GTalarm2
Application Note: Access Control System

Monitoring, alarm, control.

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

- Access control.
- Parking lot control of residential houses or offices.
- Gate control of private houses.
- Manually control doors.
- Remotely control doors from everywhere, anytime.
- Add/ Remove users for RFID card, iButton, key button, mobile phone control.
- Monitor system status and receive alarms.
- Assign access level to the user (Control door1 …. door6).
- Supervisor, employer, VIP modes.
- Change the configuration from everywhere.
- Save reports.

Benefits:

- Limit access to areas containing dangerous or hazardous equipment/materials
- Restrict access to contaminated areas or areas under construction
- Protection of personal assets (controlled access to locker rooms /staff only areas)
- Record working hours for time on site and time spent in restricted areas etc.
- Prevent off street walk-ins protecting lone or vulnerable staff.
- Restrict access to walk-in freezers
- Wandering patient protection
- Protection of infants and children in nurseries/schools
  - Restrict access by unauthorized members of public
  - Prevent unauthorized egress by unaccompanied minors
- Control of equipment or tools in and out of hazardous / restricted areas
- Restrict access to private company/hotel car parks
- Supervisor mode for teachers restricting pupil access to classrooms / workshops / swimming pools
- Supervisor mode to escort visitors/contractors into restricted areas
- Dual access for opening high risk areas to ensure individuals are not put at risk

Features of the module GTalarm2

- 3 Digital Inputs/Outputs 3.3V , 20mA,
- Wiegand interface, Dallas 1-Wire Bus
- 4 PGM outputs 24V/1000mA, Open Drain.
- Digital expansion module BUS.
- Built-in access control features
- In-field firmware upgradeable via USB and SERA2 software
- Events log buffer, 2048 events
- Program remote controls using the master or installer codes
- Up to 800 users remote controls with mob phone,
- Up to 800 users remote controls with iButton or RFID keycard
- Up to 800 user code. To control with Wiegand keyboard.
- Built-in-real-time clock backup battery
- Unlimited control via SMS.
- Push button software reset

The meaning of icons in the manual:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Very important</td>
</tr>
<tr>
<td>i</td>
<td>Important</td>
</tr>
<tr>
<td>📖</td>
<td>About the manual</td>
</tr>
</tbody>
</table>
## Contents

1.1 General view of the module .......................................................... 4  
1.2 Meaning of LEDs and contacts .................................................. 4  
1.3 First steps to prepare GTalarm2 module and Sera2 software ............. 4  
2 Power supply, Battery Wiring ....................................................... 5  
3 Application examples .................................................................. 5  
3.1 One or multiple door control with mobile app .................................. 5  
3.2 Door control during specified time interval with RFID card ............... 6  
4 Logging entry, exit and other events. Monitoring ................................ 6  
4.1 What could be controlled ........................................................... 7  
4.2 Door control methods ................................................................ 8  
4.3 Lift control example ................................................................. 9  
5 System Management ................................................................... 9  
6 Step by step how to build access control system ................................ 9  
7 Arming / disarming the system ..................................................... 10  
8 Outputs PGM ............................................................................. 10  
8.1 Output definitions and timing diagrams ....................................... 11  
8.2 Output PGM wiring. Bell, Relay, Led Wiring ............................... 12  
8.3 Quick start outputs .................................................................. 12  
8.4 Outputs. Bell & PGM programming ........................................... 13  
9 Wiegand keypad wiring ............................................................... 14  
9.1 Wiegand probe wiring .............................................................. 14  
10 Wiegand keypad and iButton codes entering .................................... 15  
10.1 Codes entering manually in Sera2 software ................................ 15  
10.2 Codes entering automatically in Sera2 software .......................... 15  
10.3 Codes entering by sending SMS message ................................... 15  
11 Users database for iButton, RFID, key button control ....................... 16  
12 Output: doors, gates settings ..................................................... 17  
13 System remote monitoring via mobile phone. Periodic Info SMS ......... 18  
14 Connecting to the Web Server ..................................................... 19  
15 General system settings. Real-time clock (RTC) ............................. 19  
16 Access control output with logging ............................................. 21  
17 Event log .................................................................................. 21  
18 System Testing & Diagnostic tool ................................................ 21  
19 Event monitoring ..................................................................... 21  
19 Monitoring Inputs, outputs & general system info ............................ 22  
20 Software updates ..................................................................... 23  
21 Control via SMS messages ....................................................... 24  
21.1 The table of users SMS commands ........................................... 24  
21.2 The table of installers commands ............................................. 24  
22 Access control terms and definitions ......................................... 25
1.1 General view of the module

![GTalarm2 PCB Layout](image)

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

1.2 Meaning of LEDs and contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Indication variations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDG (green) built-in LED</td>
<td>Watchdog heart beat blinking, remains lit for 50ms, and turns off after 1000ms.</td>
<td>The module is functioning.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The module is out of order or no voltage.</td>
</tr>
<tr>
<td>REG (yellow) built-in LED</td>
<td>Lights continuously</td>
<td>Modem has been registered to the network.</td>
</tr>
<tr>
<td></td>
<td>Flashes, remains lit for 50ms, turns off for 300ms</td>
<td>Modem is being registered to the GSM network.</td>
</tr>
<tr>
<td></td>
<td>Blinking fast, remains lit for 50ms turns off for 50ms</td>
<td>PIN code of SIM card error. PIN code request should be removed</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Modem failed to register to the network.</td>
</tr>
<tr>
<td>DATA (red) built-in LED</td>
<td>Lights continuously</td>
<td>The memory of the module contains unsent reports to the user or to the server.</td>
</tr>
</tbody>
</table>

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

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

GTalarm2 Application Note: Automation  www.topkodas.lt
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

![Image](https://www.topkodas.lt/Downloads/GTalarm2_TPS12_AN_EN.pdf)

**Figure 2 The meaning of icons**

Each time after configuring the module press Write 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 icon. In order to save configuration go to File 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:**
[https://www.topkodas.lt/Downloads/GTalarm2_TPS12_AN_EN.pdf](https://www.topkodas.lt/Downloads/GTalarm2_TPS12_AN_EN.pdf)

**Power supply installation manual:**

![Image](https://www.topkodas.lt/Downloads/GTalarm2_TPS12_AN_EN.pdf)

**Figure 3 Power supply connection**

## 3 Application examples

### 3.1 One or multiple door control with mobile app

When the user activates the output from mobile app, the information is sent to the door controller. The controller compares data to a list of authorized users in the database. If there is a match, the controller will send a signal to release the door lock, gate, or barrier.

Could be specified which user will control which output. For example, the first user can control only the first door (Out1), and the second user can control door lock, gate, barrier (Out1, Out2, Out3).
3.2 Door control during specified time interval with RFID card

- **Start date**: 20180226
- **Door control time interval**: 10:00
- **End date**: 20180228
- **12:00**

![Figure 4 Door control during specified time interval](image)

It is possible to set a certain time and date interval during which the user will be able to control the door using an RFID card. After and before the specified time and date range, the card will become inactive.

The date, time interval, card number information could be set via mobile phone, PC via internet, GSM network or connected the module to the computer via mini USB cable.

**The field temporary should be market.**

Regarding user table Temp - means temporary date limited access. You have to check this to enable reservation Date/Time interval.

En- User enable/ Suspended. This function is not working now is reserved for furfure use.

![Figure 5 Web APP interface.Add/Edit/Delete User.](image)

4 Logging entry, exit and other events. Monitoring.

Entry, exit, alarms is recorded to the log file and to the memory of controller. Events log buffer contains up to 2048 events. Unlimited events can be logged in SERA Cloud Linux server. All events can be monitored in Standard web browser or in Android App.

The log file is saved. If the AC power is loss, events is saved to the memory of the controller. Then, once the communication with the system PC or controller is re-established, the log of access and alarm events will be uploaded with date & time stamp.

It is possible to chronologically register up to 2048 time stamped records (if more events needed, it is possible log events to the server). System events reflects: Contact ID code, event, time, and note. It is possible to save the event log to .log file or clear it.

The event log allows the system to automatically replace the oldest records with the latest ones.

Outputs state monitoring could be performed via mobile phone, PC or SMS message. 8 user's phone numbers for remote monitoring purpose identified as Users from 1 through 8. When the phone number is set, the user will be able receive the input alarm SMS text messages from the system.
It is possible to control up to 6 doors, connected to Out1…Out4, I/O1… I/O2 outputs of the controller GTalarm2. One or more readers (iButton probes) and the relevant door hardware are connected to the controller. Control of the door hardware is run from the controller to the access point and will act depending on signals from the controller.

A GTalarm2 controller hold information required to decide whether a user is allowed through a door. Subject to how the controller communicate, alarm events may be passed to controller. This communication can be used for event driven actions, such as activating a sounder in a different area.

### 4.1 What could be controlled

**Door Status Monitoring.** A door contact is used for sensing opening and closing of a controlled door. Door contacts are used to monitor events such as:
- Door forced alarm – a door being opened without the use of the reader or normal egress device
- Door held alarm – someone holding the door for another party or blocking the door for delivery or to return later if they have no card.

Door contacts are recommended for higher grades of security BS EN 60839-11-1 requires the monitoring of doors in grades 2 to 4.

**Lock Status Monitoring.** Lock monitoring is used to indicate whether a closed door is locked or not. This is not an alternative to monitoring the door and should only be used in addition to door contacts.

**Egress devices.** Having replaced (or disabled) standard lock sets in most access control installations, a means of providing controlled and authorized egress may be required so that any door monitoring contact is isolated for the approved period of the door release. This is commonly achieved with a simple Request-to-Exit switch, a movement sensor or a reader.

**Microphone speaker.** The system utilizes telephone communications between visitors and residents for granting access. The four relay output channels can be programmed to control electric door strikes, magnetic locks, or barrier gates. Microphone and speaker control.

**Entrance control includes barriers, automatic gates, and doors.** The entrance control product increases the security level of the access control system by either providing a physical barrier to restrict unauthorized access or by providing a method of detecting unauthorized access and generating an alarm. 800 users could control access via mobile phone and/ or with iButton, RFID, key button. When the phone number is set, the user will be able to control the system by app, SMS text messages as well as by free of charge phone call. The module GTalarm2 allows to assign one or several outputs to a certain user. By default, the system ignores any incoming call and SMS text message from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user's phone number.

Automatic output control is possible: control the door or gate, when the inputs of the module is activated. Turns ON the output (s) for the preset time period (pulse) resulting in the gate opening or closing, depending on the current gate state.

Typically, the inputs are used to receive notifications regarding jammed gate or gate state. Each input’s sensitivity level can be customized by a delay time. If an input is left triggered until the delay time expires, the input is considered violated. Each input has a name that can be customized, for example: “Gate Open”. Once disabled, input alarm event will no longer be followed by an SMS text message.

The system comes equipped with internal real-time clock (RTC) that keeps track of the current date and time.
4.2 Door control methods

Up to 800 users is able to 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 control the outputs.

Unlimited iButton probes could be connected to the controller. It is possible to specify which door the user can access.

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 5]
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.

4.3 Lift control example

Lift control is an extension to the concept of access control, using the user’s iButton keys to grant access to floors, rather than granting access through a door. For instance, a token reader is fitted in each lift cab, using technologies compatible with the rest of the system. Depending on the user’s access rights, access to one or more floors may be granted. If the user does not have access to a given floor, the button for that floor is disabled. “Free access” is sometimes provided to allow anyone access to certain floor(s) (e.g. ground floor). For maximum flexibility, the lift control system may be capable of controlling multiple lift shafts simultaneously.

5 System Management

As with any system, efficient management is key to ensuring the security and operability of the access control system is maintained.

Backups. It is possible to save the configuration file and event log file to ensure that in the event of any failure configuration and historic events can be recovered if required.

Token Management. The management of tokens is critical to the secure operation of the system. The control and security of access to the system is password protected to ensure that the registration of new users is controlled.

Reporting. To ensure that the system remains efficient regular reports should be run that check a range of events from the system, such as unauthorized access attempts, usage lists etc.

Information Security. Access to any terminals and servers that run the access control system is secured from inadvertent access.

6 Step by step how to build access control system.

1. Connect the Wiegand keypad/ RFID reader. Go to Sera2> System Options> Digital I/O Settings and set Digital I/O D2 to Wiegand (1) interface DATA0 and Digital I/O D3 to Wiegand (1) interface DATA1. Write configuration by pressing write icon.
3. Connect the automatic gate, door hardware, barrier to the outputs Out1…Out4 of the module GTalarm2. Go to Sera2 Outputs (PGM). Parameters of the selected output should be set: output operation description (OUT definition): disable, bell, buzzer, flash, system state, ready, automation/CTRL, ARM/DISARM, Set State type: flash, timer, steady mode. If necessary output operation might be inverted. Write configuration by pressing write icon.
4. Go to Users/ Access control and set user name, type, phone, iButton code, RFID keycard, keypad code, which output will be controlled, ARM/DISARM, MIC, temp, start date, end date.
5. Go to GSM Communication> SMS/DIAL reporting and enter phone numbers for alarm events monitoring.
7 Arming/ disarming the system.

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 sirenbell 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 to the user phone number that the SMS text message was sent from. The user can also set a custom text, which will be sent 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.

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.

8 Outputs PGM

The module GTalarm2 has:
- 4 open drain (1A) outputs: OUT1 (1A)... OUT4 (1A). The outputs can be used for siren, relay, and lamp connection. These outputs can be controlled via short call or SMS. Output operation algorithms: Automation /CTRL, Siren, Buzzer, ARM state, Zones OK, Light Flash, inverting, pulse mode
- 2 open drain (20mA) outputs: I/O1 (20mA)... I/O2 (20mA). These outputs can be used for solid state relays, LEDs, to control devices up to 20mA.
- 3 outputs: D1 (10mA, Max Voltage 3.3V) for LED, solid state relays control. Max voltage 3.3V
- 1 programmable output BUS. Voltage 8-15V, Current 20mA
- OUT4 max current = (-V) 1000 mA
- All outputs can be controlled via short call DIAL or via SMS message. This feature may be used for gate opening
- Output alarm parameters may be programmed.
- Programmable algorithms for outputs operation: CTRL/SMS/DIAL, SIREN, BUZER, ARM state, Zones OK, Light Flash, inverting, pulse mode

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

GTalarm2 comes equipped with four open-drain 24V/1A PGM outputs allowing to connect up to four devices or relays. Also GTalarm2 comes with two programmable 20mA outputs, three 10 mA and max voltage 3.3V outputs, and with one 20mA programmable output expansion module BUS. Each PGM output has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined PGM output, for Example: Lights.

<table>
<thead>
<tr>
<th>ID</th>
<th>Output Location in Hardware</th>
<th>Output Label</th>
<th>Out definition</th>
<th>Mode</th>
<th>Out Timer</th>
<th>Invert</th>
<th>Pulseing</th>
<th>Pulse ON Time</th>
<th>Pulse OFF Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OUT1 (1A)</td>
<td>Heat Pump ON/OFF</td>
<td>Automation/CTRL</td>
<td>Steady</td>
<td>10s</td>
<td>False</td>
<td>False</td>
<td>100ms</td>
<td>100ms</td>
</tr>
</tbody>
</table>

If the output is not in use, it should be disabled. Once a PGM output is disabled, it can no longer be turned ON or OFF unless it is enabled again. It is possible to instantly turn ON an individual PGM output for a determined time period and automatically turn it OFF when the time period expires. When the PGM output is turned ON or OFF, the system will send a confirmation by SMS text message to the user phone number that the SMS text message was sent from.

The automatic action of the determined PGM output can be set as follows: Turn ON, Turn OFF, and Pulse. The PGM output action can automatically switch ON or OFF under the following conditions: System armed or disarmed, Alarm begins or stops, Temperature falls below the set MIN value, Temperature rises above the set MAX value, Zone violated, Zone restored. The user can also set a custom text, which will be sent by SMS text message to user phone number when the automatic PGM output action is carried out.

Set output's parameters step by step:
1. Open SERA2 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.

GTalarm2 Application Note: Automation  www.topkodas.lt
8.1 Output definitions and timing diagrams

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.

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.

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

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.

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.
8.2 Output PGM wiring. Bell, Relay, Led Wiring

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

1. Connect devices to the selected outputs as shown in the figures below. For sound signaling we recommend to use siren DC 12V up to 1500mA. It is recommended to connect the siren to the system by using 2 x 0.75 sq. mm double insulation cable. Auxiliary BUZZER is recommended to be installed inside the premises not far from the entrance. Buzzer operates together with the main siren also when the system starts calculating the time to leave the premises and the time till alarm response of the security system after entering the premises (see clause 7.1). It is possible to use buzzer of hit point PB12N23P12Q or similar modified piezoelectric 12V DC, 150mA max Buzzer. Standard AC/DC adapter with the voltage 10V-14V and current >=1A might be used to powering the module.

8.3 Quick start outputs

1. Install SERA2 software.
2. Connect the module to the computer via mini USB cable.
3. Go to Outputs (PGM) window in the SERA2 software
4. Parameters of the selected output should be set:
   - output operation description (OUT definition): disable, bell, buzzer, flash, system state, ready, automation/CTRL, AC OK, battery OK, ARM/DISARM, alarm indication, lost primary channel, lost secondary channel, fire sensor, RH sensor trouble.
5. State type: flash, timer, steady mode.
6. If necessary output operation might be inverted.
7. Write configuration by pressing write icon.
8. Outputs can be controlled only in Automation/CTRL mode.

9. If you need to control outputs by short call or SMS, go to “Users & Remote Control” window and enter telephone numbers of users, who will be able to control selected outputs via free short call.

10. Write configuration by pressing write icon

---

8.4 Outputs. Bell & PGM programming

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

---

Table 2 Explanation of every field in “Outputs” window

<table>
<thead>
<tr>
<th>ID</th>
<th>Output Location in Hardware</th>
<th>Output Label</th>
<th>Out definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Output sequence number.</td>
<td>The outputs hardware location.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disable</td>
<td>Output disabled</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Bell</td>
<td>Output for connection of audible sounder (siren). After the alarm system actuation a continuous or pulse (fire) signal is generated.</td>
<td></td>
</tr>
</tbody>
</table>
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.

---

### Mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Steady</td>
<td>Steady ON/OFF mode</td>
</tr>
<tr>
<td>6 Out Timer</td>
<td>Pulse time duration can be from 1 to 999999 sec.</td>
</tr>
<tr>
<td>7 Invert</td>
<td>Inversion is activated</td>
</tr>
<tr>
<td>8 Pulsating</td>
<td>Pulsating mode is activated. Then output is activated it will pulsate according pulse ON/OFF time.</td>
</tr>
<tr>
<td>9 Pulse ON Time</td>
<td>Pulsating mode pulse ON duration.</td>
</tr>
<tr>
<td>10 Pulse OFF Time</td>
<td>Pulsating mode pulse OFF duration.</td>
</tr>
</tbody>
</table>

---

9 Wiegand keypad wiring

Sera2> System Options> Digital I/O Settings

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

Wiegand keypad wiring diagram:

Connect Wiegand keypad as shown in the Fig.

How to configure Wiegand keypad:
1. Connect Wiegand keypad as shown in the Fig.
2. Go to “System options”> Digital I/O Settings
3. Set Digital I/O D2 to Wiegand interface Data0
4. Set Digital I/O D3 to Wiegand interface Data1
5. Write configuration

Figure 18 How to find “System Options > Digital I/O Settings window

Figure 9 Wiegand keypad connection

9.1 iButton probe wiring
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. By pressing Learn iButton button in the “System Options” window.
3. By sending SMS with command for new keys learning.
4. By 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.

10 Wiegand keypad and iButton codes entering

Sera2> Users/ Access Control

10.1 Codes entering manually in Sera2 software

It is possible to enter manually iButton or RFID Keycard codes. In that case, you have to:
Install SERA2 software
  1. Go to “Users& Remote Control” table.

Figure 20 How to find Users/ Access control window

1. Enter iButton or RFID Keycard codes for users.
2. Select iButton or RFID Keycard action OUT ARM/DISARM.
Write the configuration into the module by pressing “Write” icon

10.2 Codes entering automatically in Sera2 software

![Diagram of iButton connection](image)
It is possible to enter automatically iButton or RFID keycard codes via special programming mode. This special programming mode could be in Sera2 software by pressing Start iButtons/RFID programming mode “button”.

If enter iButtons learning mode by SERA2 software, needed, it is necessary:
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.

10.3 Codes entering by sending SMS message

When SMS message in relation to activation of iButton key programming mode received, touch the key to the reader and its unique code will recorded into system memory. Buzzer will notify about successful recording by beeping twice. The system allows to associate up to 800 iButton keys. Each time when the key is touched, 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, SMS message should be send.

It is possible to disable recording of new keys into memory by sending SMS message. 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 the installer have the key, that wanted to delete from the memory, installer have to send SMS and touch the key to the reader. 2 minutes later, the module will deactivate the keys deletion mode.

11 Users database for iButton, RFID, key button control.

GTalarm2 panel supports 4 – 6 doors. For each door, the readers, inputs, and outputs should be configured. A reader is a device that reads cards and either grants or denies access at the door. When the reader is disabled, neither exit nor entry by Card or PIN mode is allowed. Also, free egress is not allowed.

Different access method could be assigned to the users: RFID cards, i Button keys, Key button, and mobile phone. Enable the Card Only, PIN Only and Card or PIN access modes.

Each user can control different doors (door1…door6)

Several different modes could be configured. For example:
- Supervisor - After the supervisor disarm the system with his RFID card, iButton, key button or mobile phone, employers are allowed to open the door with their RFID cards, iButton keys, key buttons or mobile phones. If the supervisor arm the system, employers cannot open the door (The access control system has denied access to the specified users).
The 422 and 421 codes will be stored to the log.
- VIP users- users do not need a supervisor card to gain access.
The doors could be controlled with additional timer or steady mode.

![Figure 22 the example of Start/Stop iButton/RFID programming mode](image)
Figure 23: The example of Users/ Access control> Remote Control Users Table window

The field temporary should be marked.

Table 3: Explanation of every field in "Users & Remote Control" window

<table>
<thead>
<tr>
<th>No</th>
<th>ID</th>
<th>En</th>
<th>Type</th>
<th>Name</th>
<th>Phone</th>
<th>iButton Code</th>
<th>RFID Keycard</th>
<th>Keypad Code</th>
<th>OUT</th>
<th>ARM/DISARM</th>
<th>Temp</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>En- User enable/ Suspended. This function is not working now is reserved for future use.</td>
<td>Type: User, Master, Supervisor. This function is reserved for future use. Please use User or Master at the moment.</td>
<td>The name of users who will be able to control the module should be entered in this column. 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.</td>
<td>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.</td>
<td>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.</td>
<td>Key button code might be entered manually. In order to delete the code, it is necessary to enter 000000000000.</td>
<td>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.</td>
<td>If this check box is checked, a user will be able to ARM/DISARM the module by dialing.</td>
<td>Temporary data limited access. This field should be marked if it is needed to enable reservation Date/Time interval.</td>
<td>Reservation interval start date.</td>
<td>Reservation interval end date.</td>
<td></td>
</tr>
</tbody>
</table>

12 Output: doors, gates settings.

An output, or output relay, is a switch on the panel that either activate, de-activate or pulses an output device, such as a door lock or an LED. For example, a successful card read at a reader (input device) causes the output relay switch on the panel board to change the normal state of a door lock (output device), so that the normally locked door strike releases and permits entry.

The Outputs tab enables to enter a unique name to identify the device, pulse time, specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will sound or a door strike will remain released.

GTalarm2 comes equipped with four open-collector PGM outputs allowing to connect up to four devices or relays. If the output is not in used, it should be disabled. Once a PGM output is disabled, it can no longer be turned ON or OFF unless it is enabled again. It is possible to instantly turn ON an individual PGM output for a determined time period and automatically turn it OFF when the time period expires. When the PGM output is turned ON or OFF, the system will send a confirmation by SMS text message to the user phone number that the SMS text message was sent from.

The automatic action of the determined PGM output can be set as follows:
Turn ON/ OFF, pulse, system armed or disarmed, alarm begins or stops, zone violated, zone restored.

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

Step by step to configure outputs:
1. Go to Outputs (PGM) window in the SERA2 software
2. Parameters of the selected output should be set:
3. output operation description (OUT definition): disable, bell, buzzer, flash, system state, ready, automation/CTRL, AC OK, battery OK, ARM/DISARM, alarm indication, lost primary channel, lost secondary channel, fire sensor, RH sensor trouble.
4. Mode: flash, timer, steady mode.
5. If necessary output operation might be inverted.
6. Write configuration by pressing write icon.
Figure 24 the example of Outputs (PGM) window

7. If control outputs by short call or SMS needed, go to “Users & Remote Control” window and enter telephone numbers of users, who will be able to control selected outputs via free short call. More information: System remote monitoring via mobile phone. Periodic Info SMS

8. Write configuration by pressing write icon.
   - In order to control big power alternating current equipment, it is comfortable to use solid state relays.
   - Standard AC/DC adapter with the voltage 10V-14V and current >=1A might be used to powering the module.

<table>
<thead>
<tr>
<th>ID</th>
<th>Output sequence number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Outputs hardware location.</td>
</tr>
<tr>
<td>3</td>
<td>Output name</td>
</tr>
<tr>
<td>4</td>
<td>Selection of output operation mode.</td>
</tr>
<tr>
<td>21</td>
<td>Disable</td>
</tr>
<tr>
<td>22</td>
<td>Bell</td>
</tr>
<tr>
<td>23</td>
<td>Buzzer</td>
</tr>
<tr>
<td>24</td>
<td>Flash</td>
</tr>
<tr>
<td>27</td>
<td>Remote Control</td>
</tr>
<tr>
<td>30</td>
<td>ARM/ DISARM</td>
</tr>
<tr>
<td>31</td>
<td>Alarm Indication</td>
</tr>
<tr>
<td>5</td>
<td>Output control mode.</td>
</tr>
<tr>
<td>36</td>
<td>Steady ON/OFF mode</td>
</tr>
<tr>
<td>37</td>
<td>Timer ON pulse mode</td>
</tr>
<tr>
<td>6</td>
<td>Pulse time duration can be from 1 to 999999 sec.</td>
</tr>
<tr>
<td>7</td>
<td>Inversion is activated</td>
</tr>
<tr>
<td>8</td>
<td>Pulsating mode is activated. Then output is activated it will pulsate according pulse ON/OFF time.</td>
</tr>
<tr>
<td>9</td>
<td>Pulsating mode pulse ON duration.</td>
</tr>
<tr>
<td>10</td>
<td>Pulsating mode pulse OFF duration.</td>
</tr>
</tbody>
</table>

Table 4 Explanation of every field in “Outputs” window

13 System remote monitoring via mobile phone. Periodic Info SMS

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.
   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. 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.

![The example of GSM Communication> SMS DIAL Reporting window](image)

Table 5 Explanation of every field in “SMS DIAL Reporting” window

<table>
<thead>
<tr>
<th></th>
<th>The SMS/auto DIAL Phone Numbers</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SMS Character Set</td>
<td>SMS character set selection.</td>
</tr>
<tr>
<td>2</td>
<td>Limit of Dialing</td>
<td>Indicate maximum number of unsuccessful calls</td>
</tr>
<tr>
<td>3</td>
<td>Show Object Name</td>
<td>Object name will be displayed in the SMS message</td>
</tr>
<tr>
<td>4</td>
<td>Show Zone Number</td>
<td>Zone number will be displayed in the SMS message</td>
</tr>
<tr>
<td>5</td>
<td>Show Event Time</td>
<td>Event time will be displayed in the SMS message</td>
</tr>
<tr>
<td>6</td>
<td>Show CID Code</td>
<td>Report Contact ID code</td>
</tr>
<tr>
<td>7</td>
<td>Zone1- Zone32 Alarm/ Restore</td>
<td>Zone1- Zone32 alarm and restore events reporting is enabled.</td>
</tr>
<tr>
<td>8</td>
<td>System Open/ Close (CID 400 group)</td>
<td>System ARM/DISARM/STAY reporting is enabled.</td>
</tr>
<tr>
<td>9</td>
<td>System Troubles (CID 300 group)</td>
<td>System trouble reporting is enabled.</td>
</tr>
<tr>
<td>10</td>
<td>Sensor1- Sensor32 Alarm/ Restore</td>
<td>Sensor 1 – Sensor32 alarm and restore events reporting is enabled.</td>
</tr>
<tr>
<td>11</td>
<td>Test Events (CID 600 group)</td>
<td>Communication test reporting is enabled.</td>
</tr>
<tr>
<td>12</td>
<td>Other Events</td>
<td>Other events reporting is enabled.</td>
</tr>
<tr>
<td>13</td>
<td>Send SMS to USER</td>
<td>SMS reporting to selected index of telephone number is enabled.</td>
</tr>
<tr>
<td>14</td>
<td>Auto DIAL to USER</td>
<td>Auto DIAL to selected index of telephone number is enabled.</td>
</tr>
</tbody>
</table>

14 Connecting to the Web Server.

If remote monitoring, control, configuring, FW updating over the internet is needed, please refer to the “Connecting to the Web Server” application note.

15 General system settings. Real-time clock (RTC)

The general system options settings let you control system options, system general settings, systems timers, let you program iButton keys and reset the module.
Table 6 Explanation of every field in "General System Options" window

<table>
<thead>
<tr>
<th>No.</th>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SIM Card PIN</td>
<td>SIM card PIN code. Default 1234</td>
</tr>
<tr>
<td>2</td>
<td>Installer Password</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>SMS User Password</td>
<td>The default SMS User Password is 123456. This code allows you to utilize arming method, as well as program user codes.</td>
</tr>
<tr>
<td>4</td>
<td>User Access Code Format</td>
<td>A 4-digit or 6-digit user access code format can be selected.</td>
</tr>
<tr>
<td>5</td>
<td>I/O1 Settings</td>
<td>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</td>
</tr>
<tr>
<td>6</td>
<td>I/O2 Settings</td>
<td>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</td>
</tr>
<tr>
<td>7</td>
<td>0-10V Analog Input (Zone or Sensor)</td>
<td>0-10V Analog sensors will be connected to the input</td>
</tr>
<tr>
<td>8</td>
<td>Output</td>
<td>Input will be used as output</td>
</tr>
<tr>
<td>9</td>
<td>2-Wire Smoke Detector (Fire current loop)</td>
<td>2-Wire Smoke detectors will be connected t the input.</td>
</tr>
<tr>
<td>10</td>
<td>0-10mA, 4-20mA Current Loop Sensor</td>
<td>0-20mA, 4-20mA Current Loop Sensors will be connected to the input.</td>
</tr>
<tr>
<td>11</td>
<td>Clear Event Buffer After Reset</td>
<td>When the cell is checked, the memory of unsent reports will be deleted after the module resetting</td>
</tr>
<tr>
<td>12</td>
<td>Door Chime</td>
<td>When this box is checked, violations of set Delay zones at the alarm turned off will be accompanied by keyboard audible (Buzzer) signal</td>
</tr>
<tr>
<td>13</td>
<td>Bell squawk on ARM/ DISARM</td>
<td>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.</td>
</tr>
<tr>
<td>14</td>
<td>Auto re-ARM</td>
<td>The module can be programmed to arm the module if there is no activity in the area after the system disarming.</td>
</tr>
<tr>
<td>15</td>
<td>Start iButton/RFID programming</td>
<td>All added iButton keys or RFID cards will be registered in the order of sequence by clicking Start programming</td>
</tr>
<tr>
<td>16</td>
<td>STOP iButton/RFID programming</td>
<td>To finish entering iButton keys or RFID cards, click Stop programming button</td>
</tr>
<tr>
<td>17</td>
<td>Test Time</td>
<td>Auto Test report time of day</td>
</tr>
<tr>
<td>18</td>
<td>Test Period</td>
<td>Auto Test report period</td>
</tr>
<tr>
<td>19</td>
<td>Entry Delay</td>
<td>This delay gives you time to enter the armed premises and enter your code to disarm your system before the alarm is triggered.</td>
</tr>
<tr>
<td>20</td>
<td>Exit Delay</td>
<td>The system will trigger the Exit Delay Timer to provide you with enough time to exit the protected area before the system is armed.</td>
</tr>
<tr>
<td>21</td>
<td>Bell/ Sirel Cut – off Timer</td>
<td>Duration of audible signal (sirens, Bell) after the alarm system activated. Time shall be written in seconds, duration from 0 to 9999.</td>
</tr>
<tr>
<td>22</td>
<td>Time Zone</td>
<td>To set the clock click Set time from PC button and the clock will be set using computer’s clock.</td>
</tr>
<tr>
<td>23</td>
<td>Daylight saving time</td>
<td>To read the clock of panel.</td>
</tr>
</tbody>
</table>
16 Access control output with logging

As long as the GTalarm2 module is not turned off, the employee cannot open the door. The module can be disabled only by a VIP employee. When the module is off, an employee can open the door using the iButton key, an RFID card, a mobile phone.

This function is allowed only if the output definition is set to [Access Gained]. Then the output generates event if access device is granted by user who controls this output.

- If user has right to ARM/DISARM system, it always has access to this output.
- If ARM/DISARM flag is not set user can access this output only if system is Disarmed (Open).
- If access is granted by user, 421 event Access granted is stored into the log. If not Access denied event 422
- if output will have definition [Automation / CTRL] it also can be controlled by user in any ways but it will not generate 421 and 422 events,

And will not care about ARM/DISARM

Event log e.g.

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

17 Event log

The Event Log window show real time information of the events that has been occurred. Every enabled new event is stored in log. Internal event log has some limitations. It is possible to store 2048 events in the events log buffer. Events could be saved to the file. If you need to store more events, you can use Sera cloud server. The user is able to see every event remotely via web app.

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

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

Table 7 Explanation of every field in “Events Log” window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Read Event Log</td>
</tr>
<tr>
<td>2</td>
<td>Clear Event Log</td>
</tr>
<tr>
<td>3</td>
<td>Event Number</td>
</tr>
<tr>
<td>4</td>
<td>Event</td>
</tr>
<tr>
<td>5</td>
<td>Time</td>
</tr>
<tr>
<td>6</td>
<td>Note</td>
</tr>
</tbody>
</table>

18 System Testing & Diagnostic tool

Trouble shooting information can be retrieved from the panel using “RT Testing & Diagnostic” window.

Event monitoring

The following GTalarm2 status could be monitored:
• Alarms — Alarms are events, or system transactions, that have been assigned alarm status. • Events — Events are the recorded transactions of the Gtalarm2 system. For example number of users logged in. • Inputs — Inputs are terminals located on the Gtalarm2 panel; the inputs are wired to input devices. • Outputs — Output relays are relays located on the Gtalarm2 panel that are connected to the outputs of the Gtalarm2 panel.

This information could be monitored in “RT Testing & Diagnostic” window “Event Monitoring” Tab and in the “Events Log” window.

<table>
<thead>
<tr>
<th>Table 8</th>
<th>Explanation of every field in “Event Monitoring” window</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Event number</td>
</tr>
<tr>
<td>2</td>
<td>CID</td>
</tr>
<tr>
<td>3</td>
<td>Time</td>
</tr>
<tr>
<td>4</td>
<td>Note</td>
</tr>
</tbody>
</table>

19 Monitoring Inputs, outputs & general system info

Sera2> RT Testing & monitoring > Hardware

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

Table 9 | Explanation of every field in “Hardware” window |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start Monitoring</td>
</tr>
<tr>
<td>2</td>
<td>Stop Monitoring</td>
</tr>
<tr>
<td>3</td>
<td>IMEI</td>
</tr>
<tr>
<td>4</td>
<td>SIM ICCID</td>
</tr>
<tr>
<td>5</td>
<td>SIM Card</td>
</tr>
<tr>
<td>6</td>
<td>Signal level</td>
</tr>
<tr>
<td>7</td>
<td>Registration</td>
</tr>
<tr>
<td>8</td>
<td>SMS Service Centre Address</td>
</tr>
<tr>
<td>9</td>
<td>System Voltage</td>
</tr>
<tr>
<td>10</td>
<td>System Voltage</td>
</tr>
<tr>
<td>11</td>
<td>RTC Clock</td>
</tr>
<tr>
<td>12</td>
<td>Module Real Time Clock</td>
</tr>
<tr>
<td>13</td>
<td>Set RTC Clock</td>
</tr>
</tbody>
</table>
Inputs In1…In4

In1…In4 is the indicated input ADC and voltage value V.

I/O1…/O2

I/O1…/O2 is the indicated voltage ADC value and current ADC value mA.

D1…D3 (I/O)

Check box nearby the digital inputs D1…D3 (I/O) means that the input has ‘0’ or ‘1’ state.

BUS (I/O)

Check box nearby the zone expansion module BUS (I/O) means that the input has ‘0’ or ‘1’ state.

Out1…Out4 On/Off

Check box nearby the appropriate output Out1…Out4 means that this output currently has ‘0’ or ‘1’ state. The output could be activated by pressing On/Off button.

I/O1…I/O2 On/Off

Check box nearby the appropriate input/output I/O1…I/O2 means that this input/output currently has ‘0’ or ‘1’ state.

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.

BUS (I/O) On/Off

Checked check box BUS (I/O) means that the output currently has ‘0’ or ‘1’ state.

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

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

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

<table>
<thead>
<tr>
<th>Zone1…Zone32</th>
<th>Zone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>If checked and the color is red the zone is alarmed</td>
</tr>
<tr>
<td>Alarm Shutdown</td>
<td>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.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>If checked and the color is red, the zone is bypassed.</td>
</tr>
<tr>
<td>Forced</td>
<td>If checked and the color is red, the zone is forced</td>
</tr>
<tr>
<td>Tamper/Fault</td>
<td>If checked and the color is red, the zone is tampered.</td>
</tr>
<tr>
<td>Tamper Shutdown</td>
<td>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.</td>
</tr>
<tr>
<td>System State</td>
<td>Indication that at the moment the module is in waiting ARM, ARM, DISARM, SLEEP or STAY mode</td>
</tr>
<tr>
<td>DISARM</td>
<td>After pressing the button DISARM, disarm mode should be entered</td>
</tr>
<tr>
<td>ARM</td>
<td>After pressing the button ARM, arm mode should be entered</td>
</tr>
<tr>
<td>SLEEP</td>
<td>After pressing the button SLEEP, sleep mode should be entered</td>
</tr>
<tr>
<td>STAY</td>
<td>After pressing the button STAY, arm mode should be entered</td>
</tr>
<tr>
<td>System Voltage</td>
<td>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.</td>
</tr>
<tr>
<td>RTC Clock</td>
<td>If the checkbox is checked and the color is red RTC clock is not set. If color is green, RTC clock is set.</td>
</tr>
<tr>
<td>Module Real Time Clock</td>
<td>Real time and date is indicating.</td>
</tr>
<tr>
<td>iButton Read</td>
<td>The number of iButton Maxim iButton key DS1990A - 64 Bit ID code that is arming the system.</td>
</tr>
<tr>
<td>Incoming call</td>
<td>The number of users phone that is calling to the module’s SIM.</td>
</tr>
<tr>
<td>Wiegand RFID Card Key</td>
<td>The number of Wiegand RFID Key Card that is arming the system.</td>
</tr>
</tbody>
</table>

Software updates

If receive software updates needed, go to Settings and mark “Check for Updates Automatically”. When new update will be available, the program will inform the user, and the user have to start the update. After that the user have to connect the module to the computer via mini USB cable. And to write this update to the module GTalarm2 by pressing “Update” in the bottom line in SERA2 software.
If update the module manually needed, got to "About" and press "Check for updates"

![Check for Updates]

If contact the seller with the questions about the configuration needed, it is necessary:

- 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.

---

21 Control via SMS messages

21.1 The table of users SMS commands

Table 11 The table of user's commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER123456_020 N</td>
<td>Change state of selected OUT output to the inverted state. Output state changes every time after sending command code. 020= command code (Change state of selected OUT output to the inverted state.) N = output number from 1 to 10.</td>
</tr>
<tr>
<td>USER123456_021 N#ST</td>
<td>Activate or deactivate selected output N. 021= command code (Activate or deactivate selected output N) N = output number from 1 to 10. ST= output mode: 0 – deactivated output, 1- activated output</td>
</tr>
<tr>
<td>USER123456_022 N#TIME#</td>
<td>Output activation for the time interval 022= command code (Output activation for the time interval) N = output number 1-10 TIME = 0-999999 Time interval in seconds for the output activation.</td>
</tr>
<tr>
<td>USER123456_030 ST</td>
<td>Change security system’s mode (ARM/DISARM/STAY/SLEEP) 030= command code (Change security system’s mode (ARM/DISARM/STAY/SLEEP) ST = Security system mode 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP</td>
</tr>
</tbody>
</table>

21.2 The table of installers commands

Table 12 The table of installers commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INST000000_001 N#TEL#SMS#DIAL#</td>
<td>Programming of users telephone numbers to send SMS and to make a call if the event occur: 001= programming user’s tel. numbers for DIAL and send SMS N = user ID number 1-8 TEL = user’s telephone number (max 16 digits) without (+) country code, operator’s code and user’s telephone number included. The end symbol #: SMS = event filter for sms. 1- send event, 0- don’t send event. Sequence of the events 1.2.3…n For example: 001000 DIAL = event filter for DIAL. 1-DIAL if the event occur, 0- don’t DIAL Sequence of the events 1.2.3…n For example: 101000 # = delimiter</td>
</tr>
<tr>
<td>INST000000_002 N</td>
<td>Delete user’s phone number according the user ID number. Phone number used for receive user’s information. 002= command code (deleting user’s numbers according the user ID number) N = user ID number from 1 to 8</td>
</tr>
<tr>
<td>INST000000_004 N#TEL#OUT#OPT#</td>
<td>To enter user’s telephone number for remote control via short call 004= command code (enter user’s telephone number for remote control via short call) N = user ID number 001-800 TEL = user’s telephone number (max 16 digits) without (+) comprised of country code, operator’s code and user’s telephone number, the end symbol #: OUT= output number, that will be controlled, 1-10. OPT = DIAL function: 0 – disabled 1 – enabled, Sequence from the left to the right: ARM/ DISARM, MIC. For example: 010</td>
</tr>
<tr>
<td>INST000000_005 TEL</td>
<td>To delete user’s phone number for remote control, according phone number 005= command code (delete user’s phone number for remote control, according phone number) TEL = user’s phone number (max 16 digits) without (+) comprised of country code, operator’s code and user’s telephone number. User’s phone number must be the same as in the memory of the module.</td>
</tr>
</tbody>
</table>

Figure 31 How to update the module manually
Delete user's phone number whose ID number is N.
006= command code (Delete user's phone number according user's ID number)
N = user's ID number from 001 to 800.

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

To activate the connection to the remote control server
010= command code (To activate the connection to the remote control server)
E= 1-enabled, 0-disabled

To change the operation algorithm of the output
019= command code (To change the operation algorithm of the output)
N = output number from 1 to 10
P = output operation algorithm. 0 – output disabled, 1 – siren, 2 - buzzer, 3- flash led, 4- system state LED, 5- LED „system ready”, 6- remote control, 7- low system voltage, 8 – System DISARMed, 10-alarm indication, 14-automatic sensor reset, if the sensor stops sending data.

Invert output state
020= command code (outputs inversion)
N = output number from 1 to 10.

Output activation or deactivation
021= command code (Output activation or deactivation)
N = output number 1-10
ST = output mode 0 – OFF, 1- ON

Output activation for the time interval
022= command code (Output activation for the time interval)
N = output number 1-10
TIME = 0-999999 Time interval in seconds for the output activation.

Change security system’s mode (ARM/DISARM/STAY/SLEEP)
030= command code (Change security system’s mode)
ST = 0-DISARM, 1-ARM, 2-STAY, 3-SLEEP

Zone bypassing by sms command
031= command code (Zone bypassing)
ZN = zone number from 1 to 32
BYP= 1 – zone bypass 0- zone active.

iButton keys learning/deleting mode
063= command code (iButton keys learning/deleting mode)
S=iButton keys entering/deletion mode.
0-Disable iButton/RFID keys learning mode
1-Enable iButton/RFID keys learning mode
2-iButton/RFID keys deleting mode. To delete these keys from memory, which will be touched to the reader

Request a part of information regarding configurations of the module via SMS message:
090= command code (Request a part of information regarding configurations of the module via SMS message)
1. Request about active input’s state parameters;
2. Request about output states (Out1 – Out10);
3. Request information about the module (: IMEI, FW, LEVEL etc.)
4. System state request. The module will send information on input/output states and system state
   (ARM/DISARM).

Change installer’s password (Installers password should be changed before exploitation of the module)
090= command code (Change of installer’s password)
PSW = New Installer’s password.

Change user’s password (User’s password should be changed before exploitation of the module)
091= command code (Change user’s password)
PSW = New user’s password.

Remote reset of the module via SMS messages
092= command code (Remote reset of the module via SMS messages)

Time of the module setting via SMS message
093= command code (Time of the module setting via SMS message)
Time format of the module:
dd/MM/yyyy#HH:mm#
dd - day of the month 1-31
MM-month 1-12
yyyy-year
HH-hours 0-23
mm- minutes 0-59

System state request:
100= command code (System state request)
N = System state request type
1- System test request, Request information about the module (: IMEI, FW, LEVEL etc.)
2- the values of active sensors request
3 -Request about active zone states
4- Request about output states
5 - System state request. The module will send information on input/output states and system state
   (ARM/DISARM/STAY).
22 Access control terms and definitions

Access Card - A card is used in conjunction with an access reader to grant or deny access. These cards are usually the same size as a credit card. Technologies can vary from encoded magnetic strips, Wiegand, proximity, barium ferrite and smart cards.

Access Control - A term used to describe a method of controlling or restricting the entrance and/or exit of a premise or area. These methods can be electrical or non-electrical, depending on the type of equipment used.

Access Level - Also known as "Authority Level". An access level is either a single entrance or combination of entrance points that a user is allowed to enter or exit.

Access Point - A specific entrance point of an access control system. This can consist of a card reader, monitor switches and/or latches. Access points are wired to an access control panel.

Alarm Input - This is a security device that is tied into and monitored by the access control panel.

Door Forced Open - This signal indicates that a door was opened without the validation or an access card or a request to exit device. In order to do this a status switch and a request-to-exit device is needed.

Door Held Open - This signal indicates that a door was open longer than allowed based upon a preset time period. The advantage of this feature is to prevent someone from using a card to gain access and then propping the door open for others to gain access also. In order to utilize this feature a status switch on the door is required.

Door Open Time - This is a preset time period that is allowed for a access door to be open after a valid entry. At the end of this time period, if the door is not closed, the access system will make a transaction of this occurrence as a "door held open" and may also sound an alarm.

Exit Button - Also known as a request to exit device or button. This is a button that must be pushed in order to release the locking mechanism on the door.

History - This is a memory of the activity of the access system which can be recalled later for reporting and logging purposes. Most access system will notify the user if the memory begins to reach full capacity in order to prevent loss of data. This information can usually be saved to diskette or printed.

Keypads - This type of device utilizes a numeric pad. The user would simply enter a set of numbers into the keypad to gain entry. This type of system is less secure than a card reader type system since it would be possible for a user to be seen entering an access number.

Output Relays - These are the auxiliary relays found in access control panels that control external devices.

PIN - This a Personal Identification Number that is assigned to each user. It is either used by itself or in conjunction with an access card.

Proximity - This is one of the most secure and best types of reader technologies. No direct contact is required between the card and the reader, therefore reducing wear and tear on the access card. The card must only come within a certain proximity to the reader. Depending on the type equipment used, the reader's range can be over 30 feet (this type of long range reader capability is generally used with automated highway turnpike systems). Most installations generally require a reliable read range of about 2 inches. In this technology the reader generates a RF field which causes specially designed wires in the card to resonate, transferring the card information to the reader. These types of cards are immune to electromagnetic and RF interference, and they can offer "hands free" operation. Although the upfront cost of these cards is higher, the long term expense of replacing cards is lower. Also this type of reader is suitable for outdoor use and it is nearly impossible to duplicate a access card.

Reader - Refers to the "front end" that a user must interact with to allow access. Readers can be keypads, card readers, and proximity readers.

Remote Host - A system where the main computer that controls the system is remotely located. It allows a single computer to control multiple systems.

Shunt Time - When a door is released the status switch is automatically "shunted" for a period of time to allow the person to enter/exit. If the time is exceeded a door held open signal will occur.

Stand Alone - A system where the entire system is contained in the card reader.

Status Switch - A magnetic contact mounted on the controlled door. It is used to detect door held or door forced.

Time Schedules - Allows for Access based on time of day, date and user. Also allows for holidays, etc.

Time Zones - "Schedules" that allow cards to function or not function depending on the time of day. This is used to limit access to the facility. The schedule may include not only time but which days of the week a card is valid.

Wiegand - These cards are essentially magnetic field effect devices. As the card is inserted or swiped through the reader an electromagnetic field generated by the reader induces a voltage in the card causing it to transmit its code. Unlike some insertion type systems, Wiegand readers are completely sealed against weather conditions and as a result have a long live span. These cards are difficult to duplicate, highly damage resistant, and offer a high level of security, but as with proximity cards expensive, and generally can only be programmed by the manufacturer.