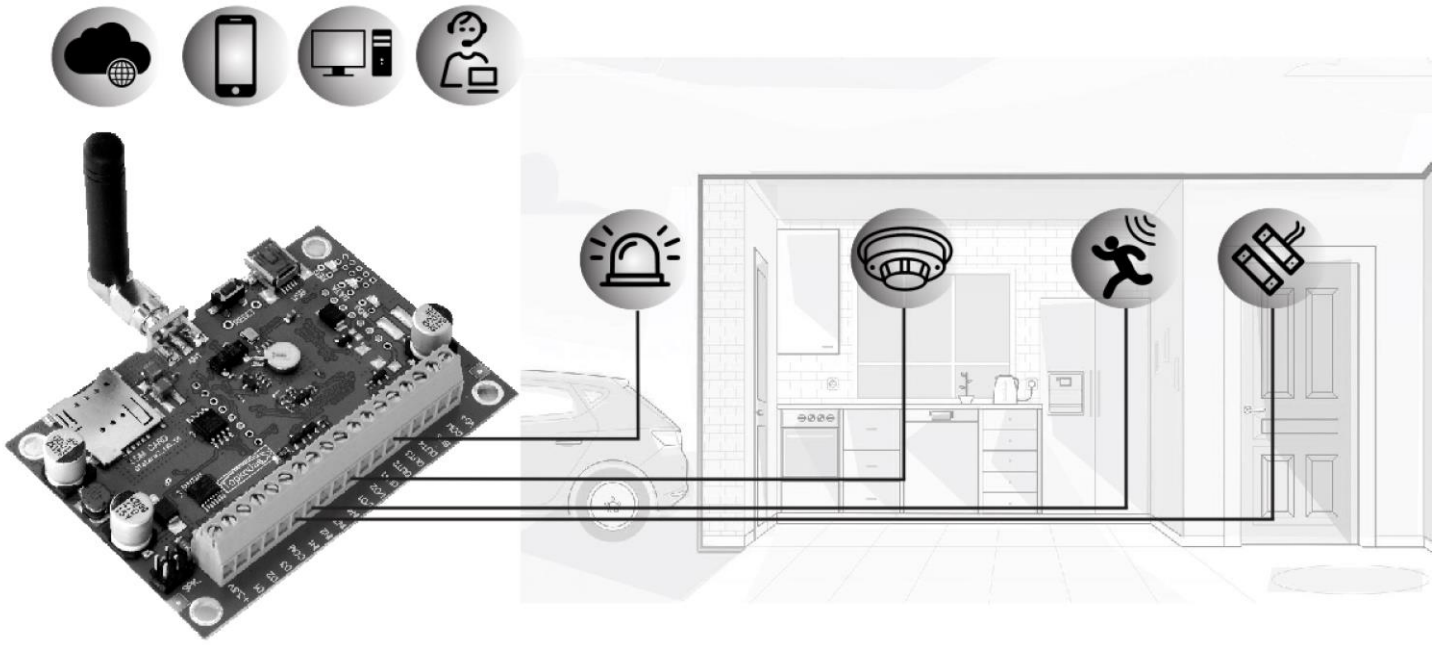
GTalarm2

Application Note: Security, Alarm System



Monitoring, alarm, control.

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

Topkodas

GTalarm2 is a user-friendly security system that monitors your site's detectors and alarms. Fully programmable, the module GTalarm2 allows you to control hundreds of critical security functions from one menu-driven interface.
The system consists of a central control unit, an operating panel, and up to 32 protection points. While monitoring protection points 24 hours a day the controller itself is electronically monitored by trained central monitoring station personnel. If a hazard or security breach occurs, the appropriate authorities (police, fire) are alerted.
All functions are accessed through the system operating panels or through card/key readers.

- Attractive, easy-to-use operating panel.
- Control of up to 32 protection points from one central location.
- Manual activation or deactivation of any function.
- Ability to on in either the AWAY or STAY mode.
- Ability to bypass points for maintenance or service.
- Capacity of up to 800 individual operating panel users, each having various security privileges.
- Capacity of up to 800 individual card/key reader users, each having various levels of access.
- Control and recording of employee access to workplace areas.
- Recording of security-related activities.
- Ability to send messages to up to 8 users.

The GTalarm2 module – the brains of your security system – is a powerful microcomputer that manages every function of your security system. All information about your site's security is stored in this unit or in the server.

Features of the module GTalarm2

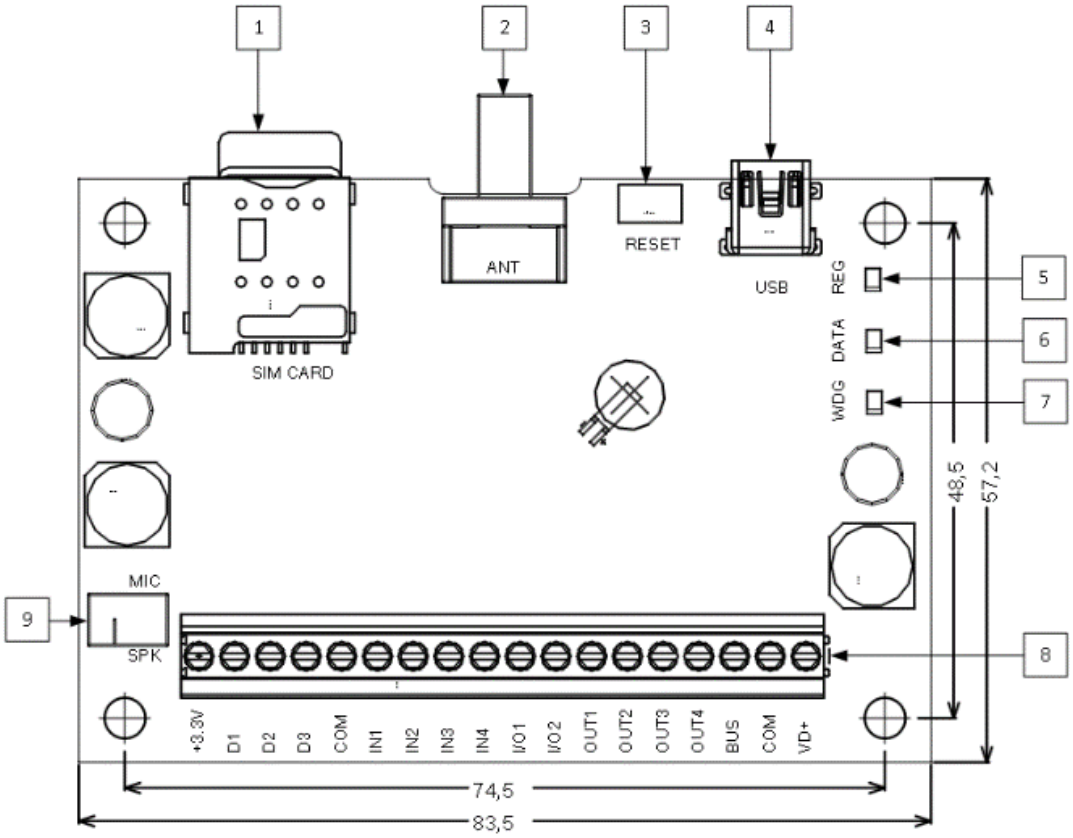
- Communication via SIA IP DC09 protocol
- 6 on-board zones. Input EOL/NO/NC and Tamper
- Tamper supervision available, ensuring product is always secure
- Built-in access control features
- Automatic Daylight Savings Time feature
- I/O1 and I/O2 can be used as a 2-wire smoke input
- 4 Analog inputs (pull up 5.1K) 0-10V
- 2 Analog Input/ Output , 0-10V , 0-20mA
- 3 Digital Inputs/Outputs 3.3V , 20mA,
- Wiegand interface for Keypad and RFID card reader
- Dallas 1-Wire Bus
- 4 PGM outputs 24V/1000mA. Open Drain.
- Digital expansion module BUS.
- In-field firmware upgrade via USB, SERA, Cloud Remote Service
- 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 reset

The meaning of icons in the manual:

!	i	📖
Very important	Important	About the manual

Contents

1.1 General view of the module



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

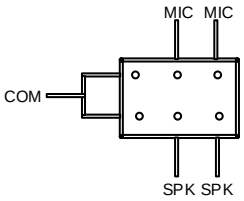


Figure 1 GTalarm2 PCB Layout

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

1.2 Meaning of LEDs and contacts

Table 1 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.

1.3 First steps to prepare GTalarm2 module and Sera2 software

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.

Install configuration software SERA2.

SERA2 configuration and monitoring 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]

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 micro 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

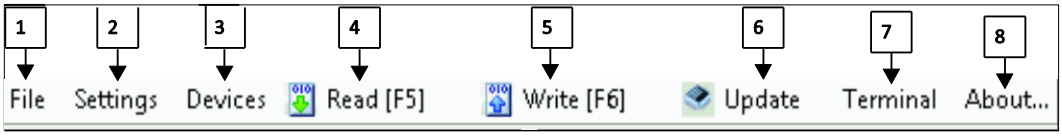


Figure 2 The meaning of icons

Each time after configuring the module press Write 5 icon thus the software SERA2 will write configuration changes into the module!

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.

2 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.

Power supply application note:

Application Note: Power Supply TPS12 comnnection to GTalarm2

Power supply installation manual:

Installation Manual TPS12

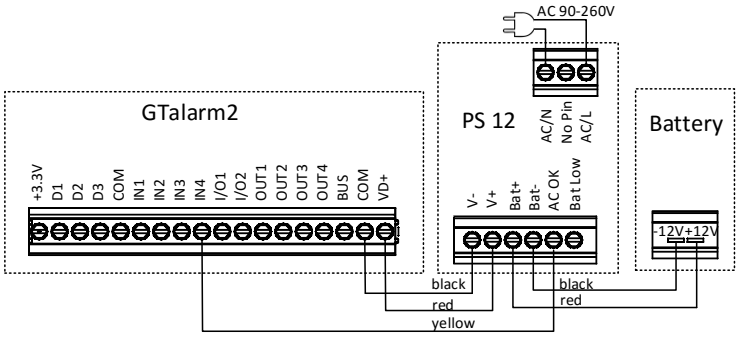


Figure 3Power supply connection

3 Application examples

3.1 Home security system

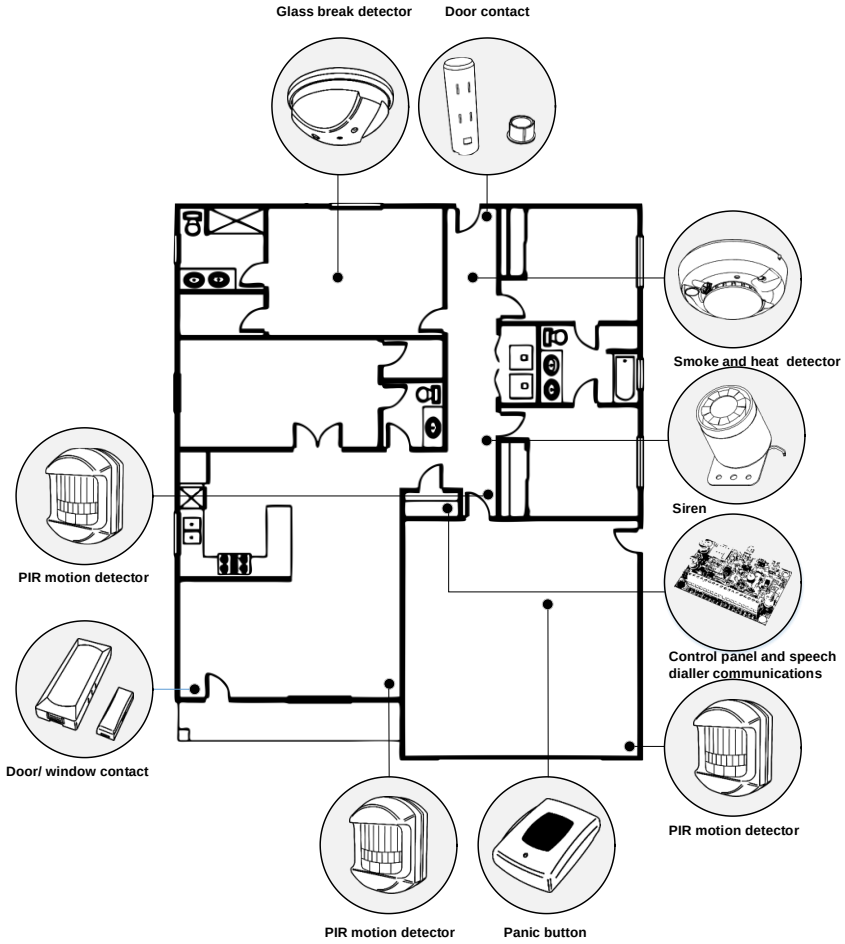


Figure 4 Example of home security system

Up to 32 standard security system detectors could be connected to the GTalarm2 module's inputs. The system can be arm in STAY, AWAY modes. It is possible to connect local alarm devices: sirens.

Inputs:

4 analog inputs (In1...In4 (0-10V)) that can be used or 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)) that can be used or used 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 Wiegand interface DATA0/ DATA1, FID reader, Keyboard.

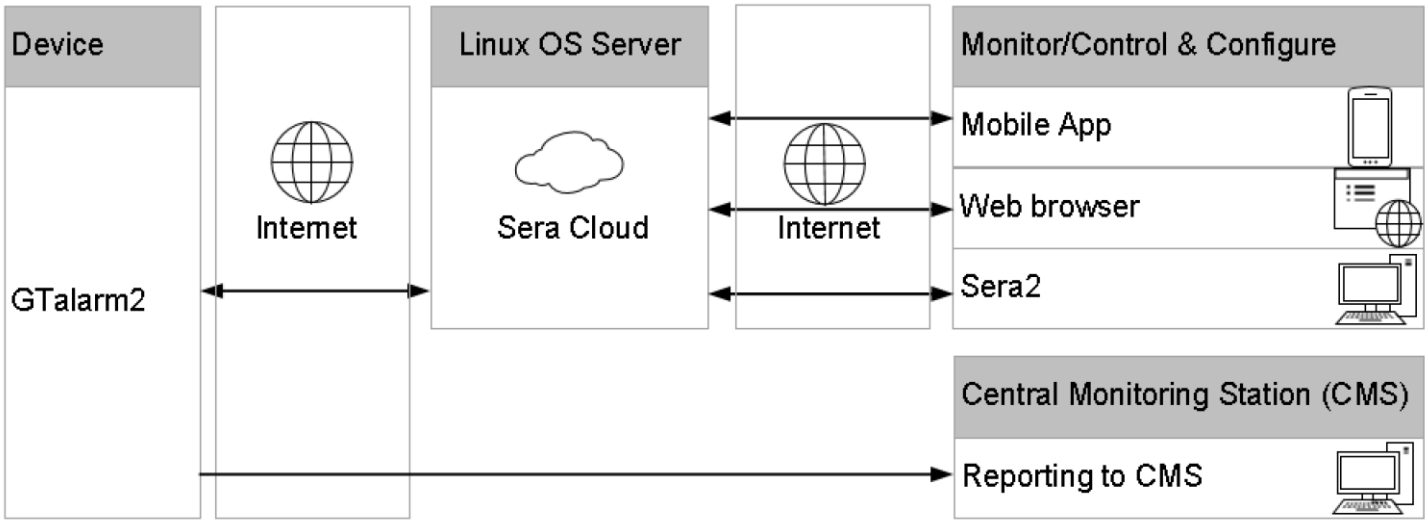
Outputs:

4 open drain (1A) outputs: OUT1 (1A)… OUT4 (1A). The outputs can be used for siren. Output operation algorithms: Siren, Buzzer, ARM state, Zones OK, Light Flash, inverting, pulse mode

OUT1… OUT4 max current – (-V) 1000 mA.

Output alarm parameters may be programmed.

4 System Monitoring and Remote Cloud Service



The ways of Monitoring, control your home alarm, security system:

- Mobile app;
- Web browser
- Free Sera2 software
- SMS
- Reporting alarm events to central monitoring station.

4.1 Monitoring, control via mobile phone, web browser. ARM/DISARM via mobile app.

A single, long range acoustic sensor is mounted in the large room with several windows. In case of breaking the window, the sensor transmit the signal to the module GTalarm2. The module GTalarm2 will send SMS messages and call to 8 user's mobile phone. It is possible connect to the module via mobile phone or PC via standard browser.

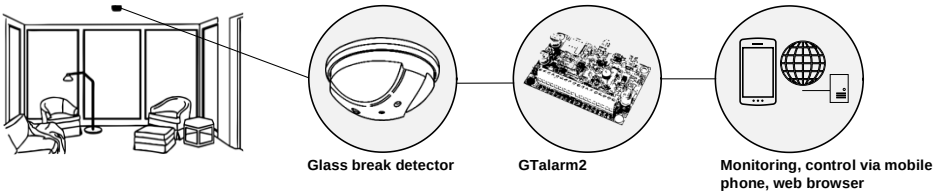


Figure 5 Monitoring, control via mobile phone, web browser

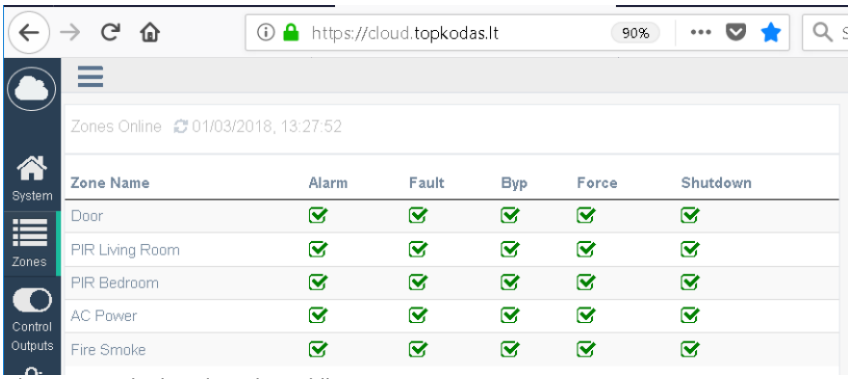


Figure 7 Monitoring via web, mobile app. Zone status.

Figure 6 ARM/DISARM via mobile app

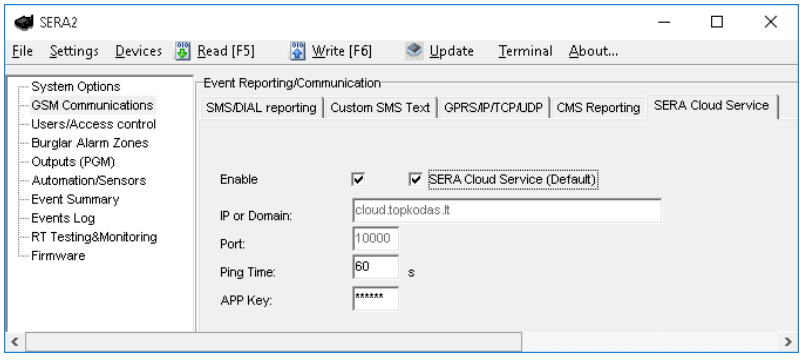
4.2 Monitoring via SERA2 software. Zone status.

User can monitoring system parameters and events using configuration software SERA2 in two ways:

- Directly via USB interface
- Remotely via SERA Cloud Service

Steps to connect to the module remotely:

- GTalarm2 must be online with activated SERA Cloud Service. *[GSM Communication->Sera Cloud Service Enabled]*
- If module is online. Go to Main Menu->Settings
- Check "SERA Cloud Service Default"
- Enter Device IMEI
- Enter App Key
- Press Connect
- Open RT Testing&Monitooring , Press Start Monitoring



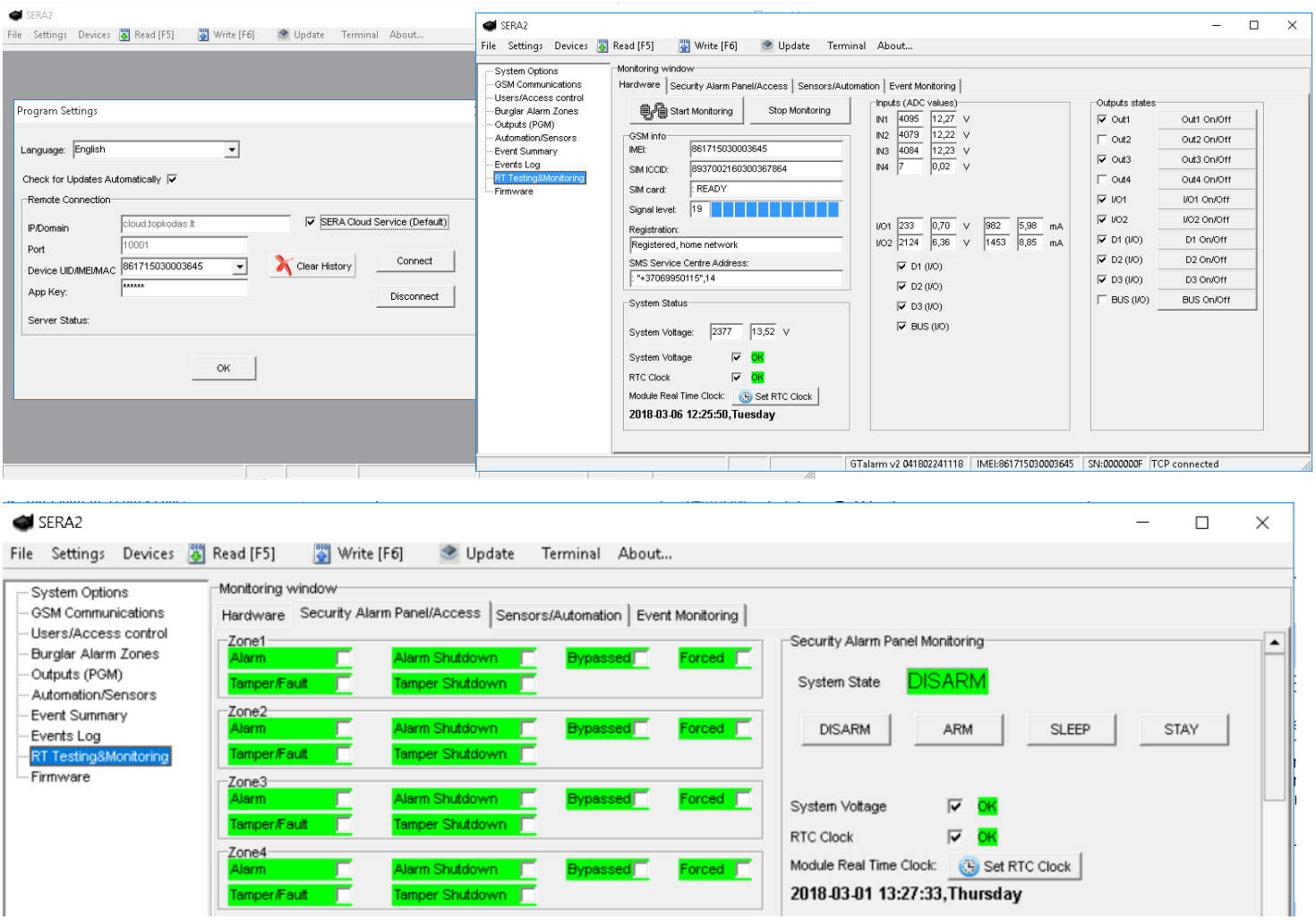


Figure 8 Monitoring via free Sera2 software. Zone status.

4.3 Reporting to the central monitoring station

Shock sensors is mounted on the window with roll up metal shutters in the retail shop because of falls alarm immunity. In case of the broken window, the shock sensor transmit the signal to the module GTalarm2. The module GTalarm2 send alarm signal to the central monitoring station.

The system can be configured to report events to the monitoring station. The system connects to the central monitoring station (CMS) when the CMS mode is enabled. 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 system supports GPRS network –SIA IP protocol (ANSI/SIA DC-09-2012; configurable as encrypted and non-encrypted).

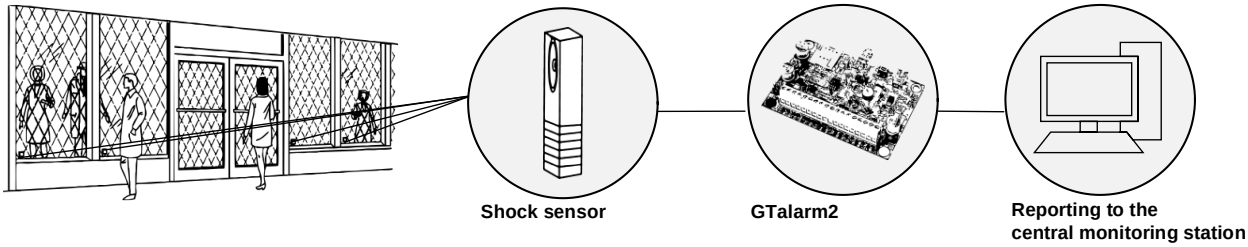


Figure 9 Reporting to the central monitoring station

4.4 Local alarm

For protecting plastic skylights, a shock sensor mounted in a corner of the skylight. In case of alarm event, the shock sensor transmit the signal to the module GTalarm2. The module GTalarm2 activates the siren for local alarm signaling.

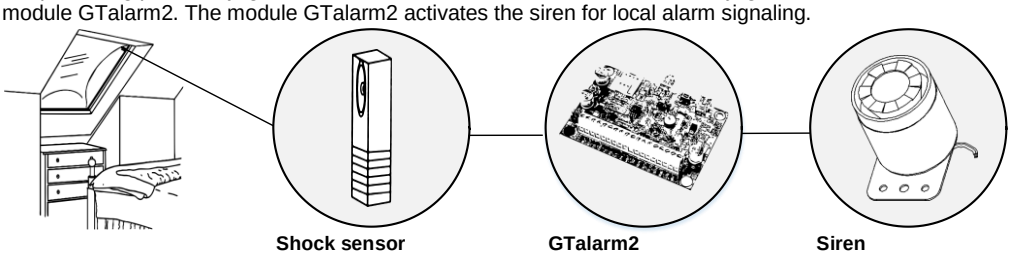


Figure 10 Local alarm system

4.5 Alarm, remote monitoring system

- Monitoring up to 32 sensors via mobile phone, PC via standard web browser.
- AWAY or STAY mode.
- Ability to bypass points for maintenance or service.
- Capacity of up to 800 individual operating panel users, each having various security privileges.
- Capacity of up to 800 individual card/key reader users, each having various levels of access.
- Control and recording of employee access to workplace areas.
- Recording of security-related activities.
- Ability to send messages to up to 8 users.

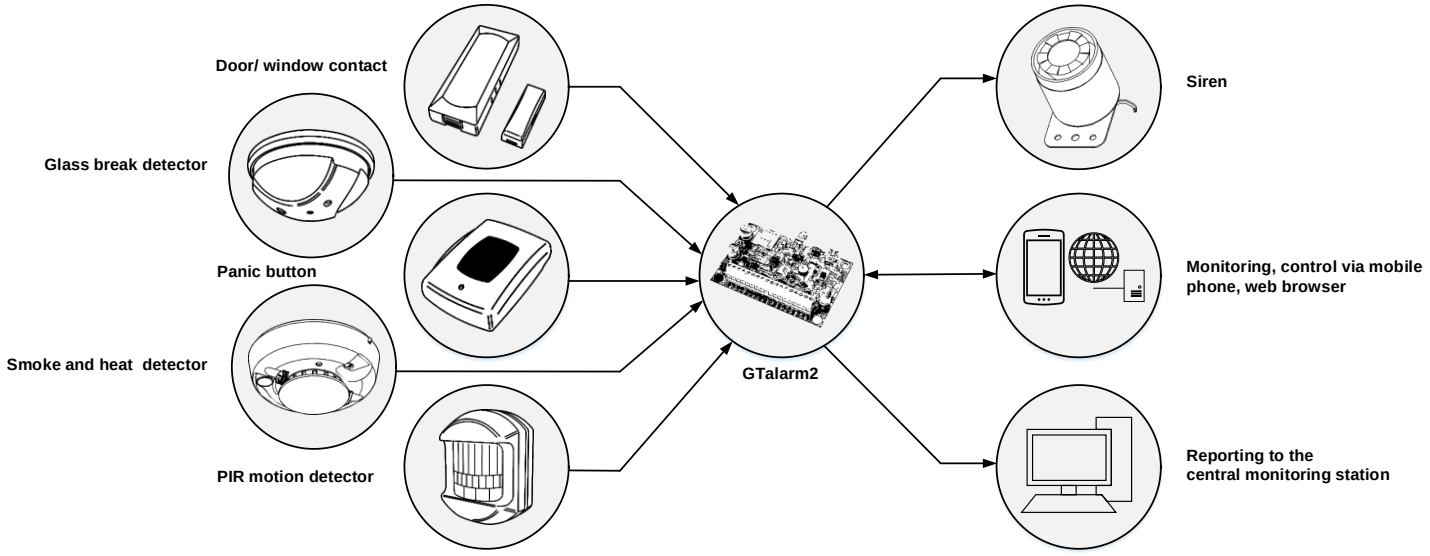


Figure 11 Alarm, remote monitoring, security system

5 Inputs. Zones.

The module GTalarm2 can be used to connect up to 32 detection devices. Each device requires a row in Sera2 software for configuration purpose.

Step by step to set detection devices:

1. Connect the detection device to the zone according the connection diagram
2. Programming the zone definitions
3. Programming the wiring type
4. Programming the zone speed
5. Programming the event repeat timeout
6. Programming the max alarm count
7. Assign the output, which will be activated, when the zone will be triggered
8. Mark the required zone options:

Alarm report enabled, Restore report enabled, Tamper enabled, Bypass enabled, Shutdown if max alarm count enabled, Zone force ARM enabled.

9. Press “write” icon.

The module GTalarm2 has:

- 4 analog inputs (In1...In4 (0-10V)) for analog sensors connection. Or can be used or use it 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

5.1 NC, NO, EOL detectors wiring.

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.

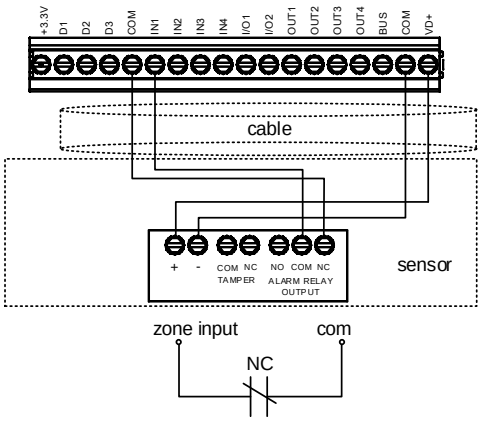


Figure 12 NC Contacts, No EOL

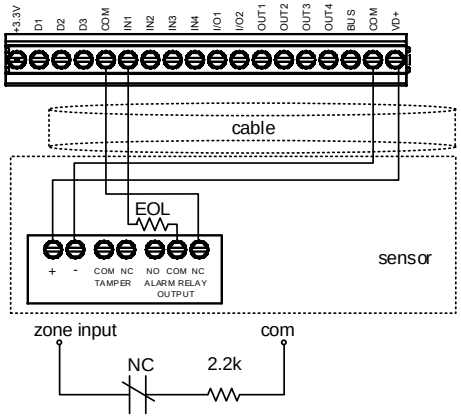


Figure 13 NC, With EOL

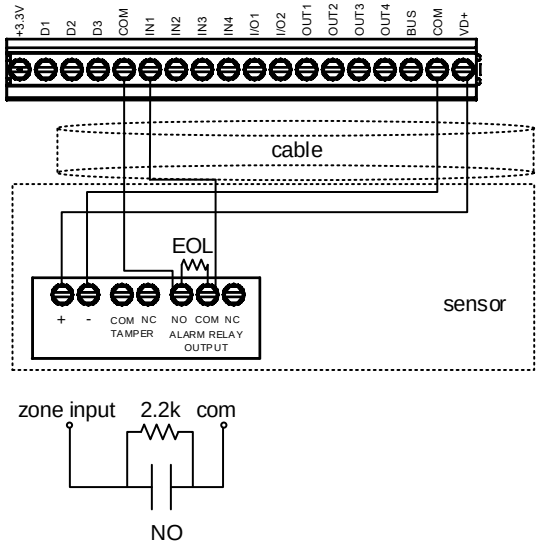


Figure 14 NO, With EOL

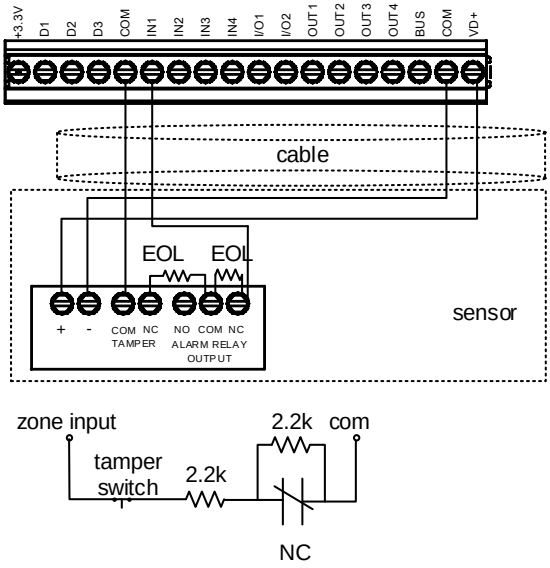


Figure 15 NC With EOL, With Tamper & Wire Fault Recognition

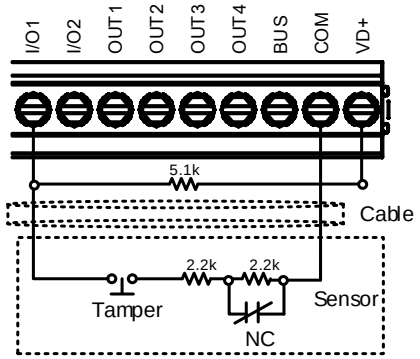


Figure 16 EOL+Tamper sensors connection to I/O1, I/O2

The module has 2 I/O analogue input/ output circuits I/O1and 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.

- 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.

5.2 NC, NO, EOL detectors programming.

Sera2> Burglar Alarm Zones

Detection devices such as motion detectors and door contacts are 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.

- The difference between stay and sleep zone types: "stay" zone type has delay zone timeout, in "sleep" zone type delay zone becomes instant
- The system will NOT activate siren and keypad buzzer only when Instant, Silent zone types is violated.
- 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.
- 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.

- 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

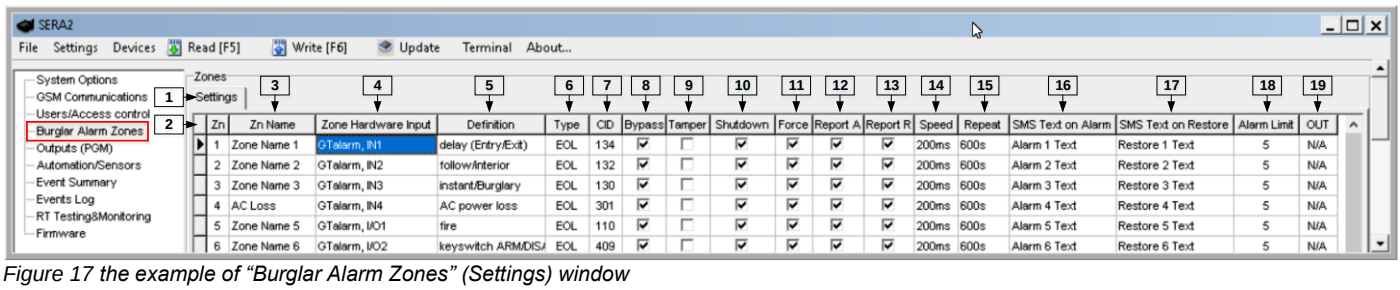


Figure 17 the example of "Burglar Alarm Zones" (Settings) window

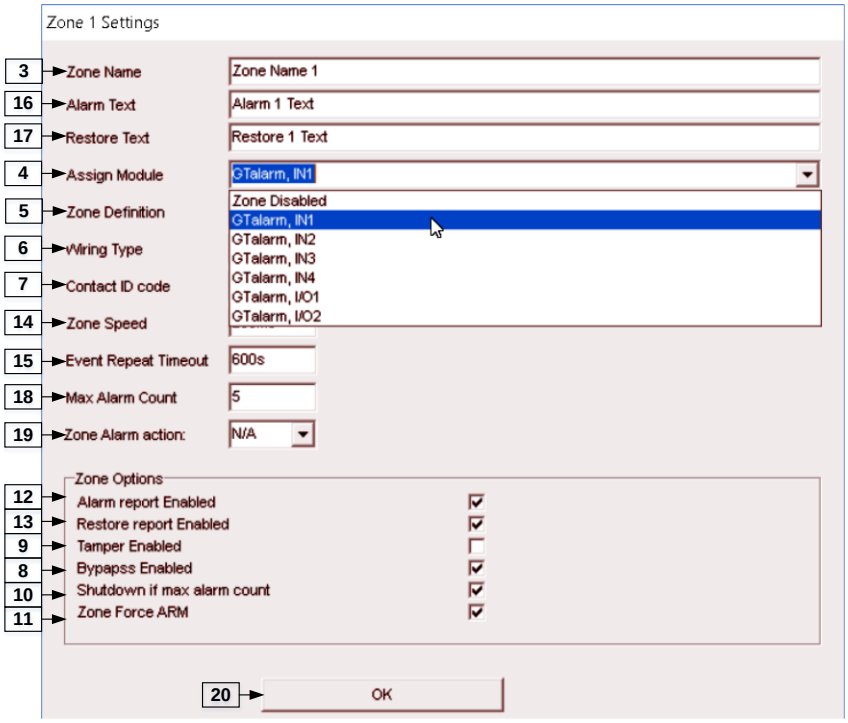


Figure 18 the example of Double click on the required zone window

Table 2 Explanation of every field in "Zones" window

3	**Zone Name**	Zone name should be entered.
4	**Assign Module=** **Zone Hardware Input**	Select the zone hardware input **Zone Disabled** Disables the corresponding zone. **GTalarm, IN1…IN4** The zone hardware input 1… input 4 assigned **GTalarm, I/O1… I/O2** The zone hardware optional Input/ Output 1… Input/ Output 2 assigned
5	**Zone Definition=** **Definition**	**Delay** When armed, provides entry delay when violated. Recommended for door sensors. **Interior** When armed, instant alarm will sound first if the zone is violated; instant alarm will follow the entry delay if entry delay is active. Recommended for motion sensor in front of the door. **Instant** When armed, instant alarm when violated. **24 hours** Instant alarm when violated, audible alarm at default not depending from ARM, DISARM modes. Recommended for safes, storehouses, tampers. **Silent** Always active, not depending from ARM, DISARM modes. The sms will be send, but the siren will not be activated. Recommended for voltage, temperature control, AC mains failure control and for alarm of silent panic. **Fire** Instant alarm and communication when violated not depending from ARM, DISARM modes. Siren signal with interruptions will be generated. Recommended for smoke, fire detectors. **ON/OFF** **Interior STAY** Similar to 'Instant' except the module will auto bypass the zone if Armed in the Stay mode **Instant STAY** Similar to 'Instant' except the module will auto -bypass the zone if Armed in the Stay mode
6	**Wiring Type= Type**	**EOL** End of line resistor. Input type with resistor. **NC** Normal Close. The alarm will be send when the circuit between input and ground (-V) will be broken. **NO** Normal Open. The alarm will be send when the input will be connected with ground (-V)
7	**Contact ID code= CID**	The module supports Contact ID reporting. If any other data is programmed the module will automatically generate the reporting event when transmitting to the central station.
14	**Zone Speed= Speed**	The Input Speed defines how quickly the module responds to an open zone detected on any hardwired input terminal (does not apply to addressable motion detectors and door contacts).
15	**Event Repeat Timeout=** **Repeat**	Insensitive time to recurrent zone events
18	**Max Alarm Count=** **Alarm Limit**	When the particular number of zone events set has occurred, the other events of the same zone will not be responded for the time set in Event Repeat Timeout. After this time expired (or when disarmed), a new count of the number of zone events will be started.
12	**Alarm Report Enabled=** **Report A**	The system will report alarm event and log it to the event buffer
13	**Restore Report Enabled=** **Report R**	The system will report restore event and log it to the event buffer
9	**Tamper Enabled= Tamper**	The system will detect a *tamper* condition with one or more sensors on the system
8	**Bypass Enabled= Bypass**	The system will allow zones to be Manually Bypassed.
10	**Shutdown if max alarm count= Shutdown**	The system will stop generating alarms once the **max alarm count** Limit is reached. It resets every time the system will be armed.
11	**Zone Force ARM= Force**	Only **force** zones can be bypassed when the module is Force armed. Fire Zones cannot be Force Zones.

19	**Zone Alarm Action= OUT**	determines which output will be activated

5.3 Smoke detector Wiring

The module GTalarm2 has two independent 2-wire lines on inputs I/O1 and I/O2

[4-Wire] Smoke detector Wiring
Connect the 4-wire smoke detectors and a relay as shown in the figure below.

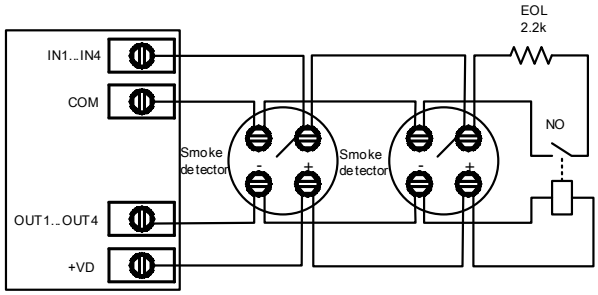


Figure 19 4-Wire Smoke Detector Installation

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

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

[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.

1. Connect the [2-wire] smoke detector (current sensor).
2. Connect the power supply.
3. Install SERA2 software.

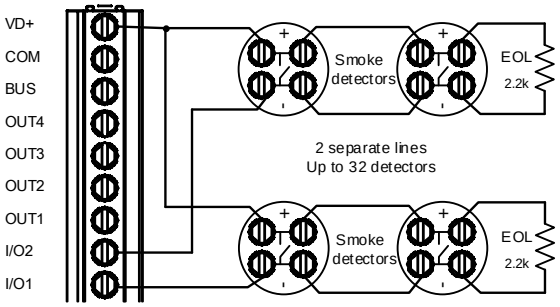


Figure 20 2-wire smoke detector wiring diagram

- If I/O1 (I/O2) set as 2-wire, don't need connect 5.1k resistor to +VD.
- 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

5.4 Smoke detectors programming.

Sera2> System Options> General System Options
Sera2> Ouputs
Sera2> Burglar Alarm Zones

- Go to "System Options> General System Options" from the menu and select 2-Wire Smoke Detector (Fire current loop)
- In the Burglar Alarm Zone table set I/O1 (I/O2) definition to "Fire"
- In the output table I/O1 (I/O2)(20mA) set to "Fire Sensor"
- Write configuration by pressing "Write" icon.
- **For more information, please look to the „Zones programming"**

6 Outputs. Wiring & Programming.

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 controled via short call or SMS. Output operation algorithms: Automation /CTRL, Siren, Buzzer, ARM state, Zones OK, Light Flash, inverting, pulse mode
- OUT1… OUT4 max current – (-V) 1000 mA.
- Output alarm parameters may be programmed.
- Connect the positive side of the device to be activated to the VD+ terminal. Connect the negative terminal to the selected output.

Connect devices to the 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 >=1A might be used to powering the module

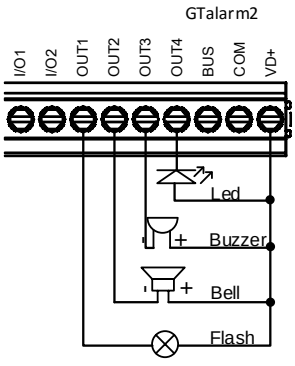


Figure 21OUT1-OUT4 Open drain 1000 mA connection

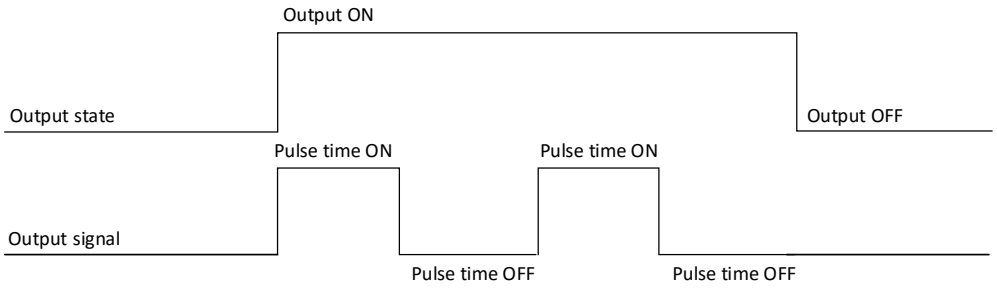
Set output's parameters step by step:

1. Open Sera2 software , Select Device "GTalarm2">

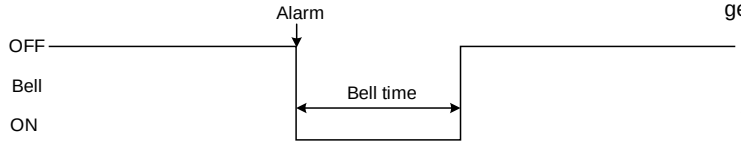
2. Go to “Outputs (PGM)” window>
3. Enter the required parameters>
4. If the output is not in used, it should be disabled
5. Press “Write” icon.

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.

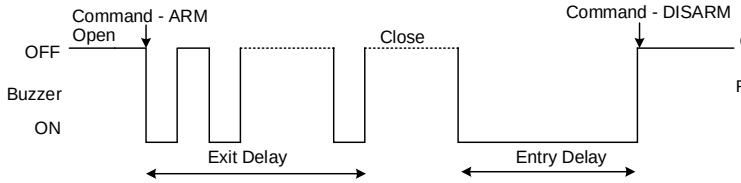


Bell: Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.

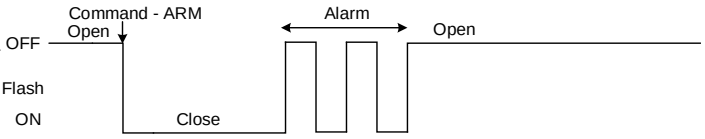


ARM/DISARM: Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.

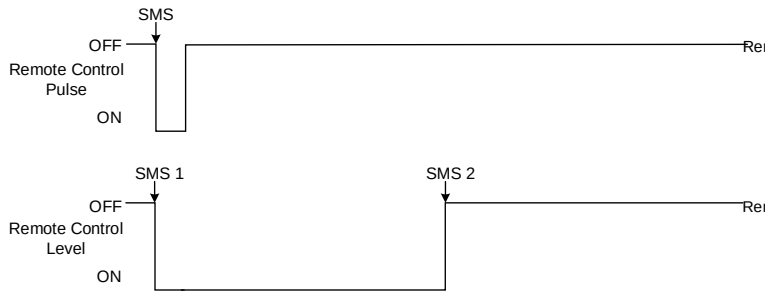
Buzzer: Output for connection of audio indicator. After the alarm system activated a pulse signal is generated within Exit Delay time, and continuous signal - within Entry Delay time or when the alarm system is disturbed. When the alarm system is turned off, operates like keyboard buzzer.



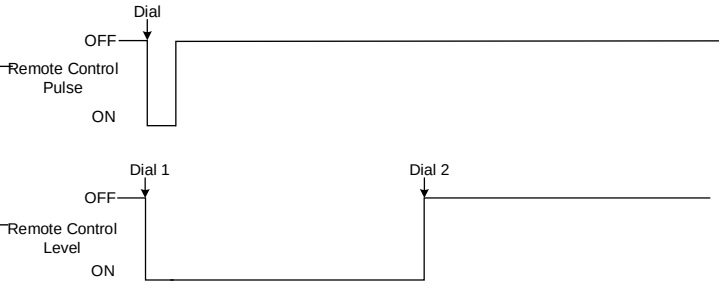
Flash: Output for connection of light indicator. When the alarm system is on, a continuous signals generated, and if the alarm system is disturbed - pulse signal. Signal is terminated by turning off the alarm system.



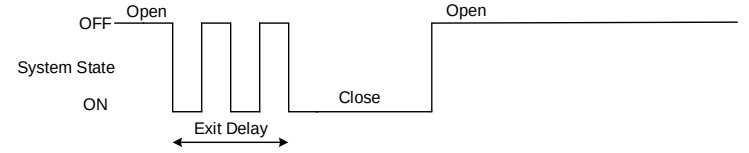
Remote Control: Output designed for connection of electrical devices which will be controlled by SMS message or phone call a) control by SMS message



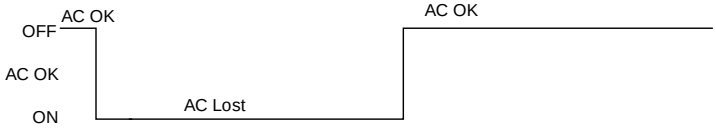
Remote Control b) control by phone call



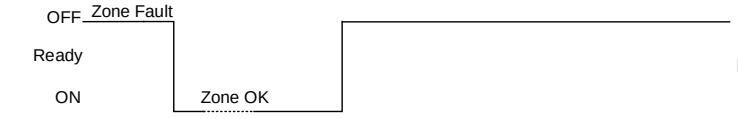
System State: Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.



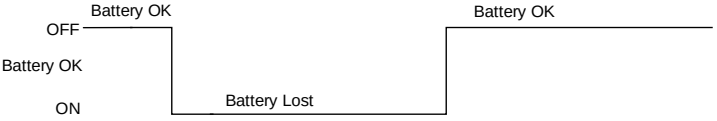
AC OK: Output for connection of indicator about control panel supply from alternating current



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

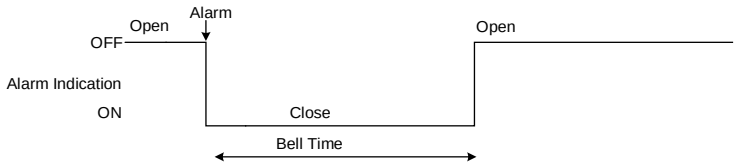


Battery OK: Output for connection of indicator about control panel supply from battery.

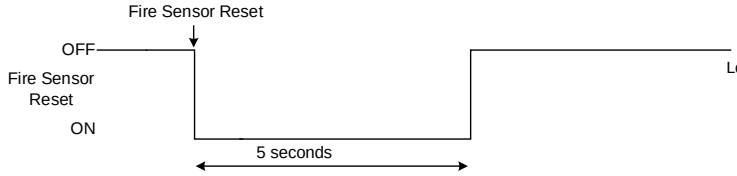


Alarm indication: Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.

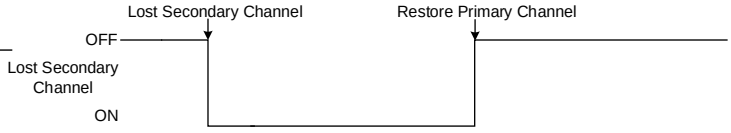
Lost Primary Channel: Output where a continuous signal is generated when communication with primary channel was lost.



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.



Sera2> Outputs (PGM)

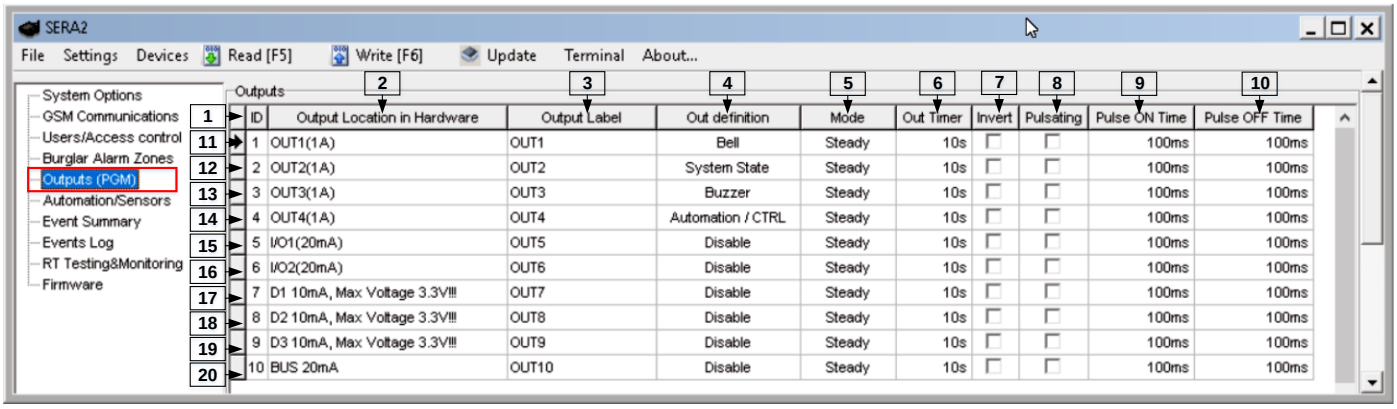
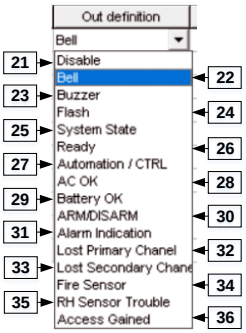


Figure 22 The example of Outputs (PGM) window

Table 3 Explanation of every field in "Outputs" window

1	**ID**	Output sequence number.
2	**Output Location in Hardware**	The outputs hardware location.
3	**Output Label**	Output name
4	**Out definition**	Selection of output operation mode.



21	Disable	Output disabled
22	Bell	Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.
23	Buzzer	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.
24	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.
25	System State	Output for connection of light indicator of the alarm system status. Within Exit Delay time a pulse signal is generated, and when the alarm system activated – continuous. Signal is terminated by turning off the alarm system.
26	Ready	Output for connection of light indicator of input statuses. If all zones are clear (none violated), a continuous signal is generated.
27	Remote Control	Remote control by call mode is enabled. Output designed for connection of electrical devices which will be controlled by SMS message or phone call
28	AC OK	Output for connection of indicator about control panel supply from alternating current.
29	Battery OK	Output for connection of indicator about control panel supply from battery.
30	ARM/ DISARM	Output for connection of light indicator of the alarm system status. When the alarm system is on a continuous signal is generated.
31	Alarm Indication	Output for connection of light indicator showing alarm status of the alarm system. After the alarm system actuation a continuous signal is generated.
32	Lost Primary channel	Output where a continuous signal is generated when communication with primary channel was lost.
33	Lost secondary channel	Output where a continuous signal is generated when communication with secondary channel was lost.
34	Fire Sensor Reset	Output for reset of fire sensor operation. Its status changes 5 sec. and returns to the initial one.
35	RH Sensor Trouble	Output for RH Sensor trouble operation. In this mode output can automatically reset Humidity sensor if trouble occurs.

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

7 Arming/ disarming, system control methods

Up to 800 users is able to ARM/DISARM the system and control the door with:

- Wiegand keypad/ RFID reader;
- iButton keys
- Mobile phone

The door could be controlled via mobile app, short call, SMS, iButton key, RFID card.
When iButton, RFID or key button codes is entered, the users will be able to ARM/DISARM the system and control the outputs. Unlimited iButton probes could be connected to the controller. It is possible to specify which door the user can access.

For example:
The user Zivile allowed to ARM/ DISARM the system and control door that is connected to the OUT1.
Allowed control methods:

- Keypad code (123456),
- Phone (+37065558449),
- iButton (000000FBC52B).

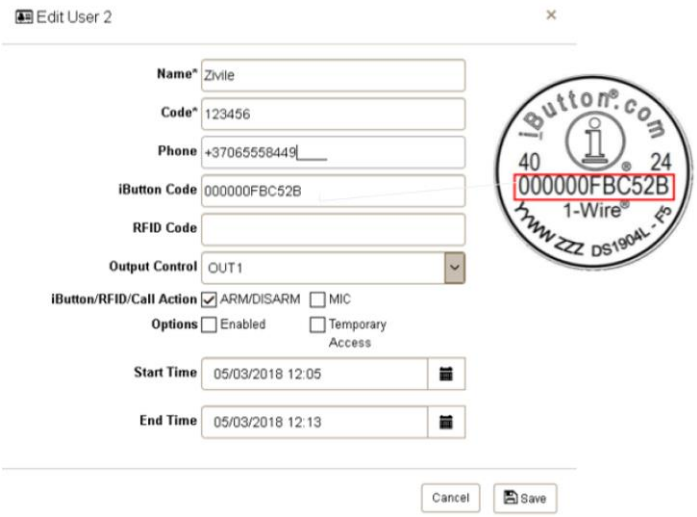


Figure 24 the example of system configuration via mobile, web app

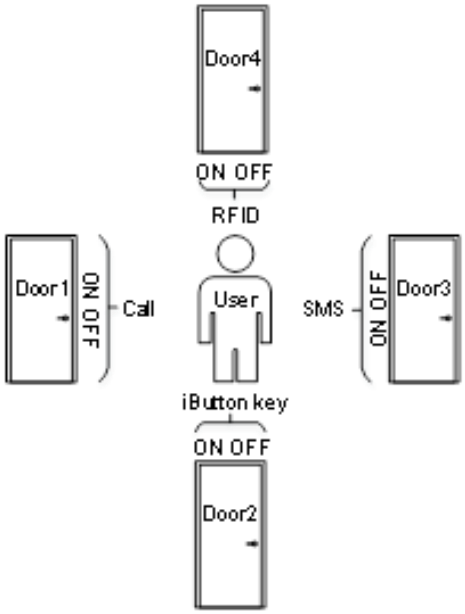


Figure 23 ARM/DISARM the system and control doors with: mobile call, iButton, SMS, RFID

Arm/Disarm, door control by standard web browser.
It is possible to connect to the module via Sera Cloud service and arm, disarm the system and control the door from the computer, via standard web browser.
Arm/Disarm, door control from Android app.
It is possible to arm, disarm the system and control the door from mobile phone, Android app.

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

Arm/Disarm by sms
The system ignores any incoming 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 arm the system by SMS text message, send the following text to the system's phone number USER 000000␣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.
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.

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.

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. When the security system is to be turned in ARM mode, the bell will beep once, when in DISARM mode - the bell will beep twice.

Exit Delay is a short period of time after the system is armed for the customer to leave the premises without tripping the alarm.
Entry Delay is a short period of time after an armed sensor is tripped for the customer to enter a valid security code before the alarm sounds.
Arm Away: All family members will be away from the house
Arm Stay: There are family members inside the house
When the Alarm Sounds
If (1) an armed Entry/Exit Zone is tripped and the system is not disarmed before the Entry Delay countdown completes, or (2) an armed Perimeter Zone is tripped, the alarm will sound. At this point, you still have an additional 30 seconds (the Alarm Transmission Delay) to enter a valid 4or 6-digits Security Code before the Central Monitoring Center (CMS) is notified. If a valid Security Code is not entered within the 30 seconds, then a message is sent to the CMS.
Note: If a Panic Alarm is tripped, there is no 30-second Alarm Transmission Delay, and the CMS is notified immediately.

General operation description

When the system is being armed, it will initiate the exit delay countdown intended for the user to leave the secured area. During the countdown period the buzzer will emit short beeps. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the system until the violated zone or tamper is restored. In case it is required to arm the alarm system despite the violated zone presence, the violated zone can be bypassed or Force attribute enabled.

After the system is armed and if a zone (depending on type) or tamper is violated, the system will cause an alarm. During the alarm, the siren/bell will provide an alarm sound along with the buzzers of the keypads. By default, the system will also makes a phone call and send an SMS text message containing the violated zone or tamper number to a listed user phone number and indicate the violated zone or tamper number on the keypad. If another zone or tamper is violated or the same one is restored and violated again during the alarm, the system will act as mentioned previously, but will not extend the alarm time.

After the user enters the secured area, the system will initiate the entry delay countdown intended for system disarming. During the countdown period, the buzzer will emit a steady beep.

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.

8 Wiegand Keypad & RFID Card Reader. Wiring & Programming.

Sera2> System Options> Digital I/O Settings
Sera2> Users/ Access Control

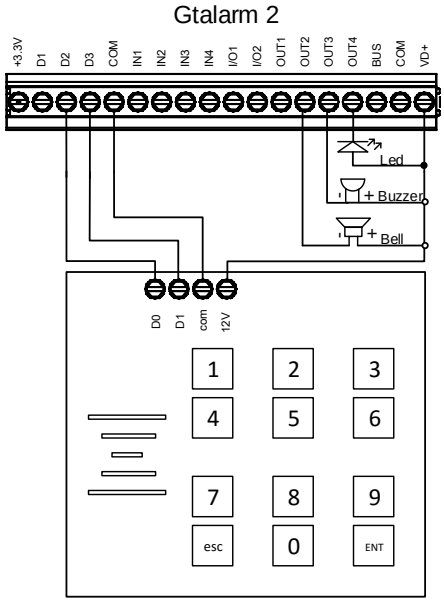


Figure 25Wiegand keypad connection

Wiegand bus specifications:

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

Steps to configure Wiegand keypad:

1. Connect Wiegand keypad as shown in the Fig
2. Install SERA2 software.
3. Connect the module to the computer via mini USB cable.
4. „Go to System options“> Digital I/O Settings
5. Set Digital I/O D2 to Wiegand interface Data0
6. Set Digital I/O D3 to Wiegand interface Data1
7. Write configuration

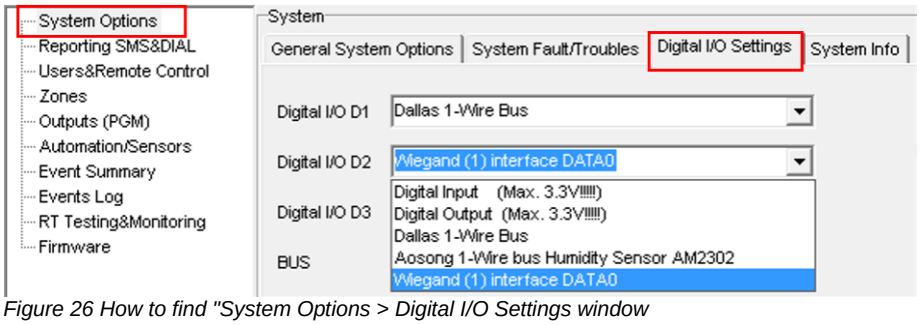


Figure 26 How to find "System Options > Digital I/O Settings window

There is 3 different ways, to enter iButton, RFID keycard codes:

A) Manually in Sera2 software. (The picture below)

In that case, you have to:
Install SERA2 software

1. Go to “Users& Remote Control” table.
2. Enter iButton or RFID Keycard codes for users.
3. Select iButton or RFID Keycard action OUT/ARM/DISARM, etc.
4. Write the configuration into the module by pressing “Write” icon

B) <u>Automatically</u> in Sera2 software.

Association of iButton keys or RFID Keycards is carried out by activating special programming mode - by sending SMS or by pressing „Learn iButtons/RFID mode“ in the SERA2 configuration program.
If you need to enter iButtons learning mode by SERA2 software, you have to:
Install SERA2 software.

1. Go to the “System options> General system options” and press “Start iButton/RFID programming mode” to start entering iButton keys.
2. Press “Stop iButton programming” to stop entering iButton keys.
3. Write configuration by pressing “Write” icon.

C) by sending SMS message:

INST123456␣063␣S
INST = Install. Configuration of the parameters.
123456= 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,
3- Delete these keys from memory, which will be touched to the reader.

When you receive a message into your mobile phone in relation to activation of iButton key programming mode, touch the key to the reader and its unique code will recorded into system memory. Buzzer will notify you about successful recording by beeping twice. The system allows to associate up to 800 iButton keys. Each time when touching the key, the system records its code till all desirable keys will be recorded. If during 2 minutes not a single iButton key will not be learned, the system will automatically exit keys learning mode. After finishing programming of the keys, you might send SMS message.

You can disable recording of new keys into memory. In the event of failure to send this message, ARM/DISARM of the system via iButton key will not operate. 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.

You can delete all iButton keys from the memory. If you have the key, that you want to delete from the memory, you have to send SMS, and touch the key to the reader. 2 minutes later, the module will deactivate the keys deletion mode.

9 iButton keys. Wiring & Programming.

Sera2> System Options> General System Options
Sera2> Users/ Access Control

Maxim-Dallas iButton keys (iButton DS1990A – 64 Bit ID)) can be used to ARM/DISARM security panel or control selected output. Up to 800 iButton keys can be assigned to the system.
The First iButton key may be learned (recorded) by touching it to the reader. Without the need to send any SMS. The system will notify about successfully recording of the key into memory by shortly beeping twice via buzzer. The system will automatically assigns control function (ARM/DISARM).
The first key is the main key (MASTER) other keys might be learnt thus:
1. To enter key codes directly into configuration users table.
2. Pressing Learn iButton button in the "System Options" window.
3. Sending SMS with command for new keys learning.
4. Using MASTER key
The total length of the bus from 10 to 100 m. Depending of cable quality, and environment noise.
LED is without resistor. External resistor required.

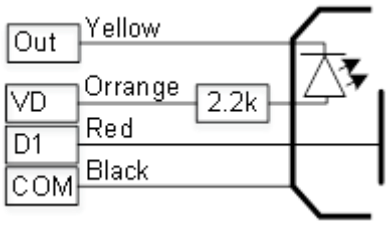


Figure 27 iButton reader wiring diagram

9.1 Enter iButton keys with Sera2 software

Sera2> Users/ Access control

It is possible to enter iButton keys to the module GTalarm2 by using free software Sera2. In that case go to www.topkodas.lt website and install Sera2 software to the PC. It is possible to enter iButton codes automatically by activating iButtons learning mode or manually.

1. **iButtons learning mode:**
   a) Go to the "System options> General system options" and press "Start iButton programming" to start entering iButton keys or "Stop iButton programming to stop entering iButton keys.
   b) Write configuration by pressing "Write" icon.
2. **Manually entering:**

Go to the "Users/ Access control" window and enter manually iButton codes. It is the code in red rectangular in the picture below.

Figure 28 iButton code

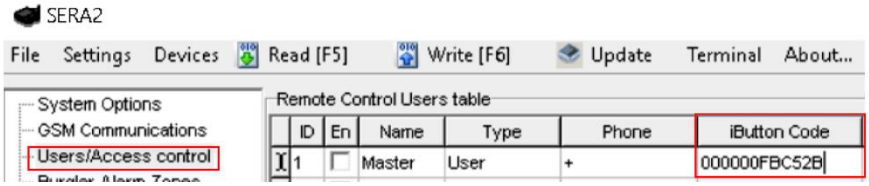


Figure 29 Enter iButton codes manually

9.2 Enter iButton keys by sending SMS message

A) **Send SMS message to the module GTalarm2:** INST123456␣063␣S
INST = Install. Configuration of the parameters.
123456= 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.
3- delete these keys from memory, which will be touched to the reader

When the message about iButton codes learning mode activation received, touch the key to the reader and its unique code will recorded into system memory. Buzzer will notify you about successful recording by beeping twice. The system allows to associate up to 800 iButton keys. Each time when touching the key, the system records its code till all desirable keys will be recorded. If during 2 minutes not a single iButton key will not be learned, the system will automatically exit keys learning mode. Or after finishing programming of the keys, you might send SMS message.
It is possible to disable recording of new keys into memory. In the event of failure to send this message, ARM/DISARM of the system via iButton key will not operate. 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.
It is possible to delete all iButton keys from the memory. If you have the key, that you want to delete from the memory, you have to send SMS and touch the key to the reader. 2 minutes later, the module will deactivate the keys deletion mode.

9.3 ARM/DISARM with mobile phone

Sera2> Users/ Access control

Arm/ disarm the module GTalarm2 with mobile phone step by step:

1. Go to "Users/ Access control" window in Sera2 software
2. Enter Phone numbers (up to 800 users)
3. Press "Write" icon.

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

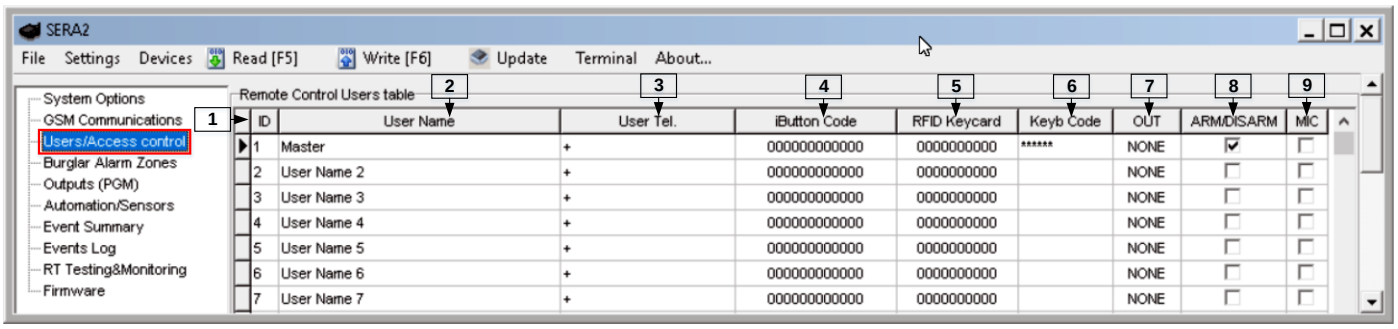


Figure 30 The example of Users/ Access Control > Remote Control Users Table window

Table 4 Explanation of every field in "Users & Remote Control" window

1	**ID**	
2	**User Name**	The name of users who will be able to control the module should be entered in this column.
3	**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.
4	**iButton Code**	iButton Maxim iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000
5	**RFID Keycard**	RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
6	**Keyb Code**	Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
7	**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.
8	**ARM/DISARM**	If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
9	**MIC**	If checked, by calling from the specified phone, the controller responds and you can hear what's going on in the premises

10 DISARM /ARM/SLEEP/STAY the security system

Sera2> System Options> System Fault/ Troubles

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

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

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

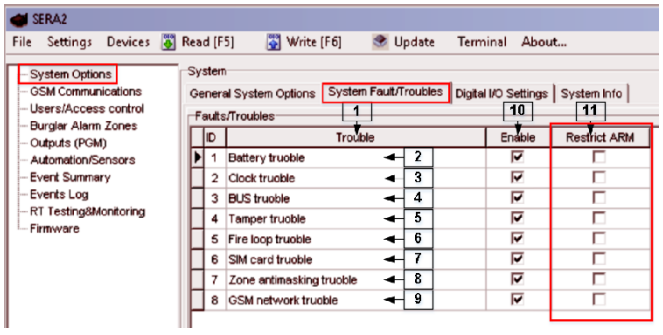


Figure 31 System Options> System Fault/ Troubles window

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> Users/ Access control

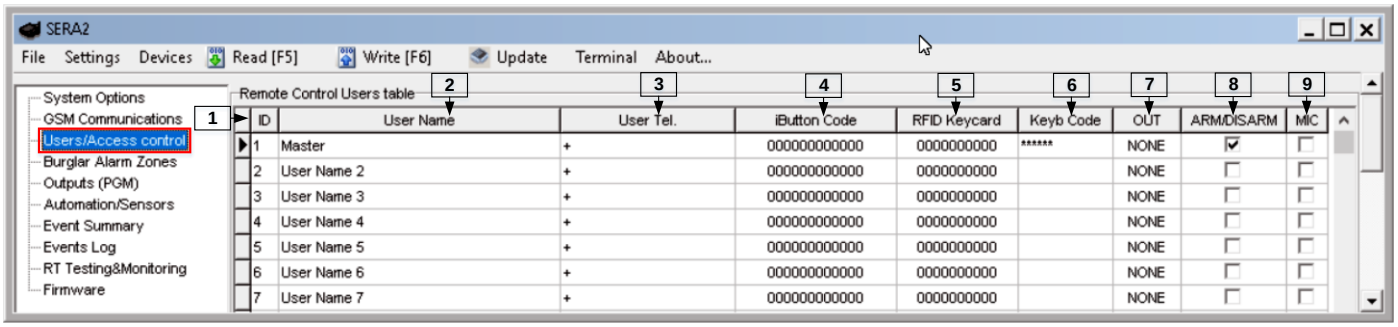


Figure 32 the example of Users/ Access control> Remote Control Users Table window

Table 5 Explanation of every field in "Users & Remote Control" window

1	**ID**	
2	**User Name**	The name of users who will be able to control the module should be entered in this column.
3	**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.
4	**iButton Code**	iButton Maxim iButton key DS1990A - 64 Bit ID code. Might be entered manually or automatically registered after the module enters keys association mode. In order to delete the code, it is necessary to enter 000000000000
5	**RFID Keycard**	RFID Keycard code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
6	**Keyb Code**	Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000
7	**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.
8	**ARM/DISARM**	If this check box is checked, a user will be able to ARM/DISARM the module by dialing.
9	**MIC**	If checked, by calling from the specified phone, the controller responds and you can hear what's going on in the premises

11 System Fault/ Troubles Programming

Sera2> System Option> System Fault/ Troubles

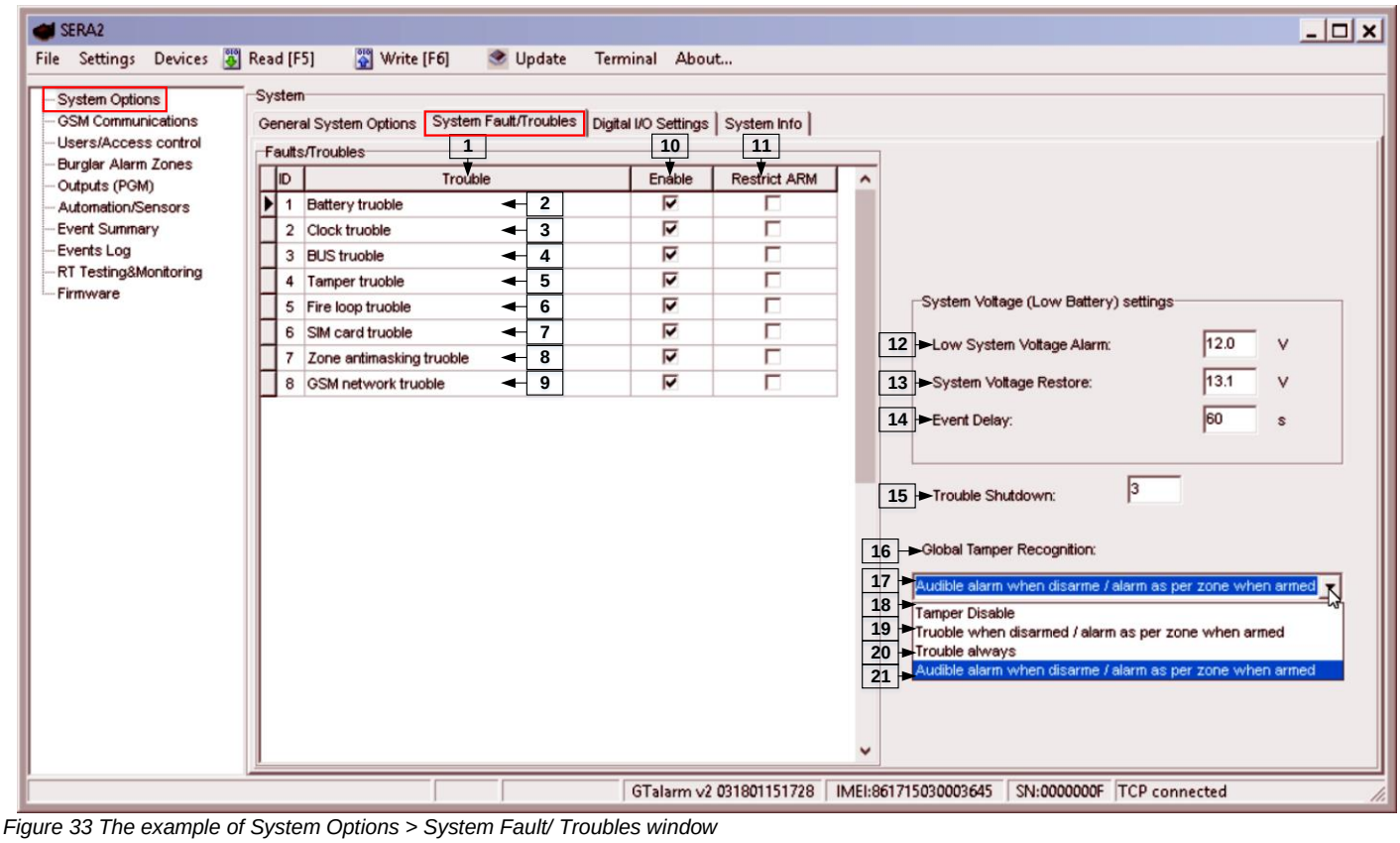


Figure 33 The example of System Options > System Fault/ Troubles window

Table 6 Explanation of every field in "System Fault/Troubles" window

1	**Trouble**	This column lists potential system troubles
10	**Enable**	The system will detect a marked trouble
11	**Restrict ARM**	In case of such trouble, the arming activation will be restricted.

2	**Battery trouble**	Low system voltage. Power supply or backup battery voltage is low, needs to be recharged, or replaced.
3	**Clock trouble**	The time and date has not been set.
4	**BUS trouble**	The expansion device is no longer communicating with the module.
5	**Tamper trouble**	The zone(s) that was tampered
6	**Fire loop trouble**	The trouble is occurring with your smoke detectors.
7	**SIM card trouble**	Not available or impossible to read SIM card.
8	~~**Zone ant masking trouble**~~	Do not available in this module
9	**GSM network trouble**	SIM card is not registered with the GSM network provider
12	**Low System Voltage Alarm**	The module has detected a low voltage. This means that your system is running on the backup battery and voltage is dropped below allowed value.
13	**System Voltage Restore**	The module has detected that the system voltage has been restored.
14	**Event Delay**	System low voltage trouble event report delay.
15	**Trouble Shutdown**	Setting of the allowable number of the same trouble event, where in case of excess of such number the trouble reporting will be off. The number of such events is counted until the arming mode is changed (On/Off).
16	**Global Tamper Recognition**	How the control panel will operate after tamper recognition 18 **Tamper Disable** The module will not generate an alarm or trouble. 19 **Trouble when disarmed / alarm as per zone when armed** When disarmed: Generates Trouble Only The module transmits the defined report code. When armed: Follows Zone Alarm Type 20 **Trouble always** Generates Trouble Only (when armed or disarmed) 21 **Audible alarm when disarmed / alarm as per zone when armed** When disarmed: Generates Audible Alarm The module transmits the defined report code and generates an audible alarm. When armed: Follows Zone Alarm Type The module follows the zone's alarm type.

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

12 Custom SMS Text

Sera2> GSM Communications> Custom SMS Text

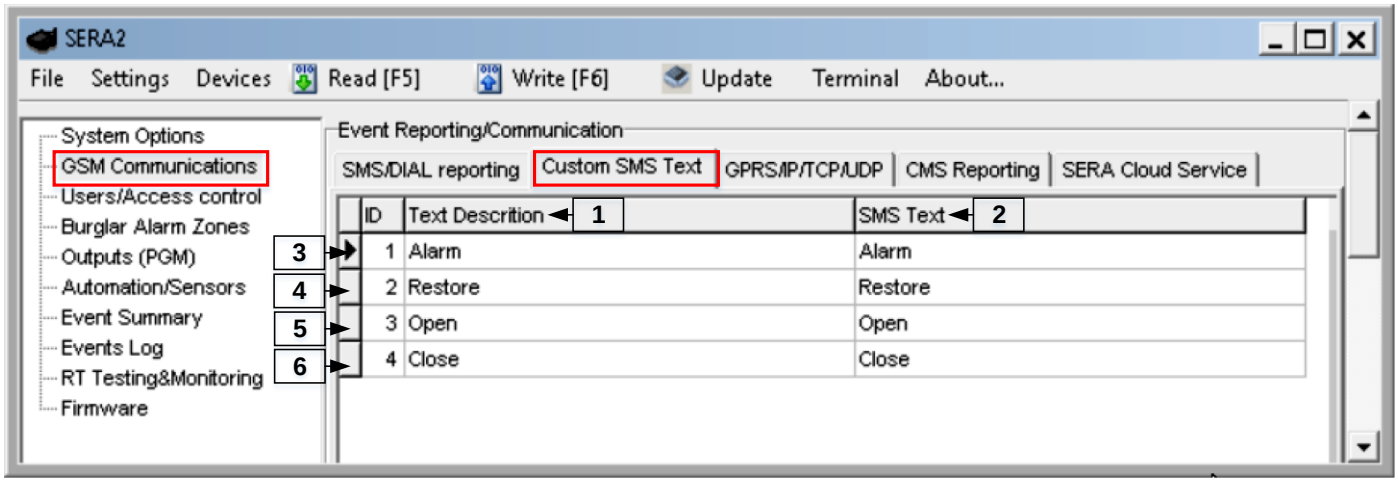


Figure 34 the example of GSM Communication > Custom SMS Text window

Table 7 Explanation of every field in "Custom SMS Text" window

1	**Text Description**	Event type text
2	**SMS Text**	Text which will be visible in SMS message is entered.
3	**Alarm**	SMS message text of alarm report can be entered.
4	**Restore**	SMS message text of restore report can be entered.
5	**Open**	SMS message text of open report can be entered.
6	**Close**	SMS message text of close report can be entered.

13 Reporting SMS&Dial in Case of Alarm Events

Up to 8 users for call/SMS monitoring. Only listed in the memory phone numbers can receive information about alarms.

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

14 Reporting to the user‘s mobile phone

Sera2> GSM Communications> SMS/DIAL reporting

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.
4. 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:
   a. Mobile phone was switched off, mobile phone was out of GSM signal coverage or provided “busy” signal.
   b. 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

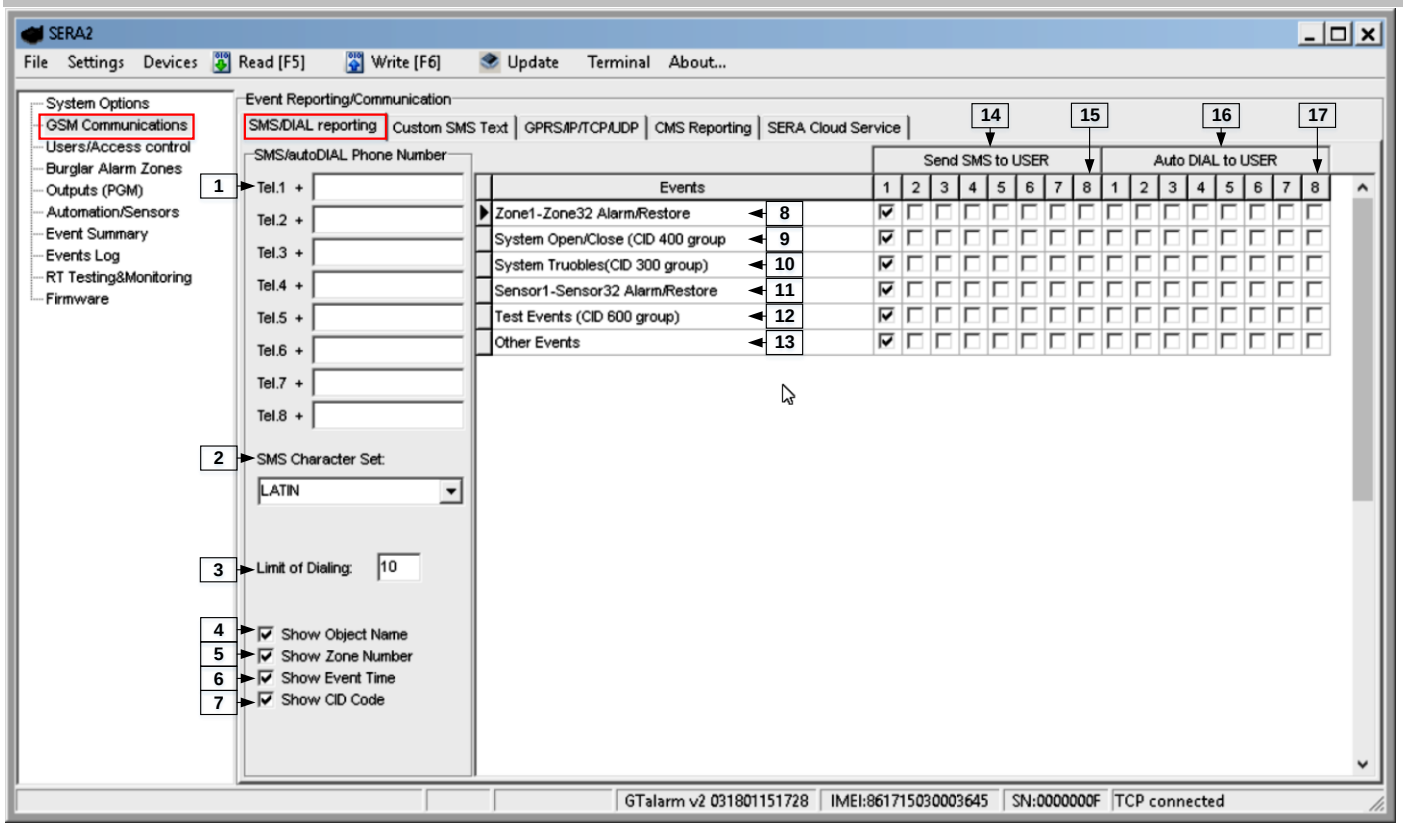


Figure 35 The example of GSM Communication> SMS DIAL Reporting window

Table 8 Explanation of every field in "SMS DIAL Reporting" window

1	**The SMS/auto DIAL Phone Numbers**	**The SMS/auto DIAL Phone Numbers** whom SMS messages will be send and calls will be made should be entered. User number up to 8. User numbers should be entered with international code. Near the telephone number of each user, check boxes which events will be sent to that user. User must type mobile number in the international format (it consist of only those digits that overseas callers must type: **[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 Incorrectly entered user number: 440113xxxxxxx or 0113xxxxxxx
2	**SMS Character Set**	SMS character set selection.
3	**Limit of Dialing**	Indicate maximum number of unsuccessful calls
4	**Show Object Name**	Object name will be displayed in the SMS message
5	**Show Zone Number**	Zone number will be displayed in the SMS message
6	**Show Event Time**	Event time will be displayed in the SMS message
7	**Show CID Code**	Report Contact ID code
8	**Zone1- Zone32 Alarm/ Restore**	Zone1- Zone32 alarm and restore events reporting is enabled.
9	**System Open/ Close (CID 400 group)**	System ARM/DISARM/STAY reporting is enabled.

10	**System Troubles (CID 300 group)**	System trouble reporting is enabled.
11	**Sensor1- Sensor32 Alarm/ Restore**	Sensor 1 – Sensor32 alarm and restore events reporting is enabled.
12	**Test Events (CID 600 group)**	Communication test reporting is enabled.
13	**Other Events**	Other events reporting is enabled.
14	**Send SMS to USER**	SMS reporting to selected index of telephone number is enabled.
15	**1…8**	To which from the specified phone numbers will be send SMS messages if the specified event will occur in the system
16	**Auto DIAL to USER**	Auto DIAL to selected index of telephone number is enabled.
15	**1…8**	To which from the specified phone numbers will be dial if the specified event will occur in the system

15 Reporting to the Central Monitoring Station

15.1.1 GPRS/ IP/ TCP/ UDP details programming

Sera2> GSM Communications> GPRS/IP/TCP/UDP

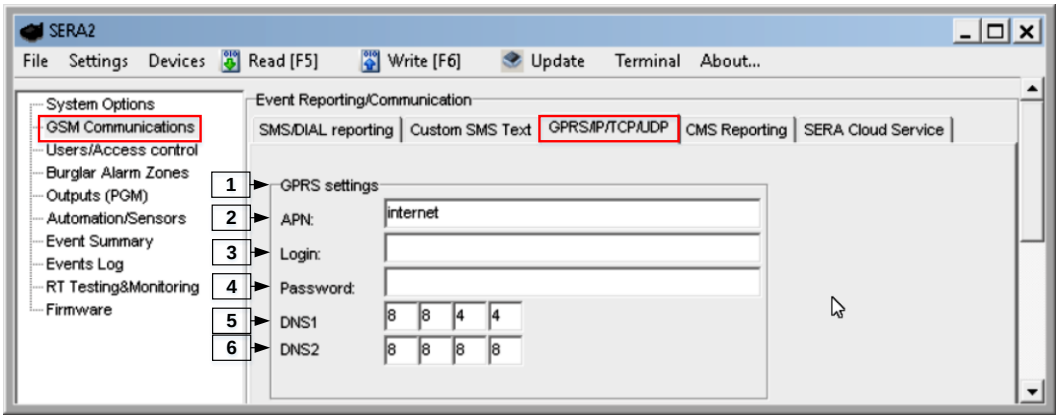


Figure 36The example of GSM Communication > GPRS/ IP/ TCP/ UDP window

Table 5 explains every field in the Reporting SMS & DIAL > GPRS/ IP/ TCP/ UDP window

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

15.1.2 Central Monitoring Station details programming

Sera2> GSM Communications> 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:

1. GPRS network –SIA IP protocol (ANSI/SIA DC-09-2012; configurable as encrypted and non-encrypted).
2. 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.

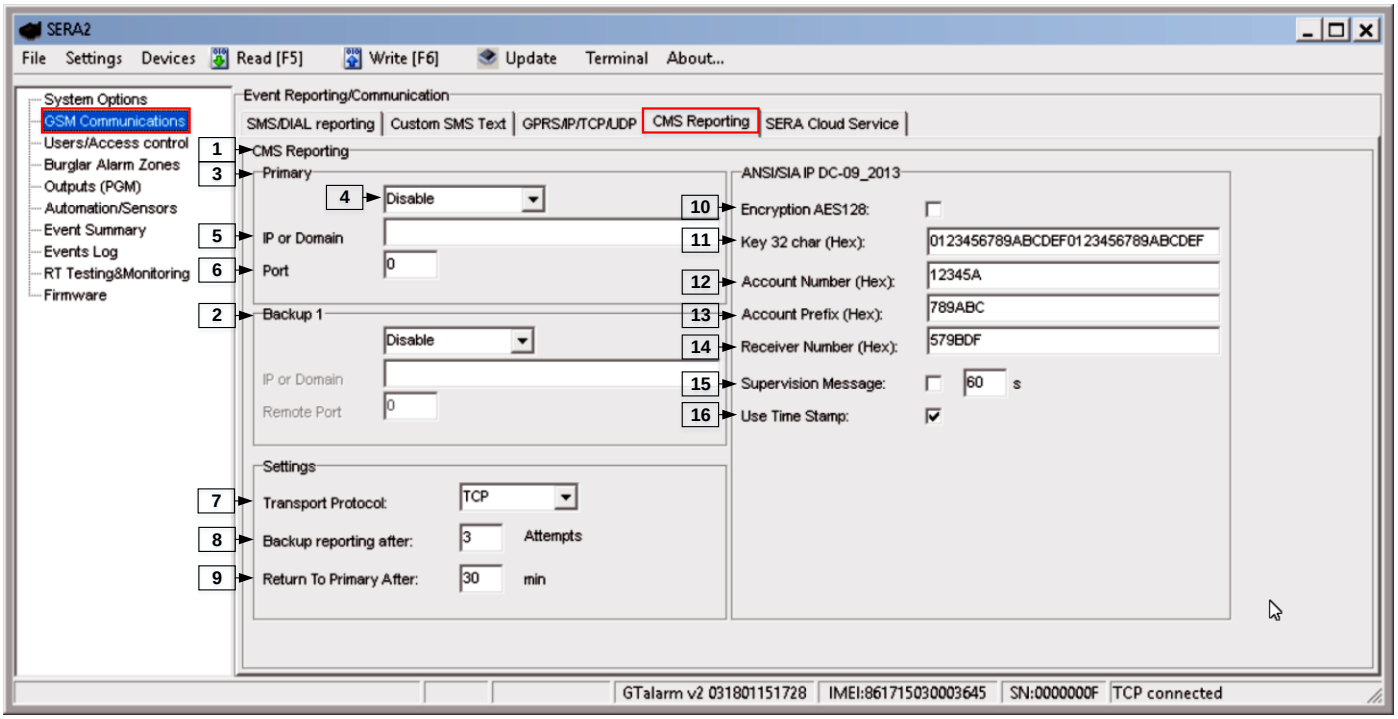


Figure 37 the example of GSM Communication > CMS Reporting window

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 9 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.

16 General system options programming

Sera2> System Options> General System Options

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.

> **!** 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.

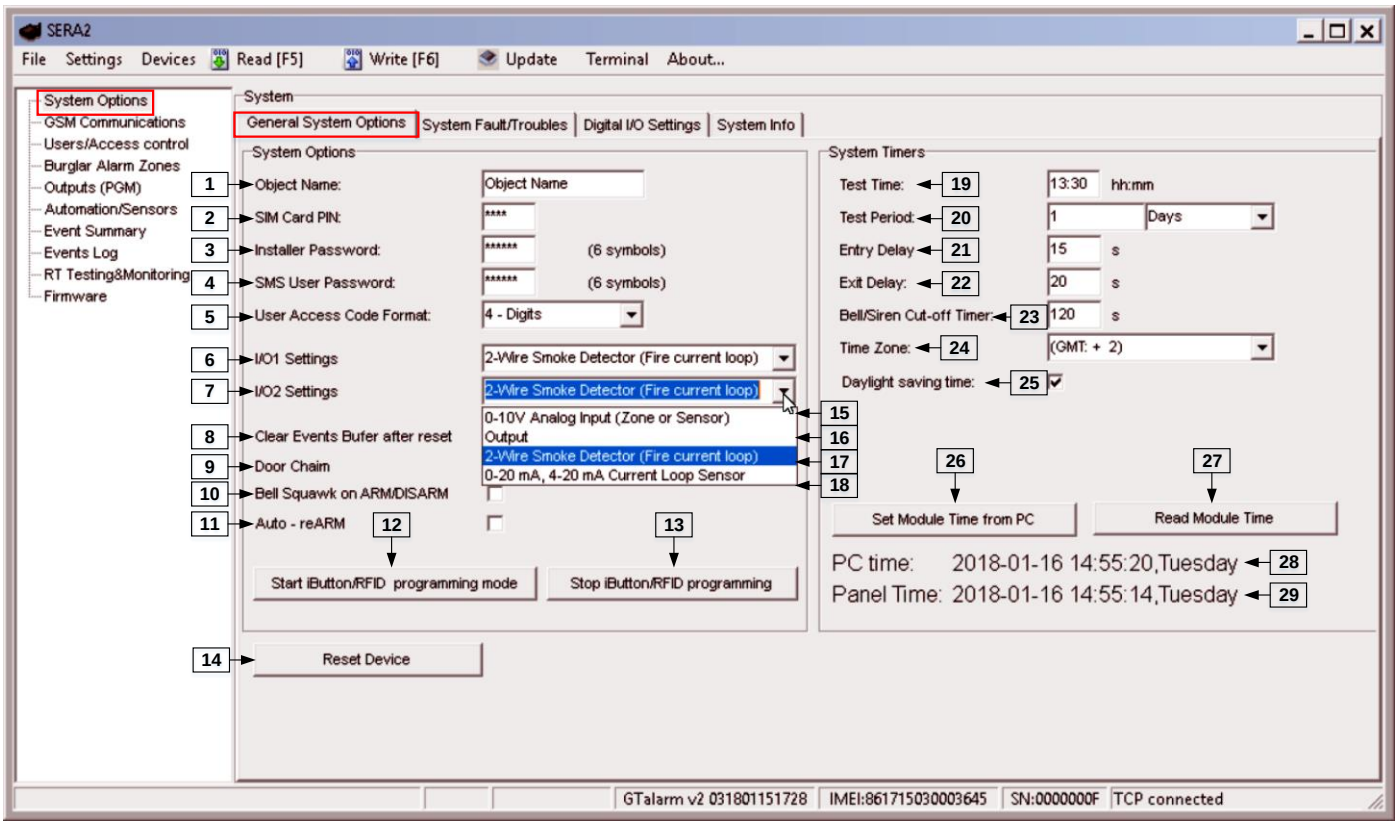


Figure 38 The example of System Options > General system Options window.

Table 10 Explanation of every field in "General System Options" window

1	**Object Name**	
2	**SIM Card PIN**	SIM card PIN code. Default 1234
3	**Installer Password**	The default installer password is **000000**. This password allows you to enter programming mode, where you can program all features, options, and commands of the module.
4	**SMS User Password**	The default SMS User Password is **123456**. This code allows you to utilize arming method, as well as program user codes.
5	**User Access Code Format**	A 4-digit or 6-digit user access code format can be selected.
6	**I/O1 Settings**	2-Wire Smoke detector (Fire current loop) **or** 0-10V Analog Input (Zone or Sensor) **or** Output **or** – 0-20mA, 4-20mA Current Loop Sensor could be assigned to the I/O1
7	**I/O2 Settings**	2-Wire Smoke detector (Fire current loop) **or** 0-10V Analog Input (Zone or Sensor) **or** Output **or** – 0-20mA, 4-20mA Current Loop Sensor could be assigned to the I/O2
15	**0-10V Analog Input (Zone or Sensor)**	0-10V Analog sensors will be connected to the input
16	**Output**	Input will be used as output
17	**2-Wire Smoke Detector (Fire current loop)**	2-Wire Smoke detectors will be connected t the input.
18	**0-10mA, 4-20mA Current Loop Sensor**	0-20mA, 4-20mA Current Loop Sensors will be connected to the input.
8	**Clear Event Buffer After Reset**	When the cell is checked, the memory of unsent reports will be deleted after the module resetting
9	**Door Chime**	When this box is checked, violations of set Delay zones at the alarm turned off will be accompanied by keyboard audible (Buzzer) signal
10	**Bell squawk on ARM/ DISARM**	The module can activate the bell output briefly causing the squawk to alert users that the module is being armed, disarmed or that an Entry or Exit Delay was triggered. Enable or disable the desired option.
11	**Auto re-ARM**	The module can be programmed to arm the module if there is no activity in the area after the system disarming.
12	**Start iButton/RFID programming**	All added iButton keys or RFID cards will be registered in the order of sequence by clicking Start programming
13	**STOP iButton/RFID programming**	To finish entering iButton keys or RFID cards, click Stop programming button
19	**Test Time**	Auto Test report time of day
20	**Test Period**	Auto Test report period

21	**Entry Delay**	This delay gives you time to enter the armed premises and enter your code to disarm your system before the alarm is triggered.
22	**Exit Delay**	The system will trigger the Exit Delay Timer to provide you with enough time to exit the protected area before the system is armed.
23	**Bell/ Sirel Cut – off Timer**	Duration of audible signal (sirens, Bell) after the alarm system activated. Time shall be written in seconds, duration from 0 to 9999.
24	**Time Zone**	
25	**Daylight saving time**	
26	**Set module time from PC**	To set the clock click Set time from PC button and the clock will be set using computer's clock.
27	**Read module time**	To read the clock of panel.
28	**PC Time**	
29	**Panel Time**	
14	**Reset Device**	Reset module command

17 RT Testing & Monitoring. Hardware.

Sera2> RT Testing&Monitoring> Hardware

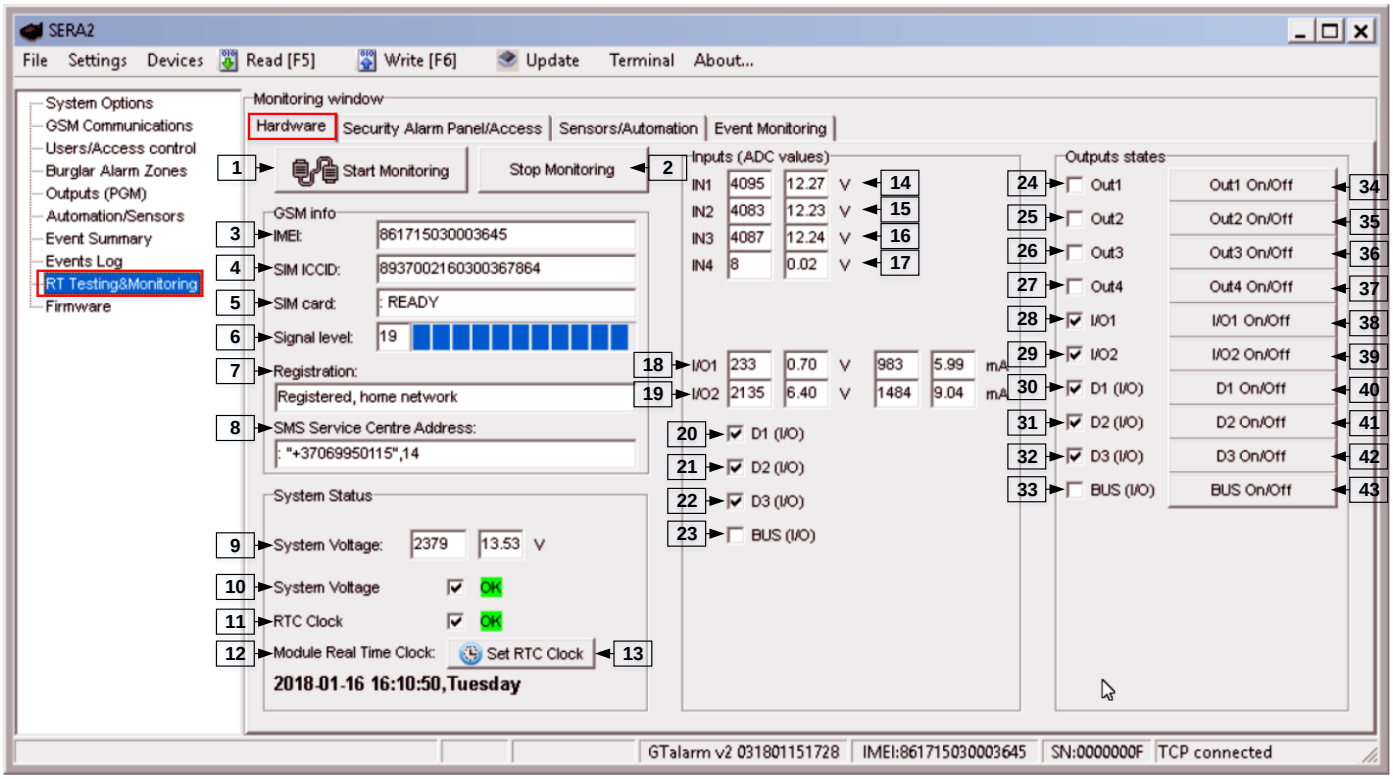


Figure 39 The example of RT Testing & Monitoring > Hardware window

Table 11 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.

18 RT Testing & Monitoring Security Alarm Panel/ Access

Sera2> Testing & Monitoring> Security Alarm Panel/ Access

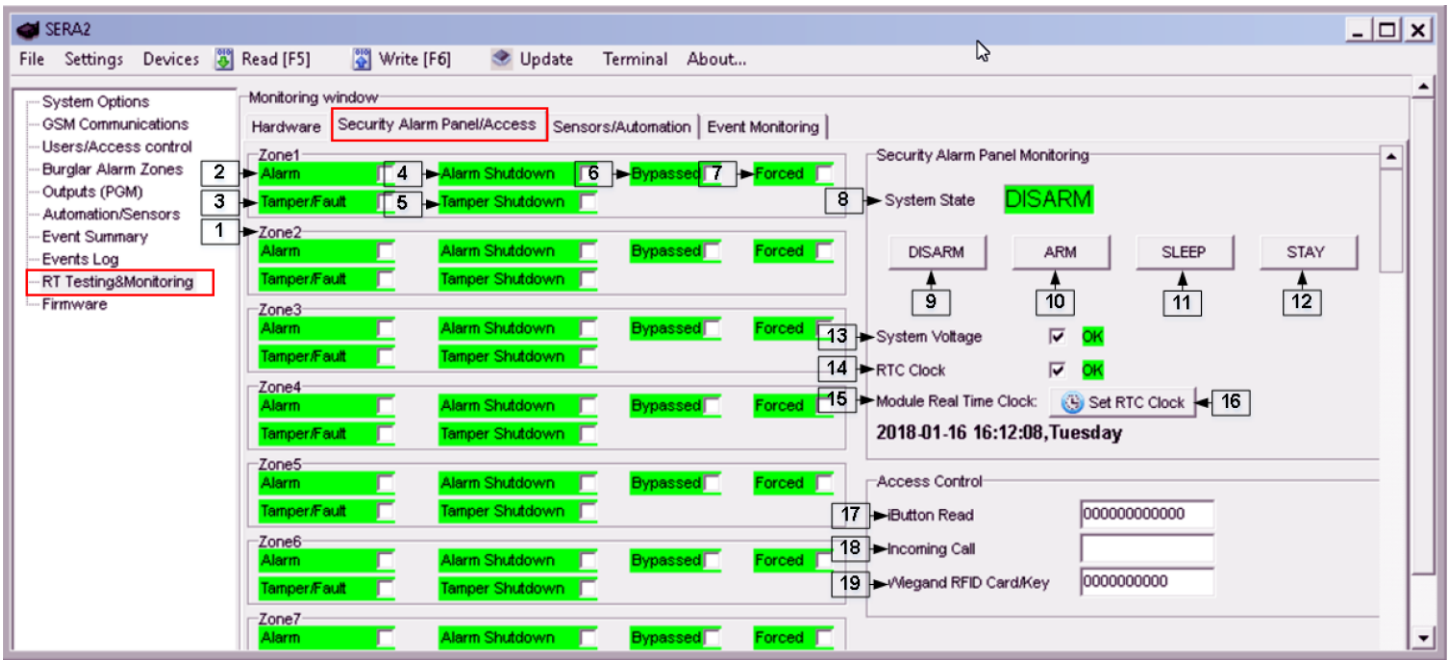


Figure 40 the example of RT Testing & Monitoring > Security Alarm Panel/ Access window

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 12 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.

19 Event Summary (Events)

Sera2> Event Summary

1 ID	2 Name of Status Event	3 Code	4 Enable	5 Alarm SMS Text	6 Restore SMS Text	7 Type
1	A non-specific medical condition exists	100	☑	Medical Alarm	Medical Restore	SER
2	Emergency Assistance request	101	☑	Personal Emergency	Personal Emergency	NONE (8) / USER (9) / ZONE (10) / NUM (11)
3	A user has failed to activate a monitoring device	102	☑	Fail to report in	Fail to report in	
4	A non-specific fire alarm condition exists	110	☑	Fire Alarm	Fire Restore	

Figure 41 the example Event Summary (Events) window

Table 13 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**	9	None
		10	USER — Refer to USER Report Options
		11	ZONE — Refer to Zone Report Options
		12	NUM — Refer to Numerical Report Options

20 Software updates

Sera2> About (in the command line)

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

Figure 42 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.

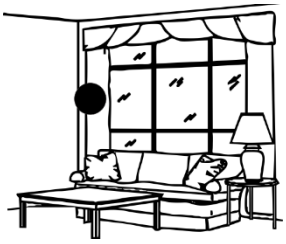
These steps will let better understand the problem and will reduce the time to find the solution.

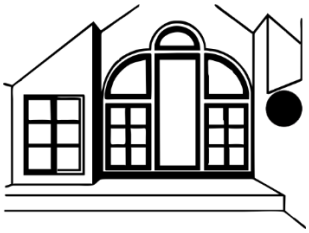
! If you want to receive software updates, go to Settings and mark "Check for Updates Automatically". When new update will be available, the program will inform you, and you have to start the update. After that you have to connect the module to the computer via mini USB cable. You have to write this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

21 Recommendations to the installer

21.1 Glass break, shock sensors

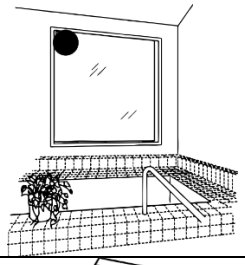
Glass break sensors
Acoustic sensor recess mounts in a 1 in. (2.54 cm) hole. One sensor can protect an entire room. Sensor range is 25 ft. (7.62 m) to the bottom of the glass in a 360˚ pattern, so the sensor can be ceiling mounted, mounted on the opposite wall, or on an adjoining wall.





Shock sensors in bathroom

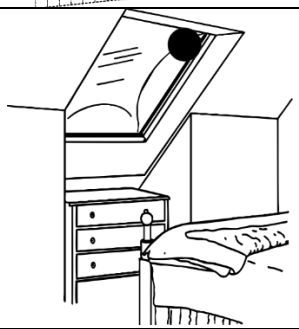
In residential installations, bathroom windows may have to be protected as part of a complete perimeter system. Bathrooms are challenging environments for glass break sensors for two reasons. 1) Humidity can be very high when a shower or tub is used. 2) Bathrooms are acoustically live rooms — they are typically small, with bare floors and many sound-reflecting surfaces. Acoustically live rooms have a greater potential for false alarms when acoustic glass break sensors are used. Humidity can also be a problem for most glass break sensors. Shock sensors have fewer problems than acoustic sensors in high humidity environments. For best false alarm immunity in bathrooms, if possible use a hermetically sealed shock sensor mounted on the glass or a frame mounted shock sensor.



Shock sensors for skylights

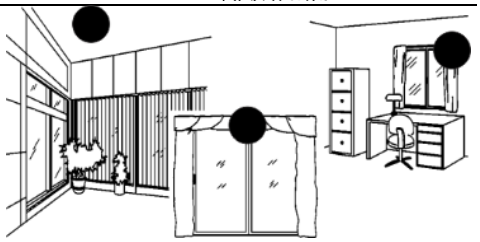
Skylights can be a vulnerable entry point to many homes and businesses. Many skylights are made of Plexiglas™, Lexan™, or other type of plastic. This eliminates the option of using acoustic glass break sensors since they are designed for detecting breaking glass, not plastic.

For protecting plastic skylights, mount a shock sensor in a corner of the skylight 1 in. (2.54 cm) from the frame. Note: The plastic material in the skylight will absorb much of the shock energy from a break. The range of a shock sensor on plastic is typically 50% less than the range on glass. A shock sensor with a 7 ft. (2.13 m) range on glass would generally have a 3-1/2 ft. (1.07 m) range on a plastic skylight. When protecting plastic skylights, it is essential to thoroughly test the sensor by rapping the far opposite corner of the skylight with the handle of an 8"-10" screwdriver. If the sensor trips to the rap test, its range is sufficient to detect an actual break-in. An acoustic glass break sensor can be used for glass skylights. The sensor can be mounted on any wall within range of the skylights, or on the ceiling.



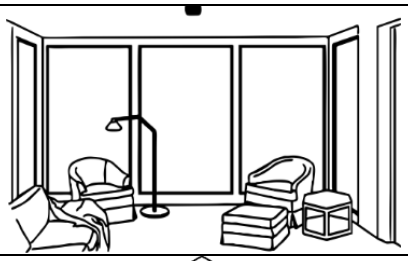
Shock sensors for rooms with curtains and blinds.

Glass mounted or frame mounted shock sensors are unaffected by curtains and blinds. The sensor should be mounted in the corner of the glass, 1 in. (2.54 cm) from the frame. Mount the sensor on the window frame to protect one or more windows. It will protect a 10 ft (3.05 m) area. However, its range can be reduced if window coverings are touching the glass. The sensor can be mounted anywhere in a room except on the frame (as long as the glass to be protected is within its range), and can detect breaking glass when blinds and light drapes are present. Mount the sensor on the ceiling, on an adjoining wall, or on a wall opposite from the glass to be protected. Mounting the sensor on the same wall as the glass should be avoided because the signal may be dampened before it bounces back to the sensor.



Long range acoustic sensor for large rooms with multiple windows.

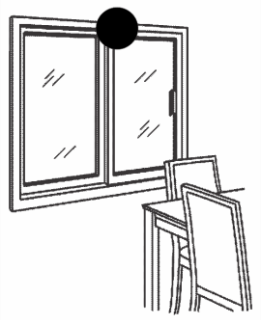
Most large rooms have several windows, often widely spaced from each other. The most economical way to protect large rooms with multiple windows is with a single, long range acoustic sensor. However, care should still be taken to match sensor range to room size. A sensor whose range extends well beyond the boundaries of the room is acoustically “hot” and vulnerable to false alarms. For protecting glass on more than one wall, ceiling mounting is most desirable. Make sure that all protected glass is within the radius coverage of the sensor. For any glass to be protected by an acoustic sensor, the distance from the bottom of the window to the sensor must be no more than the sensor’s maximum range. For protecting one wall of glass, mounting an acoustic sensor on the opposite wall is best (if all the glass to be protected is within the sensor’s range).

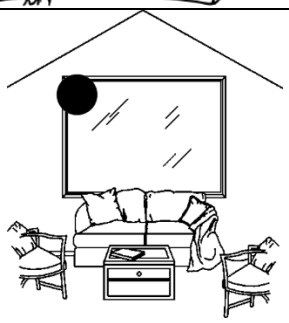


Shock sensors for small rooms

False alarms are more likely in small, acoustically live rooms such as small kitchens, glass entry airlocks, stairwells, small glass offices, and utility rooms. For best false alarm immunity the range of the sensor should be matched to the size of the room and glass area to be protected. Shock sensors offer the best false alarm immunity in acoustically live rooms, and are the most economical if there is only one window to protect. Acoustic sensors will provide good false alarm immunity if selected properly.

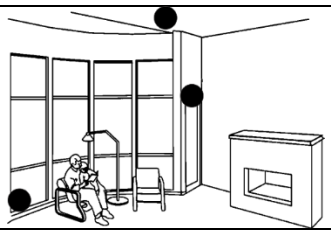
If it can be avoided, do not install acoustic sensors with large range into small rooms. A sensor with 25 ft. (7.5 m) diameter range into a 10 ft. (3.05 m) room increases the risk of false alarm. Choose an acoustic sensor with range comparable to the size of glass to be protected.





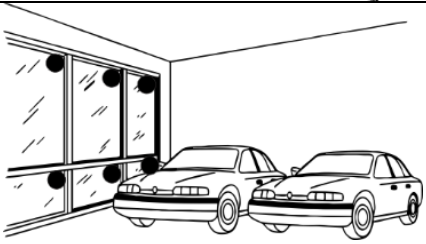
Magnetic contact, glass break, shock sensors in occupied areas.

Glass break sensors can be armed while rooms are occupied to alert the family inside a home or the employee working late or on the weekend. Occupied area protection means sensors are armed when the perimeter loop of the system is armed. In contrast to 24-hour loops, which are armed continuously, all day and all night, a perimeter loop containing glass break sensors is armed only when the magnetic contacts on doors are armed — generally, after hours, when buildings are quieter. Today’s advanced acoustic sensors provide excellent false alarm immunity in occupied areas if installed on the perimeter loop. Shock sensors provide 24-hour loop protection without false alarms.

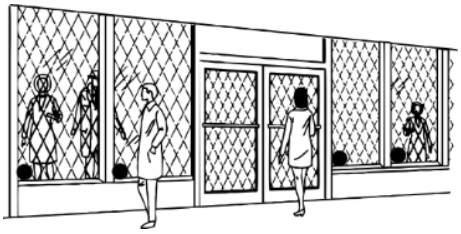


Shock, acoustic sensors for storefront glass.

Merchants often want glass break protection on their front windows, in order to have the alarm sound as soon as the glass breaks. While this does not prevent “smash and grab” losses, it will prevent most burglars from actually entering the building. For storefront windows shock sensors are always the best choice. A shock sensor is visible from the outside, which might deter burglars before the glass is broken. And shock sensors are less likely to be set off by street noise, or by rolling metal shutters, than are acoustic sensors. Due to range limitations, however, shock sensors can be more expensive to install. Multiple sensors may be required to cover the same glass area that one acoustic sensor can protect. Acoustic sensors can be successfully used to protect storefront glass if store personnel are properly trained to not block the glass. Acoustic sensors must be able to “see” all the glass that they are protecting. If a sensor’s line of sight to the glass is blocked by store displays or furniture, the sensor is unlikely to detect a break-in through the blocked glass.

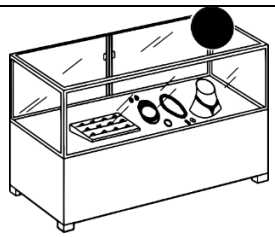


Acoustic sensor for store window and roll – up metal shutters.



Retail shops in high crime areas will often have roll-up metal shutters to protect the glass windows at night. The clanging and banging sounds of these shutters can cause acoustic sensors to false alarm. False alarms can also be caused by people rattling the shutters, and by other vibrations. For windows with roll-up shutters, shock sensors provide the best false alarm immunity. On-the-glass shock sensors have better false alarm immunity than frame-mounted shock sensors, and are therefore the preferred choice. On-the-glass sensors are also easily visible from the outside, which may help deter a break-in. If using acoustic sensors, use only an advanced sensor with excellent false alarm immunity. Mount the sensor back into the room, away from street and roll-up shutter sounds. An advanced sensor mounted 15 ft. back from the glass should provide false-alarm-free operation in most applications.

Shock and acoustic sensors for display and jewelry cases.



Museum curators and retailers with glass display and jewelry cases often want the extra protection of glass break sensors inside their cases. Both shock sensors and acoustic sensors are options for such protection. Note: Acoustic glass break sensors sealed within a glass box are extremely “live,” and are vulnerable to false alarms if the case is accidentally struck by keys or other metal objects. For this reason, acoustic sensors are appropriate only if the sensor will be armed while the premises are not occupied. For occupied or 24-hour protection of display cases, it is best to use shock sensors. A frame mounted shock sensor will provide the most economical protection if there is more than one piece of glass to protect. Note: An actual glass break generates twice as much energy to the shock sensor as a rap test. More than one shock sensor may be needed to protect all the glass in a display case. If, for cosmetic reasons, this is not a viable solution, a single acoustic sensor may be used. To protect a glass case when a room is not occupied, use an acoustic sensor with limited range.

21.2 Smoke, CO Detectors

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

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

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

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

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

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

• Do not locate detectors in areas of high humidity.

• Do not locate detectors in areas where the temperature rises above 38ºC (100ºF) or falls below 5ºC (41ºF).

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 -10ºC or exceed 40 ºC.

• 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 un switched AC power. Install hardware in the sequence indicated in the following pages. Do NOT apply power until installation is complete.

22 Warning! The limitations of this alarm system.

While this system is an advanced design security system, it does not offer guaranteed protection against burglary or fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

• Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.

• Intrusion detectors (e.g., passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.

• Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.

• A user may not be able to reach a panic or emergency button quickly enough.

• While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second-floor detector, for example, may not sense a first-floor or basement fire. Moreover, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper

storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson. Depending upon the nature of the fire and/or the locations of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.

• Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of protected area approaches the temperature range of 90° to 105°F, the detection performance can decrease.

• Alarm warning devices such as sirens, bells, or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices sound on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm warning devices, however loud, may not warn hearing-impaired people or waken deep sleepers.

• Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.

• This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 10 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly.

Installing an alarm system may make one eligible for lower insurance rates, but an alarm system is not a substitute for insurance. Homeowners, property owners, and renters should continue to act prudently in protecting themselves and continue to insure their lives and property.

The UAB “Topkodas”, the module GTalarm2 does not offer any guarantee of protection against burglary, robbery, theft, or any type of emergency.