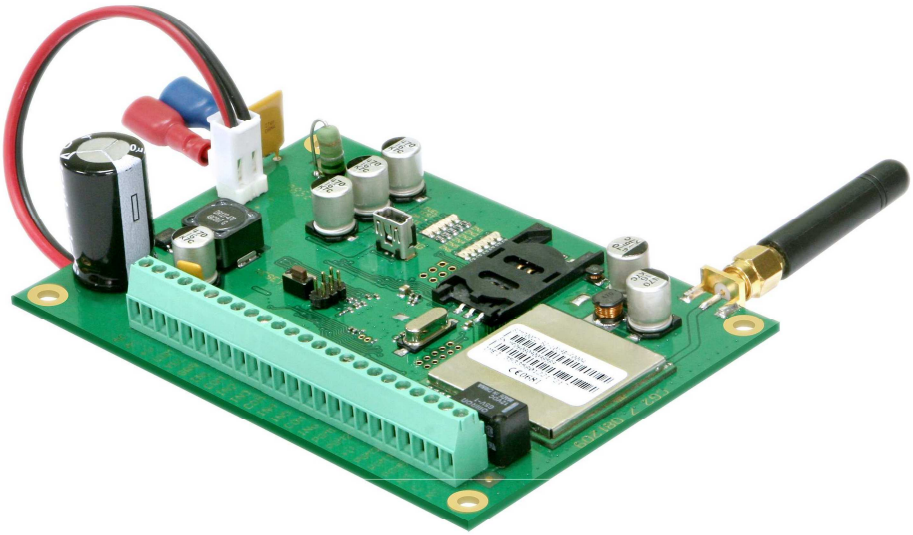


SECURITY MODULE *CG3*

(v.YYMMDD)

Installation manual

JSC “UAB “Trikdis”
Draugystės str. 17,
LT-51229 Kaunas
LITHUANIA
Email: info@trikdis.lt
Web: www.trikdis.lt

TABLE of CONTENTS

Safety requirements

Please read this manual carefully before using the security module *CG3*.
Security module *CG3* should be installed and maintained by qualified personnel, having specific knowledge regarding the functioning of GSM devices and safety requirements. The device must be disconnected from external power supply source before starting device installation.

Module *CG3* should be mounted in places with restricted access and in safe distance from any sensitive electronic equipment. The device is not resistant to mechanical effects, dampness and hazardous chemical environment.

Casings, transformers, batteries and programming devices must conform to LST EN60950 standard safety requirements.

Security module *CG3* is powered with 16-18 V voltage through a 2^{nd} class power transformer from a 50 Hz frequency alternating current power grid or from batteries with 12 V/4-7 Ah capacity. The amount of current used depends from the amount of power used by connected external devices.

An automatic bipolar overload cut-out must be installed in the electricity supply circuit to safeguard from a current overload in the power grid. Release contacts separation must be ≥ 3mm. Cut-out must be installed in a place well known to the personnel maintaining the module.

The device is disconnected from the power source:

- From alternating current source – by switching off the automatic cut-out;
- From direct current source (e.g. accumulator) – by unplugging the clamps.

Liability restrictions

- When buying the Device, the Buyer agrees that the Device is a part of a security system of premises, which sends messages about security system status. The Device, when installed, does not diminish the probability of burglary, fire, intrusion or other breach of premises.
- UAB “TRIKDIS” is not responsible for burglary, fire or any other breach of Buyer’s and/or User’s premises and is not liable for any direct or indirect damages incurred thereof.
- When buying the Device, the Buyer agrees that the Device supplied by UAB “TRIKDIS” fully meets his requirements for intended use.
- UAB “TRIKIDIS” provides no guarantees that the Device shall function as declared if the Device is installed and used not according to its original purpose, user manual and relevant electronic and technical conditions.
- UAB “TRIKDIS” is in no way associated with GSM/GPRS/Internet service providers (operators), thus UAB “TRIKDIS” is in no way responsible for any defects in Device operation if they have occurred because of the loss of GSM/GPRS/Internet connection, or because of other defects in the service provider network.
- UAB “TRIKDIS” has no control and is not responsible for the prices and marketing of network services provided by the GSM/GPRS/Internet service providers.
- UAB „TRIKDIS” is not responsible if GSM/GPRS/Internet services are not provided to the Buyer and/or User of the Device or were cancelled and any direct or indirect damages were incurred thereof.
- UAB „TRIKDIS” is not responsible for any direct or indirect damages incurred by the Buyer and/or User of the Device due to loss of electricity.
- UAB „TRIKDIS” is not liable if Device firmware versions were not updated by the Buyer and/or the User on time.
- User manual of the Device can contain technical inaccuracies, grammatical or typographical errors. UAB “TRIKDIS” reserves the right to correct, update and/or change information in the installation manual.

Security module *CG3*

Module *CG3* is a security control panel with an integrated GSM modem, which can transmit messages about sensed events through GPRS connection and in SMS messages. Messages contain of codes of protocol Contact ID and/or text.
Features:

- The main board has six inputs, which number can be expanded up to 32. Up to 16 various expansion modules can be connected.
- Inputs can be partitioned to 8 independent groups;
- Every input can be described as an On/Off, Delay, Interior, Interior STAY, Instant, Instant STAY, 24 hours, Fire or Silent zone;
- The security system can be armed/disarmed with a code keypad, telephone call or by breaking the circuit of input ON/OFF;
- Possible arming modes are ARM/STAY/OFF;
- Automatic arming of the system (AutoARM), sound signal indicating the security system arming/disarming (Bell Squawk) and temporary bypass a zone (BYPASS) functions are presented;
- Six programmable (PGM) outputs. These operating options can be assigned to every output: Buzzer, State, Read, Flash, Bell, AC OK, Battery OK, Remote Control by SMS or Remote Control by DIAL. When Remote Control by SMS or Remote Control by DIAL operating mode is assigned, output state can be controlled remotely with an SMS message or with a telephone call;
- Module operating parameters can be set with a computer program CGconfig or remotely with SMS messages.

Description of module features

1. The security system can be armed (arming mode ***ARM***) or disarmed (mode ***OFF***) by these ways:

- Entering control (User) code with Paradox keypad MG32LED or K636, MG10LEDV, MG10LED;
- Telephone call. Up to 40 telephone numbers can be entered into device memory, with which the security system can be controlled remotely by calling;
- By breaking the external circuit of the input ***ON/OFF*** with a device having a switched OC type output (e.g., code switch).

2. When the arming mode ***STAY*** is turned on (arming mode which allows freely roaming inside premises while the perimeter is fully armed), the control panel will not trigger an alarm if input ***Interior STAY*** and ***Instant STAY*** circuits are broken. Ways of turning on the mode ***STAY***:

- By pressing the keypad button [*STAY*] and entering a User code. When the security system is armed in this way, the control panel will immediately trigger an alarm if input ***Delay*** circuit is broken;
- By entering a User code without breaking the input ***Delay*** circuit. When the security system is armed in this way, the triggering an alarm will be delayed after breaking circuit of the input ***Delay***.

3. The module has a function for automatic arming of the system ***AutoARM***. If the security system is disarmed with a phone call and during the time for entry into the premises (***Entry Delay***) none of the secured zones are disturbed, the module will automatically arms to previous arming mode.
4. The security module has a function for sound indication of the security system arming/disarming ***Bell Squawk***. When the security system is armed, one short siren signal is created and when it is disarmed – two short siren signals.
5. The zones can be temporary bypassed for one security system arming period (***BYPASS*** function). This function is used when arming of the security system with disturbed zones is necessary. This function can be activated only with a keypad by bypassing every zone separately.
6. External circuit connection mode (NC, NO or EOL=2,2 kΩ) can be chosen to every input and can be set one of these 9 options defined how control panel should react to the break of the input external circuit:

ON/OFF Security system can be armed and disarmed by breaking the input circuit. The security system will arm after the specified duration of time (***Exit Delay***), during which one can freely leave the secured premises;

Delay When the security system is armed, during the time period for leaving the premises (***Exit Delay***), break of input circuits is allowed. If after this duration of time the circuits remain disturbed, output ***Bell*** and ***Flash*** signals will be created and messages will be sent. If a circuit is broken while the security system is armed, this will start the counting of time for entry into the premises (***Entry Delay***). The security system must be disarmed during this time period, otherwise output ***Bell*** and ***Flash*** signals will be created and messages will be sent;

Interior If an input circuit is broken while the security system is armed, output ***Bell*** and ***Flash*** signals will be immediately created and messages will be sent. Break of input circuits is allowed during the time periods for entering or leaving the premises (***Entry Delay*** and ***Exit Delay***);

Interior STAY Operates similarly to ***Interior***, however when the arming mode ***STAY*** is turned on, the control panel will not react to the break in input circuits.

Instant If input circuit are broken while the security system is armed, output ***Bell*** and ***Flash*** signals will be immediately created and messages will be sent;

Instant STAY Operates similarly to ***Instant***, however when the arming mode ***STAY*** is turned on, the control panel will not react to the break in input circuits;

24 hours If an input circuit is broken, output ***Bell*** and ***Flash*** signals are immediately created and messages are sent;

Fire If an input circuit is broken, output ***Bell*** and ***Flash*** fire signals are immediately created and messages are sent;

Silent If an input circuit is broken, messages are immediately sent, however ***Bell*** and ***Flash*** signals are not created.

7. Every programmable (*PGM*) output can be set to operate in one of these modes:

Buzzer For connecting a sound signalling device. During the time periods for entering and leaving the premises (***Entry Delay*** and ***Exit Delay***) cause an pulse sound signal and security system disturbing – continuous;

State For connecting a light-emitting device. Security system being armed causes a continuous light signal and during the time periods for entering and leaving the premises (***Entry Delay*** and ***Exit Delay***) – pulse;

Ready For connecting light-emitting device. Input external circuits being on the right position causes continuous light signal;

Flash For connecting a light-emitting signalling device. Security system being armed causes continuous light signal and security system disturbing – pulse;

Bell For connecting sound-emitting signalling device (e.g. a siren). Security system disturbing causes either a continuous or pulse sound signal;

Remote Control by SMS Output which state can be controlled remotely. It is applied for controlling electro-technic devices with an SMS message;

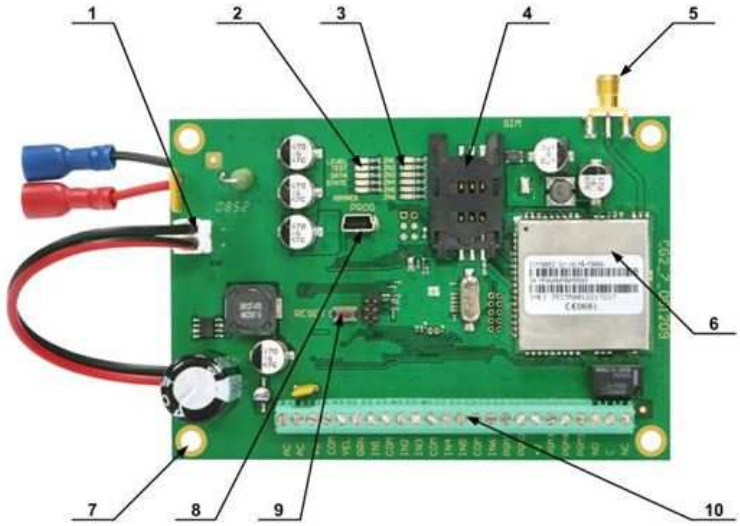
Remote Control by DIAL Output which state can be controlled remotely. It is applied for controlling electro-technic devices with a telephone call;

AC OK For connecting a signalling device informing about the status of power supply from the AC main;

Battery OK For connecting a signalling device informing about the status of power supply from the accumulator;

8. The security module can send periodic connection control messages ***Test*** according to the set duration of time and period.

Module components



1. Port for connecting the accumulator;
2. LEDs for presenting connecting to the GSM network status;
3. LEDs for presenting input states,
4. SIM card holder,
5. GSM antenna connector;
6. GSM modem;
7. Holes for fastening the module;
8. USB socket for configuring the module;
9. Button RESET;
10. Terminal block.

Terminal block description

Contact		*Description*
AC, AC		Clamps for connecting alternating voltage (16 VAC)
+V		Clamps for powering the keypad, signalling-devices and sensors with +13,6 V voltage
COM		Common clamp for connecting the keypad, signalling-devices and sensors
YEL		Clamp for connecting the keypad circuit YEL
GRN		Clamp for connecting the keypad circuit GRN
IN1, ..., IN6		Input clamps (by default EOL=2,2 kΩ)
PGM1, ..., PGM5		Output clamps (OC type)
NO	PGM6	Relay NO clamp (normally open contact)
C		Relay C clamp (common contact)
NC		Relay NC clamp (normally closed contact)

Light indication

LED	*Operation*	*Description*
ZN1 ... ZN6 shows input (zone) status	Red ON	Input circuit is broken
	OFF	Input circuit is on the right position
LEVEL shows GSM network strength	Red flashing	Number of red flashes presents the strength of GSM connection in conventional units
TEST is for presenting module operation	Green flashing	Power supply is on, module operates properly
DATA is for presenting message transfer	Red ON	Module memory contains of unsent messages
STATE is for presenting GSM modem operation	Yellow flashing	GSM modem is functioning
GSMREG shows status of registration in the GSM network	Yellow flashing	Module registration in GSM network is in progress
	Yellow ON	Module is registered in the GSM network
	Yellow flashing rapidly	SIM card PIN code is entered incorrectly

Technical parameters

Power supply voltage	Alternating 16–18 V
Used current	Up to 2 A
Backup power supply	12 V accumulator with 4-7 Ah capacity (charging current for the accumulator – 0.6 A)
Power supply for connected security devices	Direct 13.6 V voltage from [+V] and [COM] contacts, current up to 1.1 A
GSM modem frequencies	900/1800/1900 MHz
Messages about troubles in power supply are sent when:	Alternating power supply is lost/restored; Voltage of the accumulator has dropped to 11,5 V, Voltage of the accumulator has restores to 12,6 V.
Inputs	Six inputs in the main board, input circuit type can be set to NC, NO or EOL=2,2 kΩ
	Expandable to up to 32 inputs with input expansion modules, input circuit type can be set to NC, NO or EOL=2,2 kΩ
Various expansion modules	Up to 16, including keypads
Outputs	Three, open collector type, 30 V / 50 mA
	Two, open collector type, 30 V / 1 A
	Relay contacts, commutating voltage up to 30 V and 1 A current
Control codes	Up to 40
Time period for entering or leaving the premises (***Entry Delay*** and ***Exit Delay***)	0-255 seconds
Time period for siren operation	0–9999 seconds
Connection protocols	TCP/IP, UDP/IP, SMS, CSD
Messages sent to the monitoring station	With Contact ID protocol codes, up to 2 IP addresses
SMS messages to users	Text up to 5 mobile phones
Calls to users	Up to 2 mobile phones, according to selected event types
Operating environment	From -10 °C to 50 °C, when relative air humidity is 80 % at +20 °C
Dimensions	120 x 80 x 16 mm

Package content

Security module *CG3*	1 pc.
Straight GSM antenna	1 pc.
Wire for connecting the accumulator	1 pc.
Resistors 2,2 kΩ	6 pcs.
Fastening bushings	4 pcs.
Installation manual	1 pc.

Installation steps

1. Set module operating parameters;
2. Install the module in a metal casing with a transformer. Fasten the module with screws or with plastic bushings. Place the batteries inside the casing;
3. Connect the sensors and signalling devices to module clamps. Possible connection scheme is provided in Annex **B**;
4. Screw on the GSM antenna to the antenna connection socket. Insert a SIM card into the SIM card holder;
5. Connect the power supply from the alternating current source, then connect the power supply from the accumulator;
6. Check security system operation and sending of the messages.

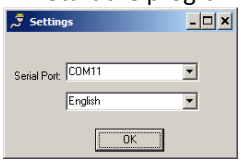
Setting up operating parameters with a computer

Module *CG3* operating parameters are set with a program *CGconfig*. The program can be found in website www.trikdis.lt.

1. Connect the module *CG3* with a computer USB port using a USB cable. Computer must have USB driver installed.

USB driver installation: download the driver installation file *CDM_2.04_.06.01.exe* from the website www.trikdis.lt, save in a computer and double-click it with a mouse. USB driver will be installed automatically. The installation process will end when the progress window closes.

2. Start the program *CGconfig;*



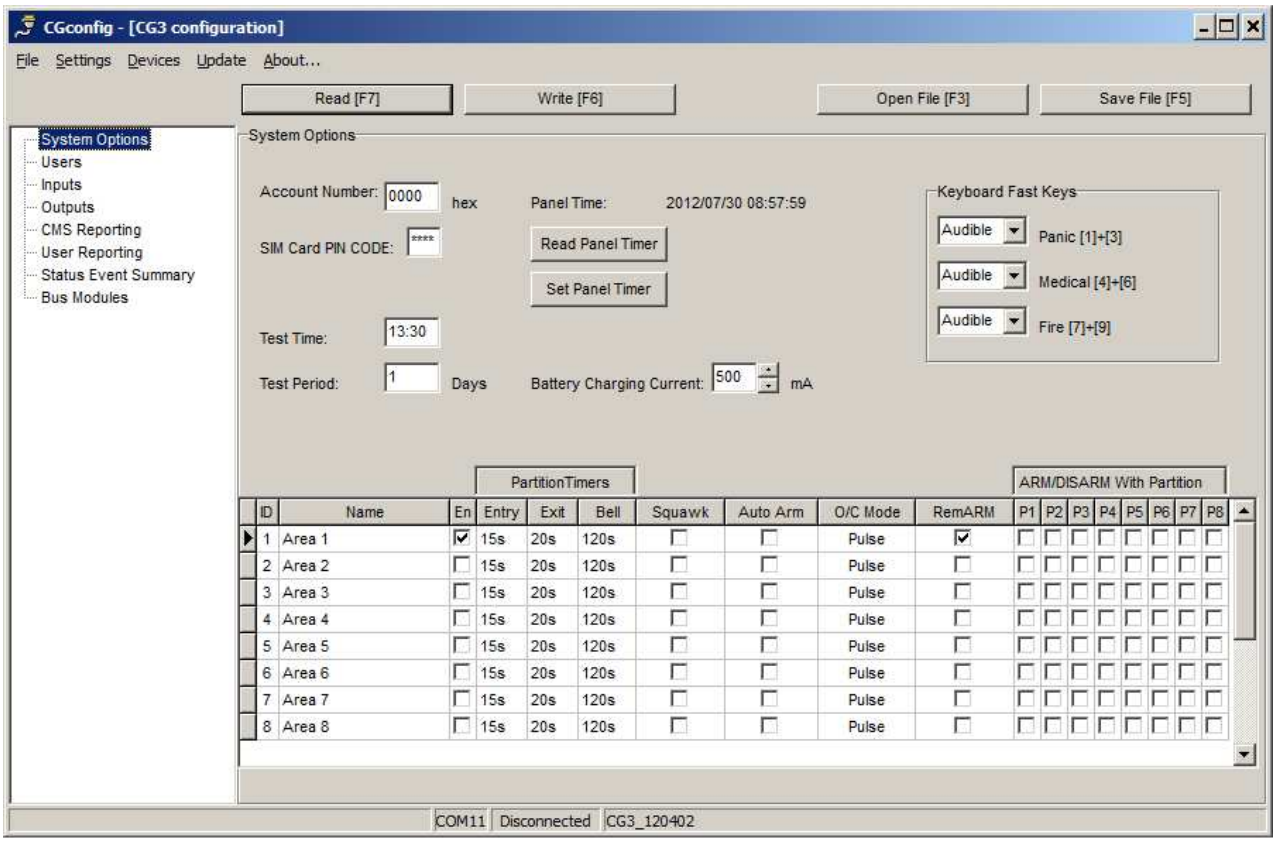
3. Choose the command ***Settings*** in the menu bar and select in the ***Serial port*** list the port to which the module is connected. Press the button ***Ok***.

Note: specific port appears when the module is connected.

4. Choose the command ***Devices*** in the menu bar and select ***CG3***;
5. Press the button ***Read [F7]*** for the program to read the operating parameters already set in the module. Information about the connected module should be displayed in the status bar of the program *CGconfig;*

Setting control panel parameters

Choose the directory ***Control panel*** and set the necessary parameters:



Account number	Section for entering a 4-digit code for identifying the module. This number will be included in SMS messages sent to the user;
SIM card PIN code	Section for entering the SIM card PIN code. If PIN code request is disabled, leave this section blank;
Test	The module will send connection control messages according to the time set in this section;
Period	Section for entering a time period for sending test messages;
Read time	Press this button to show the time of the module internal clock;
Set time	Press this button to set the module internal clock according to the computer time;
Keypad buttons	If the option ***Audible*** is selected in the list, pressing the ***Paradox*** keypad keys for causing emergency alarm message will be followed by a keypad sound signal. If the option ***Silent*** is selected, the message will be sent without the keypad sound signal.

Security system can be divided into several independently secured areas, and every input in the *CG3* main board or in expansion module can be defined to control the status of any zone in any area. Input parameters can be set in the directory ***Inputs***. In the table in directory ***Control panel*** set the following parameters for areas:

No. Area number;

Area Name of an area;

S Choose by selecting the checkboxes to which areas the security system will be divided;

Time intervals Desired duration of time can be set in the columns for free entering into and leaving area and for duration of siren operation when a zone is disturbed;

With sound Checkbox for activating the sound signal which follows security systems arming/disarming (***Bell Squawk***);

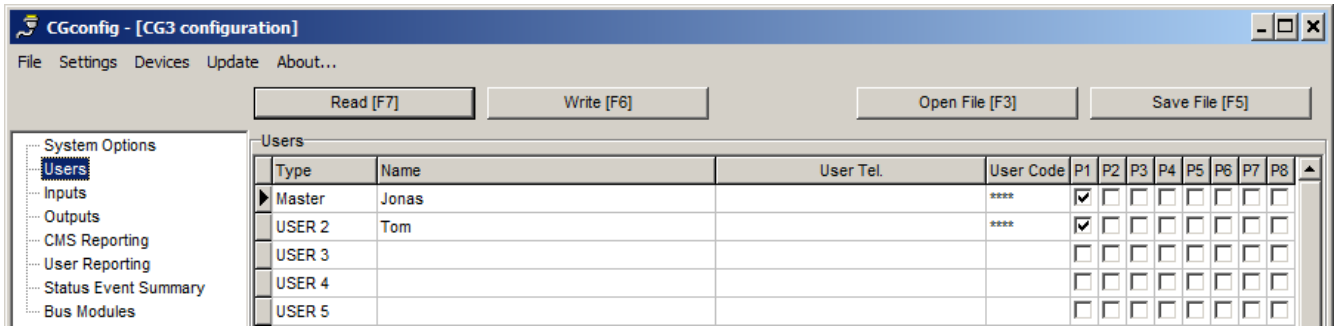
AutoARM Checkbox for activating the function for automatic arming of the security system;

Control Depending from the type of device (e.g., code switch) used to arm/disarm the security system, choose ***Pulse*** or ***Level*** type of input ***ON/OFF*** disturbance. If the security system is controlled by a telephone call, this section must be set to ***Pulse***.

Dist. ARM Selected areas can be controlled (armed/disarmed) remotely;

Common area control This table should be filled only then, when the security system is divided into several independently secured areas, and there is necessary that common area (A_m) would be armed/disarmed automatically when any area was armed/disarmed (e.g., if there is needed that protection for a corridor which is common to several independently secured offices would turn on/off when any of the offices is armed/disarmed). Protection for common area A_m will turn automatically on when the last area from areas selected in the table ***ARM/DISARM with partition*** is armed. Protection for common area A_m will turn automatically off when at least one area from areas selected in the above-mentioned table is disarmed.
Note: conditions for arming/disarming the common area are set by marking the boxes in row of common area A_m in the table ***ARM/DISARM with partition***.

Telephone numbers, names and user codes of the users who will be able to control the security system should be entered in the directory ***Users***.



User User title;

Name Section for entering true name of the user;

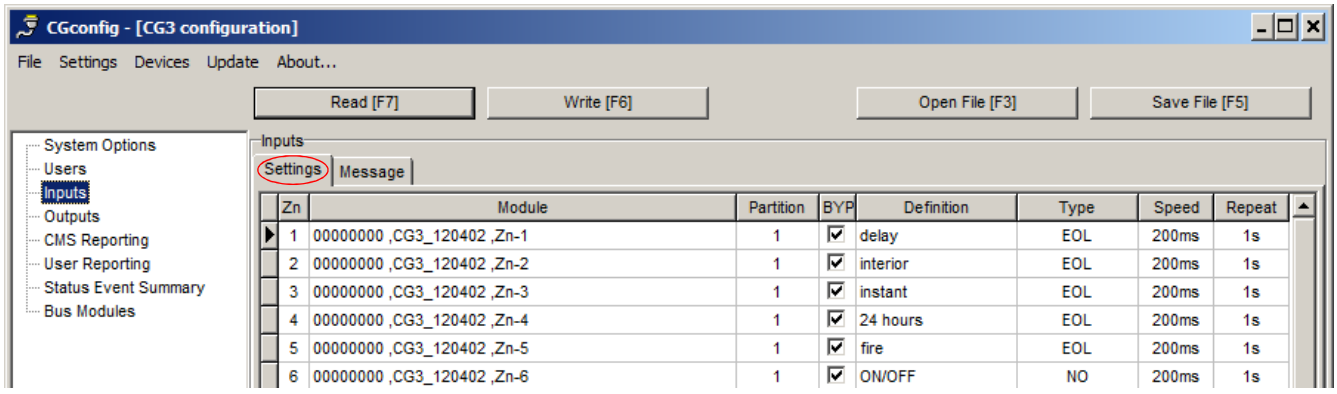
User telephone User will be able to arm/disarm the security system with a telephone which GSM number will be entered in this section. Telephone numbers must be entered with international country code, but without the "+" (plus) sign;

User code Section for entering a user code, with which the security system can be armed / disarmed by entering it into the keypad;

A1 ... A8 Sections for selecting areas, which the user will be able to control with his user code or telephone;

When this table is fully filled, the name of a user who has armed/disarmed the security system will be included in the SMS message text.

Directory ***Inputs*** (tab ***Settings***) is for setting input operating parameters. By double-clicking an input row with a mouse a window will open, intended for setting parameters of the necessary input.



Zn Number of a secured zone;

Zone name Any input from the main board of module CG3 or from expansion module in the drop-down list can be set to protect a desired zone;

Partition An area can be selected to which the zone will belong;

BYP It can be set by selecting the checkbox, that the protection of a secured zone could be temporary bypassed;

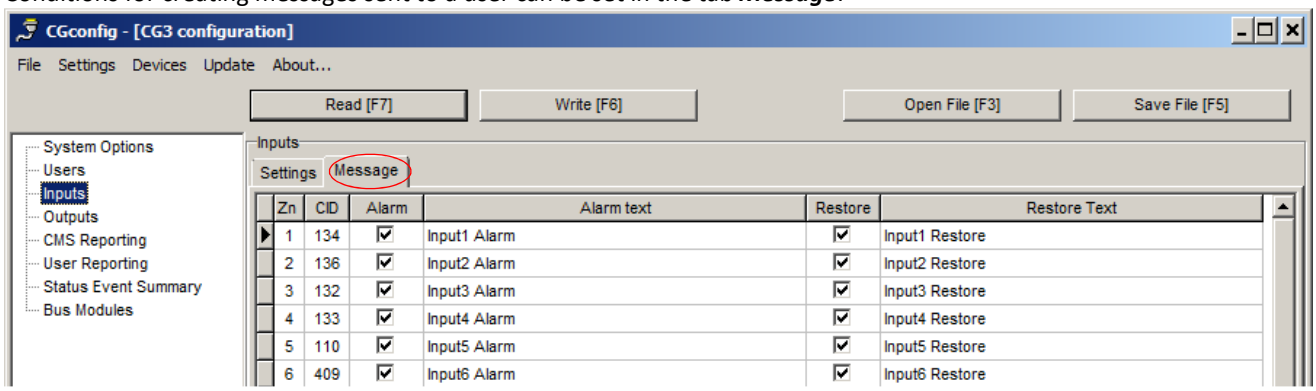
Definition Section for selecting a preferred control panel reaction to zone disturbance;

Type Section for selecting a preferred input external circuit type;

Speed The module will not react to disturbances in a protected zone if their duration will be shorter than set in this section;

After... The module will not react to disturbances in a protected zone if their recurrence period is shorter than set in this section;

Conditions for creating messages sent to a user can be set in the tab ***Message***:



Zn Running number of a secured zone;

CID When an event occurs written in this table in Contact ID format, an SMS message about the event will be sent to a user. We do not recommend changing ***CID*** codes;

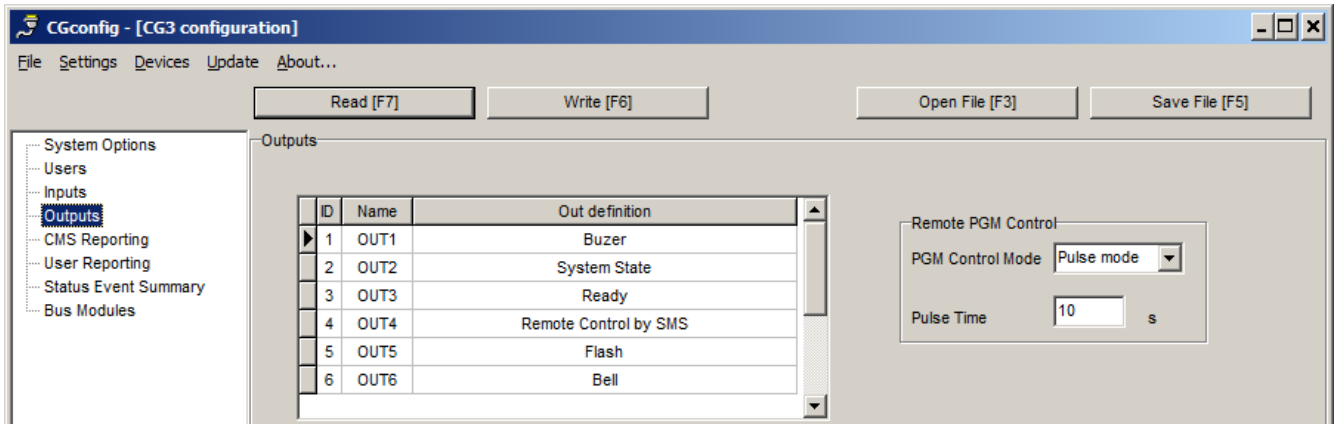
Event Enabling or disabling the SMS messages sending when zone disturbing event occurs;

Event SMS Text Here can be entered text which describes particular zone disturbing event. This text will be included in the SMS message to the User;

Restore Enabling or disabling the SMS messages sending when zone disturbances have been eliminated;

Restore SMS Text Here can be entered text which describes eliminating disturbances in particular zone. This text will be included in the SMS message to the User.

Directory ***Outputs*** is applied to set PGM output options.

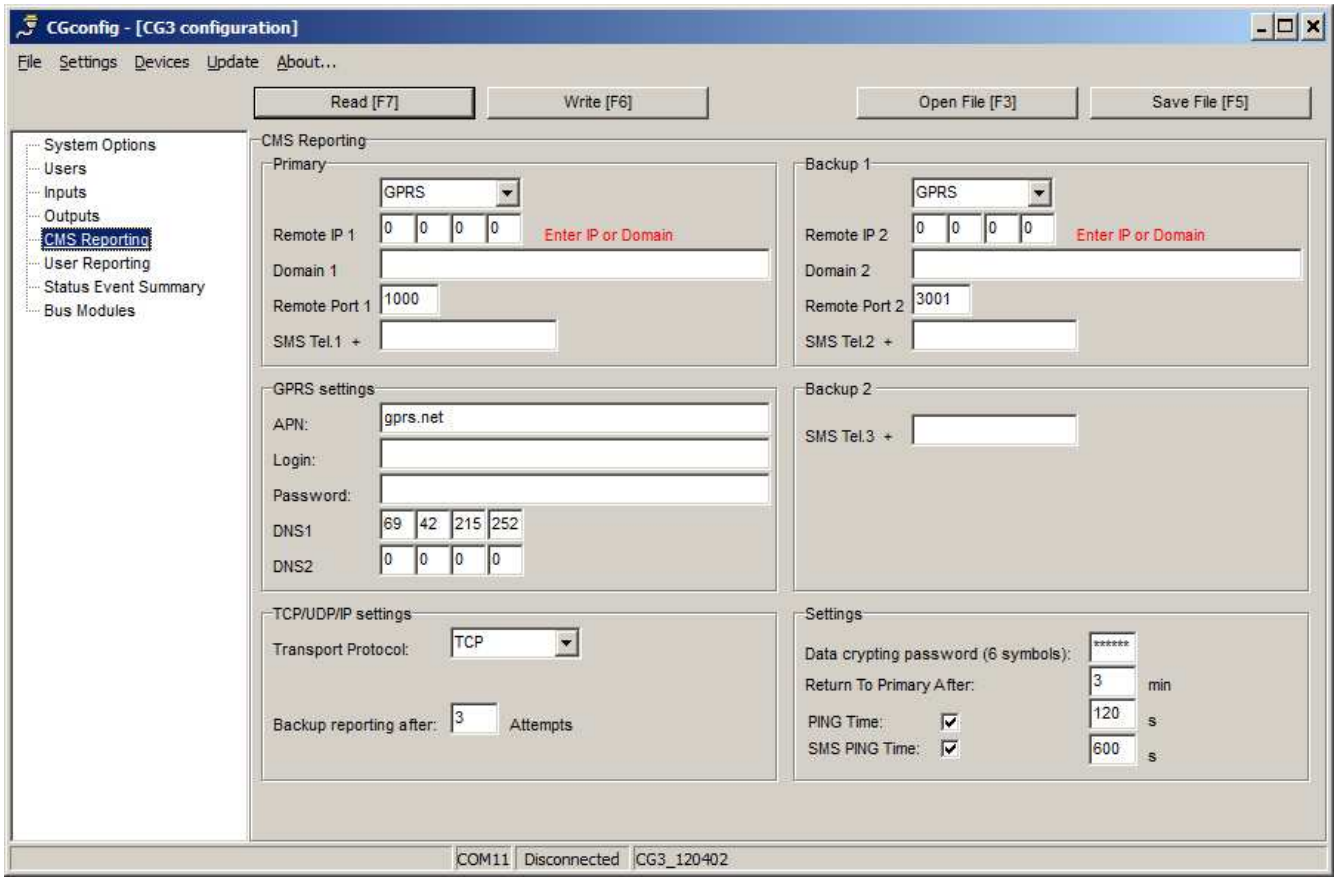


Out definition Drop-down list presents output operation options. Every output can be set to operate in particular mode;

Remote PGM control Area is applied to set how output with option ***Remote control with SMS*** or ***Remote control with DIAL*** should operate after receiving output switching command from an User. If ***Level mode*** is selected, when a control message is received, output status will change to the opposite. If ***Pulse mode*** is selected, output status will change to the opposite for the length of time set in section ***Pulse duration***.

Sending of messages to the monitoring and alarm receiving centre (MARC)

Enter parameters in the directory ***Reporting to CMS***, which are necessary for the module to operate in a GSM network and send messages to the monitoring station:



GPRS connection Area to enter parameters necessary for sending messages to the monitoring station through GPRS connection:

APN: Access point name for connecting to the GSM operator's network;

User: User name for connecting to the GSM network (Login);

Password: Password for connecting to the GSM network;

Dial Tel: Number for calling, when connecting to the GPRS network;

GSM network provider, from which you have received the SIM card, shall provide you with APN, user name, password and dialling number.

Remote IP 1 IP address of the monitoring station. In order to send to the entered IP address, select the checkbox ***enable***.

Remote Port 1 Port number of IP receiver at the monitoring station;

Transport Protocol TCP/IP or UDP message-transmitting protocol can be selected;

Data Protocol List for selecting an encryption protocol for transmitted messages;

PING interval Time period for sending *PING* signals can be set. To enable the sending of these signals select the checkbox ***PING enable***;

Number of GPRS connection requests If message transmission fails at first attempt, the number of attempts to transmit the message can be set;

To next IP If this checkbox is selected, the message will be transmitted to the second IP address if message transmission to the first IP address has failed;

Monitoring station administrator shall provide you with the IP addresses, port numbers, protocol, encryption key and other parameters necessary for connection with the monitoring station.

SMS to CMS Options Area is applied to enter parameters necessary for sending encrypted SMS messages to the monitoring station:

Tel.x + GSM telephone number of the monitoring station to which SMS messages will be sent. Enter the telephone number with international country code without the "+" (plus) sign. After entering the telephone number, select the checkbox ***enable***.

SMS data protocol Encryption protocol should be selected in the drop-down list;

CSD to SMS options Area to enter parameters necessary for sending encrypted messages to the monitoring station through CSD connection:

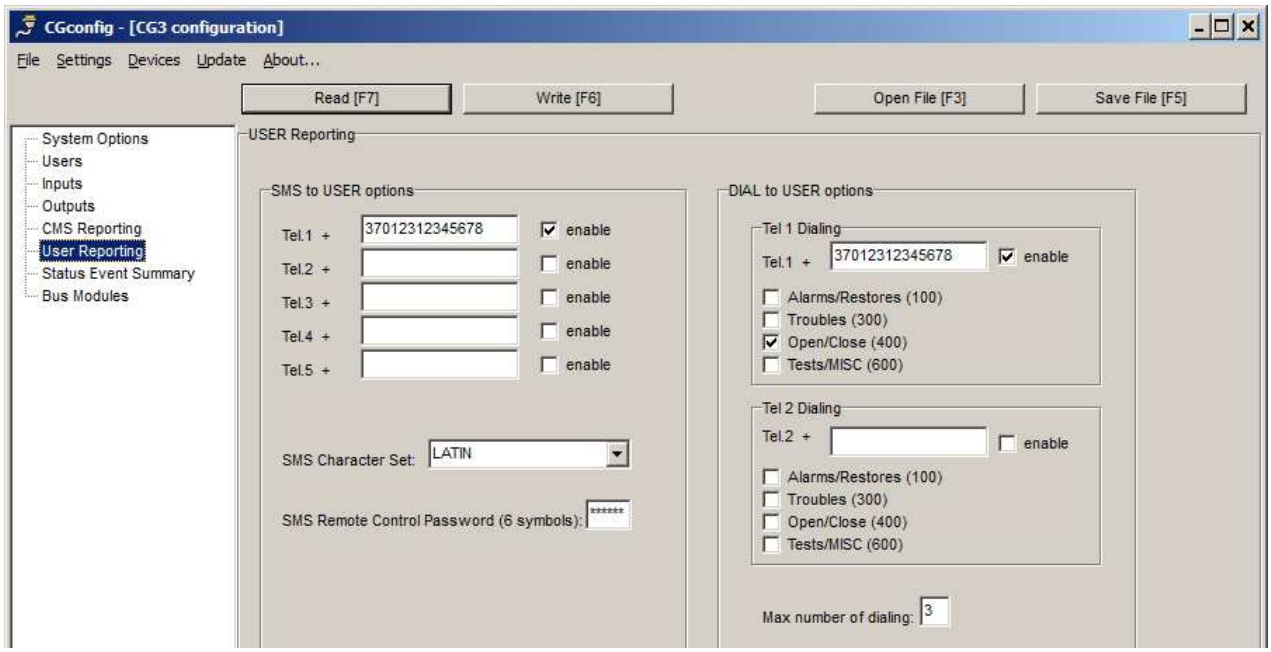
Tel. CSD GSM telephone number of the monitoring station to which messages will be sent through CSD connection. Enter the telephone number with international country code without the „+“ (plus) sign. After entering the telephone number, select the checkbox ***enable***.

Encryption key Encryption password for encrypting transmitted messages. The password must be the same as the decryption password entered in the server program *IPcom* at receiving site.

Monitoring station administrator shall provide you with the GSM number, protocol and encryption password.

Sending of messages to User

In the directory ***Reporting to User*** parameters necessary for sending messages to user should be entered:



SMS to USER options Area to enter parameters necessary for sending SMS messages to user:

Tel.x + GSM number of a user telephone to which SMS messages will be sent. The telephone number should be entered with international country code without the „+“ (plus) sign. After entering the telephone number, select the checkbox ***enable***.

SMS Character Set Desirable character encoding of SMS message text can be selected;

SMS control password Enter a six-digit password. It is used to control the module by sending SMS messages (remotely).

DIAL to USER options Area to enter parameters necessary to inform a user about the sending of SMS message addressed to him:

Tel.x + GSM number of a user telephone to which will be called. The telephone number should be entered with international country code without the “+“ (plus) sign. After entering the telephone number, select the checkbox ***enable***.

Alarms / Restorations, Troubles, Open / Close, Text/MISC By selecting the checkboxes it can be set, after which event will be followed by the dialling;

Max number of dialling The number of attempts to make a call to a User can be set.

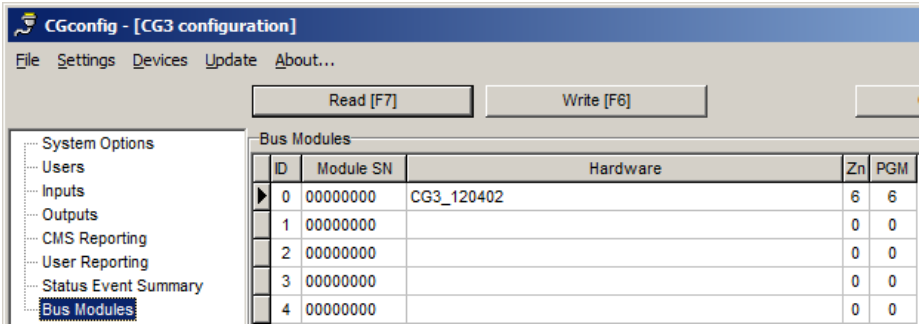
Event list

The directory ***Status event summary*** presents event list with their codes in Contact ID format. Upon event from the list occurs the module will send a message. SMS message text which describes an event can be modified. If you would like that a message would be sent informing about the event, select the checkbox ***E***.

Name	*CID code*	*SMS message text*	*Description*
Periodical test	602	Test	Periodic connection control signal
GSM Level	660	GSM level	GSM network strength
Open	400	Open	Security system armed
Close	400	Closed	Security system disarmed
System Reset	305	Reset	Module operation was reset
Remote Open	407	Remote open	Security system was armed remotely
Remote Close	407	Remote closed	Security system was disarmed remotely
Armed STAY	441	Armed STAY	Security system operates in STAY mode
Medical	100	Medical	Medical help call
Fire	110	Fire	Fire help call
Panic	120	Panic	Panic help call
Auto Close	403	Auto close	Security system has armed automatically (function “autoARM“)
Low Battery	302	Low battery	Battery voltage is lower than 11,5 V
Battery Restore	302	Battery restore	Battery voltage has restored to 12,6 V
AC failure	301	AC failure	No power supply from the power grid
AC Restore	301	AC restore	Power supply from the power grid has restored
Expansion Module Registered	333	MOD registered	No connection with an expansion module
New Module added	531	MOD added	New expansion module registered

Registering of expansion modules

Registered expansion modules can be viewed in the directory ***Expansion modules***.



No. Module line number in the system;

Module SN Module serial number;

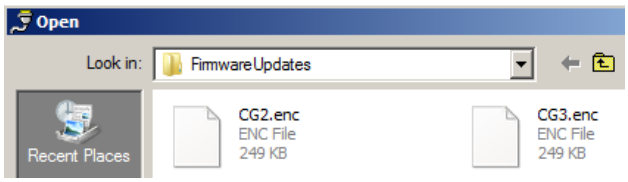
Hardware Name of the module;

ZN Number of inputs in the module;

PGM Number of outputs in the module.

Updating of module firmware

Module *CG3* firmware version can be updated or changed to other by selecting the command ***Update*** in the program menu bar.



Select a firmware program file of the device and press the button ***Open***.

Press the button ***Reset*** on the device mainboard.

When ***Updating*** progress bar is full, press the ***Reset*** button once more.

Remote module control with a mobile phone

Some of module parameters can be changed with a mobile phone (all module *CG3* parameters can be changed only with program *CGconfig*). An SMS message with structure presented below should be sent to change module parameters remotely:

PSW[Password]$_{space}$[Command code]$_{space}$[Command content]

Attention!: Change the default password (123456) to new one known only by you.

SMS text for changing the password:

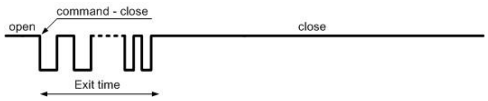
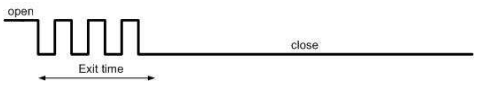
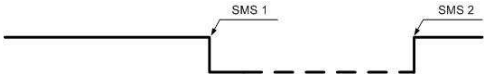
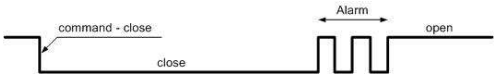
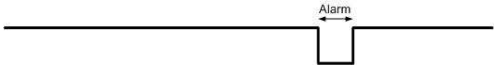
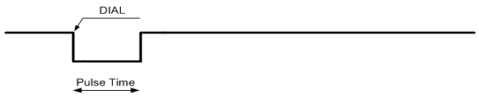
PSW123456 ␣ 98 ␣ 000000	98	command to change the password;
	000000	new password (6 digits);
	„␣„	space between values.

Command and request examples:

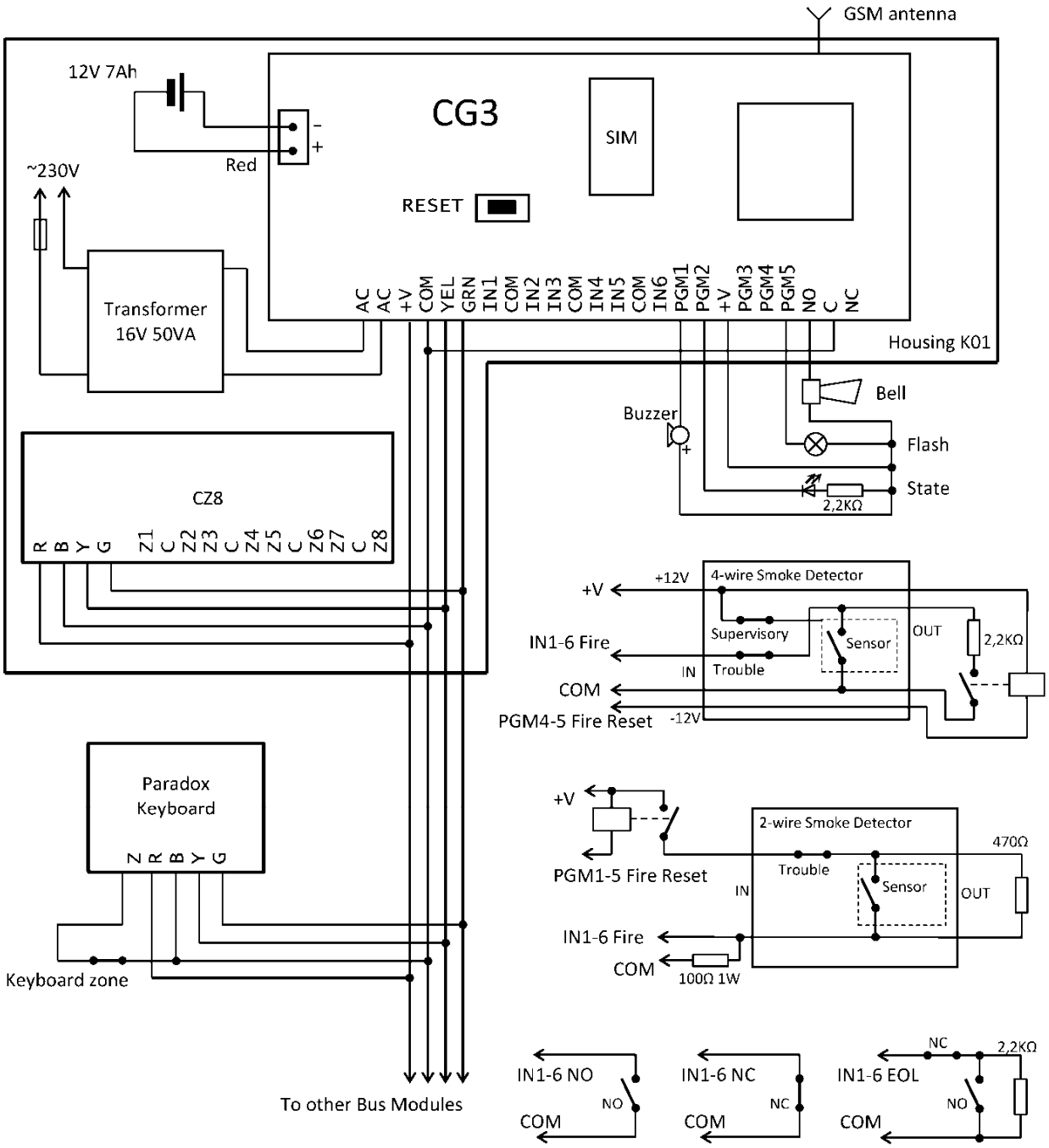
SMS text	*Description*
PSW000000 ␣ 97 ␣ 3	Module will send an SMS message about the status of inputs;
PSW000000 ␣ 97 ␣ 4	Module will send an SMS message about the status of the security system, inputs and power supply;
PSW000000 ␣ 97 ␣ 5	Module will send an SMS message about GSM network strength and module IMEI number;
PSW000000 ␣ 50 ␣ N	N^{th} output status will be changed to opposite; N values: 1, 2, 3, 4, 5, 6
PSW000000 ␣ 5N ␣ 0	N^{th} output status will be changed to [0]; N values: 1, 2, 3, 4, 5, 6
PSW000000 ␣ 5N ␣ 1	N^{th} output status will be changed to [1]; N values: 1, 2, 3, 4, 5, 6
PSW000000 ␣ 10 ␣ xxx.xxx.xxx.xxx_yyyy#	To set the first IP address and port number. xxx.xxx.xxx.xxx IP address yyyy Port number
PSW000000 ␣ 11 ␣ xxx.xxx.xxx.xxx_yyyy#	To set the second IP address and port number. xxx.xxx.xxx.xxx IP address yyyy Port number
PSW000000 ␣ 96 ␣ yy/mm/dd#hh:mm#	To set the date and time of the control panel. yy – year, mm – month, dd – day, hh – hour, mm – minutes.
PSW000000 ␣ 99	Command: Restart the module

SMS messages have to be started with a capital letter combination PSW and a six-digit password entered in the module. The symbol „␣„ indicates a space in SMS message text.
The module will send the SMS message – a response to request – to the phone, from which the request was received.

Annex A. PGM output operation

Output	*Description*	*Operation*
PGM1 ***BUZZER***	To connect a sound emitting device. The signal is created during the time for entering/leaving the premises.	
PGM2 ***STATE***	To connect a light emitting indicator. The signal is created during the time for leaving the premises.	
PGM3 ***READY***	To connect a light emitting indicator. The signal is created if all secured zones are in order.	
PGM4 ***Remote Control by SMS***	Output is controlled with SMS messages.	
PGM5 ***FLASH***	To connect a light-emitting signalling device. The signal is created if security system is disturbed.	
PGM6 ***BELL***	To connect a sound-emitting signalling device. The signal is created if security system is disturbed.	
PGM ***Remote Control by DIAL***	Operation of output controlled with a phone call if ***Pulse mode*** is set.	
	Operation of output controlled with a phone call if ***Level mode*** is set.	

Annex B. Wiring diagrams



Annex C. Default (factory) parameter list

Parameter	*Function, type*	*Description*
Input IN1	**Delay**, EOL	To control entry/exit zone. Zone disturbance is allowed during the time for entry/exit out of premises (*Entry* and *Exit Delay*).
Input IN2	**Interior**, EOL	To control the passageway zone. Zone disturbance is allowed during the time for entry/exit out of premises (*Entry* and *Exit Delay*).
Input IN3	**Instant**, EOL	Instant zone. If this zone is disturbed, while security system is armed, security system will alarm instantly.
Input IN4	**24 hours**, EOL	Constant protection zone. If this zone is disturbed, security system is alarmed instantly even though if it is disarmed.
Input IN5	**Fire**, EOL	To connect fire sensors. If this zone is disturbed, security system is alarmed instantly even though if it is disarmed.
Input IN6	**ON/OFF**, NC	Control zone. To arm/disarm the security system.
Output PGM1	**Buzzer**	To connect a sound-emitting signalling device.
Output PGM2	**State**	To connect a security system status signalling device.
Output PGM3	**Ready**	To connect an input status signalling device.
Output PGM4	**SMS**	Output, which status can be switched with a SMS message.
Output PGM5	**Flash**	To connect a light-emitting signalling device.
Output PGM6	**Bell**	To connect a siren. Sound is emitted when security system is alarmed.
Entry Delay	15 sec	The period of time allowed, after entry to the premises, to disarm the security system before triggering an alarm.
Exit Delay	20 sec	Duration of time, during which zone disturbing is still allowed after the security system is armed.
Duration of siren operation	120 sec	Duration of siren operation, when security system is alarmed.
Period of *Test* messages	24 hours	Period for sending *Test* messages.
Bell Squawk function	ON	A **Buzzer** signal is created when security system is armed or disarmed.
AutoARM function	OFF	The security system will not turn automatically on after disarming

Annex D. Controlling the security system with a keypad

1. **Arming the security system** (when the security system is not divided into partitions).

   [4321]
   Enter the *User code*.
   The time countdown for leaving the premises (Exit Delay) will start. Indicator *ARM* will start flashing. During this time zone ***Delay*** must be disturbed. When the security system arms indicator *ARM* starts shining. If *Bell squawk* function is enabled, siren will make a short signal.
   Note. If secured zones are disturbed, the security system cannot be armed.

2. **Arming in the mode STAY** (1 s t m e t h o d).
   Note. At least one input must be defined to operate as zone either ***Instant STAY*** or ***Interior STAY***.

   [STAY] + [4321] + [1] + [ENTER]
   Press the button [STAY], enter the *User code,* enter the Partition number and press the key [ENTER].
   Indicator *ARM* will start shining and *STAY* – flashing. Zones secured in *STAY* mode will be disabled. Input zone ***Delay*** will start functioning as instant operation zone ***Instant***.

3. **Turning on the protection mode STAY** (2 n d m e t h o d).
   Note. At least one input must be defined to operate as zone either ***Instant STAY*** or ***Interior STAY***.

   [4321]
   Enter the *User code*.
   If during the time for exit zone ***Delay*** will not be disturbed, protection mode STAY will turn on. Indicator *ARM* will start shining and *STAY* – flashing. When the ***Delay*** zone will be disturbed, *Entry delay* time countdown will start, during which the security system must be disarmed.

4. **Disarming the security system.**

   [1234]
   Enter the *User code*.
   You must enter your code during *Entry delay* time. When the security system turns off, indicator OFF will start shining.
   If Bell squawk function is enabled, siren will make two short signals.

5. ***BYPASSING*** **a zone.**

   [BYP] + [4321] + [12] + [ENTER]
   Press the button [BYP] and enter the *User code*. Indicator *BYP* will start flashing. Enter a two-digit line number of the zone which control you want to disable. Press the button [ENTER]. Indicator *BYP* will start shining.
   Now security system is ready to be armed while a zone is disturbed. Zone control can be disabled for one period of arming the security system.

6. **Changing the administrator (*Master*) code.**
   Note: Master code can be edited but cannot be deleted.

   [⏻] + [1234] + [01] + [XXXX] +[XXXX] + [1] + [ENTER]
   Press the button [⏻]. Enter the *Master* code (default is 1234). Button [⏻] will start flashing and key [1] - shining. Enter the two-digit Master code line number and after enter the new four-digit *Master* code. Repeat the new four-digit *Master* code.
   Enter the numbers of Partitions, which will be controlled with this code. Press the button [ENTER].
   To cancel the programming, enter the *Master* code and press the button [CLEAR].

7. **Entering of new *User code*.**

   [⏻] + [1234] + [02] + [XXXX] +[XXXX] + [1] + [ENTER]
   Press the button [⏻]. Enter the *Master* code. If the code is correct, button [⏻] will start flashing and button [1] – shining. Other flashing keypad buttons shows serial numbers of users, which *User codes* are already entered.
   Enter the two-digit user line number and the four-digit code of the new user. Repeat the new code.
   Indicate the areas, which will be controlled by entering this code. Press the button [ENTER].
   Other user codes are entered in the same way. To cancel the programming, press the button [CLEAR].

8. Deleting of *User code*.

[⏻] + [1234] + [02] + [SLEEP]
Press the button [⏻]. Enter the *Master* code. If the code is correct, button [⏻] will start flashing and button [1] – shining. Other flashing keypad buttons shows serial numbers of users, which user codes have been already entered.
Enter the two-digit serial number of user whose code you want to delete. Press the button [SLEEP]. A sound signal will be heard and key lighting, indicating the serial number of the code being deleted, will turn off. The code is deleted. To cancel the programming, press the button [CLEAR].

9. When the system is divided into Partitions, the way to see arming status of Partitions.

Simultaneously press the buttons [1] and [2] for 2-3 seconds.
If number keys flash it means that these partitions are armed in STAY. If number keys shine, it means that these Partitions are armed in ARM mode.
To cancel the programming, press the button [CLEAR].

10. Arming of the Partition.

[ARM] + [4321] + [2] + [ENTER]
Press the button [ARM]. Enter the *User code*, Partition number and press the button [Enter].
The time countdown for leaving the premises will start. ***Delay*** zone of the partition must be disturbed. Indicator ARM will start flashing and when the security system will arm – shining.

11. Arming in STAY of the Partition (1 s t m e t h o d) (when several Partitions are controlled with a *User code*).

[ARM] + [4321] + [2] + [ENTER]
Press the button [ARM]. Enter the *User code*, Partition number and press the button [Enter]. If during the for exit zone ***Delay*** will not be disturbed, area protection mode *STAY* will turn on. To see which one partition is armed in STAY, simultaneously press the buttons [1] and [2] for 2-3 seconds.
When entering the secured premises, countdown of Entry Delay time will start.

12. Arming in STAY of the Partition (2 n d m e t h o d) (when several areas are controlled with a user code).

[STAY] + [4321] + [2] + [ENTER]
Press the button [STAY]. Enter the control code, area number and press the button [Enter].
To see which one partition is armed in STAY, simultaneously press the buttons [1] and [2] for 2-3 seconds. Zones protected with *STAY* modes will be disabled. Zone ***Delay*** will start functioning as instant operation zone ***Instant***.

13. Disarming of the Partition.

[OFF] + [4321] + [2] + [ENTER]
Press the button [OFF], enter the User code, Partition number and press the button [Enter].

14. Reviewing security system alarm memory.
After security system is disturbed, indicator MEM will start shining and indicator for the disturbed zone will start flashing rapidly. Press the button [MEM]. Indicator of the zone, which was disturbed, will start shining. In order to erase the memory press the button [CLEAR].

15. To cancel the programming mode, erase or edit incorrectly entered command, press the button [CLEAR].