GPS SYSTEMS BULGARIA
www.smart-hitech.eu

HI-TECH

☎ +359 700 20 820, +359 887376336
4004 Plovdiv, 75A D. Talev Str

Intruder Alarm System

SMART GUARD

Installation Manual

Table of Contents:

I. TECHNICAL SPECIFICATION

1. SMART GUARD PANEL

1.1. Description

GPS Systems Bulgaria has created hi-technology intruder alarm system that incorporates rich functionality and numerous technological solutions for home and office protection. The **SMART GUARD** alarm system combines all advantages of the traditional intruder alarms but even goes beyond them. It expands and improves all functionalities to a level of highly intelligent system for management and control.

- Can be used as a standalone system or connected to a control center for monitoring and security.
- Supports remote programming and update for all system components.
- Integrated with the **CloudSG** system. Provides the end user the ability to monitor and control the alarm system via mobile application or web browser. Supports real time notification for all system events.
- With the built-in GSM Dialer functionality, the alarm system can be used as a standalone device that can notify for any event via call and/or SMS. Its PGMs can be control also via call or SMS.
- All events are stored with their real time stamp and can be transmit independently to control center and cloud system through different communication channels – GSM/GPRS, Wi-Fi and Ethernet.
- All connections to control center and Cloud system is two-way encrypted. The security of the information is guarantee by especially designed algorithms for protection and encryption and no data can be lost or manipulated in any way.
- Supports AUTO ARM after various scenarios – at specified time schedule, after specified time of inactivity or both.
- Supports special control for electromagnetic locks **Smart Door Control (SDC)** – its advantage is the very low consumption versus conventional methods that needs an additional power supply.

System capabilities:

- supports 8 completely independent partitions (areas);
- supports up to 135 programmable logical zones;
- supports up to 48 programmable outputs (PGM);
- supports up to 500 users (with numeric codes and contactless proximity card);
- can work with 8 keypads simultaneously (has built-in proximity reader for access control);
- support up to 32 standalone proximity readers;
- support up to 6 zone/PGM expanders;

1.2. Technical specification

Parameter	Value
Power supply	18VAC ±10%, fuse 2A
Backup power supply	12V lead acid battery
System output (AUX)	13,8VDC / 1,6A
Protections	double protection to all power outputs with electronic and blowable fuses
System bus	RS485
Zones	8 zones (up to 16 logically doubled)
PGMs	4 PGMs, 2A max (open collector type)
Operational temperature	0°C ÷ +50°C
Dimensions	140 mm x 74 mm x 15 mm

2. SMART GUARD KEYPAD

2.1. Description

SG KEYPAD has stylish and elegant design with large two-line display. It is equipped with capacitive touch buttons and adjustable built-in LED backlight. An adjustable built-in buzzer can notify for all system events. Via its intuitive and user-friendly designed menu, all system parameters can be setup locally.

There are several predefined buttons for the most used actions:

- ARM/DISARM between few security modes – FULL ARM, STAY and SLEEP:

  - *FULL ARM mode* – monitor all assigned zones to the specified partition (area);
  - *STAY and SLEEP modes* – some of the assigned zones to the specified partition (area) are excluded from the monitoring;
- View alarm panel memory (LOG);
- View all technical problems;

On its large display the keypad can provide detailed information about the entire system - status, open zones, system troubles, alarm events and current ARM mode of each partition. SG KEYPAD has one hardware input, which can be double in two logical zones and one programmable output (PGM), which can directly control electromagnetic lock in standard or "SDC" mode. SG KEYPAD can work with SMART GUARD alarm panels only.

2.2. Technical specification

Parameter	Value
Power supply	9 ÷ 18VDC
Power consumption	min 20mA, max 80mA
Zones	1 zone (can be doubled logically)
PGMs	1 PGM, 2A max (open collector with SDC)
Proximity reader	Built-in 125kHz (EM4102 type)
Button type	Capacitive touch sensing
Backlight	Adjustable built-in LEDs
Audible alarms	With adjustable built-in buzzer
Tamper protection	Internal
Operational temperature	-10°C ÷ +50°C
Dimensions	121 mm x 46 mm x 22 mm

3. SMART GUARD RFID

3.1. Description

SG RFID is a proximity reader designed to operate with 125 kHz EM4102 card types. It is equipped with one hardware input, which can be double in two logical zones and one programmable output (PGM), which can directly control electromagnetic lock in standard or "SDC" mode. SG RFID can work with SMART GUARD alarm panels only.

On its front panel has three LEDs showing different statuses:

- ***Green*** – shows the communication with the alarm panel. A slow blink once in a second is for normal work. Few times per second means problems with the communication or no connection.
- ***Red*** – shows the security state of the assigned to the reader partition. Constant light is for any of the three ARM modes – Full, Stay or Sleep.
- ***Yellow*** – lights up when the user card is reject***.***

3.2. Technical specification

Parameter	Value
Power supply	9 ÷ 18 VDC
Power consumption	min 15mA, max 40mA
Zones	1 zone (can be doubled logically)
PGMs	1 PGM, 2A max (open collector with SDC)
Proximity reader	Built-in 125kHz (EM4102 type)
Range	Up to 5 cm
Audible alarms	With adjustable built-in buzzer
Tamper protection	Internal
Operational temperature	-10°C ÷+50°C
Dimensions	121 mm x 46 mm x 22 mm

4. SMART GUARD EXPANDER

4.1. Description

SG EXPANDER is using to expand the alarm system zones and PGMs. It can add up to 16 additional zones and 2 PGMs. These zones and PGMs are programming via the alarm panel.

4.2. Technical specification

Parameter	Value
Power supply	9 ÷ 18VDC
Power consumption	min 15mA, max 60 mA
Zones	8 zones (up to 16 logically doubled)
PGM	2 PGMs, 2A max (open collector type)
Operational temperature	-10°C ÷ +50°C
Dimensions	102 mm x 50 mm x 10 mm

5. SMART GUARD PIR

5.1. Description

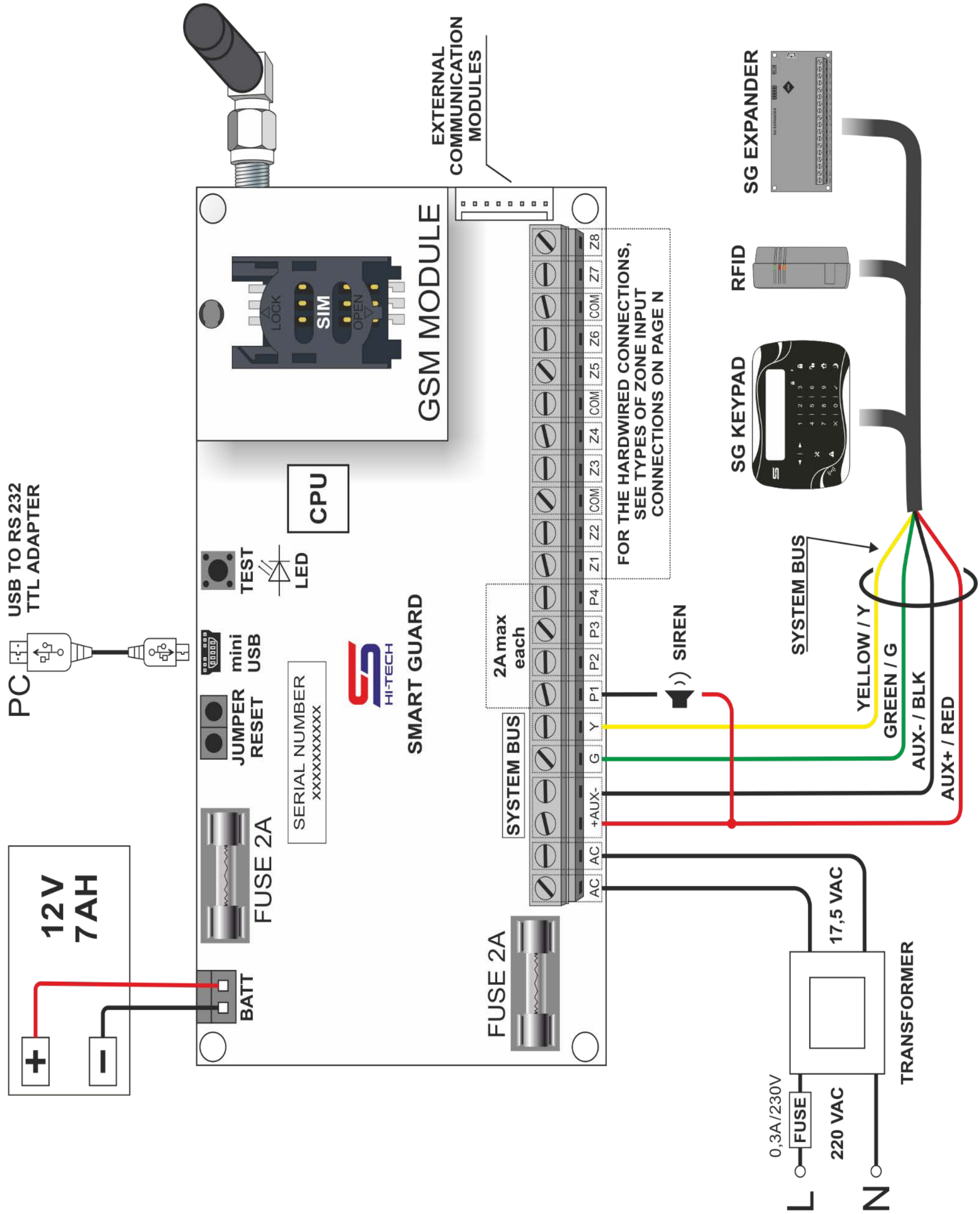
SG PIR is the latest generation of digital passive infrared motion detectors, designed for home, offices, warehouses, factories and so on. In a very small form factor with elegant and stylish design.

With its complex and highly sophisticated digital algorithms, the accidental and false alarms are decrease to the minimum level. The detector has advanced built-in temperature compensation and integrated protection against white light. Provides several levels of predefined sensitivity. It is fully compatible with all alarm systems as a conventional detector. However, its main advantage is the possibility for two-way communication with Smart Guard alarm panels over the system power bus. With this ability, it can be automatically recognized and remotely adjusted without the need to open its case and do it manually on-site.

5.2. Technical specification

Parameter	Value
Power supply	9 ÷ 18 VDC
Power consumption	min 8mA, max 14mA
Working range	1,5m ÷ 15m
Coverage angle	90°
Functionalities	Built-in digital algorithms against false alarms
Protection against white light	Yes
Protection against electromagnetic interferences	Yes
Installation height	1,5m ÷3,6m(2,1m recommended)
Operational Temperature	- 20°C÷+50°C
Dimensions	95 mm x 56mm x 44mm
Weight	75g

II. Installation and wiring



1. Installation description

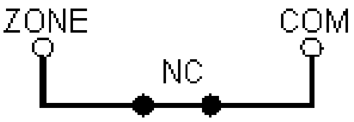
Component	Description
Transformer	Permanently connected transformer 17.5VAC, 30VA minimum
Fuse 2A	Blowable fuses for double protection
AUX + / RED **AUX - / BLACK**	System power bus controlled from the panel. Use to power the keypads, readers, extenders, detectors and other peripherals. Provide the communication for SG PIRs.
Green , Yellow	System communication bus. Use to control the keypads, readers, extenders and other SG peripherals
Z1-Z8	Zone inputs, the place to connect any detector
COM	Common point to close the loop from a detector to a zone terminal
PGM 1 ÷ 4	Programmable outputs
External communication modules	For additional communication modules – WiFi, Ethernet and so on.
GSM module	GSM/GPRS Communication module
CPU	Central processor unit
TEST	Multi-purpose button. Mainly used to make a test signal
LED	System status indication
Mini USB	Connection to PC
JUMPER RESET	Restore the system to factory settings
BATT	Connection to a backup 12V lead acid battery

2. Zone wiring

Nine different connections and wiring diagrams are support by the system - with single or doubled zones, with tamper detection and/or broken cable detection. Each input can be setup separately from the others.

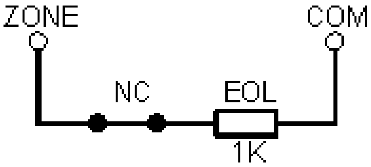
2.1. Single zones

SCHEME 1



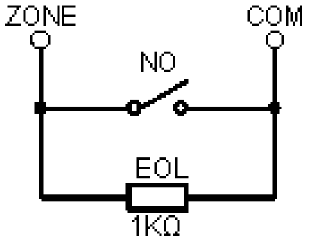
N.C. contact without EOL resistor

SCHEME 2



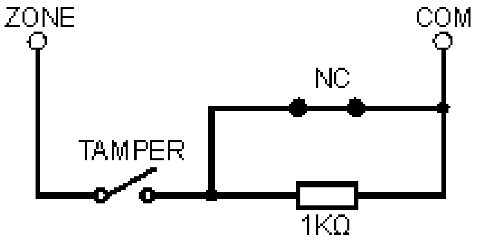
N.C. contact with EOL resistor

SCHEME 3



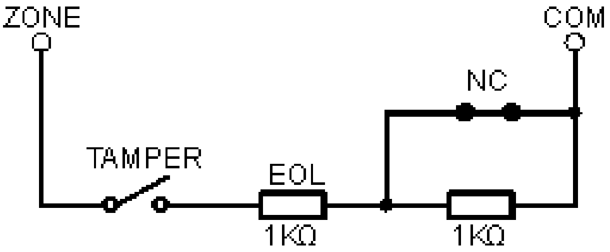
N.O. contact with EOL resistor and broken cable detection (reversed logic)

SCHEME 4



N.C. contact without EOL resistor, with tamper detection

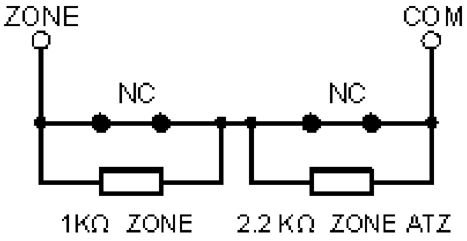
SCHEME 5



N.C. contact with EOL resistor, with tamper and cable detection

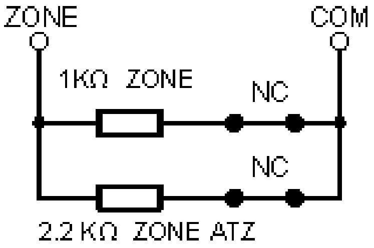
2.2. Double zones (ATZ)

SCHEME 6



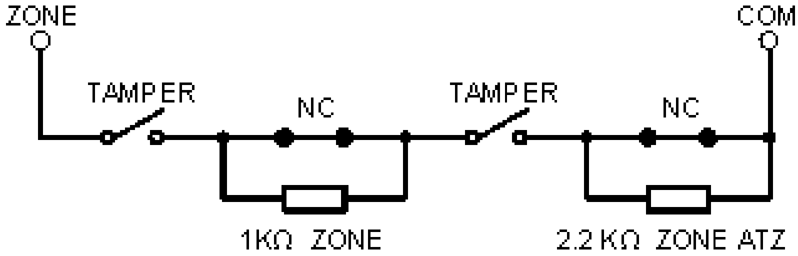
Two N.C. contacts without EOL resistors

SCHEME 7



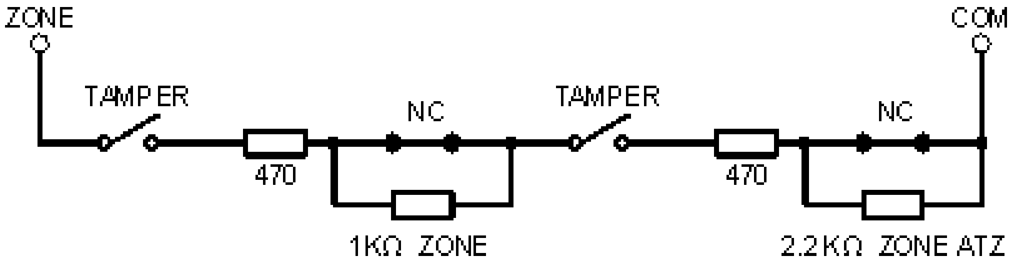
Two N.C. contacts without EOL resistors

SCHEME 8



N.C. contacts without EOL resistors, with tamper detection

SCHEME 9



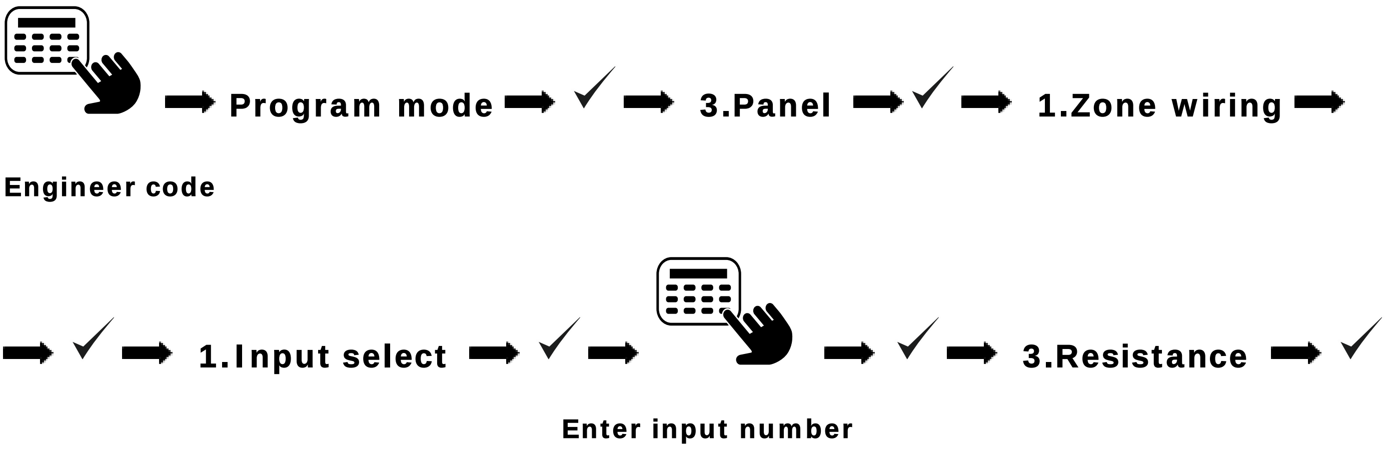
Two N.C. contacts with EOL resistors, with tamper detection

3. Input loops inspection and diagnostics

The system provides the engineer with option to make automatic real time inspection of each input loop by measuring its resistance. It can help in making easy diagnostics if there is any wiring problems. This diagnostic can be done via SG Service Programming Tool and SG Keypad.

3.1. Step by step diagnostics via SG Keypad

Here are the steps that have to be done to make diagnostics to any input loop via SG Keypad:



Engineer code ➡ **Program mode** ➡ ✓ ➡ **3.Panel** ➡ ✓ ➡ **1.Zone wiring** ➡

➡ ✓ ➡ **1.Input select** ➡ ✓ ➡ Enter input number ➡ ✓ ➡ **3.Resistance** ➡ ✓

Based on the measured resistance and the wiring diagram, the result can be easily check from the table below:

Wiring diagram		Resistance	Zone state
Single zones	**1**	< 1.6 kΩ	Restore zone
		> 1.6 kΩ	Open zone
	2	< 420 Ω	Open zone
		420 Ω ÷ 2.7 kΩ	Restore zone
		> 2.7 kΩ	Open zone
	3	< 420 Ω	Open zone
		420 Ω ÷ 2.7 kΩ	Restore zone
		> 2.7 kΩ	Open zone
	4	< 420 Ω	Restore zone
		420 Ω ÷ 2.7 kΩ	Open zone
		> 2.7 kΩ	Tamper - open loop
	5	< 420 Ω	Tamper – short loop
		420 Ω ÷ 1.4 kΩ	Restore zone
		1.4 kΩ ÷ 3.7 kΩ	Open zone
		> 3.7 kΩ	Tamper - open loop
Double zones (ATZ)	**6**	< 420 Ω	All zones are restore
		420 Ω ÷ 1.5 kΩ	Zone 1 is open
		1.5 kΩ ÷ 2.7 kΩ	Zone 2 is open
		2.7 kΩ ÷ 4.7 kΩ	All zones are open
		> 4.7 kΩ	Open loop / broken cable
	7	< 300 Ω	Short loop
		300 Ω ÷ 830 Ω	All zones are restore
		830 Ω ÷ 1.5 kΩ	Zone 2 is open
		1.5 kΩ ÷ 3.8 kΩ	Zone 1 is open
		> 3.8 kΩ	All zones are open
	8	< 420 Ω	All zones are restore
		420 Ω ÷ 1.5 kΩ	Zone 1 is open
		1.5 kΩ ÷ 2.7 kΩ	Zone 2 is open
		2.7 kΩ ÷ 4.7 kΩ	All zones are open
		> 4.7 kΩ	Tamper - open loop
	9	< 680 Ω	Tamper – short loop
		680 Ω ÷ 1.5 kΩ	All zones are restore
		1.5 kΩ ÷ 2.5 kΩ	Zone 1 is open
		2.5 kΩ ÷ 3.6 kΩ	Zone 2 is open
		3.6 kΩ ÷ 5.3 kΩ	All zones are open
		> 5.3 kΩ	Tamper - open loop

III. System programming via SG SERVICE MODULE

Launching the SG Service Module will opens its main working window. All settings are separate into different tabs, grouped by functions. There are few general system settings and additional buttons situated above and below all tabs.

- From the upper left corner in the main window can be selected the type of the communication. It can be directly via "COM" port or remotely via "TCP/IP" port. From the upper right corner can be changed the localization language.

- The buttons at the bottom of the main window are:

⇩	Read the pointed settings from device
⇧	Upload the pointed settings into device
Restart Device	Restart the system
Read all from device	Read all settings from the alarm panel
Upload all to device	Upload all settings to the alarm panel
Read from file	Load all settings from a file into the programming tool
Save all to file	Save all settings from the panel into a file

Factory settings – in order to be more flexible, the system provides several levels of factory reset:

- ***Full Reset*** - completely resets all system settings to the factory defaults.

- ***Delete only users' passwords*** – all users' passwords will be deleted but all other system settings will be kept. *(This option is very useful in cases where the protected area is not changed but the owner has changed (like offices, rentals and so on).*
- ***Keep only server settings*** – all system settings will be reset to the factory defaults except those who are related to the communication – networks, servers' addresses, ports, passwords and so on. *(This option is very useful in cases where the protected area is changed but the monitoring center is the same).*

1. Device setup

- ***Device ID*** – this is the identification number assigned to the alarm panel, used to number the protected area in the monitoring station.
- ***Serial number*** – this is the manufacturing number of each alarm panel. It is necessary for Cloud setup.
- ***Test signal*** – this is the automatic period for sending a test signal to a monitoring station.
- ***System language*** – this option changes the language of all messages that are send to the monitoring center.
- ***Update clock interval*** – this is the automatic clock update period (if the panel is connected to a monitoring station).
- ***Update clock*** – manually update the internal clock of the alarm panel.
- ***Time zone*** – sets the time zone of the alarm panel.
- ***Date format*** – sets the date format for the alarm panel. All events will be record and display with the chosen format.
- ***12 hour clock format*** – changes the keypad's clock display format from 24 to 12 hour. All records from the memory will be displayed with this format also.
- ***Password length*** – all user passwords can be 4 or 6 digits long. The system supports changing this length in real time with following constraints:
  - ***Switch from 4 to 6 digits length*** – the system will automatically add two zeros at the end of all existing passwords without changing them.

  - ***Switch from 6 to 4 digits length*** - all users passwords will be deleted. The engineer and master's passwords will be reset to factory defaults.

- ***System area*** – specifies the area number to which all system events will be assign (such as power loss, low battery, troubles and so on).
- ***Generate PGM report*** – this option will enable the information to the monitoring center when a PGM is triggering. Otherwise, this information is available via the alarm panel memory only.
- ***AC loss filter*** – sets the refresh time for sending the status of the external AC power supply to the monitoring station.
- ***Disable jumper reset*** – if this option is enable, then the alarm panel cannot be reset via the onboard jumper. It shall be done via the service program only.
- ***Zone not active period*** – if this option is enable, the system will generate an alarm for all zones that have not been activated in the last 5 months.
- ***Change installer password*** – this is the way to change the installer password. The factory default settings is **9999.**

  <u>NOTE:</u> *After changing the factory default password, you will be prompted from the service tool to enter the new password each time when you are connecting to the alarm panel.*

- ***Wireless system settings***
  - ***Lost packets alarm*** – or "*Connection loss alarm*" that is triggered after the connection with a wireless radio device is lost. Sets the number of missing packets, after which the system has to generate an alarm.
  - ***ARM sync interval*** – sync message period in ARM mode.
  - ***DISARM sync interval*** - sync message period in DISARM mode.

2. Communication

In this tab are all communication settings used to connect the alarm panel to the Cloud system or to a monitoring station.

NOTE: *all these communication features are available if the corresponding GSM/GPRS, WiFi or Ethernet module has been installed already.*

2.1. Server 1 (Server Domain/IP), Port – enter the monitoring station main server address and port. Leave blank, if not used.

2.2. Server 2 (Server Domain/IP), Port – enter the monitoring station backup server address and port. Leave blank, if not used.

2.3. Remote Support (Server Domain/IP), Port – enter the technical support server address and port. Leave blank, if not used.

2.4. Communication patterns - in the high-level security systems (such as Smart Guard), there are special mechanisms to prevent intentional alarm panel manipulations and communication jamming. These mechanisms rely on a special keep alive (sync) messages, which purpose are to inform the monitoring station for the alarm system status. If these sync messages are missing then the monitoring system will generate alarms.

Smart Guard security system supports two different setups for the sync messages based on the system states – ARM or DISARM. Each setup can be set with different modes and timeouts.

- ***Always connected mode*** – in this mode, the alarm panel is always connect to the monitoring system. In this case, the highest available security is provide, because the monitoring system will be notified immediately for any problems with the panel.
- ***Periodically connected*** - in this mode, the alarm panel connects to the monitoring system only if there is a message to be sent – a sync message, an alarm or other event. After sending the message, the communication channel is closing. The security level in this mode is correlating to the sync message interval. The bigger interval means lower security. This mode is very useful in cases when the data traffic must be kept low and/or the number

of the connected to the access point (or mobile cell) transmitters was exceeded.

- ***Sync message interval*** - this is the period to send the keep alive message to the monitoring station.
- ***Auto disconnect*** – this is the time to disconnect from the monitoring station after sending any message.

- ***Patterns*** – several predefined patterns are available for the sync messages that can be in help to the installer. They are based upon the different security level.

Pattern	ARM mode	Connection mode	Sync interval	Auto disconnect
Anti-jamming	DISARMED	Periodically connected	18 000 sec	2 min
	ARM	Periodically connected	600 sec	1 min
High security	DISARMED	Periodically connected	18 000 sec	2 min
	ARM	Periodically connected	3 600 sec	2 min
Standard	DISARMED	Periodically connected	18 000 sec	2 min
	ARM	Periodically connected	18 000 sec	2 min
Always connected	DISARMED	Always connected	300 sec	Not available
	ARM	Always connected	300 sec	Not available

2.5. Communications check – if this option is enable, the system will make automatic internal check of all enabled communication channels.

2.6. Connect to Cloud – this option will enable the connection to the cloud platform **CloudSG**. From this system, the end user can control the alarm system remotely via its mobile device.

2.7. Connect to eGuard system – if the monitoring center works with **eGuard** monitoring software then this option has to be set. It will enable the full capabilities of this alarm system.

2.8. Communication channels – a priority levels can be set for each of the available communication channels – *Primary*, *Backup 1*, *Backup 2 or Disable*. Signal level and connection state indicators provides feedback for each channel:

- ***Grey*** – not used or disabled channel,
- ***Red*** – no connection,
- ***Yellow*** – a link is established, but there is no connection with the server,
- ***Green*** – connection with the server is established.

- ***Test*** – forces manual test and diagnostics of the selected channel.

2.9. GSM Level and SIM ID – this is the level of the GSM signal. It helps the installer to select the better location for mounting the GSM antenna. SIM ID shows the serial number of the inserted SIM card (its internal chip ID).

2.10. GPRS: APN (Access Point Name), username and password – these are the GPRS related network settings, provided by the GSM network operator.

- ***Operator code (ID)*** – when roaming SIM cards are used, they can work with all available operators. The module can be set to choose always a preferred operator by its service code from this field.

- ***Preferred DNS*** – specifies the DNS servers when using any TCP/IP module. It is not mandatory in GPRS connection.

2.11. Ethernet

- ***DHCP*** – setup the network settings for automatic mode.
- ***IP, Gate, Netmask, DNS*** – manual setup of all network settings.

2.12. Wi-Fi

- ***SSID and password*** – network ID (name) and password. With the “*Refresh*” button, all available wireless networks will appear in the list. If the desired network is hidden, then all settings have to be set manually.
- ***DHCP*** – setup the network settings for automatic mode.
- ***IP, Gate, Netmask, DNS*** – manual setup of all network settings.

3. Panel wiring diagrams

In this tab can be setup each input wiring diagram. This is the place where the inputs can be logically split into two zones. A special button can show the picture of each wiring diagram.

- ***Advanced mode*** – if this option is enable, each input can be setup separately from the others. Otherwise, all inputs will be setup together.
- ***Check resistance*** – this button make the real time inspection of each input loop by measuring its resistance. This can help the installer to make diagnostics if there are any wiring problems.

4. Peripheral devices

In this tab are available for setup all peripheral SG devices that are connected to the alarm panel – keypads, proximity readers, expanders and SG PIR detectors. They are list in the table on the left with their names and serial numbers. The settings of each device are displaying on the right side of the table once selected. From here, we can add, remove or replace devices. If there are devices marked in orange, it means they are already connect to the system bus but are not allow (authorized) to operate on it. Authorizing a device to the system can be done after assigning it to an area.

- Replacing a device can be done only if another device of the same type is available on the bus. After replacing, all settings from the old device are transferring to the new one automatically and the old one will be delete (released) from the system.

  NOTE: *After changing any settings in this tab, they have to be save (uploaded) in the alarm panel with the button "**Upload to device**".*

4.1. Assigning "Smart Guard" devices and detectors to the system

4.1.1. Assigning wired SG PIR detectors

All kind of convenient detectors can be attach to the system. The process of assignment can be automated but for SG PIRs only. This automation will remove the need of manual identifying and assignment of all connected detectors to the zones of the alarm system. This will save a lot of time and effort for the installer. The process of recognition is based over a special communication between the panel and each detector, which take place over the system power bus (AUX+ and AUX- power lines).

***<u>ATTENTION</u>*<u>:</u>** The purpose of this communication is for service needs only! It cannot be used to send alarms from the sensors. It can be used for remote adjustment of each detector's sensitivity.

Based on that communication, the recognition process takes place in two phases:

- Searching and recognizing of all connected to the power bus SG PIR detectors;
- Automatic assignment of all recognized detectors based on their physical connection to system zones;

This process is started by pressing the "***Recognition***" button in the "***Wired PIR***" window.

***<u>ATTENTION</u>*<u>:</u>** During the recognition process, all detectors are inactive and cannot monitor the protected area.

After the process has been successfully finish, all assigned detectors are sort in the *Authorized devices* table by the order of their recognition. If some of them are not connect physically to any system zone, they will be highlight in orange.

If we want to add a new detector later, it is not necessary to start the whole process from the beginning. We can use the button ***"Manually appending"***. It will recognize and assign the new detectors only.

If we want to delete all assigned SG PIR sensors, we have to start the whole recognition again.

4.1.2. Assigning wireless SG devices and detectors

Only Smart Guard WL radio devices and detectors can be attach to the system. In order to achieve the radio communication with them, an additional **SG EXPANDER WL** have to be attach to the panel's system bus.
The process is starting with pressing the "*Wireless devices*" button. In the appearing window, all discovered radio devices will split in two tables – on the right side are those that are already paired with other SG panels and on the left are all available and unpaired devices that can be assigned to our system. The assignment is done by pressing the "**+**" button.

In order to appear a device in the unpaired list, it has to be started (or restarted) by its power switch or plugging the batteries.

4.1.3. Wireless device test

- ***"Walk test"*** – used to test the functionality of a particular or all devices at once without generating alarms in and out of the system.
- ***"Discovery test"*** – starting this test for a particular device will blink its LED in order to find its location easily. Starting it for all devices at once is useful for a quick functional inspection.
- ***"Wireless test"*** – will test the throughput of the radio channel for a particular device. The result is shown as a percentage. Keep in mind that this parameter is very dynamic and depends on the current radio broadcasts. The lower is this value the higher is the chance to miss alarms from this device and this will lead to a lower reliability.

4.1.4. Devices over the limit – all devices connected to the wired communication bus, which exceeds the system's capabilities, can be found when pressing the button "*Devices over the limit*". They are available (attached) to the system bus, but cannot be added to the system because the maximum number of supported devices is already reached.

4.2. KEYPADS

- ***FW, HW, SN*** – for the selected device shows information about its serial number, current firmware and hardware versions.
- ***Name*** – user defined name. This text will display on the keypad's display. This will provide easier recognition when more keypads are connect to the system. In addition, all events generated by this device will be send to the monitoring station with this user-defined name.
- ***Zones and PGM*** - shows one of the system's logical zone(s) and PGM that are assign to the hardware built in the selected device.
- ***Area*** – assigns areas to the selected device (i.e. which areas can be control via this device). Each keypad can manage up to 8 areas.
- ***Language*** – the language in which this keypad will operate.

- ***Min / Max backlight*** – setups the backlight brightness for the buttons and the display in the different modes (standby/active).
- ***Volume level*** – sets the maximum volume level for this device.
- ***Quick ARM*** – this option will enable the predefined button for quick arming on this keypad.
- ***Show active zones*** – enabling this option will display on the selected keypad all open zones (which zones are assign to the areas controlled by this device).
- ***Report RFID check in*** – this option will enable sending an information to the monitoring center for every proximity tag that was red. Otherwise, this information is available via the alarm panel memory only.
- ***Mute system sounds*** – stops all sounds from the keypad except those for the alarm events.
- ***Input wiring diagrams*** – sets the input wiring diagram for the selected device.
- ***Check resistance*** – start the real time inspection of the input loop by measuring its resistance.

4.3. PROXIMITY RFID READERS

- ***FW, HW, SN*** – for the selected device shows information about its serial number, current firmware and hardware versions.
- ***Name*** – user defined name. All events generated by this device will be send to the monitoring station with this user-defined name. Also provides easier recognition when more devices of the same type are connect to the system.
- ***Zones and PGM*** - shows system’s logical zone(s) and PGM that are assign to the hardware built in the selected device.
- ***Area*** – assigns an area to the selected device (i.e. which area can be control via this device). A single reader can manage only one area. However, for one area can be assign up to 32 readers.
- ***Report RFID check in*** – this option will enable sending an information to the monitoring center for every proximity tag that was red. Otherwise, this information is available via the alarm panel memory only.

- ***Volume level*** – sets the maximum volume level for this device.
- ***Input wiring diagrams*** – sets the input wiring diagram for the selected device.
- ***Check resistance*** – start the real time inspection of the input loop by measuring its resistance.

4.4. WIRED EXPANDERS

- ***FW, HW, SN*** – for the selected device shows information about its serial number, current firmware and hardware versions.
- ***Name*** – user defined name. All events generated by this device will be send to the monitoring station with this user-defined name. Also provides easier recognition when more devices of the same type are connect to the system.
- ***Zones and PGMs*** - shows system's logical zones and PGMs that are assign to the hardware inputs and outputs that are available in the selected device.
- ***Input wiring diagrams*** – this is the field to setup each input wiring diagram. By choosing the proper diagram, each input can be splitted logically in two zones. A separate button shows the picture of each wiring diagram.
- ***Advanced mode*** – if this option is enable, each input can be setup separately from the others. Otherwise, all inputs will be setup together.
- ***Check resistance*** – this button make the real time inspection of all input loops by measuring their resistance.

4.5. WIRELESS EXPANDERS

- ***FW, HW, SN*** – for the selected device shows information about its serial number, current firmware and hardware versions.
- ***Name*** – user defined name. All events generated by this device will be send to the monitoring station with this user-defined name. Also provides easier recognition when more devices of the same type are connect to the system.
- ***Zone and PGM*** - shows the system's logical zones and PGMs that are assign to the hardware inputs and outputs that are available in the selected device.

- ***Input wiring diagrams*** – this is the field to setup the wiring diagram of the expander's input. By choosing proper diagram, this input can split in two logical zones.
- ***Check resistance*** – this button make the real time inspection of all input loops by measuring their resistance.

4.6. SG PIR DETECTORS

- ***FW, SN*** – for the selected SG PIR detector shows information about its serial number and current firmware version.
- ***Name*** – this is the name of the zone, where the detector was recognized (i.e. the zone where the detector was connected).
- ***Sensitivity*** – each detector has 3 levels of sensitivity and they can be changed from this dropdown menu.
- ***Zone*** – this is the zone number where the detector was recognized (connected).
- ***LED*** – this checkbox allows the user to enable/disable the internal LED indictor of the selected detector remotely. This functionality is possible only if the internal jumper for LED control is not removed from the detector's PCB. If this jumper is missing then the remote control cannot be done. All settings for the LED control will be reset automatically if the jumper is removed and then put back again on the PCB.
- ***Temperature*** – shows the internal temperature for the selected detector.

4.7. WIRELESS SG PIR DETECTORS

- ***FW, HW, SN*** – for the selected SG PIR WL detector shows information about its serial number, current firmware and hardware versions.
- ***Name*** – this is the name of the zone, where the detector is assign.
- ***Sensitivity*** – each detector has 3 levels of sensitivity and they can be changed from this dropdown menu.
- ***Transmit power*** – change the radio power between *Standard* and *Low*.
- ***LED*** – turn on/off the LED operation for the selected detector.

- ***Power save mode*** – if this option is enable, the selected detector will send events to the panel only in ARM mode. If the power save mode is disabled, all events are send regardless of the ARM state. This will increase the consumption and will shorten the battery life.

- ***Zone*** – this is the zone number, where the detector is assign.

- ***Motion sensitivity*** – sets the level of sensitivity for the internal motion sensor, where the lower number means lower sensitivity and 0 means switch off. This sensor acts also as a wall tamper.

- ***Status*** – shows the real time states for the particular device:

  – *Temperature* – the internal board temperature.
  - *Battery* – battery level as a percentage and voltage.
  - *Radio delay* – this is the latency from the moment of event triggering until its reception.
  - *RSSI* – quality of the signal from the radio device. This is how “strong” the panel receives the signal from this sensor. The value shown as a percentage. It helps to find the best position to install the detector.
  - *Tamper* – gives information if the box’s front cover is open.
  - *Motion tamper* – shows if there are detector’s displacement or vibrations.
  - *PIR sensor* – shows if there is motion in front of the sensor.
  - *ARM state* – gives the current ARM state of the area where the device is assign.

4.8. <u>SG MULTI SENSOR WL</u>

- ***FW, HW, SN*** – for the selected detector shows information about its serial number, current firmware and hardware versions.

- ***Name*** – this is the name of the zone, where the detector’s magnetic input is assign.

- ***LED*** – turn on/off the LED operation for the selected detector.

- ***Power save mode*** – if this option is enable, the selected detector will send events to the panel only in ARM mode. If the power save mode is disabled, all events are send regardless of the ARM state. This will increase the consumption and will shorten the battery life.

- ***Generate motion tamper*** – if this option is enable, in case of detected motion or vibration, a dedicated event for Motion tamper will be sent to the alarm panel.

- ***Transmit power*** – change the radio power between *Standard* and *Low*.
- ***Zones*** – this device have 3 different sensors that can be assigned to 3 separate zones at the same time – a magnetic reed sensor, wired input and motion/vibration sensor. This field shows the zone number where each sensor is assign.
- ***Motion sensitivity*** – sets the level of sensitivity for the internal motion sensor, where the lower number means lower sensitivity and 0 means switch off. This sensor acts also as a wall tamper.
- ***Status*** – shows the real time states for the particular device:

  – *Temperature* – the internal board temperature.
  - *Battery* – battery level as a percentage and voltage.
  - *Radio delay* – this is the latency from the moment of event triggering until its reception.
  - *RSSI* – quality of the signal from the radio device. This is how “strong” the panel receives the signal from this sensor. The value shown as a percentage. It helps to find the best position to install the detector.
  - *Tamper* – gives information if the box’s front cover is open.
  - *Motion sensor* – shows if there are detector’s displacement or vibrations.
  - *Wired input* – shows if the wired input contact is trigger.
  - *Reed switch* – this sensor triggers when there is no magnet in front of it.
  - *ARM state* – gives the current ARM state of the area where the device is assign.

4.9. WIRELESS SG REMOTE CONTROL

- ***FW, HW, SN*** – for the selected SG Remote Control WL device shows information about its serial number, current firmware and hardware versions.
- ***Name*** – this is the name of user, to whom the remote control is assign.
- ***Transmit power*** – change the radio power between *Low* and *Standard*.
- ***User*** – this is the user number, to whom the remote control is assign.

- ***Buttons 1÷4*** – sets the alarm system actions after pressing or holding a particular button of the remote control. These actions can be:
  - arming, disarming or checking the security state of the specified area in the corresponding *Area/PGM* field.
  - turning on, turning off, toggling or checking the state of the specified PGM output in the corresponding *Area/PGM* field.
  - triggering panic alarm for the specified area.

  Pay attention to the user's permissions when setting actions for arming the system.
- ***Status*** – shows the real time states for the particular device:
  - *Battery* – battery level as a percentage and voltage.
  - *Radio delay* – this is the latency from the moment of event triggering until its reception.
  - *RSSI* – quality of the signal from the Remote control. This is how "strong" the panel receives the signal from it. The value shown as a percentage.
- ***Patterns*** – provides preset settings for quick setup of the buttons with the most used combinations:
  - arm, disarm and check the state of a single area.
  - arm, disarm and check the state of a single area with option to switch on a specified PGM output.
  - arm, disarm and check the state of two areas.
  - clear the current configuration of all buttons.

5. Areas

In this tab can be setup all the parameters of the system areas – enable/disable, naming, entry-exit timers and so on.

- ***Use*** – enable/disable the use of this area number.
- ***Name*** – user defined name. All events generated for this area will saved with this user-defined name.
- ***Alarm time*** – in general terms, this is the time for which the siren will sound after an alarm event occurred (i.e. the siren PGM output will be active). During this alarm time, any new alarms will be save

in the control panel memory without changing (extending) the current alarm time. In the meantime, if there is a connection to a monitoring station, all these new alarms will be send regularly. Any new alarm generated after the alarm time has been finished will start it again.

- ***Entry time*** – during this time, the system will be waiting for a valid user code and will not generate alarms.
  - In order to start the Entry time, the system have to be armed and then an “Entry-Exit” zone should be activate.
  - Entering a valid user code will disarm the system. Otherwise, the system will trigger an alarm after the entry time has elapsed.
  - The maximum value for entry time is 255 seconds. A zero will disable it.
  - ***Full arm, Stay, Sleep modes*** – enables/disables the entry time in the different arm modes.
- ***Exit time*** – during this time, the system will be waiting for users to leave the protected areas without generating alarms. After this time is elapsed, the system will enter in Arm mode.
  - “Entry–exit” and “follow” zone types are not monitoring during exit time.
  - Entering a valid user code will stop the exit time and the system will not be arm.
  - The maximum value for exit time is 255 seconds. A zero will disable it.
  - ***Full arm, Stay, Sleep modes*** – enables/disables the exit time in the different arm modes.
- ***Card hold arming*** – enables arming of the selected area after holding a proximity card for few seconds in front of a reader assigned to this area.
- ***Auto ARM*** – enables automatic arming for the selected area based on the selected rules.
  - After no movement - will ARM the area in one of the selected modes if there are no open zones (no movement) for the specified **Timeout** (in minutes).

- On schedule - will ARM the area in one of the selected modes at the exact hour (**Clock**) each day. If there are opened zones at the time of activation, the system will trigger an alarm.
- Mixed - will ARM the area in one of the selected modes at the exact hour (**Clock**) each day. If there are opened zones at the time of activation, the system will postpone it for the specified **Timeout** (in minutes).

6. Users

The system defines three user types with different permissions - *engineer*, *master* and *regular user*.

- **ENGINEER** – this user is **only one** for the system and has full permissions on it. Only this user can connect to the alarm panel with service program and change all system settings.
- **MASTER** – permissions for this user type can be assign to any of the 500 available users in the system.
  - A master user can be create, modified or deleted only by the engineer.
  - This user type can change its own permissions and passwords only.
  - Can bypass zones only from areas for which has permissions.
  - Can ARM and DISARM areas only for which has permissions.
  - Can create, modify or delete regular users and with permissions and access codes.
  - Can view the alarm memory via keypad.
- **REGULAR USERS**
  - A regular user can be create, modified or deleted by both an engineer and a master user.
  - The regular user can change only its own passwords.
  - Can bypass zones only from areas for which has permissions.
  - Can ARM and DISARM areas only for which has permissions.
  - Can view the alarm memory via keypad.
- ***Use*** – enable/disable the selected user.

- ***Name*** – sets a name for the selected user. It will display on the keypad's display when the user is accessing it. This name will be saved in all events related with this user (ARM/DISARM, bypassing zones, access codes entering and so on).
- ***RFID*** – a proximity card number that can be assign for the selected user. It can be filled manually by hand or automatic by the system. The second option can be do with any proximity reader connected to the system bus, by clicking on the card button standing on the right side of the RFID field. The system will wait for some time to get and fill the ID of the first proximity card accessed by any of the readers.
- ***Remote control*** – a remote control from the drop down list can be choose to assign to the selected user.
- ***Areas*** – assigns to the selected user the permissions for the areas (i.e. for which areas the user will have permissions).
- ***Time slot*** – selects one of the 9 predefined weekly schedules (time slots), when the selected user will be able to access the system. Value 0 - not used.
- ***Master*** – this option enables Master user rights to the selected user.
- ***Arming rights*** – for the selected user, permits or disables the different security modes – FULL ARM, STAY, SLEEP and DISARM.
- ***User passwords*** – changes all user password.
  - ➢ ***Keypad passwords***

    – ***Main password*** – this is the code used to ARM and DISARM the alarm system. This code is using to change the user's preferences via keypad also.

    – ***Duress code*** – if this code is set, the system will allow (imitate) disarming when the user is using it. In addition, it will trigger a silent panic alarm, which will be send to the monitoring station. It will inform that the user is force to disarm the system and is in potential danger.
  - ➢ ***Cloud PIN and pairing code*** – the cloud PIN is use every time when logging into Cloud SG system. The pairing code is used only once in the initial access in order to pair with the system for the first time.

- ***Export passwords*** – this option will export all user passwords encrypted in a file. It is useful in two cases – to backup or transfer them to another system.

7. Time slots

The time slots are predefined weekly schedules, and during this schedules (time intervals/slots) the users can access the system (ARM/DISARM and so on). Up to 9 time slots can be defined, with start and end hour for each day of the week.

8. Zones

In this tab can be setup all the parameters of the system's zones. The system supports up to 135 logical zones and they can be distribute among all available hardware inputs. Any hardware input available on SG device can be double logically. These additional logical zones are follow by ATZ after their number.

The system provides several different zone types, which are suitable for different purposes. These zone types are:

- ***Instant*** – if this zone open while the area to which it is assign is armed, an alarm will be generate.
- ***Entry-Exit*** – this zone type is monitoring by the alarm panel when the area to which it is assign is armed. It will provide delay time after opening, and the user have to disarm the area before this delay is expired. Otherwise, it will generate alarm. The "*Exit"* delay provides to user the time to leave the area when arming, without generating alarm. If the zone is still open after the "*Exit"* delay time has expired, then alarm panel will generate alarm.
- ***Follow*** – this zone type is monitoring by the alarm panel when the area to which it is assign is armed. If an "*Entry-Exit"* zone from the same area has been open before this zone type, this one will "*follow*" it and will not generate alarm until the *"Entry"* delay time has expired.
- ***24 hours*** – this zone type is monitoring by the alarm panel all the time. Each time when the zone is open, the alarm panel is generating alarm.
- ***Key switch*** – triggering a zone from this type will ARM or DISARM the area to which it is assign.

- ***Tamper*** – a predefined zone type, used to generate a Tamper event. All zones connected to system's tampers can be setup as Tamper zones. This zone type is monitoring by the alarm panel all the time.
- ***Fire*** – a predefined zone type, used to generate a Fire alarm. All zones connected to fire detectors can be setup Fire zones. This zone type is monitoring by the alarm panel all the time.
- ***Medical*** - a predefined zone type, used to generate a Medical alarm. All zones connected to SOS buttons can be setup as Medical zones. This zone type is monitoring by the alarm panel all the time.
- ***Panic*** - a predefined zone type, used to generate a Panic alarm. All zones connected to panic buttons can be setup as Panic zones. This zone type is monitoring by the alarm panel all the time.
- ***Custom*** – a custom defined zone type that is monitoring by the alarm panel when the area to which it is assign is armed. This zone type is use when custom Contact ID codes are required.
- ***Information*** – a special zone type that is not monitoring in any of the ARM modes and does not generate alarms. When triggered, only an information event is save in the alarm panel's memory.

8.1. Zone parameters

- ***Zone (number)*** – this is the system's logical zone number.
- ***Name*** - user defined name. All events generated for this zone will save with this user-defined name.
- ***Use*** - enable/disable the use of this zone number.
- ***Device: SN*** – any physical input from an existing device can be assign to the selected zone. This field provides information about the selected device type, its Serial Number, the chosen hardware input and zone name.
- ***Device: Type*** – this field provides quick information about the device type where the zone is located.
- ***Device: In*** – this field provides quick information about input number of the device, where the zone is located.

- ***PIR SN*** – the field shows the serial number of connected to the selected zone SG PIR detector. If no detector is connected, the field is blank.
- ***Zone type*** – sets the type for the selected zone.
- ***Areas (numbers)*** – selects the areas the selected zone will assigned to.
- ***Key switch: Arming*** – when the selected zone is defined as key switch, this can setup the ARM mode which will be set to the assigned area after opening the zone - *Full arm*, *Stay*, *Sleep* or *Off (disabled)*.
- ***Key switch: Disarming*** – enables DISARM of the corresponding area after the selected zone is closed.
- ***Key switch: Triggering On*** – selects the triggering event for the selected key switch zone. With constant or temporary change of the current zone state - *Level Disappear, Level Appear, Pulse Disappear and Pulse Appear (minimum pulse duration is 0.7 seconds*).
- ***Key switch: Sound on ARM/DISARM*** – enables the siren from the PGM assigned to the corresponding area, when arming or disarming from the selected key switch zone.
- ***Key switch: Exit time*** – enables the "*Exit time*" delay for the corresponding area, when arming from the selected key switch zone.
- ***User bypass: Enable*** – this checkbox allows the zone to be manually bypass.
- ***User bypass: Bypass*** - the selected zone can be manually bypass from this checkbox. It means that this zone will not be included for monitoring when the area is armed. This manual bypass can be use when users want to have access to the assigned of the selected zone area while it is armed. Other use is to bypass a defective zone (bad contact, damaged wiring) until service can be provide.
- ***Bypass partial ARM: STAY/SLEEP*** – in this field predefined partial ARM modes *STAY* and ***SLEEP*** can be setup. A checkbox in one of the modes will bypass (exclude) the selected zone from monitoring in the checked mode.

- ***Filter*** – this option can be used to reduce false alarms from external detectors. By default, this filter is switched ***Off****.*
  - ***On*** – enables zone filtration with predefined values for the filter parameters: ***2*** *count Pulses for Period of* ***300*** *seconds*. It means that the zone will generate alarm if it will open 2 times before 300 seconds timer expires.
  - ***Custom*** – enables zone filtration with user define values for the filter parameters *Pulses* and *Period.*
  - ***Custom (****alarm from one pulse, if the defined period is overshot****)*** – enables zone filtration with user defined values for the filter parameters. The difference with the previous custom filter is that this one is counting not only the pulses but their duration also. This one will generate alarm when the zone is open but not closed before the filter period expires.
- ***ContactID code*** – this field is active only when the zone type is set as *Custom*. Allows different from default *ContactID* codes to be set when the corresponding to the selected zone area is armed or disarmed.
- ***Silent alarm*** – prohibits the audible notification when the zone is in alarm. If there is a connection to a monitoring station, the alarm will be send regularly.
- ***Doorbell*** – enables keypads and readers to play an audible signal when the zone is triggering (after open and close). This signal will be play only if the zone and the device are from one area.

9. PGM

In this tab can be setup all the parameters of the system's PGMs. The system supports up to 48 PGMs (programmable outputs) and they can be distribute among all available hardware outputs also. The only exception is that first 4 PGMs are reserved for the alarm panel. These programmable outputs can be set to trigger after user selected events. Like turning on the siren after alarm is generate, resetting fire detectors after triggering, open/close doors after user identification and many more. All PGM outputs are open collector type except those in keypads and readers, where there is additional hardware.

The system provides several predefined PGM types, which can trigger upon predefined events. These types are:

- ***Siren*** – will trigger the PGM output after any alarm event. Its purpose is to drive an external siren in order to provide audible alarm for the protected area. It will not trigger after a *Silent* or *Duress code* alarms.
- ***Door Lock Standard*** – will trigger the PGM output after a user proximity card was red. The first option is available only for the output integrated in the corresponding reader. The reader must be assign to the area the user wants to access. In addition, the user must have permissions for this area. This PGM type is use mostly to drive electromagnetic locks and strikes.
- ***Smart Door Lock*** – completely follows the previous type and its requirements, with the addition that this one is design especially to drive electric strikes. It happens with extremely low current, as low as about 1/10 the nominal. This is possible due to the specially designed hardware and software available in the SG Keypads and Readers. Thanks to this, there is no need from external power supplies and bigger wires to the strikes. They can be wire directly from the corresponding keypad or reader.
- ***Reset fire detectors*** – this type is usually use to cut off the power supply of smoke and fire detectors connected to its loop. When this type was selected, the PGM can be triggered via the special option in the keypad's menu or remotely*.
- ***Alarm from zone*** – will trigger the PGM after alarm from a predefined zone appears. Restoring the zone will restore the PGM state.
- ***Arm/Disarm*** – will trigger the PGM after arming the predefined area(s). Disarming the area(s) will restore the PGM state.
- ***Panic*** – will trigger the PGM after alarm event from a *Panic* zone appears. Restoring the zone will restore the PGM state.
- ***Fire*** – will trigger the PGM after alarm event from a *Fire* zone appears. Restoring the zone will restore the PGM state.
- ***Medical*** – will trigger the PGM after alarm event from a *Medical* zone appears. Restoring the zone will restore the PGM state.
- ***24 Hours*** – will trigger the PGM after alarm event from a *24 Hours* zone appears. Restoring the zone will restore the PGM state.

- ***Tamper*** – will trigger the PGM after alarm event from a *Tamper* zone or device tamper appears. Restoring the event will restore the PGM state.
- ***Trouble*** – will trigger the PGM after *Trouble* event appears. Restoring the event will restore the PGM state.
- ***Silent*** – will trigger the PGM after alarm event from a *Silent* zone appears. Restoring the zone will restore the PGM state.
- ***Alarm time*** – same as the *Siren* PGM type, but will trigger also after *Silent* and *Duress code* alarms.
- ***Triggered by Zone*** – will trigger the PGM after a predefined zone opens. Restoring the zone will restore the PGM state.
- ***Triggered by PGM*** – will trigger the PGM after a predefined PGM triggers. Restoring the predefined PGM will restore the state of the selected one.
- ***Custom*** – custom defined PGM type. It will trigger after all predefined conditions are fulfill. Conditions that can be set are specific area(s), zone and another PGM or ContactID code. Restoring the conditions will restore the PGM state.

9.1. PGM parameters

- ***PGM (number)*** – this is the logical number for each PGM output in the system, where the first four numbers are reserved for the alarm panel only.
- ***Use*** - enable/disable the use of this PGM number.
- ***SN*** – from this dropdown menu can be selected an output from the available peripheral devices. In addition, it provides quick info about the Serial Number of the selected for this PGM hardware.
- ***Device type*** – provides quick info about the device type of the selected for this PGM hardware.
- ***Out*** – provides quick info about the output’s physical number in the selected device.
- ***Name*** - user defined name. All events generated for this PGM will save with this user-defined name.
- ***PGM type*** - sets the type for the selected PGM.

- ***Operational behavior*** – the *Mode* option specifies (program) how to operate the output when activated. The *Trigger* mode will change current output state to the opposite one until a new activation is happen. While the *Pulse* mode will change it for a predefined *Auto off* period and will be restore after its expiration.
- ***Invert*** – this option swaps the *ON* and *OFF* states of the output. Then, when the PGM is activate, the output will turn off.
- ***Activation conditions*** – from these fields the user can specify the exact trigger event generated:
  - ***Area*** – by *Selected* area number, by *Any* area or from *All* areas simultaneously;
  - ***Zone/PGM*** – by specific zone or PGM number;
  - ***Event*** – by specific *ContactID* code;
- ***Remote control*** – this option allows the selected PGM to be remotely control via CloudSG system or by phone call and SMS.
- ***Info zone*** – a zone number has to be set here. Makes a relation between the zone and the selected PGM in the CloudSG system in order to provide a feedback for their statuses. This option is useful when home automation is implement in order to check the status of the controlled devices.

10. Real time view

Provides real time information about the current state of the enabled areas, zones and PGMs. Moreover, it provides the ability to ARM or DISARM any area (or the whole system) by double clicking on them. In order to do this, a regular keypad password with permissions is necessary – from a regular user, from the master user or from the engineer.

In this tab can be monitored all system troubles and power consumptions. A dedicated button for triggering PGMs with *Fire detectors reset* is provide also.

11. PGM Phone control

All PGMs with the *Remote control* option enabled can be trigger after a phone call or SMS. The system provides this ability to 10 different phone numbers. For each number can be assign to control up to 48

PGMs via *Call* or *SMS*. The phone numbers have to be set in one of the following formats: +44… or 0044…

12. Phone notification

The system can notify up to 10 different phone numbers after predefined events. These notifications are via phone calls or SMS. The SMS text can be user defined or system defined if the text field is blank. The phone numbers have to be set in one of the following formats: +44… or 0044… All triggering conditions are based on the PGM types, where a specific area(s), zone, PGM or ContactID code can be set:

- *On triggering of Area Alarm Time*
- *Alarm from zone*
- *On ARM/DISARM events*
- *On PGM activation*
- *On Fire alarm from zone*
- *On Medical alarm from zone*
- *On Panic alarm from zone*
- *On 24 Hours alarm from zone*
- *On general Tamper or Tamper zone*
- *On Silent alarm from zone*
- *On triggering of Trouble event*
- *Custom events*

13. LOG

From this tab can be extracted the alarm panel memory. For quicker operation, few smaller predefined periods are available – for the last day, last 7 days or 30 days. Each event is show with lot of details – its type, timestamp, ContactID code, explanation text, Area/Zone/PGM numbers, the involved user and more. After reading the archive, it can be export to Excel file by clicking the right button.

14. Firmware updater

This tab provides the ability to update the firmware of all system components. Once the update file is download into control panel, it will update itself and all connected peripheral devices simultaneously and fully automatic. The update progress can be follow on each keypad connected to the system bus. The system keep its settings after update is finished.