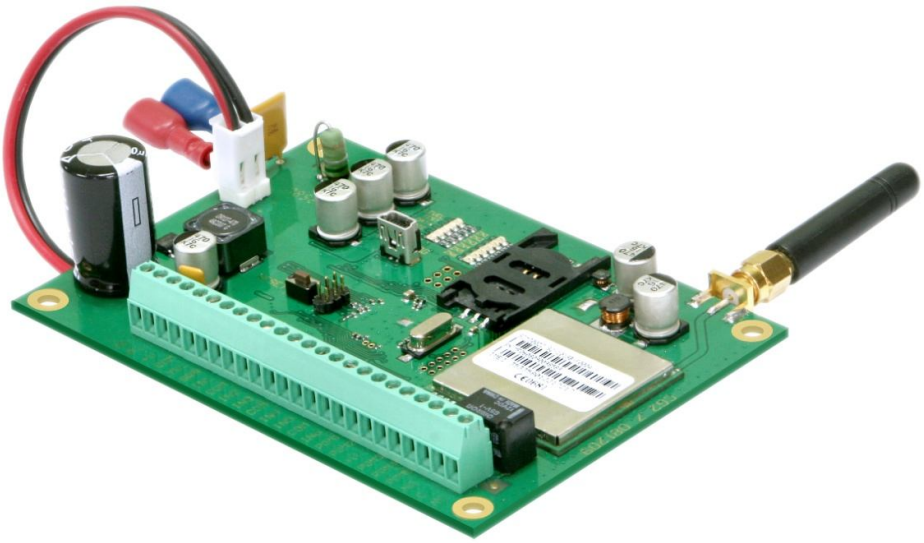
ORVOS monitooring



Security module CG2

Installation manual

Module version 091026

Save a tree...please don't print this document *unless you really need to*

Safety Requirements

Before using the module CG2 please read this user guide and follow all safety instructions!

Security module CG2 is a continuously operating component of a security system.

It is dangerous for persons provided with a security service to touch or otherwise influence internal electronic security components.

Security module CG2 should be mounted in sites of restricted access and should be used with indoor GSM antennas.

Only properly trained personnel being aware of used devices properties, operation of GSM devices and safety requirements may perform installation and maintenance of the security module. Housing, transformers and batteries and programming devices used with the module must be in compliance with safety requirements of EN 60950 standard!

Security module CG2 is powered by alternating 16-18V 50 Hz voltage via step-down II class transformer or from a 12V / 4-7 Ah backup battery. Current in operation cannot exceed 2A and depends on the current consumption of connected peripheral devices.

An automatic bipolar overload cutout must be installed to the electricity supply circuit to safeguard from a too high current.
Release contacts separation must be ≥ 3mm. Cutout must be installed in a place well known to the module maintaining personnel.

Full disconnection of the module:

- from AC mains – by turning the automatic cutout off;
- from the battery – by disconnecting terminals;

Transportation and storage:

Security module CG2 should only be transported or stored in manufacturer's package.

During transportation or storage the item should be protected from possible hits, vibration and other mechanical damage, also from sudden changes of temperature or dampness.

Security module CG2 is a six input (zone) control panel with a GSM communicator.

Main features

6 programmable inputs,
9 zone operation functions,
1 partition,
3 ways to arm/disarm the security system,
3 arming modes ARM/STAY/OFF,
6 programmable outputs PGM,
8 types of output operation,
Automatic arming Auto-ARM,
Bell squawk when arming/disarming,
Bypassing a zone,
Security systems state monitoring,
Integrated GSM modem messaging to:
- Users – by SMS messages or by short calls,
- Monitoring station – via GPRS or by SMS messages,

2 ways to configure operation parameters.

Package content

1 SET. **Security module CG2**

- Control panel CG2	1 pc
- GSM antenna, straight	1 pc
- Battery connecting cable	1 pc
- Resistors 2,2 kΩ	6 pcs
- Mounting bushes	4 pcs

2 SET. **Security module CG2 KIT**

- Metal housing (HxWxD) 200x210x75 mm	1 pc
- Control panel CG2	1 pc
- Step-down transformer	1 pc
- GSM antenna, straight	1 pc
- Battery connecting cable	1 pc
- Resistors 2,2 kΩ	6 pc

Technical parameters

Power supply source	AC 16–18V
Current	up to 2 A
Back-up power supply source	battery 12V, 4–7Ah
Six inputs IN1, ..., IN6	Selectable NC, NO or EOL=2,2 kΩ type
Outputs PGM1, PGM2, PGM3	Open collector 30V, 50mA
Outputs PGM4, PGM5	Open collector 30V, 1A
Output PGM6	Relay output switching 30V, 1A
Power supply for peripheral devices	DC 12V up to 1,1 A
User codes	40
GSM modem frequency	900/1800/1900 MHz
Transmission protocol to CMS	TCP/UDP and/or SMS
Number of IP addresses in CMS	2
Phone numbers of SMS modems in CMS	2
Information protocol to CMS	In accordance with Contact ID
Phones numbers of users whom alarm messages can be sent	2
Messages to user	changeable content SMS
Operating temperature range	from –10ºC to +55ºC
Overall dimension	120x80x16 mm

Description of parameters

1. Security system can be armed/disarmed:
   - By free of charge phone call. Up to 40 User phone numbers can be entered into module's phonebook, by which security system can be armed/disarmed and/or change state of PGM established to operate as ***DIAL*** remotely.
   - By changing the state of input established to function as control zone ***ON/OFF*** with devices that have switching contacts (keypad SZW-02, Access board, switch and etc).
   - By *Paradox*® keypad K636, MG10LEDV, MG10LEDH or MG32LED.*

2. When security system is armed in mode STAY, it allows to roam freely within the premises while the perimeter is fully armed. Alarms are ignored in circuits of inputs established to function as ***Interior STAY*** and ***Instant STAY***. Input established to function as entry zone ***Delay*** starts to function as ***Instant***. Arming mode STAY can be turned on by 3 ways:
   - By pressing [STAY] button in the keypad and entering the User code,*
   - By entering the User code without alarming the entry zone ***Delay***,*
   - By a call of the User without alarming the ***Delay*** entry zone.

3. When the security system's arming mode STAY is turned on by using the keypad, entry zone ***Delay*** starts to operate in instantaneous mode. When mode STAY is turned on by using the second or third turning on way is used zone ***Delay*** remains to operate in its mode.

4. When the security system is armed/disarmed, the module sends confirmations of command execution.

5. The security module CG2 has six external inputs, to which different sensors are connected to. It's possible to establish differently security system's reaction (zone operating function) to alarms in sensors circuits connected to inputs. Inputs circuits types: NC, NO or EOL=2,2 kΩ. Security system's reactions to either input state change:
   - ***ON/OFF*** – when this input is connected to COM, it is possible to arm/disarm the security system. After arming the system starts calculating exit delay time, during which it is possible to easily leave the premises under protection.
   - ***Delay*** – disturbances are allowed in sensor's controlled zone connected to input, during the exit time after arming and don't call security system alarm. If the zone is still being disturbed after exit time has passed, ***Bell*** and ***Flash*** output signals are generated and messages are sent. When the security system is armed, disturbance of the zone activates calculation of entry delay time during which it is possible to disarm the security system. Security system must be disarmed during the entry time period otherwise output signals ***Bell*** and ***Flash*** will be generated including alarm report.
   - ***Interior*** – when the security system is armed, alarm in sensor controlled zone results in generating output signals ***Bell*** and ***Flash*** and sending of the report. During entry and exit time disturbances in zone are allowed.
   - ***Interior STAY*** – operates the same as ***Interior***, although when security system is armed in STAY, disturbances in sensors controlled zone are ignored.
   - ***Instant*** – when the security system is armed, disturbances in sensors controlled zone result instantaneously generated signals ***Bell*** and ***Flash*** and sending the report.
   - ***Instant STAY*** operates the same as ***Instant***, although when security system is armed STAY, disturbances in sensors controlled zone are ignored.
   - ***24 hours*** – disturbances in sensors controlled zone call instantly generated signals ***Bell*** and ***Flash*** and sending the report. Signals are generated independent of security systems arming mode.
   - ***Fire*** – disturbances in sensors controlled zone call instantly generated fire signals ***Bell*** and ***Flash*** and sending the report. Signals are generated independent of security systems arming mode.
   - ***Silent*** – disturbances in sensors controlled zone call instantly sending the report, although signals ***Bell*** and ***Flash*** are not generated. Messages are generated independent of security systems arming mode.

6. It's possible to arm security system, while one or several zones are temporarily out of service by using bypass a zone function. This function must be set for every input separately and must be applied by code keypad. Bypassed zones are automatically cancelled each time the system is disarmed and must be bypassed again, if required, before the next arming.

7. Security module CG2 has 6 outputs for connecting to signaling devices and controlling them.
   - Outputs PGM1, PGM2, PGM3 switching voltage up to 30 V and current up to 50 mA.

---

* *Security system's control commands by using keypad are given in **annex D**.*

- Outputs PGM4, PGM5 switching voltage up to 30 V and current up to 1 A.
- Relay output PGM6 switching voltage up to 30 V and current up to 1 A.

Each PGM of six can be set to operate in one of the specified operating modes:*

- ***Buzzer*** – intended for control a low power sound device. Pulsating signals (periodical beep) are generated during the exit/entry delay, and after security system was alarmed – continuous signal.
- ***State*** – intended for control a light device. Pulsating signals are generated during exit delay, and after security system was alarmed – continuous signal.
- ***Ready*** – intended for control a light device. When all security zones are armed, a continuous signal is generated.
- ***Flash*** – intended for control a light device. When security system is armed, continuous signal is generated and after security system was alarmed pulsating signal is generated.
- ***Bell*** – intended for control a sound device (siren). After security system was alarmed a continuous or periodical sound signal will be generated.
- ***SMS*** – intended for remote control of electrical engineering devices by sending SMS messages.
- ***AC OK*** – intended for control light device and shows that security system is powered from the power supply main.
- ***Battery OK*** – intended for control a light device and shows availability of power supply from a backup battery.
- ***DIAL*** - intended for remote control of electrical engineering devices by free of charge call.

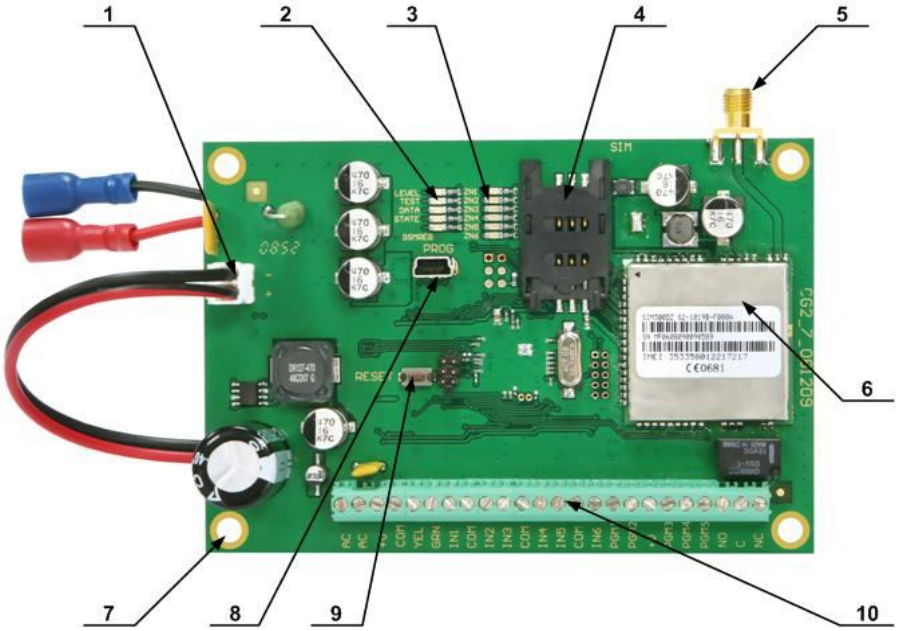
8. Entry/exit delay time may be set from 0 to 255 seconds.
9. Time of siren operation may be set from 0 to 9999 seconds.
10. The security module can automatically arm itself - *Auto ARM* function. If after the security systems disarming by a free of charge call, no zones were alarmed during the entry delay, the security system will be re-armed automatically.
11. The security module has an arming/disarming Bell squawk function. Upon arming of one short signal is generated and upon disarming – two short signals.
12. Security module sends messages:
    - SMS messages to two User telephones. User can be additionally informed about the sending of SMS messages by a free of charge call.
    - To the monitoring station (CMS) by a GPRS connection with TCP/UDP protocol to two IP addresses and/or SMS messages.**
13. Security module periodically sends test messages [Test]. Period is 1–65535 minutes.
14. The security module CG2 is supplied by 16 – 18 VAC or 12,6 VDC voltage from 4-7 A/h backup battery. Permissible range of AC voltage drop is ±20%. When power supply from AC mains has failed, the module automatically turns to backup power supply. After AC voltage has restored, the battery is charged and maintained in a standby mode. Time period necessary for the battery to fully charge is no more than 15 hours, charging current is not exceeded 0,6 A. When voltage drops below 10V, battery is automatically disconnected.
15. Security module's controller monitors power supply chains and sends reports about power supply failure:
    - AC has failed/restored,
    - Battery's voltage has fallen below 11.5 V or has risen again to 12.6 V.
16. Security module has a power supply unit to power sensors and security devices with direct 12 V voltage. Total operational current should not exceed 1.1 A. Plugs are protected from short circuit or overload by automatic cutouts.
17. Parameters of security module are set by:
    - User's mobile phone when sending SMS messages in established form,
    - PC when using GProg software.
18. Security module CG2 operates well and maintains its operational parameters when environment temperature is from –10°C to +55°C and relative air humidity is not higher than 90% in temperature of +20°C.

---

* *Outputs operations are graphically displayed in **annex A**.*

** *Messages are transmitted according to Contact ID code table.*

Essentials of the module CG2



1 – Connector and leads for battery connecting;
2 – LEDs to visualize module operation in GSM network,
3 – LEDs to visualize inputs state,
4 – SIM card holder,
5 – GSM antenna screw-connector;
6 – GSM modem;
7 – Mounting holes;
8 – USB port for configuration of module;
9 – RESET button;
10- Terminals for external connections;

Application of external terminals

AC, AC		Power supply clamp (to connect 16 V_{AC} voltage)
+V		Clamp to power supply the auxiliaries devices by +12 V
COM		Common clamp
YEL		Clamp to connect *Paradox* keyboard (Yellow)
GRN		Clamp to connect *Paradox* keyboard (Green)
IN1...IN6		Input clamps
COM		Common clamp
PGM1...PGM5		Output clamps (PGMs)
+V		Clamp to power supply the auxiliaries devices by +12 V
NO		Normally open relay clamp
C	PGM6	Common relay clamp
NC		Normally closed relay clamp

Light indication meanings

ZN1...ZN6	Inputs state	Red On Off	Zones aren't closed Zones are closed in desired partition (OK)
LEVEL	GSM level	Red flashing	Number of flashes means GSM signal level
TEST	Operation	Green flashing	Power supply is OK, the module operates
DATA	Data transfer	Yellow On	Memory of the module still contains unsent messages
STATE	GSM modem state	Yellow flashing	GSM modem is functioning*
GSM REG	Registration of the module to the network	Yellow On Yellow flashing Yellow fast flashing	Module is registered to GSM network Module has been registered to GSM network Module doesn't find the SIM card

Mounting and preparation of the CG2 module

1. The module CG2 should be mounted into housing together with a step-down transformer. Module is fastened to the housing by screws or plastic bushes through the mounting holes (7). Transformer is connected to AC terminals. A back-up battery is installed.
2. Sensors and signal devices should be connected to the terminals of security module. Examples of connection schemes are given in annex C. GSM antenna is screwed onto the antenna screw-connector (5), a SIM card is inserted into the SIM card holder (4).
3. Power supply should be switched on. At first, power supply from the AC and then from the back-up battery.
4. Module is configured.
5. Security module operation and message sending should be checked.

Configuring by PC

Operational parameters can be set up, read, modified and updated with configuration software GProg. Loaded or newly created parameter setup files with extension ".tcfg" can be saved and used to configure other The software and it's installation manual can be found at www.orvos.ee.

To connect the module CG2 to a PC follow these steps:

1. Connect module to power supply,
2. Connect the device to a computer using USB cable,
3. Start the program GProg and select *Setup/Serial port*, then specify the serial port (e.g.: COM14),
4. Then select command *Devices* and a programmable device *CG2*. A dialog window [Main window] will open,
5. Press the icon [Connect],
6. To read the operational parameters stored in the module press the icon [Receive config]. When data download has finished a window [Configuration is received] will appear.

1. Setting up control panel's parameters

1.1. In the window [Main Window] main parameters of the module should be entered:

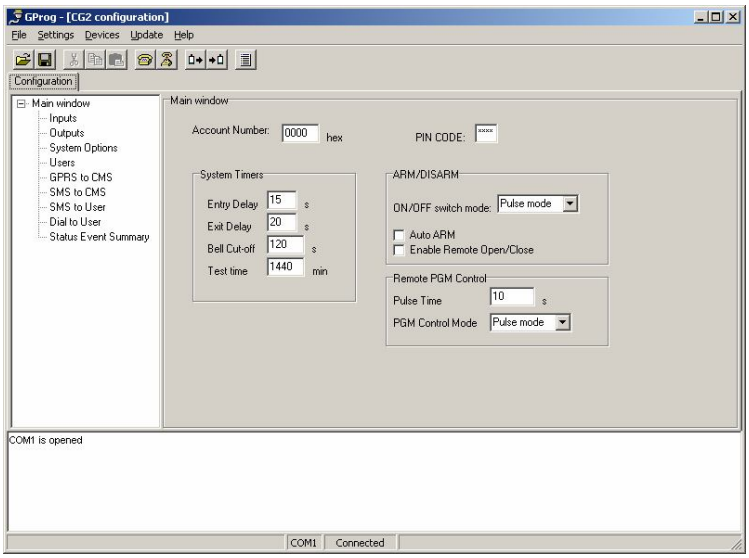
- Module's Account Number*;
- SIM card's PIN code;
- Entry delay time [Entry Delay], sec.;
- Exit delay time [Exit Delay], sec.;
- Duration of Siren operation when system is alarmed [Bell Cut-off], sec.;
- Periodicity of signal tests [Test time], min.;
- Switch mode of control input ***ON/OFF***, [Pulse mode] or [Level mode];

NOTE: If control panel is armed/disarmed by a free of charge call, [Pulse mode] should be set. If security system is armed or disarmed by changing input state ***ON/OFF*** any setting can be used. But when [Level mode] is used, input circuits are controlled constantly.

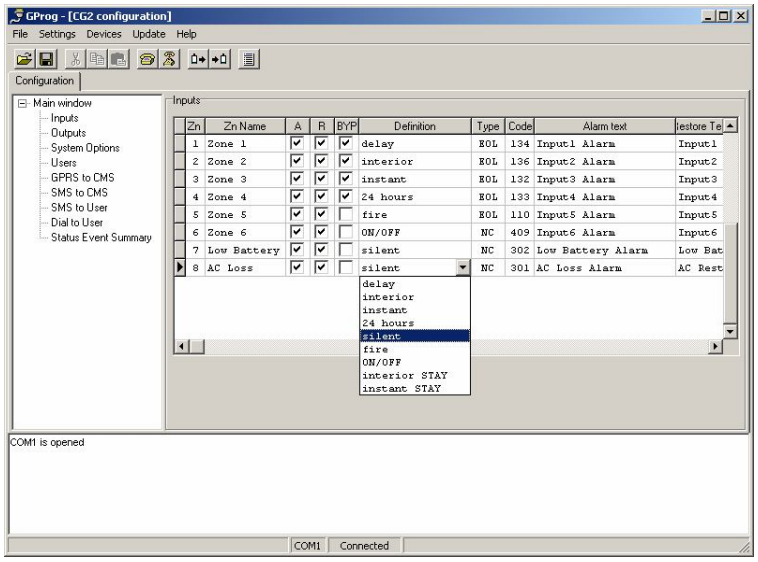
- Mark the box [Auto ARM] to activate auto-arm function.
- Mark the box [Enable Remote Open/Close] to activate the function security system arming/disarming in remote mode.
- Choose the PGM control mode [Level mode] or [Pulse mode]. When pulse mode is chosen, select relay switching pulse time of remote controlled PGM [Pulse time].

---

* *Account number of the module should be entered in hexadecimal format.*



1.2. Properties of inputs (zones) can be selected in the dialog screen [Inputs]. To alter the view of the properties use a scroll-bar in the bottom of the screen.

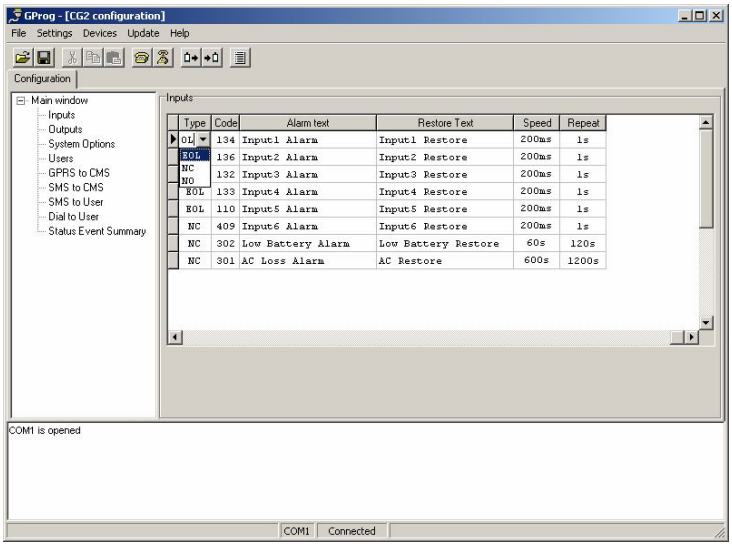


Definition of each input [Definition] can be set by a double click on a cell and selecting a desirable security zone function in a section has opened. Transmitting function of alarm [A] and restore [R] messages of each zone can be activated. A bypass function [Bypass] of chosen zone can be activated as well. A circuit type NO/NC/EOL [Type] can be set.

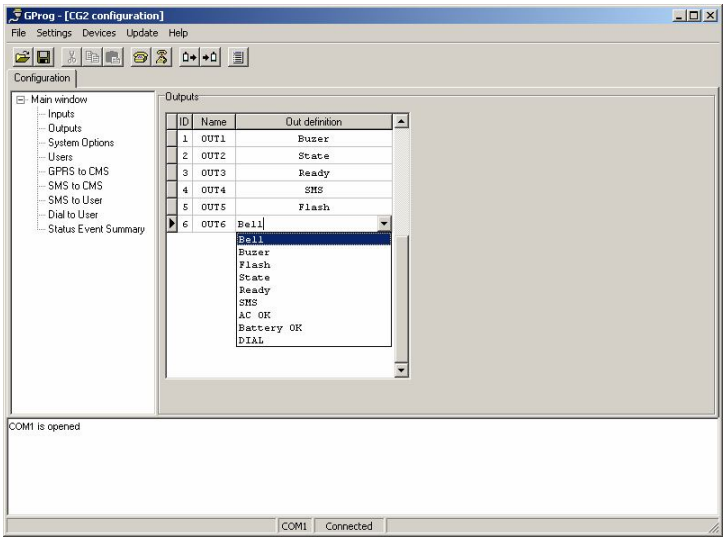
If messages are sent to the Central Monitoring Station (CMS), it is recommended not to change the message codes [Code], otherwise it is necessary to know the Contact ID message codes.

If messages are sent to mobile phone in a form of SMS, every input alarm [Alarm text] and input restore text [Restore text] can be changed. The use of Latin alphabet is recommended.

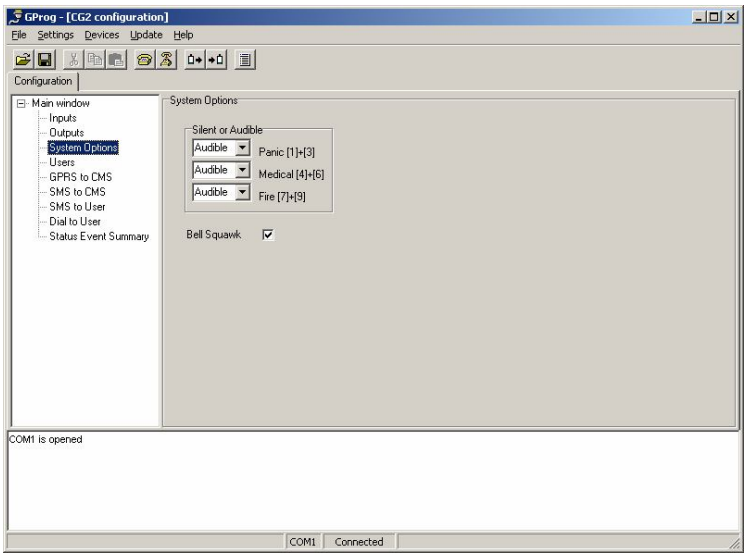
Entered or used default loop response time is displayed in column [Speed] and sensitive time to repeated alarms in column [Repeat].



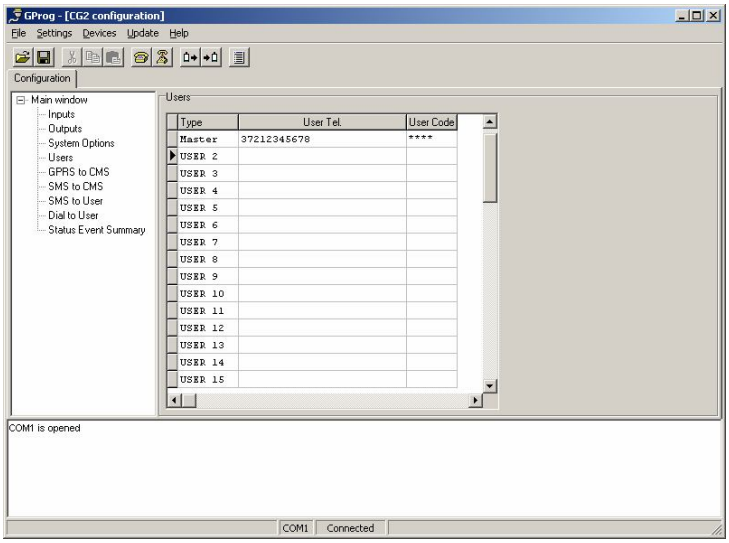
1.3. Type of output operation can be changed in the window [Outputs]. Double click on a cell [Out definition] and select a desired output operation type in a window has opened.



1.4. Operation type of *Paradox*® keypad panic buttons can be specified in a window [System options]: [Silent] or [Audible] and marked function Bell squawk to inform about security systems arming/disarming.



1.5. Telephone numbers of users with which the security system can be armed/disarmed can be entered in the window [Users]. Numbers should be entered in international format: country code (without +), operator code, a local number. SMS alarm messages about changes in security system's state are only sent to those users, who numbers were entered in the window [SMS to Users].



In this window new security system's control codes can be entered or changed [User code].

If user names, control codes and user telephone numbers were entered correctly, received messages will contain information which user has armed/disarmed security system. E.g.: if a user, which telephone number is +37212345678, uses the Master code (either default 1234, or changed), in the message will be shown that security system has armed by a user named Master.

2. Setting up GSM communicator's parameters

Parameters of communication channel, by which the messages will be transferred, are specified.

2.1. Central Monitoring Station parameters are entered in the window [GPRS to CMS]:

- Access Point Name [APN] of the network in which the module is working.
- Login name to APN [Login]. If GSM operator does not require username, leave it blank.
- Login password to APN [Password]. If GSM operator does not require password, leave it blank.
- [Number of GPRS connections requests].
- Remote ports of GPRS/IP receiver [Remote Port].
- IP addresses of GPRS/IP receiver [Remote IP].
- Message Transport Protocol [Transport Protocol].
- Periodicity of PING signal sending [PING interval].
- Message encrypting protocol [Data Protocol].
- Message encrypting password [Data crypting password].*

When both IP addresses, ports are entered and the near-by field [GPRS to next] is checked, the message will be sent to that address, to which the last message was sent. If sending to the first address has failed, sending to the second address will be attempted. If the attempt is successful, all future messages will be sent to that address.

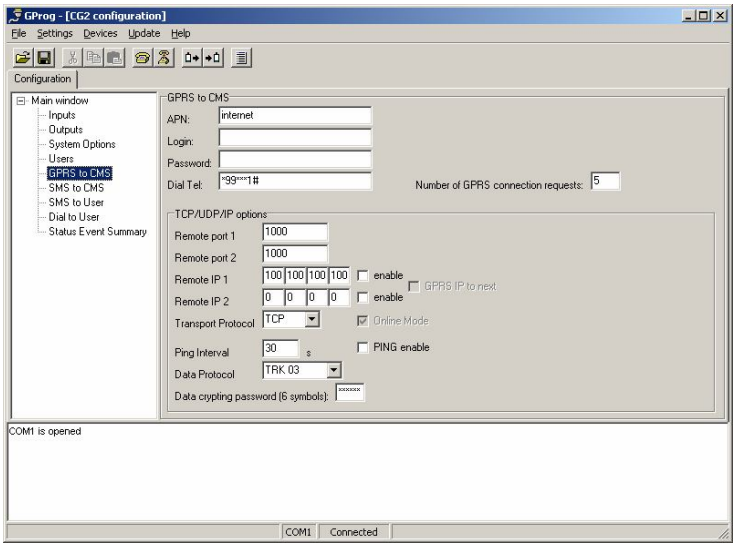
If protocol TRK 01 is checked, encrypted messages will be sent. When message is transmitted, security module disconnects from GPRS network and switches to stand-by mode. Messages can be received by a IP receiver AGSR.

If protocol TRK 03 is checked, encrypted messages will be sent. GPRS connection with a receiver is constantly tested, connection sessions are not canceled, PING control signals are transmitted. PING signals are sent in desired intervals or they can be disabled. Messages can be received by a IP receiver AGSR.

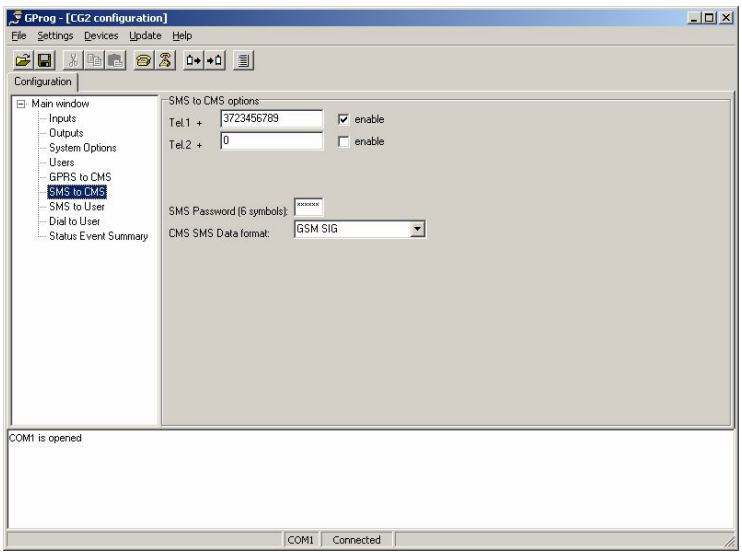
If protocol TRK 04 is checked, sent messages will not be encrypted. GPRS connection with a receiver is constantly tested, connection sessions are not canceled, PING control signals are

* *Message encrypting password entered to the security module has to be the same as password, entered to GPRS/IP receiver.*

transmitted. PING signals are sent in desired intervals or they can be disabled. Messages can be received by any IP receiver, which is capable of receiving and reading of data in TCP/IP protocol.



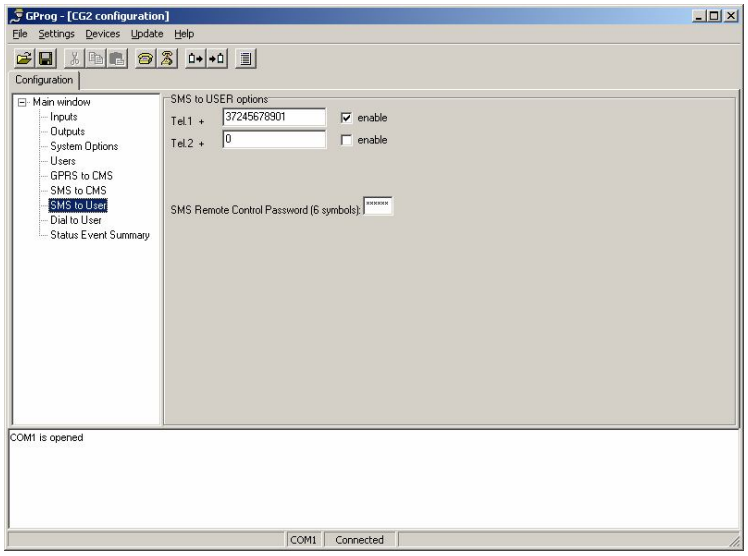
2.2. In window [SMS to CMS] Central Monitoring Station's GSM numbers are entered. Numbers should be entered in international format: country code (without +), operator code, a local number. Their operation is enabled by checking the box [Enable]. When both numbers are entered and checked, messages will be sent to both numbers. Then a six-digit password should be entered and Data format specified.*



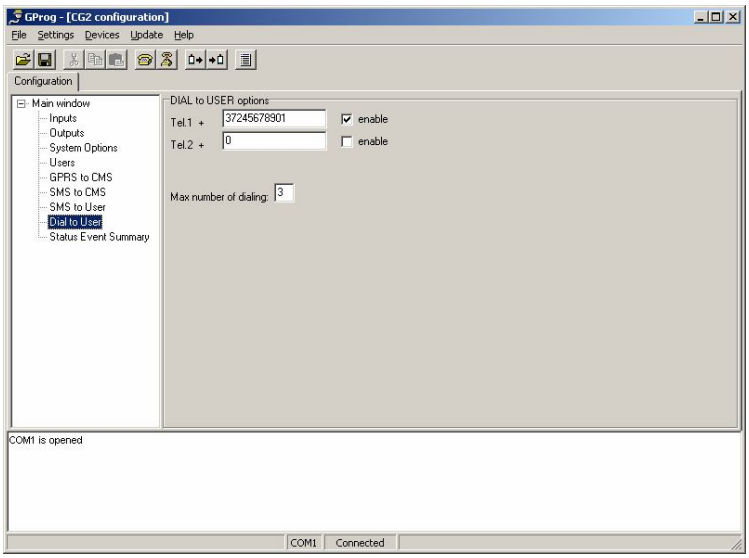
2.3. In window [SMS to User] numbers of Users' mobile phones are entered, to which SMS messages will be sent. Numbers should be entered in international format: country code (without +), operator code, a local number. Their operation is enabled by checking the box [Enable]. A password for remote configure the security module, should be entered.

---

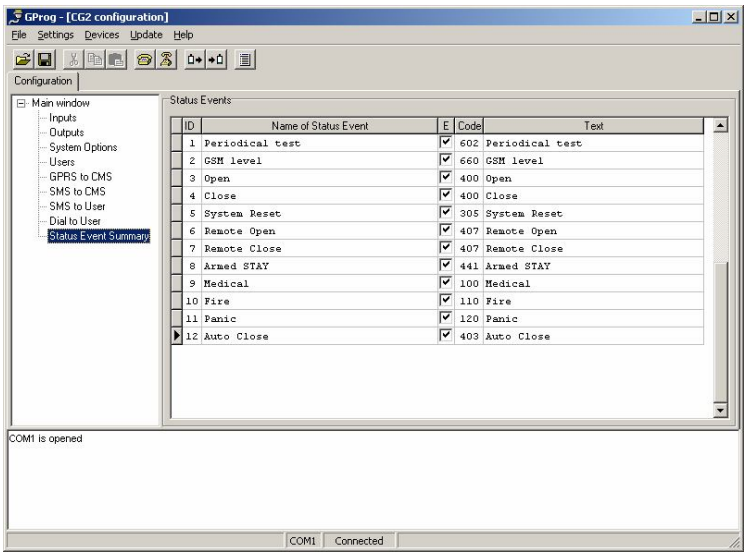
* *Message encrypting password entered to the security module has to be a same as password, entered to GPRS/IP receiver.*



2.4 In window [Dial to Users] such Users' mobile phone numbers are entered, which will be informed with free of charge calls about the sending of SMS message. Numbers should be entered in international format: country code (without +), operator code and a local number. Their operation is enabled by checking the [Enable] field. A desired number of repeating calls should be selected.



2.5 In window [Status Events Summary] can be checked, which systemic control module's messages should be sent, what their event codes [Code] are, or new SMS texts [Text] for these messages can be created.



3 Saving of parameters

Established security module's parameters are saved into the device's memory by pressing an icon [Send config]. Note [Configuration is sent] shows that saving was successful.

Configuring by mobile phone

All operational parameters can be changed only with GProg program. When programming a module SMS messages in such structure are sent:

PSW[password]space[command code]space[command content]

Several examples:

Changing of password*

PSW123456_98_654321

98	command to change password,
654321	new password (six digits).

Entering user's telephone number, with which will be possible to arm/disarm security system.

PSW654321_03_37212345678#

03	command to enter user's number,
37212345678	International telephone number (without +, up to 16 digits),
"#"	end symbol of the telephone number (required in the text).

Entering telephone number for receiving SMS messages (E.g. of the 1st user).

PSW654321_04_37245678901#

04	command to enter telephone number for receiving SMS messages,
37245678901	International telephone number (without +, up to 16 digits),
"#"	end symbol of the telephone number (required in the text).

Activating function of SMS transmission to 1st user.

PSW654321_09_00001000

09	command to turn GSM communicator ON,
00001000	command "Send to whom" (send only through the 5th channel).

Other command and inquiry examples:

PSW123456_97_3	Inquiry about input status,
PSW123456_97_4	Inquiry about security system, input and power supply status,

* *If the primary (default) password is not changed, module's user list can be manipulated. This means, that one can enter his telephone number to control the security system without an assent from the owner.*

PSW123456_50_4 Control of 4th output: output state is switched to opposite,
PSW123456_54_0 Control of 4th output: output state is switched to [0],
PSW123456_54_1 Control of 4th output: output state is switched to [1].

Commands in SMS message can be grouped: it is possible to change several parameters and to make an inquiry with one message.

PSW123456_98_654321_03_37212345678#_04_37245678901#_03_37234567890#_05_37232154321#_09_00001100

SMS commands list

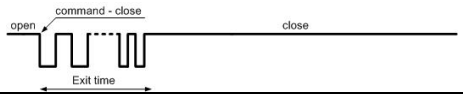
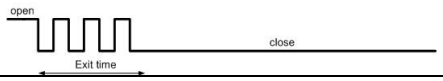
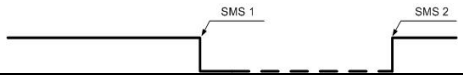
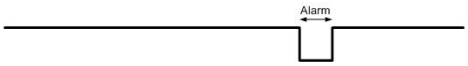
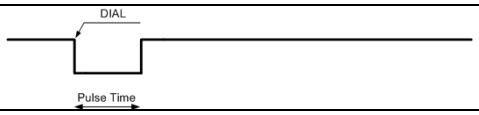
PSW[password]space[command code]space[command content]

Initial command and **password**	**Command code**	**Command content** (telephone number, PGM etc)	Command description
PSW + password (default 123456) **(uppercase)**	01		Delete all numbers from phonebook.
	02	1234567890#	Delete phone number written in *Command content* from the phonebook.
	03	12345678909#	Add new phone number written in *Command content* to the phonebook.
	04	12345678901#	Enter phone number of the 1st user to whom SMS report will be sent.
	05	12345678902#	Enter phone number of the 2nd user to whom SMS report will be sent.
	06	12345678901#	Enter phone number of the 1st user to whom a short call will be given.
	07	12345678901#	Enter phone number of the 2nd user to whom a short call will be given.
	09	00001111	8-digit sequence is entered to specify transmission channels (1-send, 0-forbidden). 1st channel – SMS1 to CMS, 2nd channel – SMS2 to CMS, 3rd channel – IP1 to CMS, 4th channel – IP2 to CMS, 5th channel – SMS to user1, 6th channel – SMS to user2, 7th channel – DIAL to user1, 8th channel – DIAL to user2.
	10	100.100.11.100space1000	Enter 1st IP address and port of receiver
	11	200.200.22.200space2000	Enter 2nd IP address and port of receiver
	50	1 6	Change state of selected PGM output to the opposite.
	51	1 or 0	Change state of the 1st output as specified in the message.
	52	1 or 0	Change state of the 2nd output as specified in the message.
	53	1 or 0	Change state of the 3rd output as specified in the message.
	54	1 or 0	Change state of the 4th output as specified in the message.
	55	1 or 0	Change state of the 5th output as specified in the message.
	56	1 or 0	Change state of the 6th output as specified in the message.
	97	3 / 4 / 5 /	Inquiry about operation of the module 3 - inquiry about output state; 4 - inquiry about general state, inputs and electrical supply; 5- inquiry about GSM signal level and IMEI.
	98	xxxxxx	Change the password.

Numbers should be entered using format: country code (without +) operator code, a local number.

Annex A

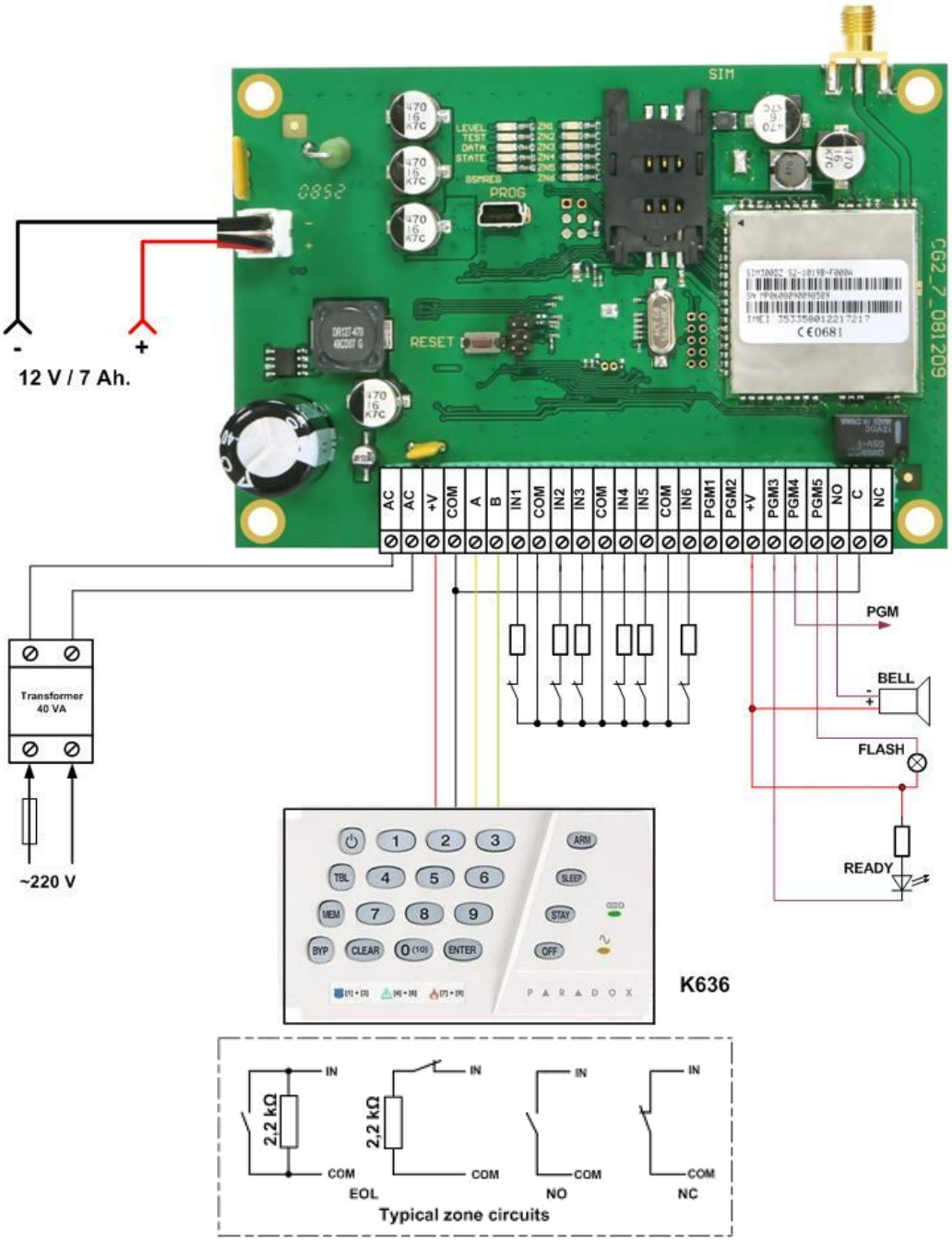
Operation of programmable outputs

OUTPUT	APPLICATION	OPERATION
PGM1 ***BUZZER****	Intended for connecting a low-power sound device. Signal is generated at the moment of entry/exit.	
PGM2 ***STATE****	Intended for connecting a light device. Signal is generated during the time to leave the premises.	
PGM3 ***READY****	Intended for connecting a light device. Signal is generated when all zones are ready.	
PGM4 ***SMS****	Output is controlled by SMS messages	
PGM5 ***FLASH****	Intended for connecting a light device. Signal is generated when security system has been alarmed.	
PGM6 ***BELL****	Intended for connecting light device. Signal is generated when security system has been alarmed.	
PGM ***DIAL***	Output is controlled by free of charge call.	

**default settings*

Annex B

Wiring diagrams of the security module CG2



Wiring diagram for connecting the module CG2 when *Paradox*® keypad K636 is used.

Annex C

Table of default parameters

		Meaning/ function	Description
Inputs (zones)	1	**Delay**, EOL, Can be bypassed	Entry/exit zone. Zone can be disturbed during the time of entry/exit.
	2	**Interior**, EOL, Can be bypassed	Interior zone. Zone can be disturbed during the time of entry/exit.
	3	**Instant**, EOL, Can be bypassed	Instant zone. When disturbed alarms instantly.
	4	**24 hours**, EOL Can be bypassed	Continuous operating zone. When disturbed alarms instantly.
	5	**Fire**, EOL Cannot be bypassed	Continuous operating zone. Used to connect fire sensors. When disturbed alarms instantly.
	6	**ON/OFF**, NC Cannot be bypassed	Control zone. Turns security system ON/OFF.
	7	**Silent**, NC Cannot be bypassed	Silent zone. Controls alternating current power supply.
	8	**Silent**, NC Cannot be bypassed	Silent zone. Controls back-up power supply from battery.
Outputs (PGM)	1	**Buzzer**	Used to connect a sound device. Signal is generated during the time of entry/exit.
	2	**State**	Used to connect a light indicator. Signal is generated during the time of entry/exit.
	3	**Ready**	Used to connect a light indicator. Signal is generated when all security zones are ready.
	4	**SMS**	Used to connect other devices in order to control them sending SMS.
	5	**Flash**	Used to connect a light device. Signal is generated when zone has been disturbed.
	6	**Bell**	Used to connect a sound device. Signal is generated when zone has been disturbed.
Entry delay time		15 s	Delay when a person can enter freely and disarm the security system.
Exit delay time		20 s	Delay when a person can leave freely the premises after arming the security system.
Duration of siren operation		120 s	Duration of siren operation, if a zone has been disturbed.
Periodicity of tests		1440 min.	Time period between test messages.
ON/OFF sound indication		Turned ON	When security system is armed, one short sound signal is generated. When is disarmed - two short signals.
Auto-ARM function		Inactive	Security system arms automatically, if during the time of exit no zones were disturbed.
GSM communicator		Is not activated	For transmitting messages.

Annex D

Control of security system using *Paradox*® keypad K636

To arm the security system

Enter the 4-digit control code. The system starts calculating exit delay, during which indicator [ARM] is flashing. When security system is armed, indicator [ARM] is shining.
If *Bell Squawk* function is turned ON, siren will squawk once upon arming.
Note! If zones are disturbed, security system will not arm.

To arm the security system in STAY mode using a [STAY] button of keypad

Press keypad button [STAY] and enter the 4-digit control code. Light indicator [ARM] will start flashing and [STAY] – shining. All zones change their operation mode. Security zones working in STAY mode will be disconnected. Entry zone *Delay* will start working as instantaneous operation zone. Like so entry to premises is impossible without security system alarm.

To arm the security system in STAY mode using the way of not disturbed Delay zone

Enter the 4-digit control code. If during the exit time ***Delay*** zone will be not disturbed, STAY mode will arm. During exit delay indicator ARM will flash. During STAY mode corresponding indicator will shine. When entering the secured premises, entry countdown will start.

To disarm the security system

Enter the 4-digit control code. When security system will be disarmed, OFF indicator will be shining.
If *Bell Squawk* function is turned ON, siren will squawk twice upon disarming.

To turn siren OFF

When ***24 hours*** zone is disturbed, to turn the siren off, enter the 4-digit control code. Arming mode of security system is not change.

Bypassing a zone

Press keypad button [BYP] and enter the 4-digit control code. Light indicator BYP will start blinking. Enter a 2-digit number of a zone You want to bypass (E.g. [0]+[2]). Press key [Enter]. Light indicator BYP will start shining. Security system now can be armed regardless of disturbance in the bypassed zone. Zone can be bypassed only for one arming.

Changing the Master control code

Master code can only be changed not deleted.
Press keypad button [⏻]. Enter the master code (default is 1234). Button [⏻] will start blinking and key “1” will start shining. Enter the 2-digit *Master* code rank number (E.g.: [0]+[1]). Enter a new 4-digit *Master* code (E.g. 4321). Repeat the entered 4-digit *Master* code (E.g. 4321). Press key [ENTER]. Enter *Master* code and press [CLEAR].

Entering a new control code

Press keypad button [⏻]. Enter the master code. Button [⏻] will start blinking and key [1] will start shining, meaning, *Master* code is entered. Other blinking buttons mean that corresponding User codes have already been entered. Enter a 2-digit User code rank number (E.g.: [0]+[2]). Enter a new 4-digit User code. Press key [ENTER].
Other User codes are entered in a similar way, only changing the User's rank number.
When finished entering codes press [CLEAR] button.

Deleting control codes

Enter the master code. Button [⏻] will start blinking. Other blinking buttons mean that corresponding User codes have already been entered. Enter a 2-digit User code rank number (E.g.: [0]+[2]), which You want to delete. Press [SLEEP] button. Sound signal will be heard and button showing corresponding User code will stop blinking.
Control code is deleted. When finished deleting codes press [CLEAR] button.

To quit programming mode press [CLEAR] button