D	Time:2016-11-12 13:43:51	Note: Sensor13, :52.80, High Temp Alarm, Zone:00D
3	4	5	6

Figure 58 the example of the Events Log window.

Table 5 explains every field in the Events Log window.

Table 13 Explanation of every field in "Events Log" window

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

To export the event log to .log file or clear it, please refer to the following configuration method.

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



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

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

How does it works?

Remote connection is established via GPRS using TCP/IP protocol;

The GSM module connects to the internet via a GPRS to SERA cloud server [cloud.topkodos.lt].
The connection is established by the SERA2 configuration tool using unique id of the module UID IMEI.

GTalarm2 ↔ SERA Cloud Server [cloud.topkodos.lt] ↔ SERA2

Or

GTalarm2 ↔ SERA Cloud Server [cloud.topkodos.lt] ↔ Standard web browser. Firefox, Chrome e.t.c

Sera Cloud Server opens tunnel between two module GTalarm2 and SERA2 or APP and lets them communicate to each other via TCP protocol.

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

Steps to activate Remote control over internet:

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

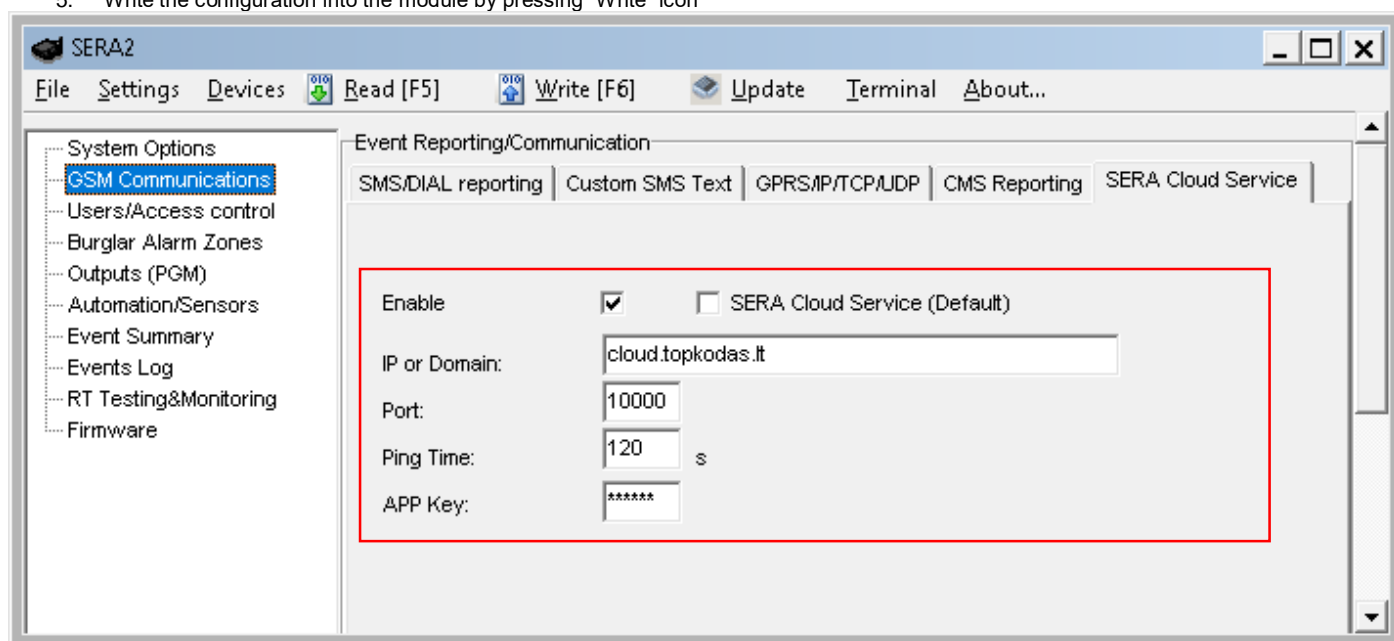


Figure 59 How to find GSM Communication> GPRS/IP/TCP/UDP window

6. Go to "Reporting SMS & Dial" window, "TCP/IP Remote control" table.
7. Public IP or domain must be entered. Enter remote port, ping time, encryption key and enable the communication.
8. If needed, APN/Password/Login/IP/Domain/ Port /PING time /KEY can be set by SMS commands

GPRS network settings

INST000000_008_APN#LOGIN#PSW#

008= command code (GPRS network settings)

APN=31 symbols

LOGIN=31 symbols

PSW=31 symbols

Remote control of the module over the Internet.

INST000000_009_ADDR#PORT#PING#KEY#

009= command code (Remote control of the module over the Internet)

ADDR = the format of IP address xxx.xxx.xxx.xxx (the numbers from 0 to 255 should be separated by dot or domain text length of up to 47 characters)

PORT= TCP port number from 1 to 65535

PING= communication control ping time from 30 to 9999s

KEY= encryption key. Encryption key should be the same as server key. Default 123456

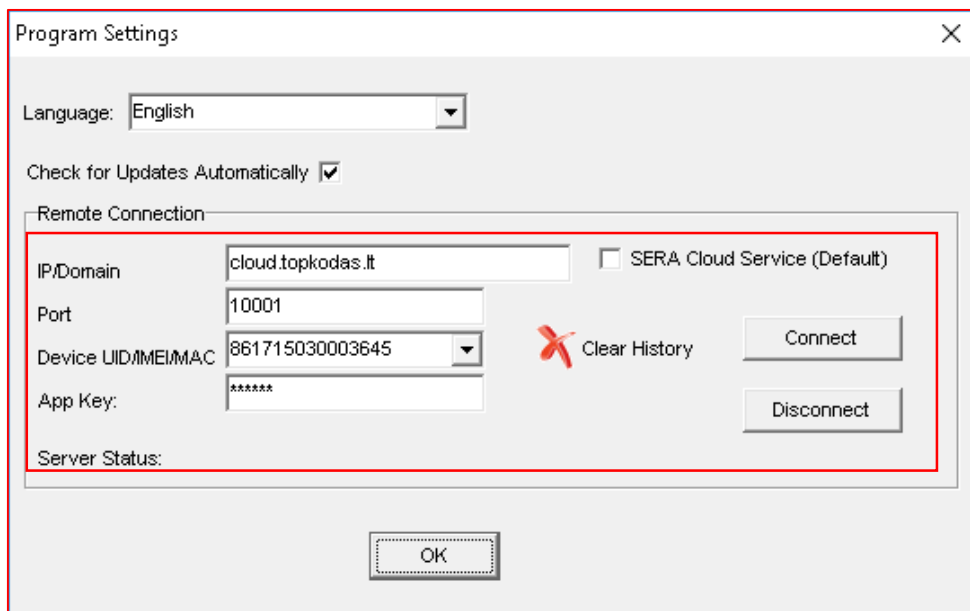


Figure 60 Command line> Settings

9. Check SERA cloud service checkbox.
10. Enter Device UID/IMEI. Press **Connect** button and wait till connection will be established. In the bottom in the task bar appears TCP connected notification.

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

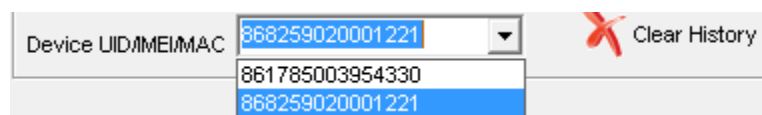


Figure 61 Command line> Settings> Clear history

5.17 Testing & Monitoring Automation



5.17.1 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.

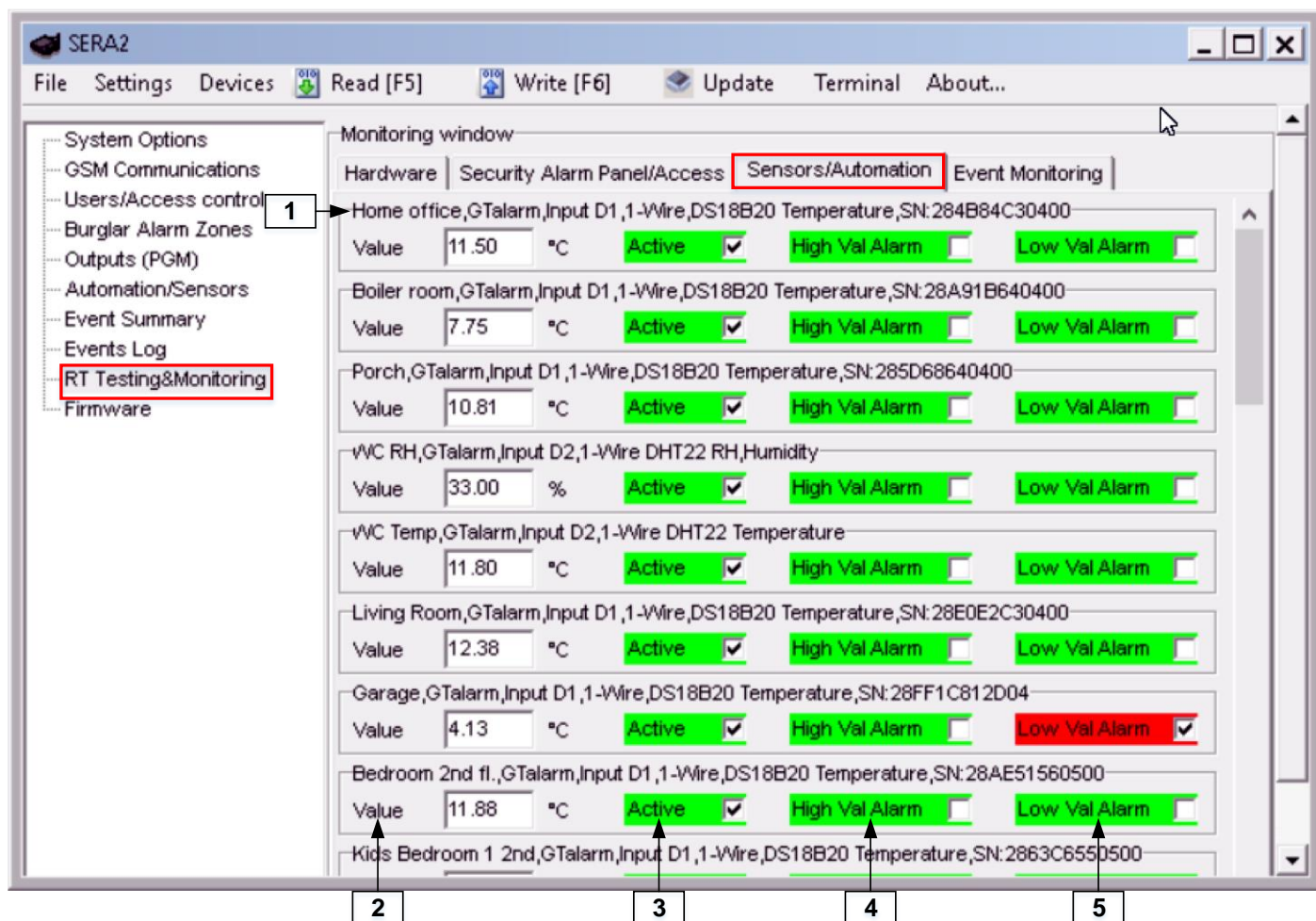


Figure 62 the example of RT Testing & Monitoring > Sensors/ Automation window

Table 14 Explanation of every field in "Sensors/ Automation" window

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

5.17.2 Realtime Testing & Monitoring > Event Monitoring



RT Testing & Monitoring > Event Monitoring

The Event Monitoring window will show real time events information

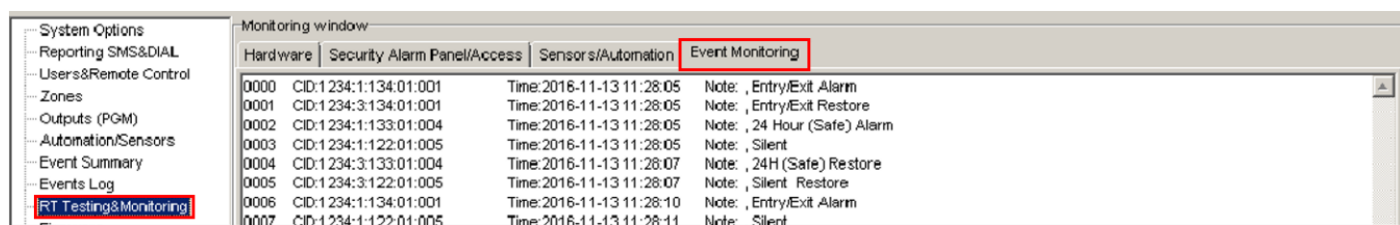


Figure 63 How to find required RT Testing & Monitoring > Event Monitoring window.

0000	CID:1234:1:134:01:001	Time:2016-11-13 11:28:05	Note: , Entry/Exit Alarm
0001	CID:1234:3:134:01:001	Time:2016-11-13 11:28:05	Note: , Entry/Exit Restore
0002	CID:1234:1:133:01:004	Time:2016-11-13 11:28:05	Note: , 24 Hour (Safe) Alarm
0003	CID:1234:1:122:01:005	Time:2016-11-13 11:28:05	Note: , Silent

Figure 64 The example of RT Testing & Monitoring > Event Monitoring window

Table 15 Explanation of every field in "Event Monitoring" window

3	...	Event number
4	CID	Contact ID Code
5	Time	Event date and time
6	Note	Event report text which was indicated.

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



System Options > System Info

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

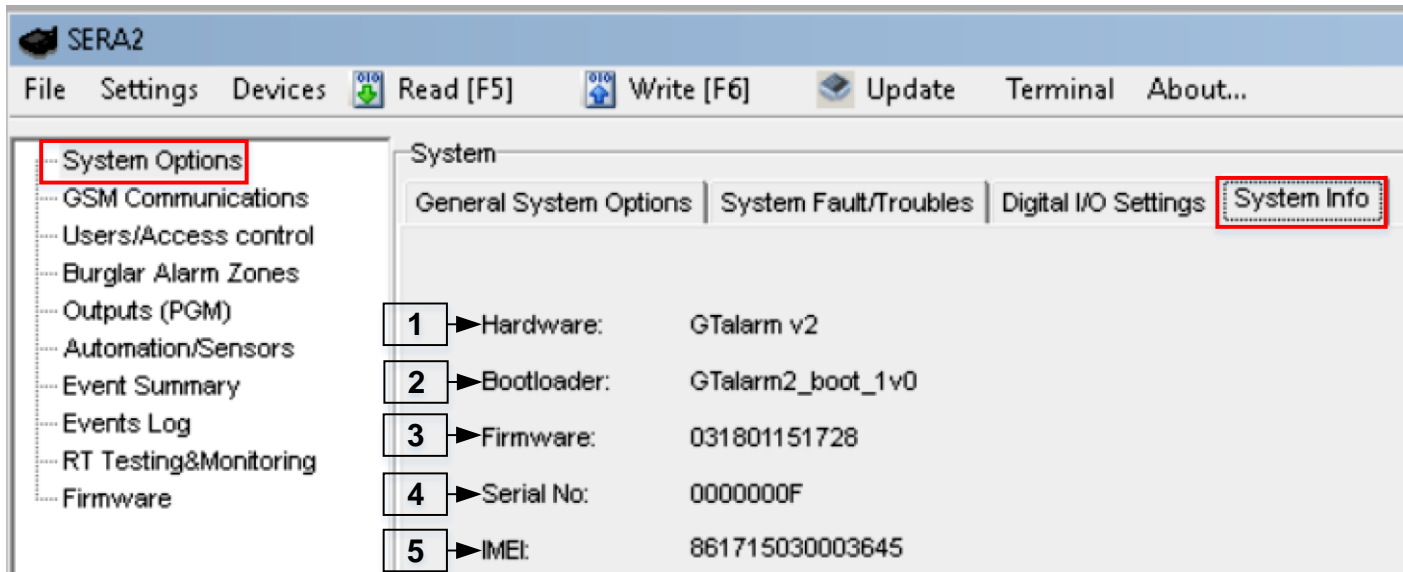


Figure 65 How to find required System Options > System Info window.

Table 16 Explanation of every field in "System Info" window

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

6.1 Firmware Update

Firmware

This window let you update the firmware of the module.

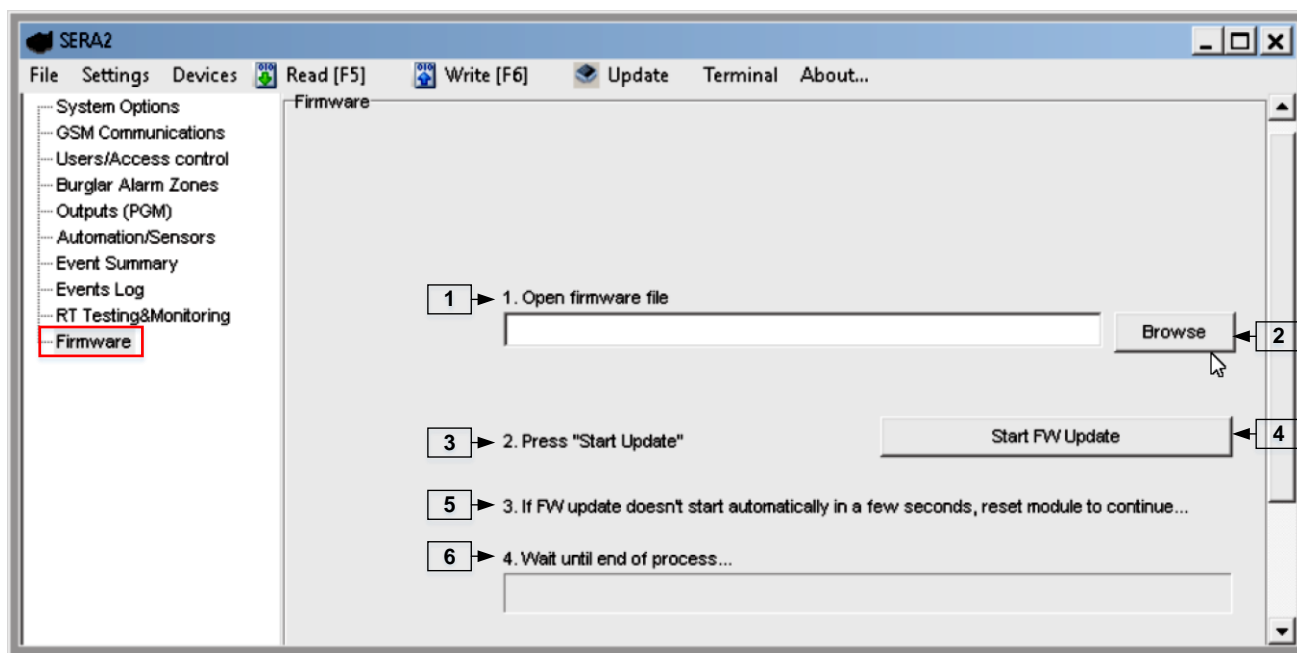


Figure 66 the example of Firmware window

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

7 Recommendations for the user & installer

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

i What should you do, if you noticed, that there is Sensor trouble in the "Event Log" window?
It is comfortable to use "RT Testing&Monitoring" window. Red field indicates sensor's troubles.
Go to Automation/ Sensors window, disabling this sensor and press "Write". Maybe there is the problem with sensor's connection to the module.
If the problem still exist, please read, save and send the configuration to the seller. Describe what and how is connected to zone: 001 and send this information to the seller.

8 Remote control and configuration using SMS Commands



Users allowed:
Control outputs,
Arm/disarm the system or select stay, sleep mode
Bypass zones
Set the time of the module
Request zone test and system state
Forward messages to other number

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

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

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



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

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

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

9 The table of installers commands



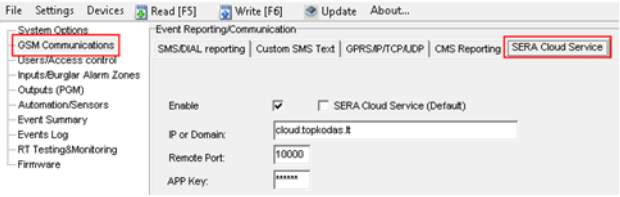
SMS commands with **correct INST password** can be send from any phone number. Keep INST password in secret!



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

Table 17 The table of installers commands

<div>INST000000_001_N#TEL#SMS#DIAL#System</div> <div>open close</div>	<p>Programming of users telephone numbers to send SMS and to make a call if the event occur: 001= programming user's tel. numbers for DIAL and send SMS N = user ID number 1-8 TEL = user's telephone number (max 16 digits) without (+) country code, operator's code and user's telephone number included. The end symbol #; SMS = event filter for sms. 1- send event, 0- don't send event. Sequence of the events 1.2.3...n For example: 001000 DIAL = event filter for DIAL. 1-DIAL if the event occur, 0-don't DIAL Sequence of the events 1.2.3...n For example: 101000 # = delimiter</p> <p>e.g.: INST000000 001 1#37066666666#0001000000#0000011111#</p> <p>Event filter eiliskumas: 1-reserved 2-system open close 10-Input/Zone4 Alarm/Restore</p>
<div>INST000000_002_ID</div>	<p>Delete user's phone number according the user ID number. Phone number used for receive user's information. 002= command code (deleting user's numbers according the user ID number) ID = user ID number from 1 to 8</p>
<div>INST000000 004 ID#TEL#OUT#OPT#NAME#</div>	<p>To enter user's telephone number for remote control via short call</p> <p>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, 1-10. OPT = DIAL function: 0 – disabled 1 – enabled, Sequence from the left to the right</p> <p>OPT: 1-ARM/DIARM 2-Reserved (GTalarm2 =MIC)</p>
<div>INST000000 005 TEL#</div>	<p>To delete user's phone number for remote control, according phone number 005= command code (delete user's phone number for remote control, according phone number) TEL = user's phone number (max 16 digits) without (+) comprised of country code, operator's code and user's telephone number. User's phone number must be the same as in the memory of the module.</p>
<div>INST000000_006_N</div>	<p>Delete user's phone number whose ID number is N. 006= command code (Delete user's phone number according user's ID number) N = user's ID number from 001 to 800.</p>

INST000000_007_P#PER#HH:mm#	Automatic periodical test settings 007= command code (Automatic periodical test) P= 0-test disabled, 1- test period by 24 hours, 2- period by minutes PER= automatic test sending period from 1 to 99999 days or minutes HH=hours 0-23 , mm= minutes 0-59 e.g. INST000000 007 2#1#14:50# The test will be send every 1 minute
INST000000_008_APN#LOGIN#PSW#	GPRS network settings 008= command code (GPRS network settings) APN=31 symbols LOGIN=31 symbols PSW=31 symbols
INST000000 009 ADDR#PORT# INST000000 009 ADDR#PORT#PING#	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 from 1 to 65535 Default parameters is in the picture below. We recommend do not change these parameters. 
INST000000_010_E	To activate the connection to the remote control server 010= command code (To activate the connection to the remote control server) E= 1-enabled, 0-disabled
INST000000_019_N#P	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 10 P = output operation algorithm. 0 – output disabled, 1 – Bell, 2- buzzer, 3- flash led, 4- system state LED, 5-LED „system ready“, 6- Automation & access control, 7- AC OK, 8 – Battery OK, 9- ARM/DISARM 10-alarm indication, 11- Lost Primary chanel 12- Lost secondary chanel 13- Fire sensor 14-RH Sensor trouble , 15- Access Gained
INST000000_020_N	Invert output state 020= command code (outputs inversion) N = output number from 1 to 10.
INST000000_021_N#ST	Output activation or deactivation 021= command code (Output activation or deactivation) N = output number 1-10 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 1-10 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 #	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 NEW_INST_PSW	Change installer's password (Installers password should be changed before exploitation of the module) 090= command code (Change of installer's password) NEW_INST_PSW = New Installer's password.
INST000000 091 NEW_USER_PSW	Change user's password (User's password should be changed before exploitation of the module) 091= command code (Change user's password) NEW_USER_PSW = New user's password.
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 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	SMS from the module forwarding to the other phone number 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 textSMS = sms text that will be send to the referred number. TEL=861611111111 local number arba international format e.g. +370616111111 INST000000 094 +370616111111#Hello SMS text =Latin Charset SMS from the module forwarding to the other phone number094= command code (SMS from the module forwarding to the other referred phone number)TEL = phone number to which will be forwarded sms textSMS = sms text that will be send to the referred number TEL=861611111111 local number arba international format e.g. +370616111111 INST000000_094_+370616111111#Hello international must be with '+' local without'+' SMS text =Latin Charset After this commands could not be other commands like: 094 SMS 030 1 because all messages will be forwarded to other numer "SMS 030 1"
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
INST000000 096	Fire sensors reset.
INST000000_100_N	System state request: 100= command code (System state request) N = System state request type 1- System test request, Request information about the module (: IMEI, FW, LEVEL etc.) 2- the values of active sensors request 3 -Request about active zone states 4 -Request about output states 5 - System state request. The module will send information on input/output states and system state (ARM/DISARM/STAY).

10 The table of users commands



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



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

SERA2

File

Settings

Devices

Read [F5]

Write [F6]

Update

About...

System Options

GSM Communications

Users/Access control

Inputs/Burglar Alarm Zones

Outputs (PGM)

Automation/Sensors

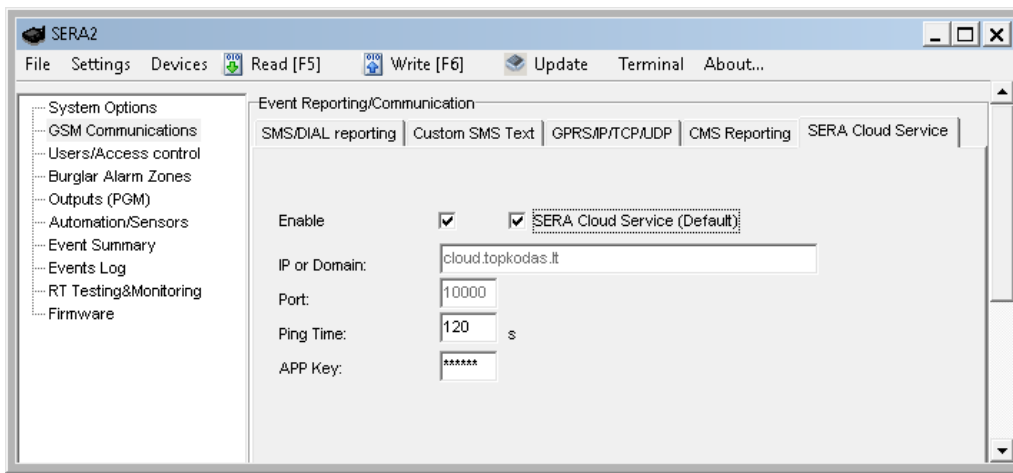
Remote Control Users table

											Temporary access Date/Time window		
ID	En	User Name	Type	User Tel.	iButton Code	RFID Keycard	Keyb Code	OUT	ARM/DISARM	MC	Date En	Start Date	Expiration Date
1	<input checked="" type="checkbox"/>	Master	User	+370000000000	000000000000	0000000000	*****	NONE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26
2	<input type="checkbox"/>		User	+	000000000000	0000000000		OUT1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2019-02-25 16:24:26	2019-02-25 16:24:26

Table 18 The table of user's commands

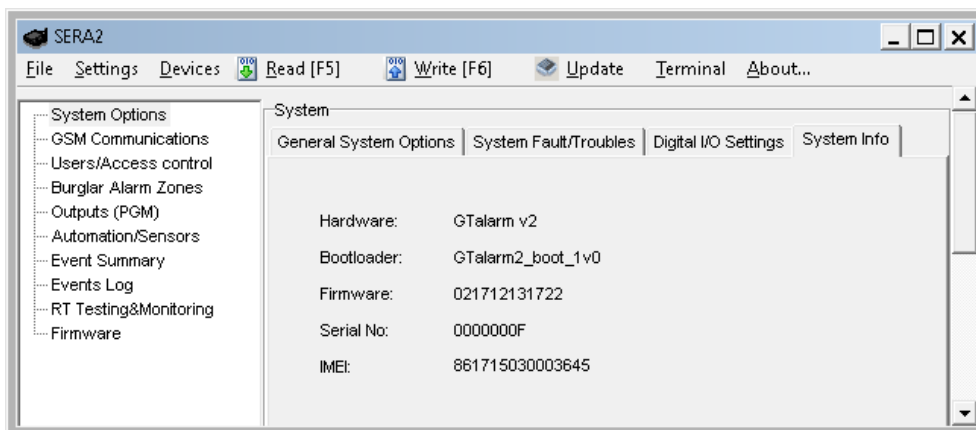
<code>USER123456_020_N</code>	Change state of selected OUT output to the inverted state. Output state changes every time after sending command code. 020= command code (Change state of selected OUT output to the inverted state.) N = output number from 1 to 10.
<code>USER123456_021_N#ST</code>	Activate 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
<code>USER123456_022_N#TIME#</code>	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.
<code>USER123456_030_ST</code>	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
<code>USER123456_031_ZN#BYP</code>	Zone bypassing by sms command 031= command code (Zone bypassing) ZN = zone number from 1 to 32 BYP= 1 – zone bypass 0- zone active.
<code>USER123456_094_TEL#SMS</code>	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
<code>USER123456_100_N</code>	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). Only for the firmware versions > 190926

11 APP configuration



SysName *
 Device UID*
 App Key*
 Object Address

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



12 Warranty Terms and Conditions

SAFETY INSTRUCTIONS FOR SERVICE PERSONS

Use the following list as a guide to find a suitable place for GTalarm2 module:

- Locate the module near a power outlet.
- Select a place that is free from vibration and shock.
- Place the module on a flat, stable surface and follow the installation instructions:
Do NOT locate the module where persons can walk on the secondary circuit cable(s).
Do NOT connect the module to electrical outlets on the same circuit as large appliances.
Do NOT select a place that exposes the module to direct sunlight, excessive heat, moisture, vapors, chemicals or dust.
Do NOT install the module near water (e.g., bathtub, wash bowl, kitchen/laundry sink, wet basement, or near a swimming pool).
Do NOT install the module and its accessories in areas where there is a risk of explosion.
Do NOT connect the module to electrical outlets controlled by wall switches or automatic timers.

AVOID sources of radio interference.

AVOID setting up the equipment near heaters, air conditioners, ventilators, and/or refrigerators.

AVOID locating module close to or on top of large metal objects (e.g., metal wall studs).

Safety Precautions Required During Installation

- NEVER install the module during a lightning storm.
- Ensure that cables are positioned so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain.
- The power supply must be Class II, FAIL SAFE with double or reinforced insulation between the PRIMARY and SECONDARY circuit/ENCLOSURE and be an approved type acceptable to the local authorities. All national wiring rules shall be observed.

Limited Warranty

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

International Warranty

UAB "Topkodas" shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

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

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- Damage incurred in shipping or handling;
- Damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- Damage due to causes beyond the control of UAB "Topkodas" such as excessive voltage, mechanical shock or water damage;
- Damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- Damage caused by peripherals (unless such peripherals were supplied by UAB "Topkodas".);
- Defects caused by failure to provide a suitable installation environment for the products;
- Damage caused by use of the products for purposes other than those for which it was designed;
- Damage from improper maintenance;
- Damage arising out of any other abuse, mishandling or improper application of the products.

Items Not Covered by Warranty

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

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

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

Disclaimer of Warranties

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

WARNING:

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

Out of Warranty Repairs

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

WARNING - READ CAREFULLY

Note to Installers

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

System Failures

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

- Inadequate Installation

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

- Criminal Knowledge

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

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

- Access by Intruders

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

- Power Failure

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

- Failure of Replaceable Batteries

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

- Compromise of GSM network

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

- System Users

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

- **Smoke Detectors**

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

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fire 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 GTalarm2 is not a substitute for property or life insurance. The module GTalarm2 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.