ritm
SECURITY SOLUTIONS

Control panels
“Contact GSM-9N”
“Contact GSM-9M”
“Contact GSM-9K”
“Contact GSM-9A”

Operating Manual. Rev. 1.2

Saint Petersburg, 2017

Contents

Introduction

Congratulations on your purchase of the security control panel Contact[1] and GEO.RITM Software Package. Much care has been taken in developing these systems and software, to provide you with unprecedented peace of mind and security. The user-friendly menu with its advanced features will professionally help you to protect your premises.

This operating manual covers the following control panels:

- "**Contact GSM-9N**";
- "**Contact GSM-9K**";
- "**Contact GSM-9A**";
- "**Contact GSM-9M TM**";
- "**Contact GSM-9M NFC**".

This manual contains data on the design, principle of operation, properties of devices, their parts, and guidelines for proper and safe operation of devices (intended use, maintenance, storage, and transportation).

We recommend reading this guide in its entirely in order to familiarize you with the system and take full advantage of its features.

To assure optimal safety and security, you should perform a system test once a week.

For any further questions, please contact your local Ritm distributor.

1) Depending on your purchase.

Designations

Term	Designation
Battery	Accumulator battery
Zone	A part of a guarded facility controlled by one hardwired zone or by a combination of hardwired zones.
Area	Independently controlled and logically dedicated part of a security system.
Monitoring server	A server to which the device transmits data through configured communication channels.
Tamper	A contact located under the device cover and triggered on removal the cover or tearing-off the device from surface.
Hardwired zone	A circuit connecting output nodes of signaling devices and designed for transmitting to the device details on controlled by signaling devices parameters.

Signs on the devices

Sing	Designation
230 V~	Operating voltage 220-240 V from the AC mains.
12 VDC	12 V operating voltage from the secondary DC power supply.
50 Hz	AC mains frequency.
300 mA	Maximum demand.
	Class II of electrical protection (under IEC 61140-2012).
	Class III of electrical protection (under IEC 61140-2012).
	Used materials can be reused after recycling.

Signs in this manual

Sing	Designation
	Warnings.
	Nota bene.
	Notes and examples.

Factory default Master code: 1234.

Product Liability Act

All products covered by this instruction manual may only be used for the purpose specified. When in doubt, consult a qualified specialist or our support team by the helpline: **007 (812) 603-47-04** or email world@ritm.ru.

Products that are supplied with voltage (in particular 220-240 V mains voltage) need to be disconnected from the power supply prior to opening them or connecting cables.

Any losses or consequential damage caused by intervention or changes made to our products or improper handling are excluded from liability. The same applies to improper storage or external effects.

When dealing with 220-240 V mains voltage or with mains-operated or battery-operated products, the applicable guidelines are to be observed, e.g. guidelines on adhering to the electromagnetic compatibility; or the low-voltage directive. The respective work should only be carried out by a qualified specialist.

Our products are in compliance with all technical guidelines and telecommunications regulations applicable in the EU and Great Britain.

	Note: Although this product does not contain any harmful materials, we suggest you return the product to the dealer, distributer or directly to the manufacturer after use.

Usual care and caution

1. This installation must be conducted by a qualified service person/staff and should strictly comply with the electrical safety regulations of the local region.
2. To avoid risk of fire and electric shock, do keep the product away from rain and moisture.
3. Do not touch components such as modem, power source and processors, which may be hot.
4. Make sure that the power supply voltage is correct before using the device/devices.
5. Please, make sure the plug is firmly inserted into the power socket.
6. When the product is installed on a wall or ceiling, the device should be firmly fixed.
7. If the product does not work properly, please contact your dealer. Never attempt to disassemble the device by yourself.
8. Do not store or install the device in extremely hot or cold temperatures, dusty or damp locations, and do not expose it to high electromagnetic radiation.
9. Only use components and parts recommended by manufacturer.
10. Do not drop the device or subject it to physical shock.
11. To prevent heat accumulation, do not block air circulation around the device.
12. Use a soft, dry cloth to clean the surface of the device. Stubborn stains can be removed using a soft cloth dampened with a small quantity of detergent solution, then wipe dry.
13. Do not use volatile solvents such as alcohol, benzene or thinners as they may damage the surface finishes.
14. Save the package to ensure availability of shipping containers for future transportation.
15. Operations under harsh environments such as out of warranted temperature, rapid temperature change, high humidity, constant moisturization may cause the unit to malfunction.
16. Electronic device such as TVs, Radios, PCs, Microwave ovens or any other device with an electric motor may cause the unit to malfunction.
17. Impact or shocks can cause severe damage to the unit. Please handle the unit with care and operate without exerting strong forces.

Warnings for installation stuff

1. This equipment is intended only for use as a Security Alarm Control Panel. Adequate ventilation away from heat and humidity must be provided. The unit must be fixed securely to a non-flammable surface using suitable fixings.
2. All mains wiring must conform to the relevant current IEEE wiring regulations (or appropriate international regulatory standards). See Mains Supply Connection section within this Manual for more detailed instructions.
3. All wiring must be protected from sharp or jagged edges.
4. All Low voltage (alarm) wiring must be to the appropriate international regulatory standards, EU regulatory standarts and comply to good wiring practice and should be routed away from the mains cables. Replacement fuses should be of the same type and rating conforming to IEC 127.
5. The Contact GSM Security Control Panels are fitted with resettable fuses. The areas protected are Battery, Aux, Bell, Keypad and Comms. In the event of a fuse tripping or an input/ output not working, remove the source of the load and check wiring for shorts. Check any added devices for full functionality before any reconnection.
6. The maximum current draw from the unit for all output combinations must not exceed the rated output.
7. The unit is intended for use with a suitable re-chargeable lead acid battery permanently connected to the appropriate terminals.
8. All documentation and manuals must be thoroughly read by suitably qualified installation personnel prior to installation and designated staff.
9. The unit has no user serviceable parts inside. Internal access should only be by suitably qualified personnel.
10. For Contact GSM-9A , Contact GSM-9M TM and Contact GSM-9M NFC, 230 V mains plug must be easily accessible for shutdown.
11. For Contact GSM-9A and Contact GSM-9N, the means of disconnecting the power must be provided, in a fixed wiring from a 12 V secondary power source.

Electrical safety tips

Keep curious kids safe from the temptation to stick foreign objects into the device or plugs!

1. Never put fingers or other objects in the device plug-and-socket.
2. Keep metal objects out of device plug-and-socket.
3. Never give or use anything with a cord or plug around water.
4. Never pull a plug out by its cord.
5. Stay away from the electrical sources, substations and power lines.
6. Obey warning signs.
7. Child proofing your home.

Panel Overview

Designation

These control panels are designed for setting up security at remote real estate objects: apartments, offices, country houses, and other objects. Messages to the monitoring software are transmitted via GSM network through GPRS, CSD, SMS channels.

The panels features are the following:

- Connection up to 3 hardwired zones of “dry contact” type or up to 6 resistive hardwired zones;
- Non-volatile memory for 65535 events;
- Remote configuration;
- 2 outputs for connection of actuation devices;
- Main power supply monitoring;
- Battery discharge monitoring.

Basic capabilities

Security areas

Areas are independently controlled and logically dedicated parts of the security system. The main function of these areas is to combine zones controlled by the system related to one security field to make one or several areas.

You can create up to 6 independent security areas.

A security area enables grouping zones by rooms, managing arming and disarming of these rooms independently and identifying which room or zone has a triggered sensor.

Transmitting messages to the monitoring software or to a user using the Ademco Contact ID protocol specify the names of areas and zones directly in the software settings.

Event history

All events and alarms detected or initiated by the panel are stored in the panel event history. The panel memory can store up to 65535 entries. As the event history is full newer events replace the older ones automatically.

The event history can be exported into a .txt file for convenience of the user.

Built-in communicator and communication channels

The panel has a built-in GSM modem. This allows to transmit details on events in the system without connecting additional devices. It is possible to install 2 SIM cards into the panel.

Tamper

The tamper button triggers on removal the panel cover or tearing-off the enclosure from the installation surface and generates an alarm message to send it to the monitoring server or to a user as an SMS.

Device Setup using PC

You can connect and setup the panel using any of the following ways:

8. Remotely using GEO.RITM and RITM-Link cloud software
9. Locally by connecting to the device through a configuration cable and using Ritm.conf and Ritm Configure multiuse configuration software
10. Remotely using CSD-modem

Partial panel setup without using PC[2]

The “Contact GSM-9N” panel could be partly setup in standalone mode. In this case the setup is performed with a built-in keypad. Commands for device setup with a keypad are listed in the “Standalone setup” section.

Touch Memory keys and NFC smart cards emarine[3]

To arm a facility Touch Memory keys could be used and for the “Contact GSM-9M” version could be used NFC-smart cards as an option. This requires installation of the proper reading devices connected to the panel.

16 keys/tags may be used at the same time.

2) Available for “**Contact GSM-9N**” version.

3) The “**Contact GSM-9M**” version could be delivered with a built-in Touch Memory key reader or a NFC-smart cards reader.

Outputs for actuation device connection

2 outputs of the panel can host a number of various actuation devices, such as sirens, illuminated panels, and indicators.

Hardwired zones

The panel allows to connect up to 3 dry contact hardwired zones or up to 6 resistive hardwired zones simultaneously.

Design

Contact GSM-9N

The panel is made in plastic enclosure and has 2 versions:

1. With built-in GSM-antenna
2. With external GSM-antenna In this case the device has a connector for the antenna (SMA connector on the fig. 1).

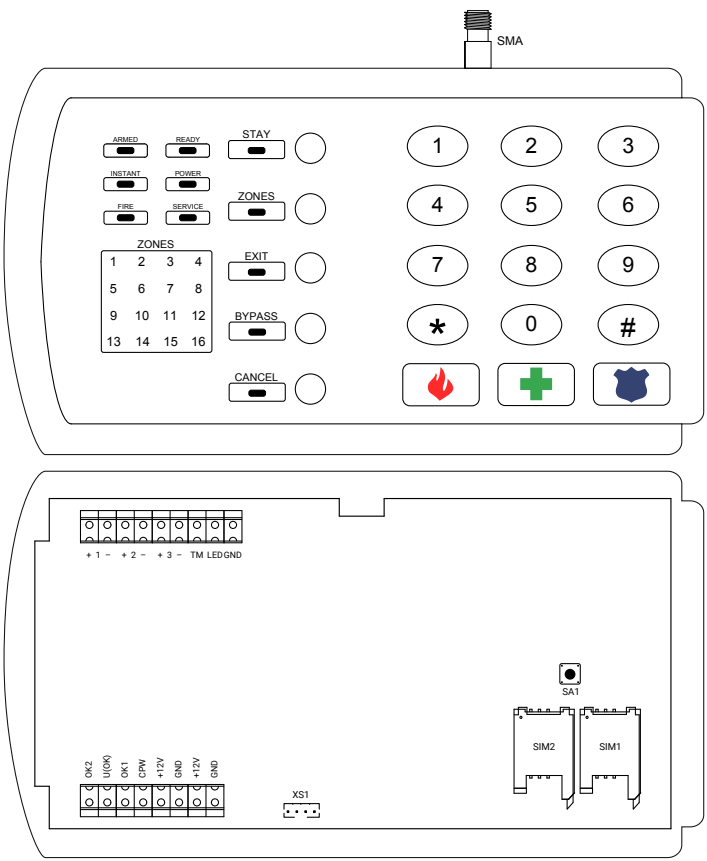

Figure 1. Contact GSM-9N

Part	Designation
CPW, +12V, GND	Panel power supply terminals: • GND — a negative terminal of main power supply • +12V — a positive terminal of main power supply • CPW — 230 V power supply availability check
+12V, GND	Terminals for powering security sensors (+12 V constant voltage is applied to connector when the panel is on)
"+1-"; +2-"; +3-"	Connectors for hardwired zones connection
OK1, OK2, U(OK)	Connectors for external actuation devices connection (siren, visual indicator or relay). Maximum load current — 300 mA. A visual indicator duplicating statuses of areas assigned to the EXIT button is connected to terminals OK1 and +U(OK) A siren is connected to OK2 and +U(OK) terminals.
TM, LED, GND	Terminals for connection a TM/Mifare reader and/ or a temperature sensor with 1-Wire interface: • TM: output (positive) for connection of TM/Mifare signaling wire and temperature sensor yellow wire; • LED: output (positive terminal) for connecting yellow wire of Touch Memory indicator; • GND: common for connection of Touch Memory reader black and blue (and/or black-blue) wire and temperature sensor black and red wire. Colours of the Touch Memory wires may vary depending on the manufacturer.
SA1	Enclosure break-in or supporting surface (i.e., wall) tear-off tamper of control panel
XS1	Configuration cable connector
SIM1	SIM card 1 holder
SIM2	SIM card 2 holder
SMA-connector (optionally)	Connector for external GSM antenna (not available in devices with built-in antenna)

Contact GSM-9A

The device is delivered in the "Contact" 1.2 Ah enclosure or in the "Contact"
7 Ah enclosure.

The panel is equipped with a built-in Touch Memory reader and a visual frame with “Armed”, “Battery” and “Ready” indicators.

Figures 2, 3, and 4 show panel circuit board design and dimensions of enclosures.

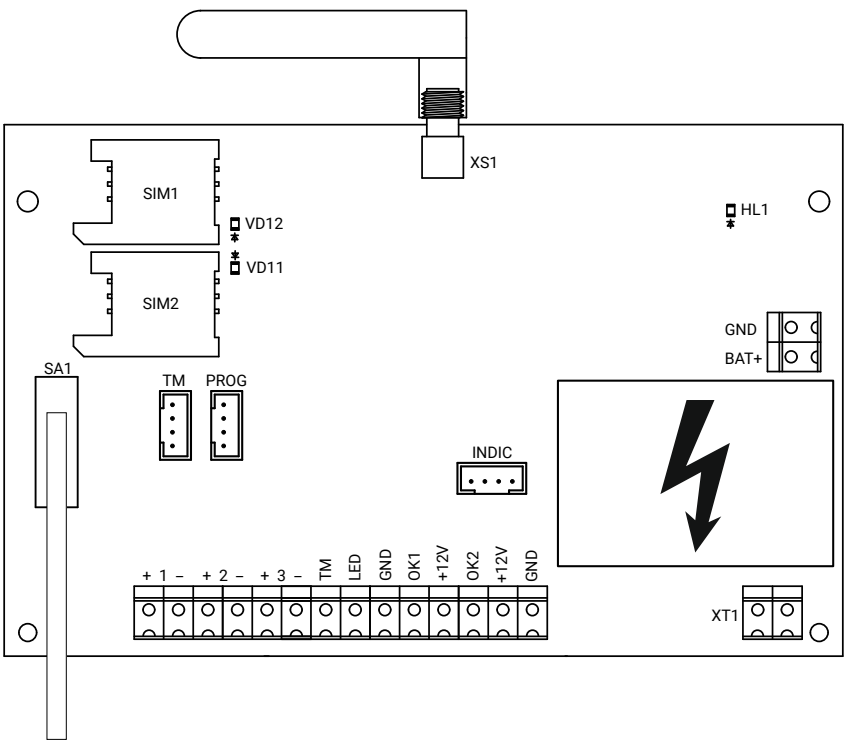

Figure 2. “Contact GSM-9A” panel card

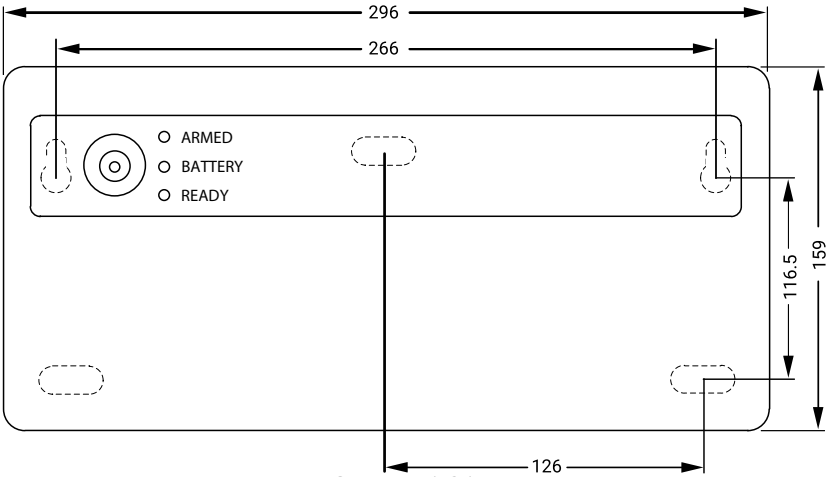

Figure 3. “Contact 1.2Ah” enclosure

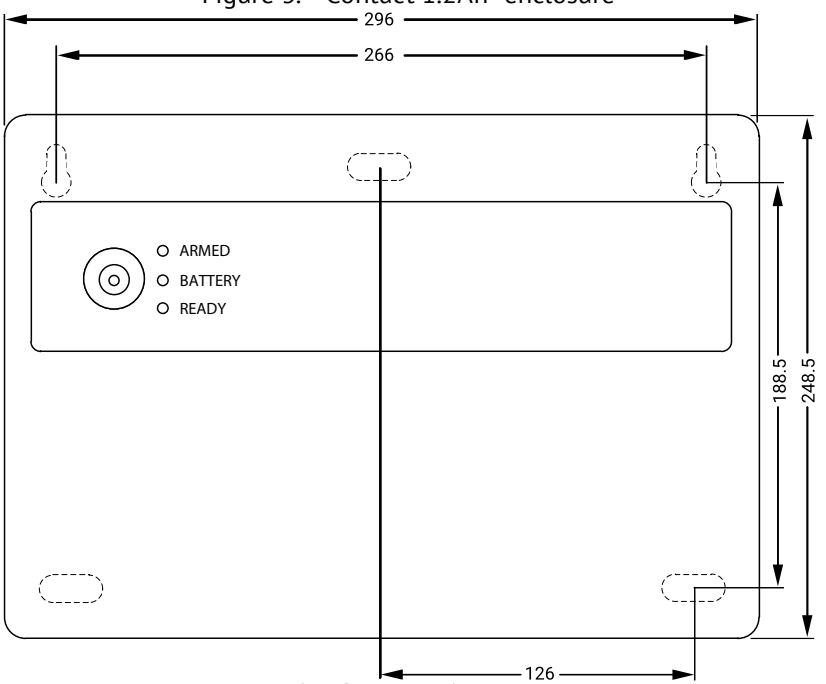

Figure 4. “Contact 7Ah” enclosure

Part	Designation
XT1	230 V power supply connector
+1-; +2-; +3-	Connectors for hardwired zones connection
OK1, OK2, +12V	Connectors for external actuation devices connection (siren, visual indicator etc.). Maximum load current — 300 mA. The OK1, OK2 terminals are negative and the +12V terminal is positive for the device.
+12V, GND	Terminals for power supply of security sensors (+12 V constant voltage is applied to the connector when the control panel is on)
GND, BAT+	Lead-acid battery connector The GND terminal is negative and the BAT+ terminal is positive for the battery.
TM, LED, GND	Terminals for connection a TM/Mifare reader and/ or a temperature sensor with 1-Wire interface: • TM: output (positive) for connection of TM/Mifare signaling wire and temperature sensor yellow wire; • LED: output (positive terminal) for connecting yellow wire of Touch Memory indicator; • GND: common for connection of Touch Memory reader black and blue (and/or black-blue) wire and temperature sensor black and red wire. Colours of the Touch Memory wires may vary depending on the manufacturer.
SA1	Enclosure break-in or supporting surface (i.e., wall) tear-off tamper of control panel
PROG	Configuration cable connector
SIM1, SIM2	SIM card slots
XS1	GSM antenna connector
TM	Connector for Touch Memory reader connection using a 4-pin cable
INDIC	Connector for indication board connection (on the enclosure)

Contact GSM-9M

The panel is made in plastic enclosure and has 2 versions:

1. “Contact GSM-9M” TM control panel is equipped with a Touch Memory key reader built in the enclosure.
2. “Contact GSM-9M” NFC control panel is equipped with a NFC key reader built in the enclosure.

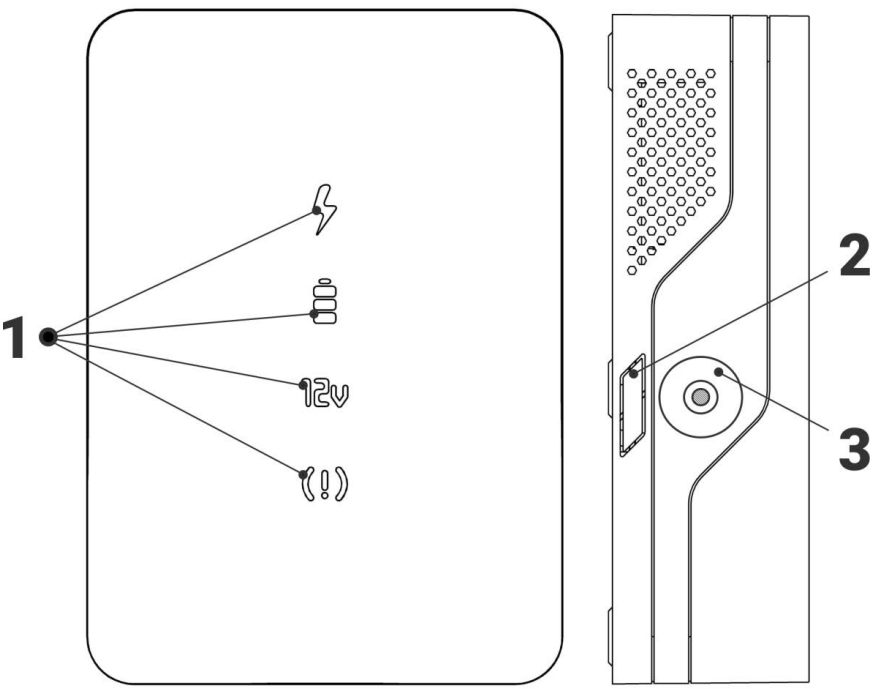

Figure 5. “Contact GSM-9M”: front and side view

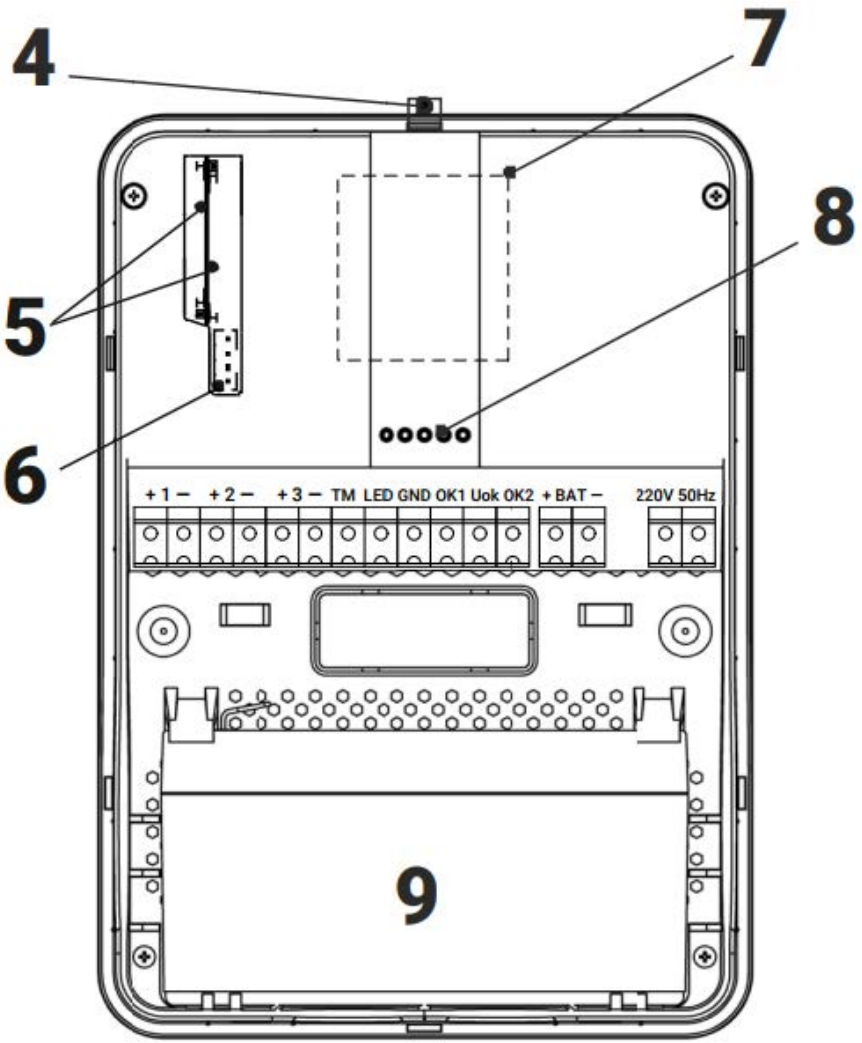

Figure 6. “Contact GSM-9M”

#	Part	Designation
1	LEDs	Device indication is described in the section "Indication"
2	Blank plug	A mounting hole designed for cable inlet/outlet
3	Touch Memory reader	TM reader built in the enclosure (optionally, depending on the version)
4	GSM antenna connector	External GSM antenna connector
5	SIM card slots	Vertical slots for SIM cards
6	Configuration cable connector	Configuration cable connector for PC communication
7	NFC reader	NFC reader built in the enclosure (optionally, depending on the version)
8	Spring contacts	Spring contacts are connected to the indication board (on the top cover of the enclosure).
9	Battery location	Backup battery compartment
	+1-; +2-; +3-	Connectors for hardwired zones connection
	OK1, OK2, Uok	Connectors for actuation devices. The OK1, OK2 terminals are negative and the Uok terminal is positive for devices.
	TM, LED, GND	Terminals for connection a TM/Mifare reader and/ or a temperature sensor with 1-Wire interface: • TM: output (positive) for connection of TM/Mifare signaling wire and temperature sensor yellow wire; • LED: output (positive terminal) for connecting yellow wire of Touch Memory indicator; • GND: common for connection of Touch Memory reader black and blue (and/or black-blue) wire and temperature sensor black and red wire. Colours of the Touch Memory wires may vary depending on the manufacturer.
	+BAT-	Lead-acid battery connector The «–» terminal is negative and the «+» terminal is positive for the battery.
	220 V 50 Hz	220-240 V power supply connector

Contact GSM-9K

The panel is made in plastic enclosure and has all the features of "Cocntact-GSM-9N" and also has the connectors to install the battery.

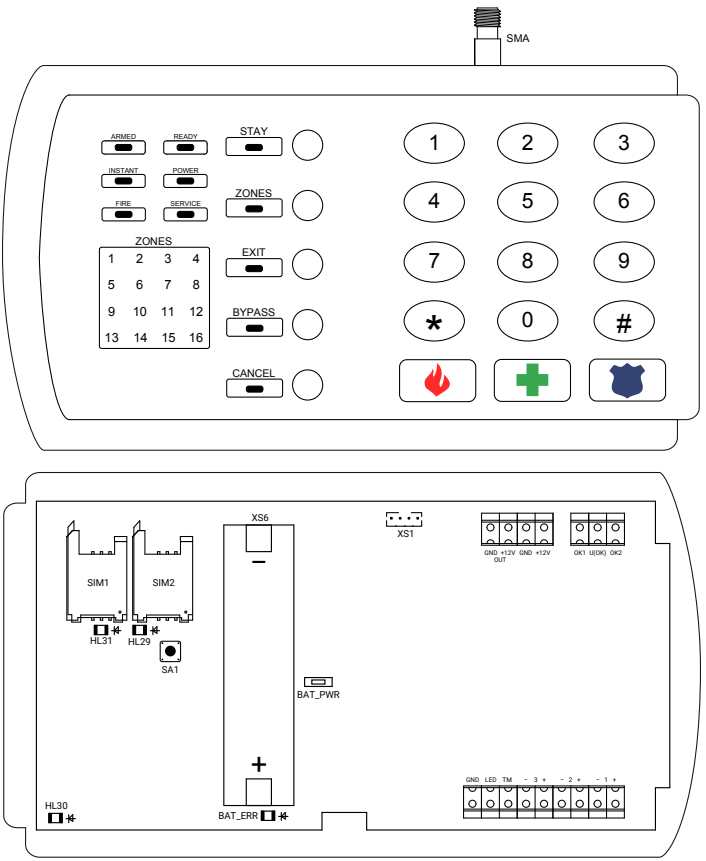

Figure 7. Contact GSM-9K

Part	Designation
+12V, GND	Panel power supply terminals: • GND — a negative terminal of main power supply • +12V — a positive terminal of main power supply
+12V, GND (OUT)	Terminals for powering security sensors (+12 V constant voltage is applied to connector when the panel is on)
"+1-"; +2-"; +3-"	Connectors for hardwired zones connection
OK1, OK2, U(OK)	Connectors for external actuation devices connection (siren, visual indicator or relay). Maximum load current — 300 mA. A visual indicator duplicating statuses of areas assigned to the EXIT button is connected to terminals OK1 and +U(OK) A siren is connected to OK2 and +U(OK) terminals.
TM, LED, GND	Terminals for connection a TM/Mifare reader and/ or a temperature sensor with 1-Wire interface: • TM: output (positive) for connection of TM/Mifare signaling wire and temperature sensor yellow wire; • LED: output (positive terminal) for connecting yellow wire of Touch Memory indicator; • GND: common for connection of Touch Memory reader black and blue (and/or black-blue) wire and temperature sensor black and red wire. Colours of the Touch Memory wires may vary depending on the manufacturer.
SA1	Enclosure break-in or supporting surface (i.e., wall) tear-off tamper of control panel
XS1	Configuration cable connector
SIM1	SIM card 1 holder
SIM2	SIM card 2 holder
SMA-connector (optionally)	Connector for external GSM antenna (not available in devices with built-in antenna)
XS6	Connector for battery installation
BAT_PWR	Button to switch the device on when powered by battery. Used to activate the device after installation/replacement of battery (if the absence of main power).

Specifications

Option	Value
GSM channel frequency, MHz	850/900/1800/1900
Communication channels	CSD, GPRS, SMS to the property owner, SMS ContactID
Status monitoring of communication lines	+
Number of SIM cards installed, pcs	2
Security arming by area	+
Configuration of (resistance) thresholds for each ribbon cable	+
Arming/disarming from keypad	+ (for “Contact GSM-9N/K” version)
Arming/disarming from monitoring software	+ (in GPRS Online mode)
Arming/disarming with TM keys/NFC smart cards	+
Max. number of TM keys/smart cards, pcs	16
Number of events in history	65,535
Configuring parameters using PC	+
GSM signal strength indication using keypad	+ (for “Contact GSM-9N” version)
Number of bare collector outputs (with 300 mA maximum load), pcs	2
Number of connected hardwired zones, pcs	up to 3 of “dry contact” type or up to 6 resistive
Main power source voltage, V	220-240 (12±2 for “Contact GSM-9N/K” version)
Backup power source voltage, V	12±2 (3.7 for “Contact GSM-9K” version)
Current consumption in standby mode, mA	max 80
Current consumption in GSM data transmission mode, mA	max 1000
Dimensions, mm	160×100×30 (**9N**) 160×100×40 (**9K**) 108×142×42 (**9A**) 170×120×50 (**9M**)
Maximum weight (without battery), g, less than	1000
Operating temperature range (non-condensing), °C	-30 – +50

The delivery package is specified in the Device Data Sheet.

Commissioning

GSM tariff plan selection

To start operation install SIM cards of a GSM mobile operator to the device.

Use your mobile operator's plans with enabled GPRS, CSD data and fax messaging channel, SMS messaging and disabled voice communication.

The best plan should have the following features:

1. The GPRS connection has the highest priority (if GPRS is used as the main channel).
2. The GPRS session opening is not charged.
3. The traffic is charged at the end of the day /session.
4. The rounding threshold for the traffic charging is the lowest.

Selecting and Installing SIM cards

To install and remove SIM cards power off panel.

The panel uses one or two standard size SIM cards (mini SIM).

To operate the panel under low temperatures it is recommended to use temperature-resistant SIM cards with extended operating temperature range and life cycle.

Before installing a SIM card into the panel please insert it into a mobile phone and disable PIN code identification in accordance with the phone's operating manual.

Installation and connection

Installation Procedure

Mount the preconfigured panel to an even vertical surface.

Do not mount the panel in close proximity to the following:

- *EMI sources*
- *Massive metal objects and assemblies*
- *Power cable main lines*
- *Heaters and ventilation systems.*

Protect the panel from moisture.

1. Open the panel enclosure.
2. Run all wires through an opening in the enclosure back cover.
3. Securely fasten the back enclosure cover on a wall.
4. Connect hardwired zones to connectors (terminals) of inputs.
5. Connect circuits with actuation devices (LEDs, sirens, etc.) to connectors of outputs, and, if necessary, the TM/NFC reader.

If it is necessary to take the device out of the guarded perimeter, protect power circuits by fuses.

Before inserting the SIM card into the panel please insert it into a mobile phone. Disable PIN code request.

Check the following:

- *The SIM card account balance is positive*
- *The text messaging option is enabled*
- *The signal level at the place of panel installation is high*

Insert the SIM card only when the device is powered off!

6. Insert SIM cards.
7. Connect terminals (+12, GND) of power supply to the power terminals (+12, GND) of Contact GSM-9N circuit board.

If the contact GSM-9N panel is connected to a Ritm power supply, connect the wire from the CPW terminal of power supply to the CPW terminal of Contact GSM 9N circuit board .

When using an power supply of a third party manufacturer:

- *Connect the wire from the CPW terminal to the secondary winding of the power source transformer (when using transformer power supply).*
- *Use an additional control relay (when using impulse power supply).*

8. Install a GSM antenna (for contact GSM 9N with external GSM antenna, Contact GSM 9A).
9. Close the enclosure cover.
10. Turn on the power source.

Indication

External indication is intended for indicating a panel operation mode and controlling states of zones and areas.

Contact GSM-9N

Panel indication in operating mode		
Indicator	**State**	**Value**
ARMED	On	All security areas (excl. fire protection areas and '24 hours') are armed.
	Blinking	Alarm in an area (excl. fire protection areas).
	Off	All areas are disarmed (excl. fire protection areas and '24 hours').
READY	On	All zones in non-armed areas are normal.
	Off	At least one zone in non-armed areas is not normalized or all areas are armed.
FIRE[3]	On	Risk of fire (one fire detector triggered).
	Blinking	Fire alarm (two or more fire detectors triggered).
	Off	Fire areas are normal.
INSTANT	On	Device keypad configuration mode.
	Blinking	Remote configuration mode or configuration cable mode.
	Off	The panel in operating mode.
POWER	On	230 V main power supply available.
	Blinking	The panel operates at backup power supply or no signal in the CPW terminal.
	Off	No power.
SERVICE	Blinking	There are non-transmitted events.
	Off	All events are transmitted or event log is empty.
STAY	On	All areas mapped to the 'perimeter' button are armed.
	Blinking	Alarm in a perimeter area.
	Off	Perimeter areas are not armed or no areas mapped to perimeter.

ZONES	On (on ZONES button pressing)	Within 1 minute, states of zones with numbers 1–6 are shown, then areas are shown (indicator goes off).
	Off	Area states are shown (default).
EXIT	On	Entry delay countdown.
	Blinking	Exit delay countdown.
	Off	No delay countdown.
CANCEL	On	Turns on for 1 second when the Cancel button is pressed to confirm the pressing.
ZONES (1-16)	**The Zones button is pressed. States of zones 1-6 are shown.**	
	Off	Zone is OK.
	On	Zone with fire alarm[3] is possible in zone.
	Blinks slowly	Zone in fire[3] alarm.
	Blinks rapidly	Zone failure.
	The Zones button is not pressed. Shows states of areas 1-6	
	Off	The area is disarmed.
	On	The area is armed.
	Blinks slowly	Alarm in area or exit delay.
	Blinks rapidly	Area failure.
	For an armed area, a zone failure means an alarm in the area.	

4) The control panel is intended for fire protection within the Russian Federation only. Do not use it as a fire control and indicating equipment within European Union.

Contact GSM-9K

"Contact GSM-9K" has the same indication as the "Contact GSM-9N" built-in keypad, and the following indication of indicators located on the board:

Indicator	State	Value
HL29, HL31	HL29 is on	SIM card #2 is used.
	HL31 is on	SIM card #1 is used.
BAT_ERR	On	Wrong battery connection
HL30	Blinks very frequently	The device is connected to the monitoring server
	Blinks frequently	Registration in GSM network
	Blinks slowly	The device modem has successfully registered in the GSM network
	Off	The device modem is switched off

Contact GSM-9A

Indicator	State	Value
On-board indicators		
VD11, VD12	On	SIM card is used.
	Off	The SIM card is not active.
HL1	On	Wrong battery connection.
Visual indication		
ARMED	On	At least one of security areas (excl. fire protection areas and '24 hours') is armed.
	Blinking	Alarm in an area (excl. fire protection areas).
	Off	All areas are disarmed (excl. fire protection areas and '24 hours').
BATTERY	On	The panel is powered from the battery.
	Off	The panel is powered from the main power supply (230 V).
READY	On	All zones in non-armed areas are normal.
	Off	At least on zone in non-armed areas is not normalized or all areas are armed.
TM reader indication in Configuration Mode		
Blinking		The panel is in the configuration mode.
On for 3 seconds		Key applied to the reader has been read.
TM reader indication in Standby Mode		
Off		The area is disarmed.
On		The area is armed.
Blinking		Alarm in area.
On for 3 seconds		The TM key registered in the device memory has been read.

Contact GSM-9M

Indicator	State	Value
 (blue)	On	At least one of security areas (excl. fire protection areas and '24 hours') is armed.
	Blinking	Alarm in an area (excl. fire protection areas).
	Off	All areas are disarmed (excl. fire protection areas and '24 hours').
 (blue)	On	The panel is powered from the battery.
	Off	The panel is powered from the main power supply (230 V).
 (blue)	On	Operational power (12 V or 230 V) available.
 (red)	On	All zones in non-armed areas are normal.
	Off	At least on zone in non-armed areas is not normalized or all areas are armed.
SIM1, SIM2 (on-board indicators)	On	SIM card is active.
	Off	The SIM card is not active.

Standalone configuration[5]

The “Contact GSM-9N” panel could be partly configured using the built-in keypad and without logging to the configuration software. To configure the device use special commands.

The following commands are available:

Designation	Command
Configuration code switching	<configuration code>**#0#**<new configuration code>*
	For example: 1234#0#4321*
Object number switching	<configuration code>**#1#**<object number>*
	For example: 1234#1#0050*
GSM signal strength check	<configuration code>**#2***
	Upon entering a command device indicators 1-5 lights up. Indication designation is the following: the indicator 1 is on - the signal strength is 20%, the indicators 1 and 2 are on - the signal strength is 40%, the indicators 1, 2 and 3 - the signal strength is 60%, the indicators 1, 2, 3 an 4 - the signal strength is 80%, the indicators 1, 2, 3, 4, 5 - the signal strength is 100%.
Adding code for arming and disarming	<configuration code>**#3#**<security code><**D**>**#**<**A**>* where: security code - a code for arming and disarming an area; D - duresse (0 - under no duress, 1 - under duress); A - numbers of arming areas (from 1 to 6).
	For example: 1234#3#11110#123456* In this example to arm areas 1, 2, 3, 4, 5 and 6 under no duress the 1111 code is added.

5) Available for “**Contact GSM-9N/K**” versions only.

Changing code for arming and disarming	<configuration code>**#4#**<**C**>#<new security code><**D**>**#**<**A**>* where: C - a code index (digit from 0 to 9, 0 refers to 10); new security code - a new code for arming and disarming an area; D - duresse (0 - under no duress, 1 - under duress); A - numbers of arming areas (from 1 to 6).
	For example: 1234#4#1#22220#123456* In this example a new value of 2222 for arming areas 1, 2, 3, 4, 5 and 6 with no duress is assigned to the code with 1 as the index number.
Deleting all codes for arming and disarming	<configuration code>**#5***
	For example: 1234#5*
Arming and disarming the selected area	*<**A**>**#**<code for arming and disarming> where: A - a number of the arming/disarming area.
	For example: *3#2222

Panel configuration

You can connect to the panel and configure it by one of the following ways:

- Using ritm.conf and Ritm Configure configuration software
- Using GEO.RITM and RITM-Link cloud software

Multiuse configuration software

Ritm Configure and ritm.conf are multiuse hardware configuration applications. These applications are available for downloading on the official manufacturer website, www.ritm.ru/en.

To connect to the panel you can use remote GSM CSD connection or a USB2 PC connection cable.

CSD connection

To establish a CSD connection use a GSM modem connected to the PC.

Before using the multiuse configuration software please install the modem driver.

To connect to the panel please specify the following settings in the configuration software properties:

- **Connection type:** CSD (GSM modem) V.110 or V.32
- **COM port**: COM port number to which the GSM modem is connected
- **Phone number**: the telephone number of the SIM card installed in the panel
- **Master code**: not used with manufacturer settings.

Figures 8 and 9 show the configuration software views when using the CSD connection.

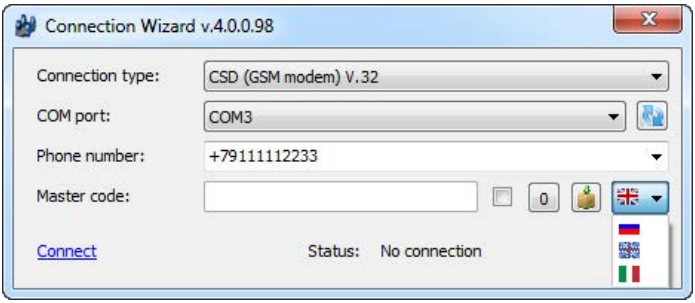

Figure 8. Configuring the CSD connection in the ritm.conf software

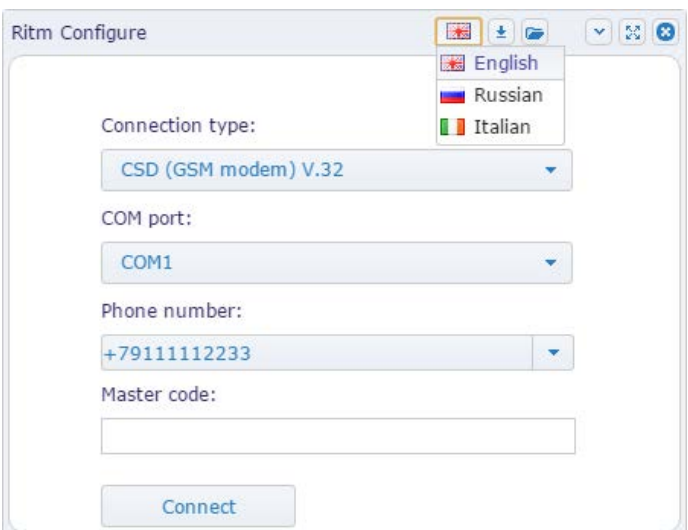

Figure 9. Configuring the CSD connection in the Ritm Configure

Connection via Cable

Before using the multiuse configuration software please install the CP210x VCP driver: http://www.ritm.ru/documentation/program/GSM-modem_Ritm/Drivers.zip.

To connect to the panel please specify the following settings in the configuration software properties:

- **Connection type**: USB/COM (cable)
- **COM port**: COM port number to which the panel is connected
- **Master code**: not used with manufacturer settings.

Figures 10 and 11 show the connection wizard window.

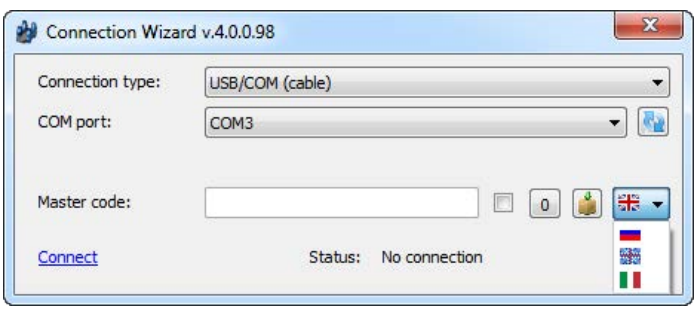

Figure 10. Configuring the USB connection in the ritm.conf software

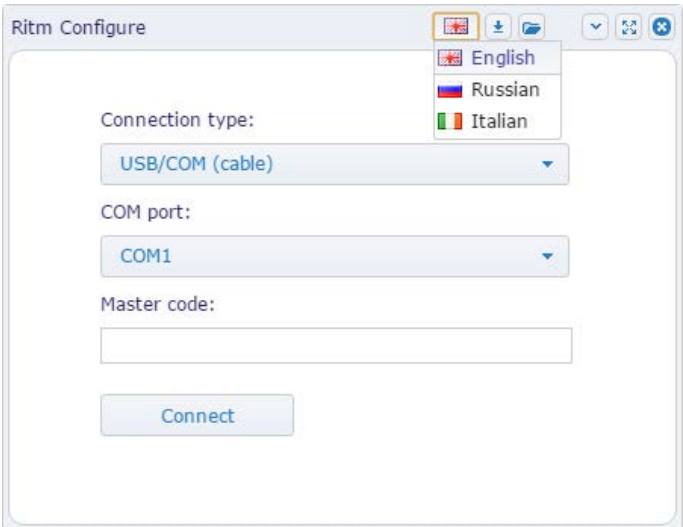

Figure 11. Configuring the USB connection in the Ritm Configure software

Use the Device Manager to identify the COM port number used by the operating system. In the "Ports" section find the port name "Silicon Labs CP210xUSB to UART Bridge" (fig. 12). Your COM port number may differ from the number shown in the Figure.

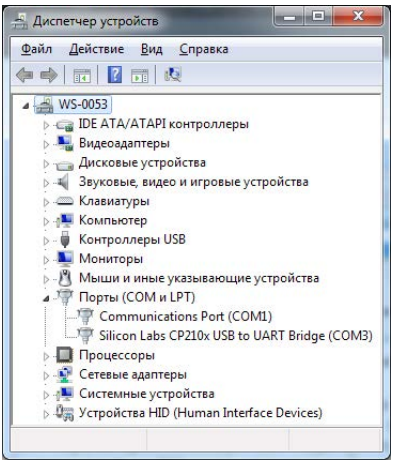

Figure 12. Driver Check

Configuration via GEO.RITM

To access the configuration software via GEO.RITM cloud software open the object card tab “Equipment” (Fig. 13). Under the panel image click **Device Setup**.

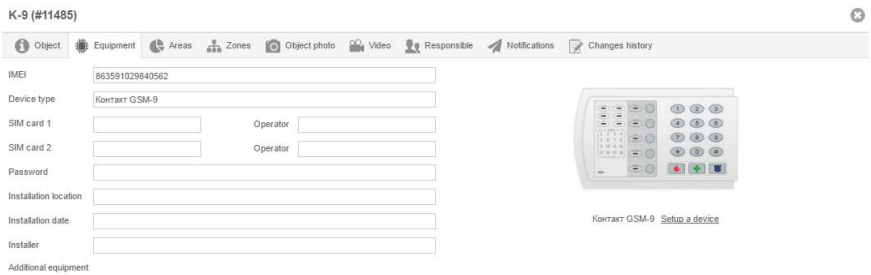

Figure 13. Configuring the panel using GEO.RITM

Configuration using Ritm-Link

To access the configuration software via RITM-Link cloud software click the Devices section (Fig. 14). Use the pop-up menu to open the configuration software clicking **Setup**.

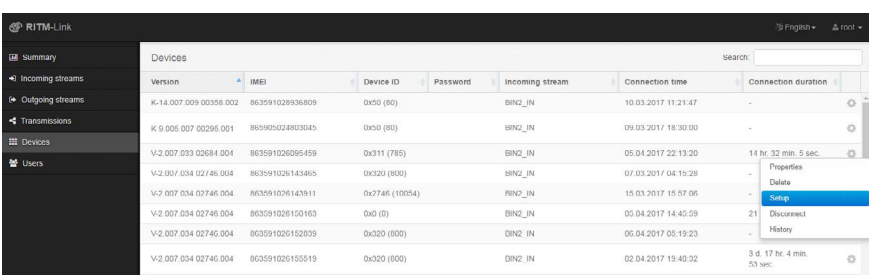

Figure 14. Configuring the panel using Ritm-Link

Configuration software sections

The setup utility is used for defining and setting operation options of the panel and data transfer channels.

Upon specifying all required options on all pages click "Save changes" (Fig. 15). Otherwise all specified settings are reset.

Figure 15. The "Save changes" button

The configuration software window is separated into the following areas (Fig. 16):

1. Configuration software sections.
2. Settings section.
3. Configuration software versions.
4. Details on:
   - Time of connection to the panel;
   - Current state and connection options;
   - Panel firmware version.

The panel configuration procedure consists of switching between different sections of the configuration software and setting the required options.

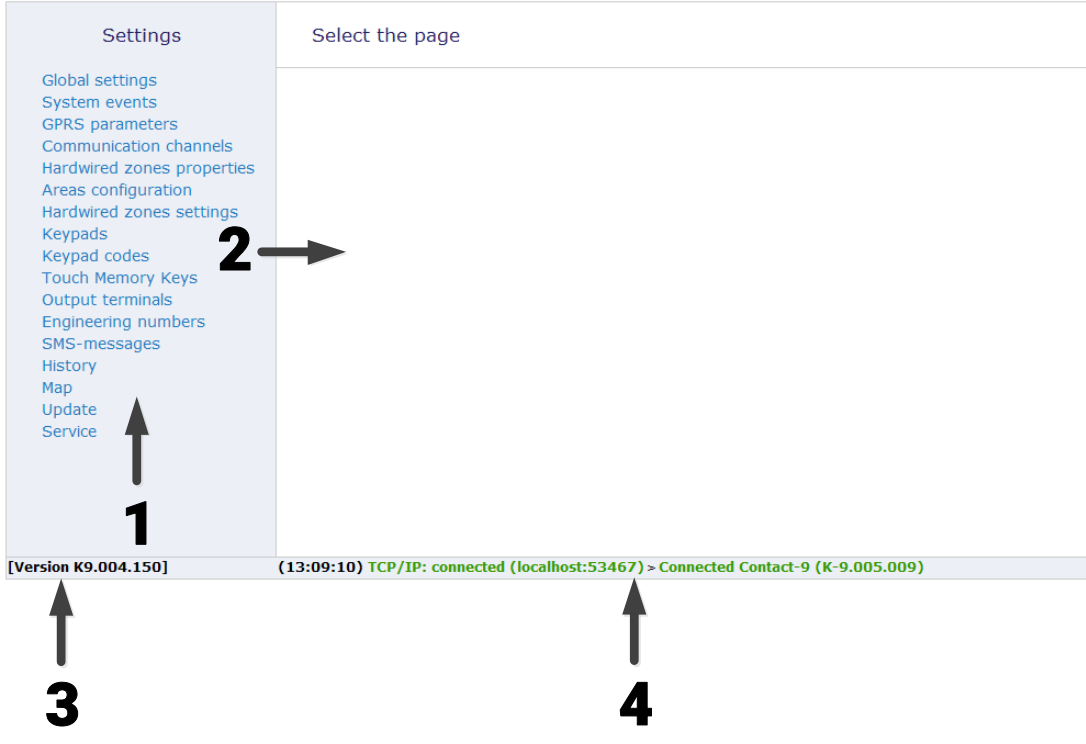

Figure 16. Configuration software window

Global Settings

This section shows current details of the panel and its main units (Fig. 17):

Object #

This field is used only when transferring information to Contact monitoring stations, third party software supporting four-digit Object #.

Master key

Four digit code to connect to the security panel for configuration. Prevents unauthorized access to panel configuration. Default value - 1234.

GSM signal level SIM 1/2

Shows the current level of GSM signal. To connect to the network and update GSM signal level details click the “Test” link.

GSM modem IMEI

IMEI code of the built-in modem.
Required for adding the panel to the monitoring software GEO.RITM.
IMEI is indicated at the GSM modem enclosure.

“Stop the device” and **“Reset the device”**

Use these links to stop and restart the device accordingly.

“LED test on the frontplate of thedevice”

Upon clicking LEDs on the device front panel light up for a short time.

Built-in battery monitoring[6]

The information on the availability of the built-in battery (Present/Not found).
The test is performed every time when closing the housing cover of the device.

Built-in battery voltage (V)

Displays the current voltage level of the built-in battery.

6) Only for **Contact GSM-9K**.

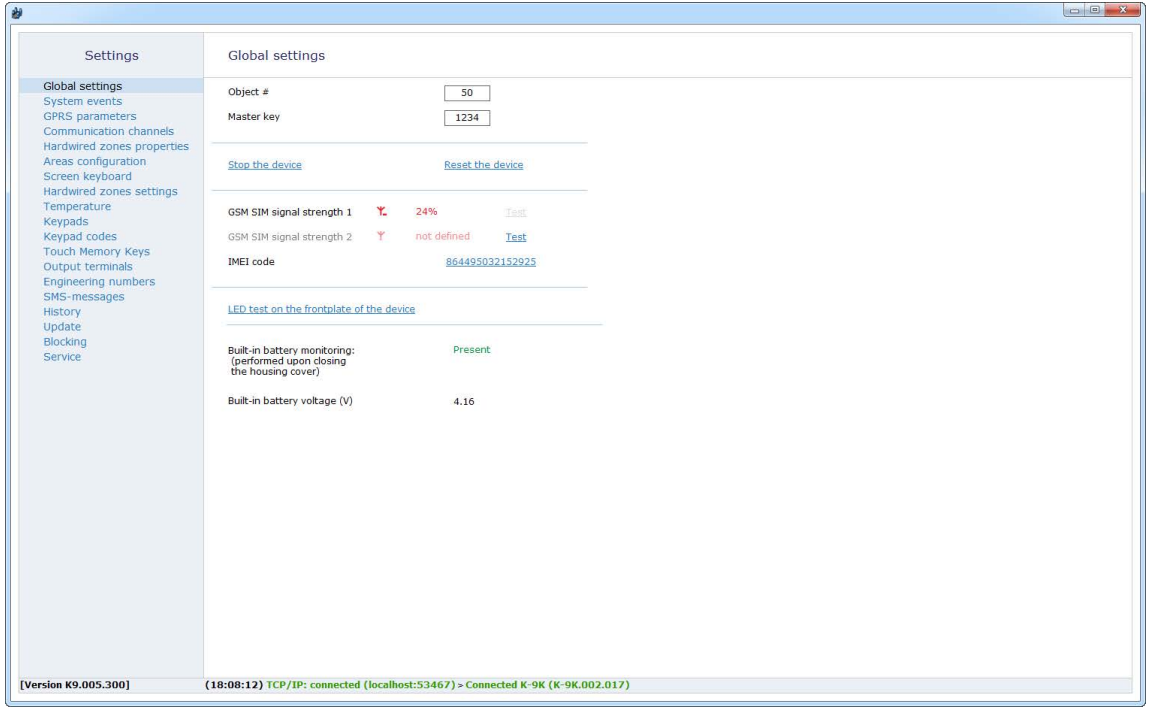

Figure 17. Global Settings section

System Events (Customizable)

System events (fig. 18) allow to track operability of the offline channels as well as ensure the panel is powered properly.

The following system events are customizable:

- Autotests;
- Events related to panel power supply;
- Details of panel rebooting.

Events are recorded automatically into History in accordance with the schedule or when events affecting the panel's operability are generated.

System events are recorded with 0 as the zonenumber and 0 as the area number.

Generate a daily autotest

An automatic test is a special event generated by the panel which is then directed and processed by the monitoring software.

You can schedule up to 3 fixed autotests to be run daily from 00:00 to 23:59.

Period of additional autotest (hours)

When three daily autotests are not enough it is possible to create an additional **periodic** autotest. It is generated in the specified period.

When the autotest is scheduled the event 602.1 "Autotest" is added to the panel history.

Generate "Battery malfunction" event[7]

Check this box if you want to receive information when the battery is suspected of malfunction (only using the CPW terminal).
Event *309.1 — Battery malfunction* will be generated when the panel switches from main power (having worked from the main power for longer then 3 hours) to backup power while the backup power has dropped down to 11 V over 15 minutes.

Generate "Low Battery" event

Check this box if you want to receive information when the battery is low (only using the CPW terminal).
Event *302.1 – Low battery* is generated when external power is off and a backup power supply voltage drops down to 11 V.

Note, in 3 hours after power supply the 302.3 – Rcv: Battery discharge" is generated.

Generate the events "220V failure/recovery"

Set the period over which the panel registers events:

- *301.1 — 220V malfunction.*
- *"Recovery: 220V malfunction.*

When using the CPW terminal the events are generated after external power off/on in period specified at configuration stage. In other words, for the specified period, a backup power supply should be used to generate the event. If the power is restored earlier, the event will not be registered.

Generate “Reboot” event

Activate to get details on panel rebooting. The *305.1: System Reboot* event is generated.

7) For **Contact GSM-9K** event is generated each time when the enclosure is closing and also when the device is restarted. In the absence of action event is generated every 24 hours. If the battery was detected an event 309.3 is generated, otherwise - an event 309.1.

The panel reboots upon turning on, device functional software update and exiting the configuration software while working over the CSD channel.

System Events (Non-Customizable)

Besides the customizable system events selected by the user the panel always registers the following events:

- *621.1: Clear event history;*
- *627.1: Enter the Programing Mode;*
- *628.1: Exit the Programing Mode.*

To identify which mode is used for panel configuration the zone encodes the following details:

- *"0"* — configuration via cable;
- *"99"* — configuration over CSD channel using the phone number not marked as an Engineering Number.

Upon remote configuration through CSD channel but using a phone number specified in the section "Engineering Numbers" as an Engineering Number the event is generated with "0" as an area number and with an engineering number's order in the engineering number list as a zone number.

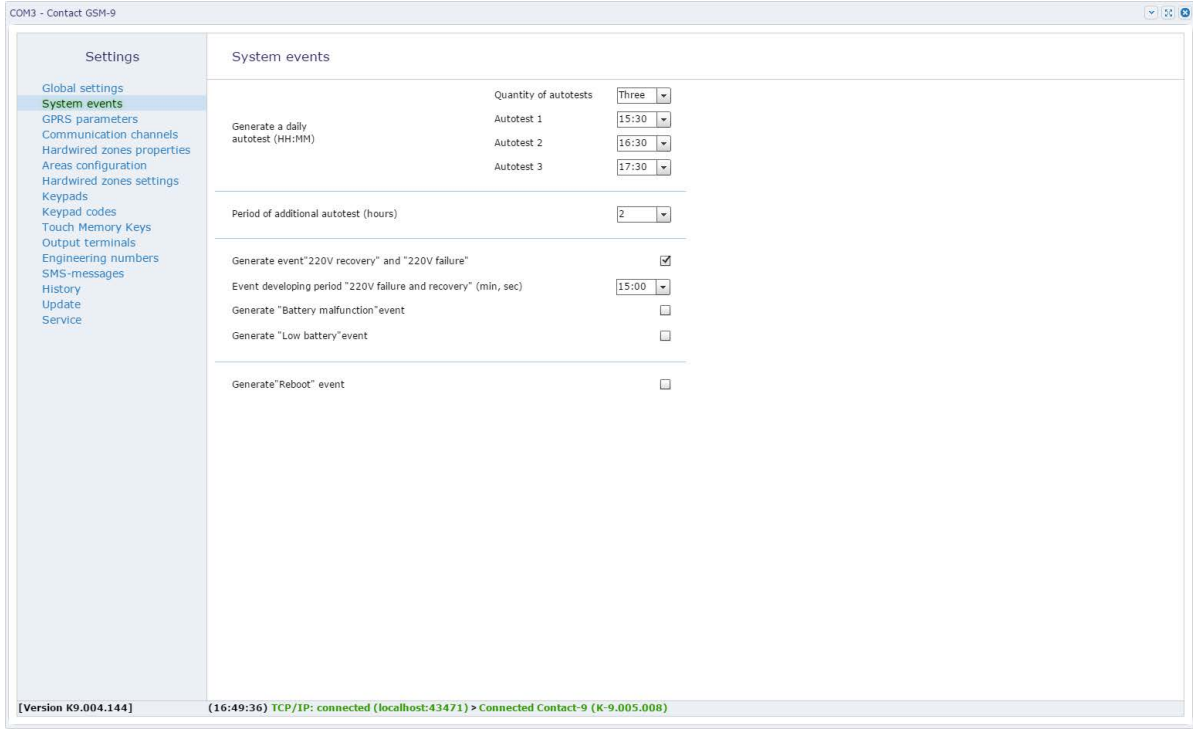

Figure 18. System Events section

GPRS parameters

This section (fig. 19) is intended for configuring settings of connection to an APN access point for SIM cards installed into the panel and for specifying monitoring system servers receiving data from the panel.

If the **“Specify APN configuration automatically”** feature is enabled all connection options are set automatically depending on the communication service provider.

The automatic detection feature uses a predefined set of providers. To view them click Additionally.

When disabling the **Specify APN configuration automatically** please specify:

- **GPRS phone number** — GPRS activation number (normally, *99#);
- **Access point** — host name;
- **Username** — user name;
- **Password** — used password.

Additionally section

To view this section click **Additionally**.

This section is used for storing settings for access points which should be used for automatic detection.

Enter options of available mobile networks in your region.

- **IMSI** – the operator code
- **Operator** — the operator name
- **Access point (APN)** – host name
- **User** — user name
- **Password** — used password

Proper APN parameters can be requested from your mobile network operator.

Mode of a data compression via GPRS

If the panel history has several untransferred events they are transferred in a single package. This decreases traffic.

Pause between attempts to establish a GPRS connection (min)

Set the value of the pause between connection attempts via Online channel. During this pause the data may be transferred via Offline communication channels (see section "Communication channels" at the page 45).

Main/Backup IP address, server port and password

Specifies system monitoring servers receiving data from the panel. Servers of the eu.ritm.ru service are used by default.

If the eu.ritm.ru service is used, do not change settings in this section.

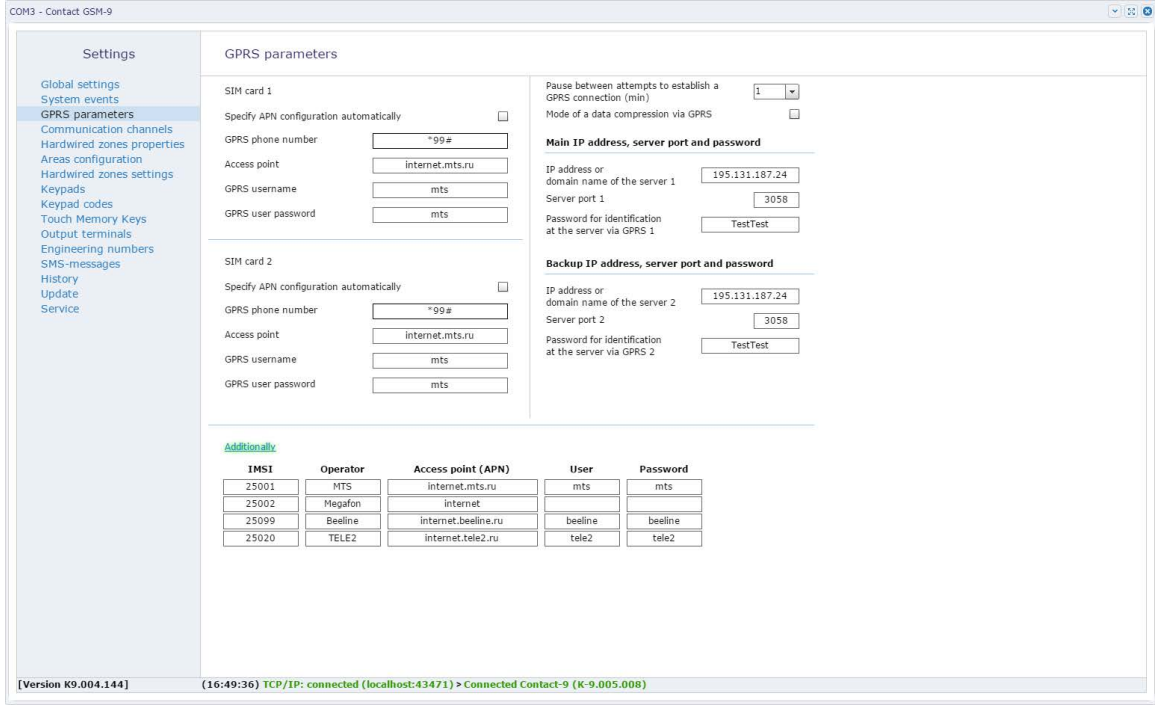

Figure 19. GPRS parameters section

Communication channels

After an event has occurred, it is recorded into the history, and the system tries to transfer it to the monitoring software or to other recipient over the preconfigured communication channels.

General Information

Communication channel is a way (including technical tools and the environment) to transfer information from the panel to a receiver of a specified type.

Direction is a combination of communication channels intended to increase the probability of the successful delivery of information to the recipient in case one of the channels is failed.

Communication channels are combined to form the direction using the OR switch, and the directions are separated using the AND switch.

It is a common practice to separate the Online communication channels, which ensure the permanent panel connection to the monitoring software and allow to evaluate the channel health in real time.

Switching between channels of the same direction is done only when data transmission via a channel with higher priority is failed.

For example with configuration shown on fig.20 switching to the communication channel 3 of the first direction will be done only if data transfer via two preceeding channels is failed.

If transmission through all communication channels is failed several behaviors are possible:

Maintain one direction till transfer of all events
In this case the system will try switching between all channels in this direction until all events are transmitted.

Go to the next direction after check of all channels in the current direction
After reaching the last channel in this direction and failing to send events the data transmission is performed through the next direction from the list.

To authenticate the panel in the monitoring software using IMEI while transferring data via CSD ContactID and SMS ContactID please check the box ***Submit the modem IMEI through CSD and SMS ContactID data channels***.

Otherwise ContactID (instead of IMEI) will have an object code and will be impossible to use Ritm-Link and GEO.RITM in the monitoring software.

Check connection with server in GPRS-Online channel in
Upon operation through a GPRS (TCP/IP) communication channel via SIM1 (SIM2) specify a rate for sending PING command to the monitoring software server.

The time allotted for the registration of the device in the operator's network
Specify time after which the built-in GSM modem will be restarted if there no registration in the network.

The time allotted for the registration of the device in the GPRS
Upon operation through a GPRS (TCP/IP) communication channel via SIM1 (SIM2) this option specifies the time the system must wait before switching to the next communication channel if connection to the server fails.

Timeout of outgoing CSD connection establishing
While working with “Contact” central monitoring stations this parameter defines the time for which the system must wait before switching to the next communication channel, if the connection to the “Contact” central monitoring system could not be established.

Types of communication channels

Depending on the number of used SIM cards the panel allows using up to 12 types of communication channels.

Turn on GPRS (TCP/IP) via SIM1/2

Intented to transfer events to the monitoring software over TCP/IP via GSM GPRS.
When using these types of communication channels the panel connects to the monitoring software server and keeps the connection alive.
The events are transferred right after they are stored into the history.

GPRS-offline SIM1/2 IP1/2

Intented to transfer events to the monitoring software over TCP/IP via GSM GPRS.
When using these types of communication channels the panel connects to the monitoring software server only to transfer the events, and disconnects after the events have been transferred.

ContactID via digital channel GSM V.32/110 SIM1 (SIM2)

Intented to transfer events to a “Contact” central monitoring station or to the monitoring software through the GSM modem over the digital CSD channel of the GSM network.
The central monitoring station processes the received message and sends it to the monitoring software (including third party software) of the guard service company via the Surgard protocol.

SIM1 (SIM2) SMS InetServer

Intended to transfer events to the monitoring software via a GSM modem in SMS messages.
Either the object code or the IMEI of the modem are used as the object ID (depending on the settings).

SIM1 (SIM2) SMS

Intended to transfer events to the property owner in SMS messages.
The rules for composing SMS messages are defined in the "SMS-messages" section.

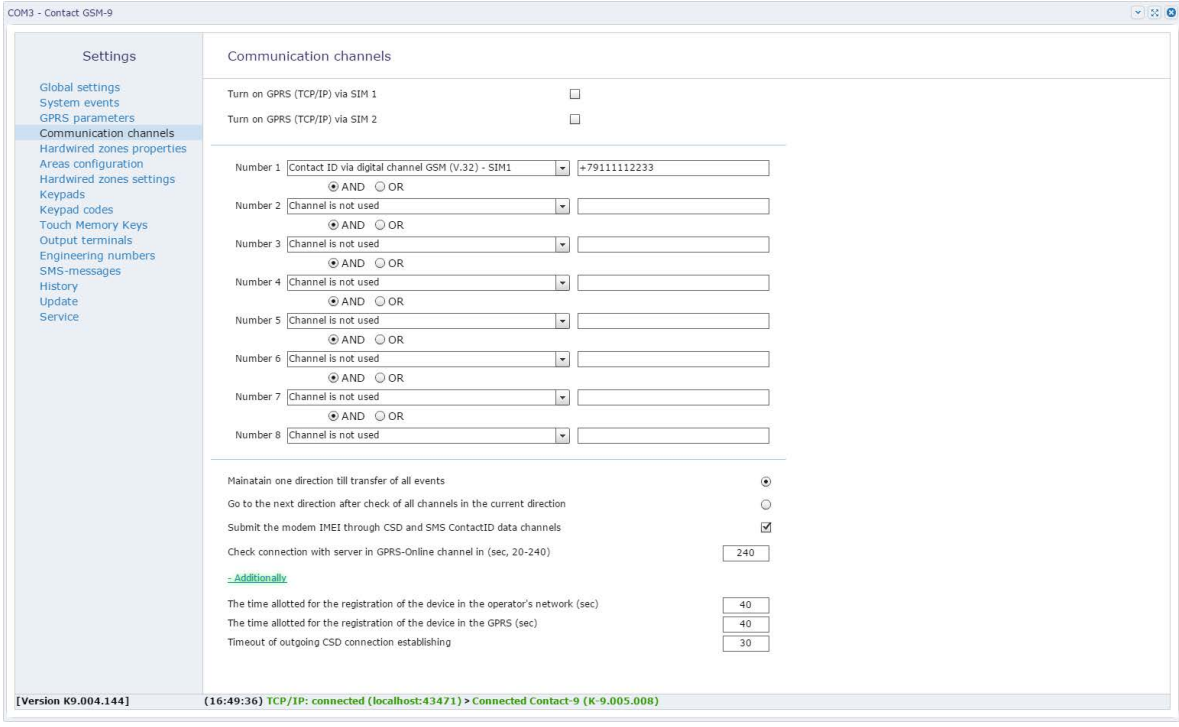

Figure 20. Communication channels section

Hardwired zones properties

The panel has 6 connectors to connect the hardwired zones which then can be configured and used in two different ways:

- as “dry contact” hardwired zones to work with the security sensors,
- as resistive hardwired zones to work with security sensors.

To reset an intrusion alarm disarm the area.

If the area was not armed, it is necessary to arm and then disarm it.

Alarm cancel (recovery) is also recorded into the history.

The hardwired zones can be configured independently from one another, but only one hardwired zone type can be used at a time.

The used hardwired zone type is defined in this section using the **Resistive/Dry contacts** switches.

Troubleshooting code

Regardless of the used hardwired zone type define the code of the event which will be generated when a failure is detected (disconnect or short circuit) of the resistive hardwired zones.
Default value: *380.1 — Zone sensor failed*.

Hardwired zone #

Hardwired zone index number for sensor identification. At every input (+1-) there are two resistive or one “dry contact” hardwired zone.

State

Indicates the current hardwired zone status (normal/failure).

Normal state

Different sensors can have different normal state (closed/opened). You can learn it from the documentation of used sensor.

AdemcoID

Specify the event code which will be generated in the ContactID message when a security sensor triggers.

Area #

Indicate the area (see "Areas Configuration") to which the custom hardwired zone (sensor) is related.

WARNING! If the indicated area is a fire area, the hardwired zone *also becomes a fire hardwired zone.*[5]

WARNING! Dry contact hardwired zones cannot be used as fire hardwired zones![5]

Entrance delay (sec)

If the hardwired zone is used to connect entry area sensors, indicate the time in seconds, which the user will have to disarm the area without activating the alarm after breaching the area.

Exit delay (sec)

The field shows details about the exit delay as defined in the section "Areas Configuration".

Hardwired zone type

Depends on a function the hardwired zone realizes in the security system (incoming, instant, fire[5] etc.)

8) The control panel is intended for fire protection within the Russian Federation only. Do not use it as a fire control and indicating equipment within European Union.

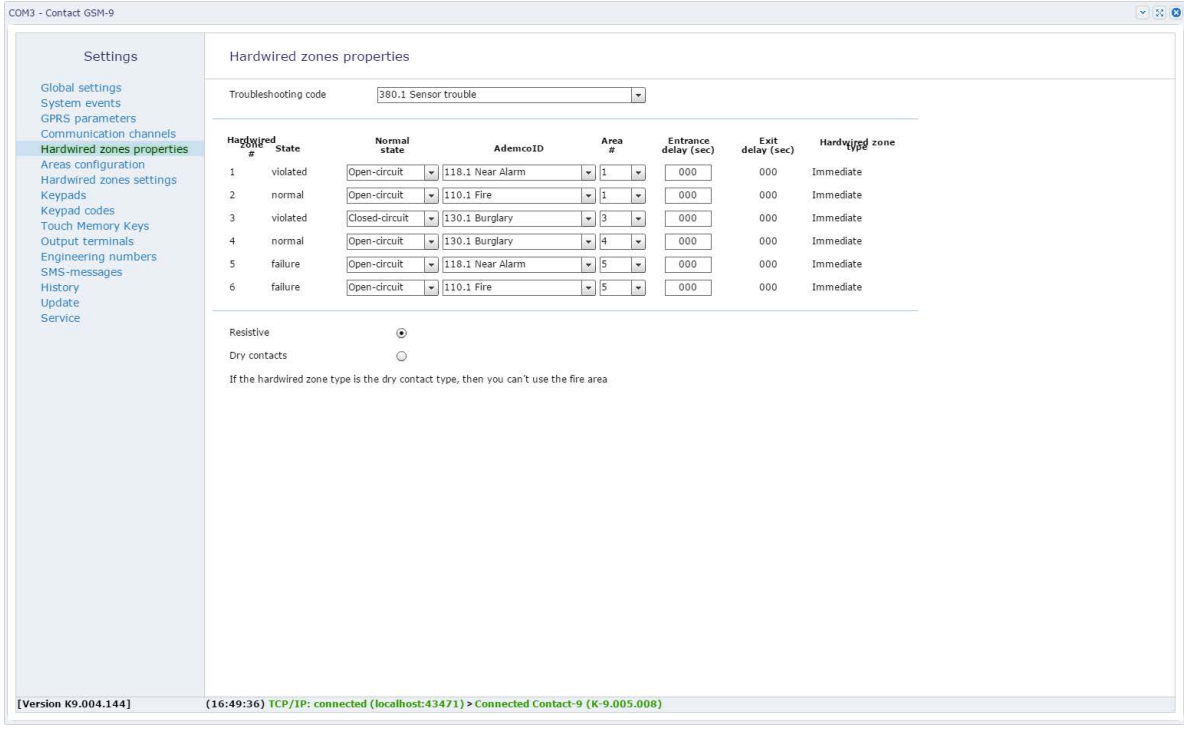

Figure 21. Hardwired zones properties section

Areas Configuration

Areas are independently controlled and logically dedicated parts of the security system. The main function of these areas is to combine zones controlled by the system related to one security field to make one security area. All events dealing with the object must relate to an area.

This section of the configuration software (fig 22) allows to define area properties and event sending limitations.

This table is used to setup properties of existing areas.

#

A unique area number from 1 to 6.
The area number allows to identify the room in which the alarm has been tripped.

Area state

This field shows the current state of the system areas:

- *Alarm* — one or several zones in the area have been triggered
- *Armed* — all zones of the area are normal and armed
- *Disarmed* — the area is not guarded, alarm events from the sensor are not recorded into the history (except 24 hour-zones)

Arm/disarm

Click to arm or disarm an area.

Quick arming

Check this box if arming an area with faulty hardwired zones is allowed. After arming such area an alert is generated.
When this check box in unchecked an area with faulty hardwired zones cannot be armed.

If the quick arming is forbidden at attempt to arm an area with faulty hardwired zones will not lead to arming and this attempt will not be recorded into the history.

Turn on the siren in case of alarm

Check this box if for alarm indication the output needs to be used.

24 hour area

24 hour area is an instant area. This is a special type of areas which is always armed and it cannot be assigned to access codes or touch memory keys.

Fire area[9]

In the case when certain resistive hardwired zones of the panel are used to connect fire sensors set the fire areas.
Fire areas are instant. Hardwired zones processing logic also changes: if two hardwired zones are in a violated state, an event *110.1 — Alarm: Fire* is generated. If only one sensor is violated, an event *118.1 — Alarm: Fire is possible* is generated.

Exit delay

After entering a personal code or arming the facility using a touch memory key the user usually needs time to leave the guarded area. This time is specified in the exit delay parameter.
For every area an exit delay can be set individually.

When the zones are breached during exit delay time an alert is not generated.

The partitions name

Specify a unique name for each area.

9) The control panel is intended for fire protection within the Russian Federation only. Do not use it as a fire control and indicating equipment within European Union.

Transferred event number limits

Set the **Limited event quantity per area** to block unnecessary messages to the monitoring software. This operation is useful to save data traffic.

For example after a guarded area has been breached through a broken window (sensor 1) the intruder moves along the room thus triggering a motion sensor (sensor 2). Since the alarm has already been transferred, the information about the intruder moving through the breached zone is no longer relevant and is not necessary to be transmitted.

This does not involve system events.

After area disarming the counter resets.

If there are no need to limit the number of generated events set the value to **No limitations**.

Arming without connection to the server

Allow arming if no connection to the server

- **The checkbox is selected** - arming areas regardless connection to the monitoring software servers is enabled;
- **The checkbox is cleared** - when trying to arm an area, a check of the first direction of communication channels (Online channel+channels, switched with OR) state will be made. The check is performed by sending a test message (with this an event "602.1 — Periodic test report" is generated). If the test message was not sent by checking channels, then an event "450.3 — Exception close" will be generated and this area will not be armed.

While checking channels, connected to the output OK1 actuation device will blink 1 time per second.

Operation with areas

Operation with partitions

If upon arming an area has a violated zone the “450.3” and “380.1” events are generated and the partition is not arming. In addition the panel buzzer notifies about arming failure — 2 short impulses with 1 second pause.

Arming of a partition group (for example using a user key/code with several partitions assigned):

- Partitions with set “Quick arming” flag are armed;
- Other partitions are not armed if even one of them has a violated zone.

Arming all partitions using the cloud GEO.RITM software is performed according to the logic of arming partitions with set “Fast arming” flag.

If at the arming time the zone is not violated but it becomes violated or faulty at the end time of exit delay than the partition is armed and the “459.1” event is generated.

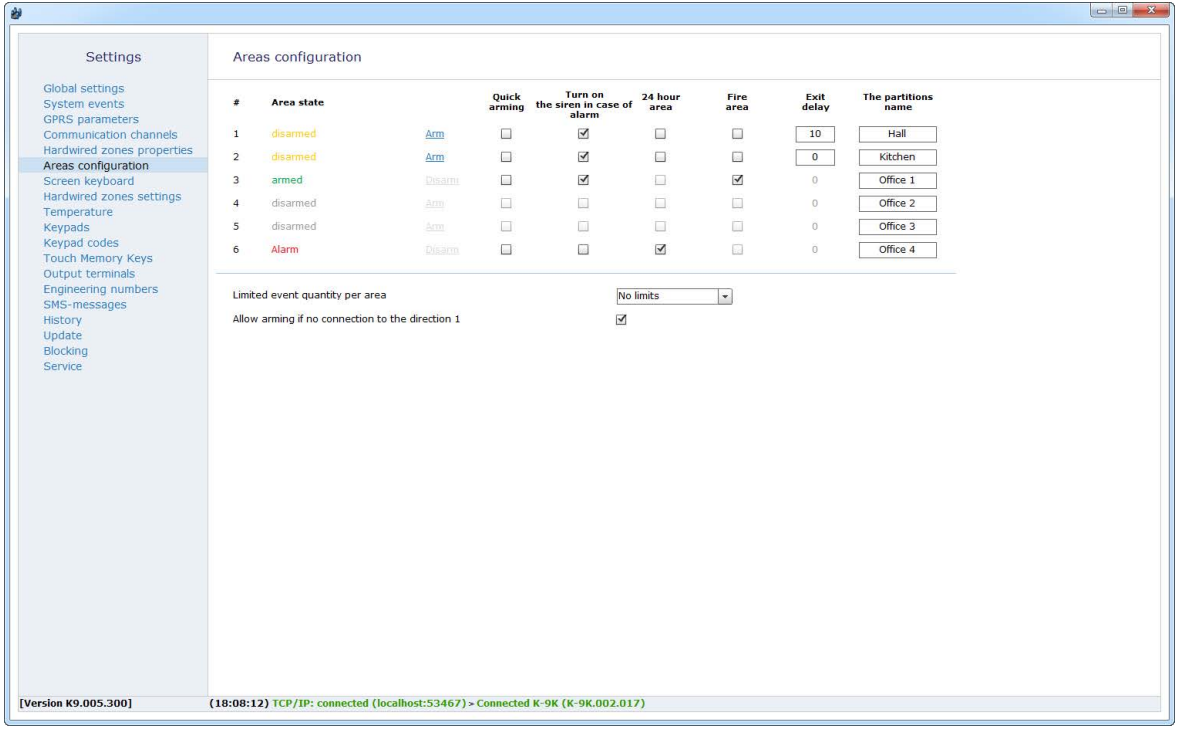

Figure 22. “Areas Configuration” section

Screen keyboard

Use the screen keyboard to arm/disarm the areas. Enter the four-digit user code defined in section "Keypad codes" and areas assigned to this code will be armed/disarmed.

Figure 23. "Screen keyboard" section

Hardwired zones settings

This section shows a sensor connection scheme as well as the state of those sensors in real time (in alarm or not).

Configuring resistive hardwired zones

To use resistive hardwired zones set the **Resistive** type in the section "Hardwired zones properties".

Using the resistive scheme allows:

- To use a large number of security sensors (limited only by power consumption).
- To detect breakage/short curcuits in the hardwired zones.
- To configure the resistance of the hardwired zones for every type of sensors individually.
- To use fire sensors[10].

If the resistors from the delivery package are used for connection it is possible to quickly configure the operating thresholds.
To do this click the **Load defaults** link and connect in accordance with the scheme.

To adjust triggering thresholds manually click the **Loop settings...** link. This will show the scale of triggering hardwired zones thresholds consisting of several parts.

10) The control panel is intended for fire protection within the Russian Federation only. Do not use it as a fire control and indicating equipment within European Union.

For the fire hardwired zone[11] on the resistance scale the following parts are located (fig. 24):

- *Breakage;*
- *Normal;*
- *Warning;*
- *Alarm;*
- *Short circuit.*

Configure the triggering thresholds: trigger each sensor one by one (the first, the second, both sensors), the breakage and its short circuit, and use the mouse to change the position of the lower indicators located under the resistance scale for the hardwired zone.

The color of each indicator corresponds to a part of the hardwired zone on the resistance scale, which it affects.

The current value of the hardwired zone resistance is indicated above the resistance scale by an indicator with a number value.

Figure 24. Fire hardwired zone operating thresholds scale

11) The control panel is intended for fire protection within the Russian Federation only. Do not use it as a fire control and indicating equipment within European Union.

For a resistive security hardwired zone the resistance scale has the corresponding parts (fig. 25):

- *Breakage;*
- *Normal;*
- *Alarm Zone 1;*
- *Alarm Zone 2;*
- *Alarm Zone 1, 2;*
- *Short circuit.*

Configure the operating thresholds: trigger each sensor one by one (the first, the second, both sensors), the breakage and its short circuit, and use the mouse to change the position of the indicators located under the resistance scale for the hardwired zone.

Figure 25. Security hardwired zone operating thresholds scale

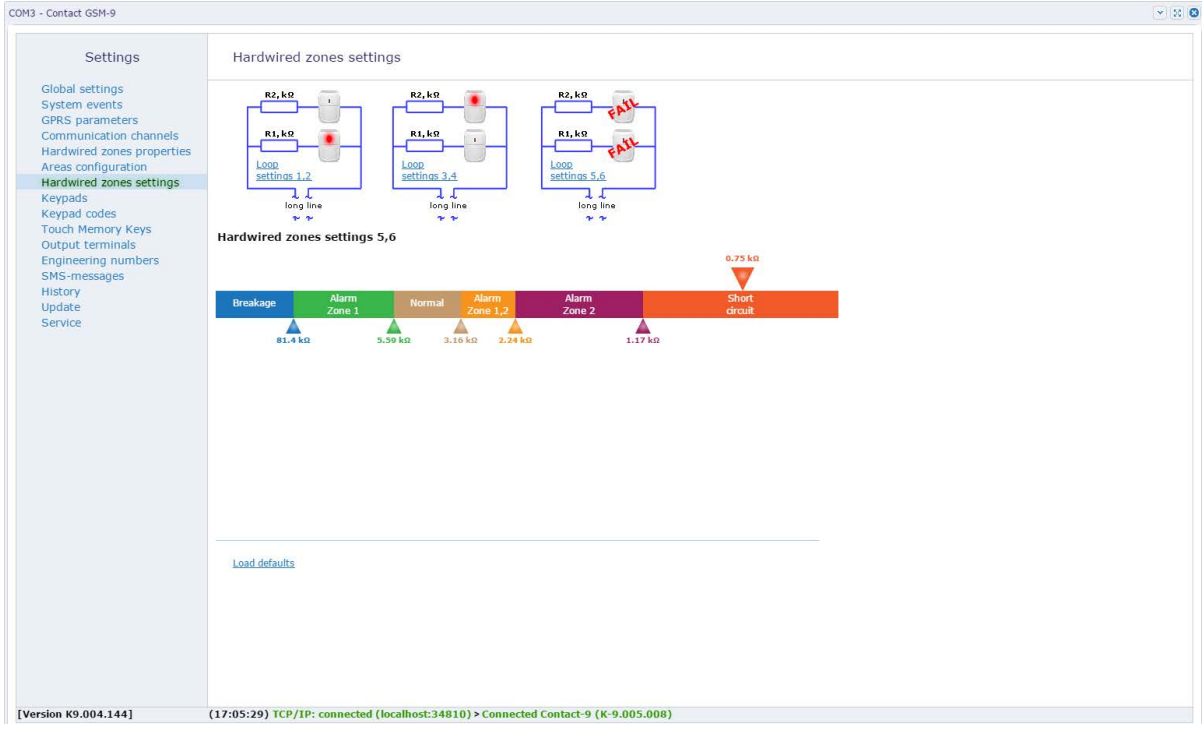

Figure 26. Hardwired zones settings: resistive hardwired zones

Configuring "dry contact" hardwired zones

When using the "dry contact" hardwired zone one input can enable only one security sensor.

Please note! For dry contact hardwired zones *the operating thresholds are not configured.*

When using the "dry contact" hardwired zone the areas can not be fire (see section "Hardwired zones properties" on page 57).

To avoid quick battery discharge connect "dry contact" sensors in normally closed state using a resistor.

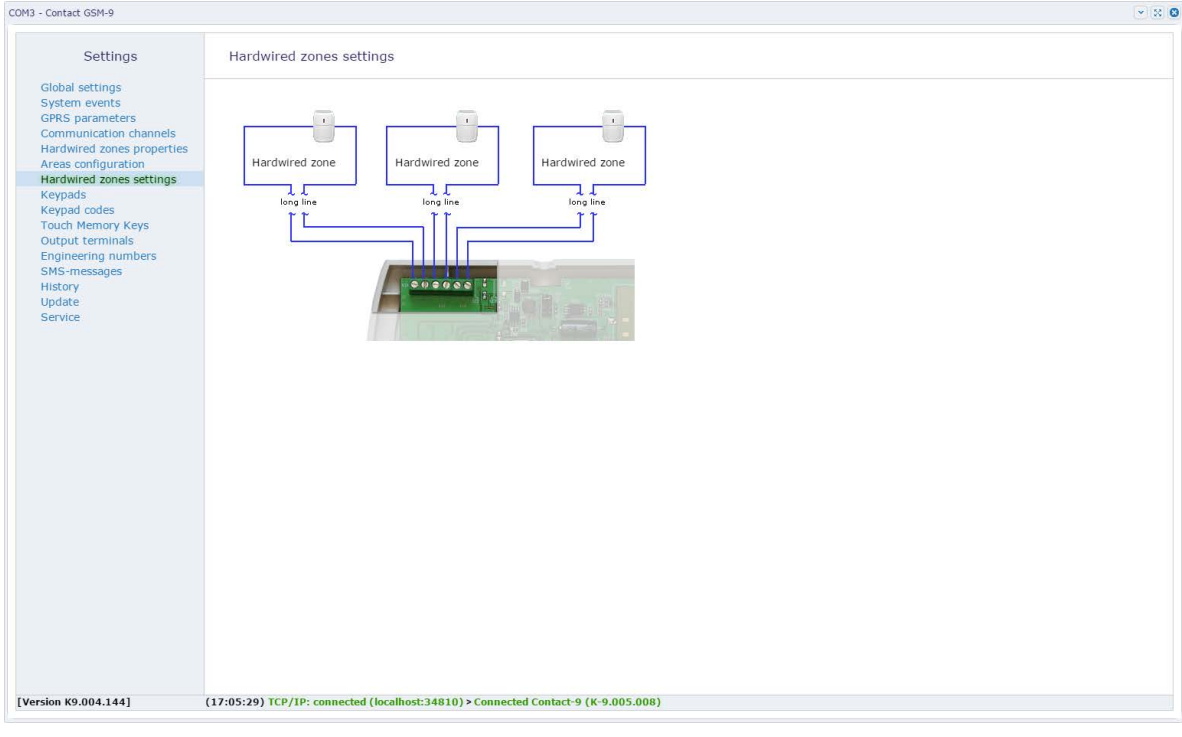

Figure 27. Hardwired zones settings: dry contacts

Temperature

The panel supports connection of temperature sensors with 1-Wire interface. This section (fig. 28) shows the current temperature of the processor and the temperature detected by the connected sensor and allows to set conditions for generating alarm events related to temperature changes.

Two plots show current temperature in real time.

To use a connected temperature sensor it is mandatory to activate "Enable Touch Memory" option in the "Touch Memory keys" section.

Processor temperature, current
Processor temperature measured by a built-in sensor. Currently this option is not used.

Temperature of external sensor, current
Temperature detected by the connected sensor.

Recordin the device events history about the temperature change
Set a value for temperature change to generate the "998.1 — Temperature changed" event. The current temperature detected by the sensor is coded by the zone:

- A zone value from 0 to 199 means positive temperature;
- A zone value from 201 to 399 means negative temperature.

For example zone value of "210" means that the measured temperature is equal to -10 degrees.

Event "Temperature of external sensor is below/above a threshold"
Set threshold temperature values to generate appropriate alarm events. To do this move red and blue dashed lines on the plot.

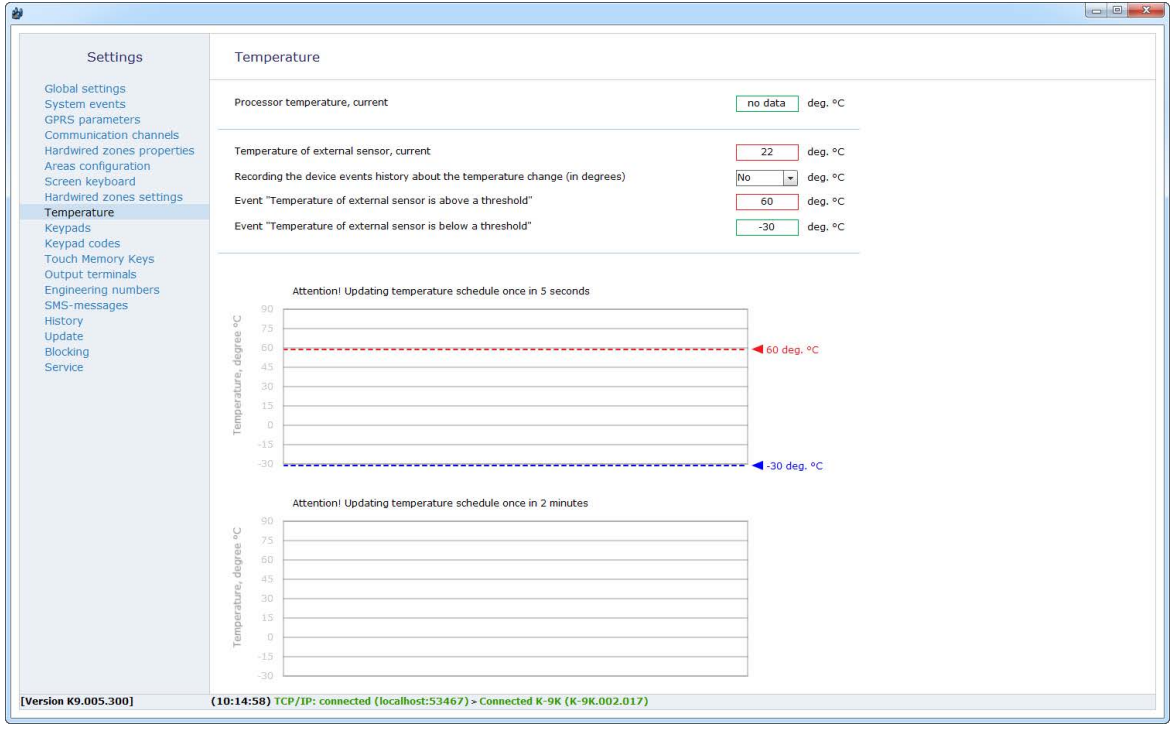

Figure 28. Temperature section

Keypads[12]

This section (fig. 29) allows to configure options for arming areas using a keypad of the “Contact GSM-9N” panel.

The following features are available:

Enable emergency call button

Specifies options for using panic button, fire alarm button and medical alarm button. You can choose the following values:

- Disabled;
- Short push;
- Press for 4 sec.

Key “Stay” — quick arming of chosen areas

To quickly arm certain (outdoor) areas using the Perimeter button without entering the user code, indicate them from the drop-down list.

*Normally, arming using the **Perimeter** button is used when a user wants to stay in an armed room, arming only those areas which are prone to breach.*

*For example, in an apartment, the **Perimeter** button can be assigned to all areas related to entry zones and windows. Your moving inside the apartment does not trigger an alarm.*

Key “Exit” — quick arming of chosen areas

To quickly arm certain (normally, all) areas using the Exit button without entering the user code, indicate them from the drop-down list.

12) For “**Contact GSM-9N/K**” versions only.

Operating mode of indication[13]

Set the desired mode of operation of the keypad indicators:

- Switch on - indication is constantly active in the presence of power;
- Switch on temporarily - specify the time during which indication will be active. After this period of time the indicators will be turned off. To activate indication press any key on the keypad of the device (for example, "Cancel").

Use the "Switch on temporarily" mode to reduce the device power consumption.

13) For "**Contact GSM-9K**" version only.

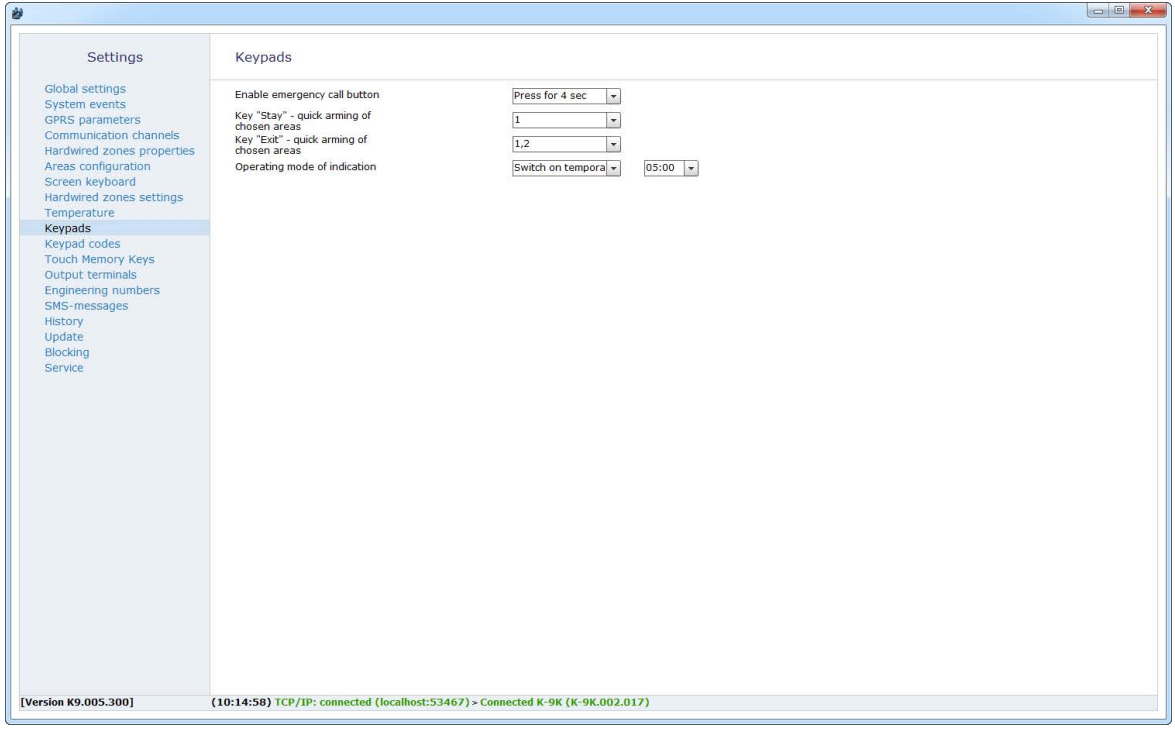

Figure 29. Keypads section

Keypad codes[14]

Arming and disarming areas with the keypad is performed using personal four-digit user codes. The personal code allows to identify users who, among the other actions, disarm the area.

This section allows to configure user access codes to control from a keypad. You can configure up to 10 unique user codes.

The system supports 4-digit access codes where each digit can be between 0 and 9.

Avoid using simple codes such as your phone number, address or combinations like 0000 or 1234.

Do not tell your combinations to third parties.

Keep the code in a secure place or remember it which is better.

Adding a new user code

To add the code click **Add** which displays the code setting line on the page. Specify the following:

- **User code:** specify a unique 4-digit code;
- **Areas** controlled using this code
- **Duresse**: check this box if this code should be used as a duresse code.

If a perpetrator threatens the user to disarm the area you can use the duresse code to disarm the area and send an alarm to the monitoring software. The alarm is not indicated at the area.

Arming the area using this code is done in a regular mode.

14) For "**Contact GSM-9N/K**" versions only.

A number is assigned automatically to any user code and is intended to identify a user who arms/disarms the area.

Removing a user code

To remove the code which is no longer used select it from the list and use the **Delete** link.

Behavior when a user code is entered

Depending on the areas controlled with this code different actions are undertaken:

- Arming the area — if all selected areas are disarmed;
- Disarming the area — in all other cases.

When areas are armed after entering of the user code including the duresse code an event *402.3 — Arming the area* is generated.

When the areas are disarmed (except using the duresse code) the *402.1 — Disarming the area* event is added to the panel history.

When areas are disarmed using the duresse code an event *121.1 — Disarming under duresse* is generated.

The events related to an Area contain the number of the relevant area armed or disarmed, and a # number of user code as the Zone.

Additional security options

Code for changing user codes
This is a special system code which is entered to access the settings (for example, upon remote connection using the configuration software or changing a user code without using a PC).

Changing user code without PC.

You can change the user code using the keypad. Use the following steps to do this.

- *Press the **Cancel** button before entering a command to cancel the digits entered earlier.*
- *Dial the following command on the keypad:*

<Master Code>#4#<Code number>#<New user code><D>#<A>

where: Code numder - a code index (digit from 0 to 9, 0 refers to 10); D - duresse (0 - under no duress, 1 - under duress); A - numbers of arming areas (from 1 to 6).

*For example: 1234#4#1#22220#123456**

*To interrupt the user code change click **Cancel** on the keypad.*

Keypad lockout at setting wrong code

Protection from user code breaking. After three unsuccessful attempts the keypad is blocked for a specified period.
If after expiring the blocking period another wrong code is entered, the keypad is blocked again from the first attempt.

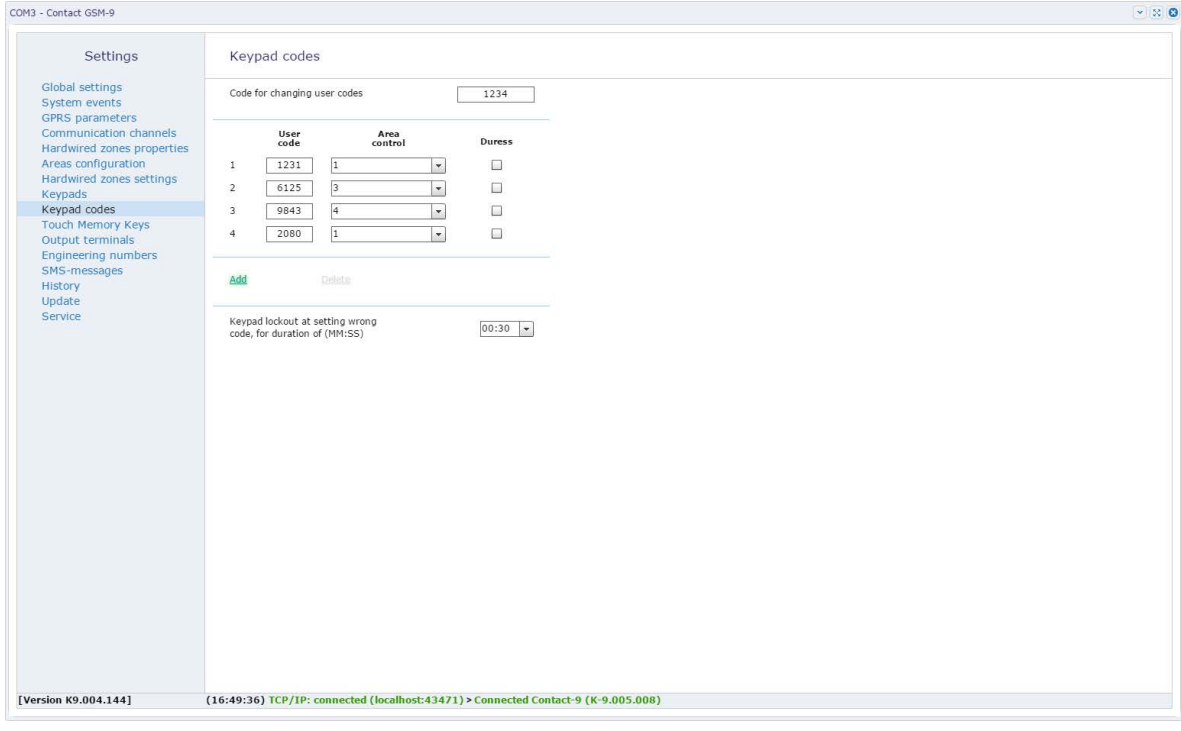

Figure 30. “Keypad codes” section

Touch Memory keys

Upon installing and configuring a reader TM keys and NFC-smart cards allow to both arm and disarm the area.

This section (fig. 31) allows to add, remove and restore keys in the panel memory and configure them.

To enable using the TM check **Enable Touch Memory**.

To set indication of the area at the TM reader LED select the section in the **Reader indicator shows the state of the chosen area** field. The LED can show three states for the selected areas:

- Off: the area is disarmed;
- On: the area is armed;
- Blinks at the frequency of 1 time per second: alarm in the area.

Adding a new key

To add a new TM key to the system click **Add**, type 16-digit key number or touch the key to the TM reader and click **Read the key**.

Additionally in the showed fields define areas for control and specify if the key is a “duresse key” or a RRT[15] member key.

*Key manufacturers can place the key code in a little-endian fashion — **in couples, and in right to left reading!***

For example, instead of a 01D7F30900000007 code the key will dhow the 0700000009F3D701 code.

Removing a Touch Memory key

To remove an unused touch memory key select it from the list and click **Delete** link.

15) RRT - Rapid Response Team. A mobile group, which upon receipt of the alarm carry out an urgent check of the object and take the necessary actions.

Working with smart readers

The panel works with the intelligent smart card readers developed by “R&D Company “Ritm” LLC.

With an intelligent reader, you can use one key to arm / disarm two different types of areas:

- Areas of the "Perimeter" type are specified using the "Areas which intelligent reader refers as perimeter" parameter, and controlled by a double application of the key;
- All areas assigned to this key are specified when the key is added and controlled by its one-time application.

Note that if you connect at least one smart reader to the panel, all other connected readers start working according to the logic of smart one (they will support the double application of the key).

You cannot assign the following types of areas to a key:

- *Areas such as "24";*
- *"Gap" areas (it highlighted in gray on the «Areas configuration» page) – the areas for which no hardwired zone is assigned.*

When assigning "the fire area" to the key, then other types of areas cannot be assigned to such.

Note that the “Perimeter” type areas assigned in this section belongs to the reader only and are not relevant for the areas assigned to the “Perimeter” button on the keyboard (for Contact GSM-9N).

An indication of the smart reader, when it's connected to the **Contact GSM-9N/A/M** panel, is shown in the table below:

Indicator	State	Value
Green	On	All areas are disarmed
	Blinking	Countdown delay for «input/output»
	Off	At least one of security areas is armed
Yellow	On	All sections of the perimeter get armed
	Blinking	No connection to the panel
	Off	At least one of security areas is not armed
Red	On	All sections get armed
	Blinking	Alarm in any area (incl. fire protection areas and «24»)
	Off	At least one of security areas is not armed

The alternating flashing of yellow and red indicators (no more than 5 seconds) means the waiting of panel to apply the key again.

Thus, with the configuration shown in Figure 28, the logic of the operation will be as follows:

*With the **one-time apply** of key allow you to put the areas 1-6 under guard (if all sections are disarmed) or disarm any section under protection;*

*With the **double-apply** of key the sections (1-3) will be armed.*

Note that to manage the perimeter sections, they must be controlled by this key (specify them with checkmarks when adding a key).

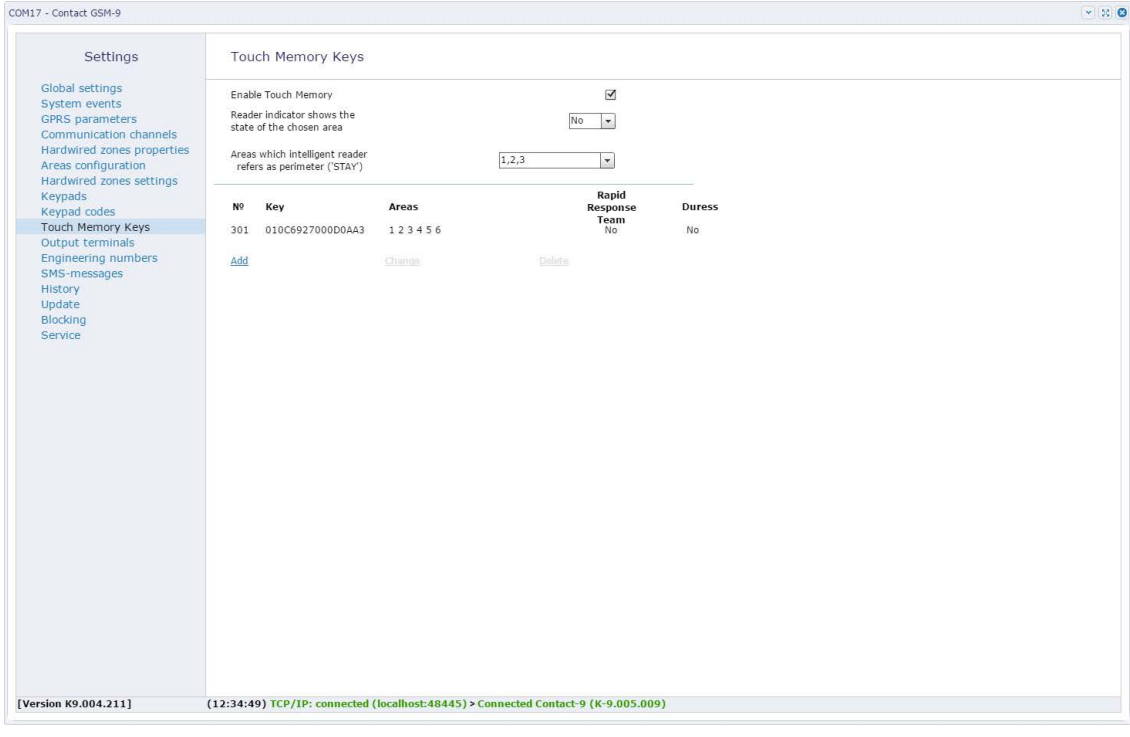

Figure 31. Touch Memory Keys section

Output terminals

This section (fig. 32) is intended for configuring panel outputs. The panel has two open collector type outputs to connect actuation devices, such as sirens and light displays.

OK1 output

OK1 output is designed to connect actuation devices (light displays, indicators). Connected actuation device:

- For **Contact GSM-9N** - duplicates the condition of the areas, assigned to the "Exit" button (in the section "Keypads");
- For **Contact GSM-9A/M** - duplicates the condition of the selected areas (parameter **Indication of area status**);

OK2 output

OK1 output is designed to connect the siren. Operation mode of the siren is configured in the section "Areas Configuration" (parameter **Turn on the siren is case of alarm**).

Siren running time
Set connected siren running time (sec), 30 sec is default.

Turning off the siren with “CANCEL” button on the keypad
Using “Cancel” button to turn off the siren.

Outputs test mode

Click the **Test** link to turn both of outputs into the manual control mode. The mode is intended for testing outputs.

Note that to exit from the test mode requires a restart of the panel.

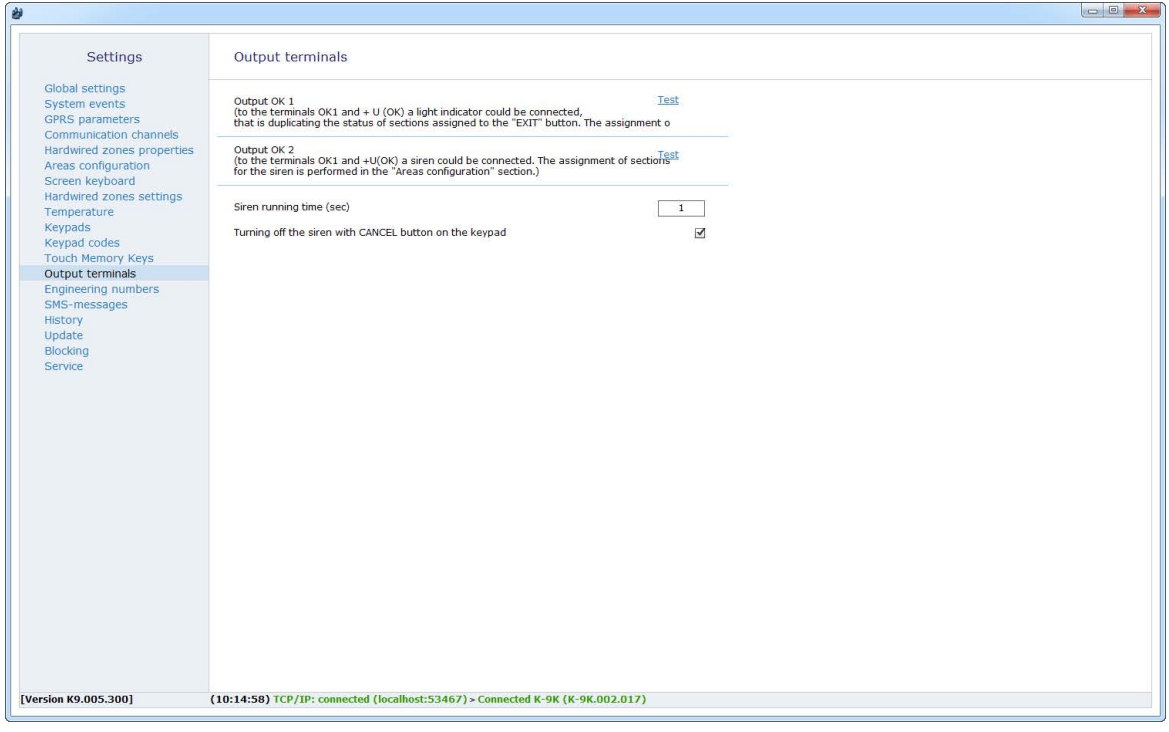

Figure 32. “Output terminals” section

Engineering Numbers

Engineering numbers are used to indicate a list of people who have access to the configuration of the panel via a CSD connection (GSM network).

This section (fig. 33) shows phone numbers from the white list. These numbers can be used for connecting and configuring the equipment.

Setup through a CSD connection is enabled only with designated equipment (modems) and configuration software.

If the box **Turn on the engineer's numbers** is not checked the configuration may be done using any phone number.

To enable configuring of the panel from specific engineering phone numbers only fill in the blank fields in this section in the format used by the communications provider. For example +XXXXXXXXXXX and check **Turn on the engineer's numbers**.

To find out the format that the operator is using for phone number transmission, remove the SIM card from the panel, insert it into a mobile phone and call that number from an engineering number. The incoming call number will be indicated on the mobile phone screen.

*To disable remote configuration via a CSD connection, leave the phone fields blank and check the box **Turn on the engineer's numbers**.*

If the number is not detected, the panel will take the call for 2 seconds, after which the connection will be terminated.

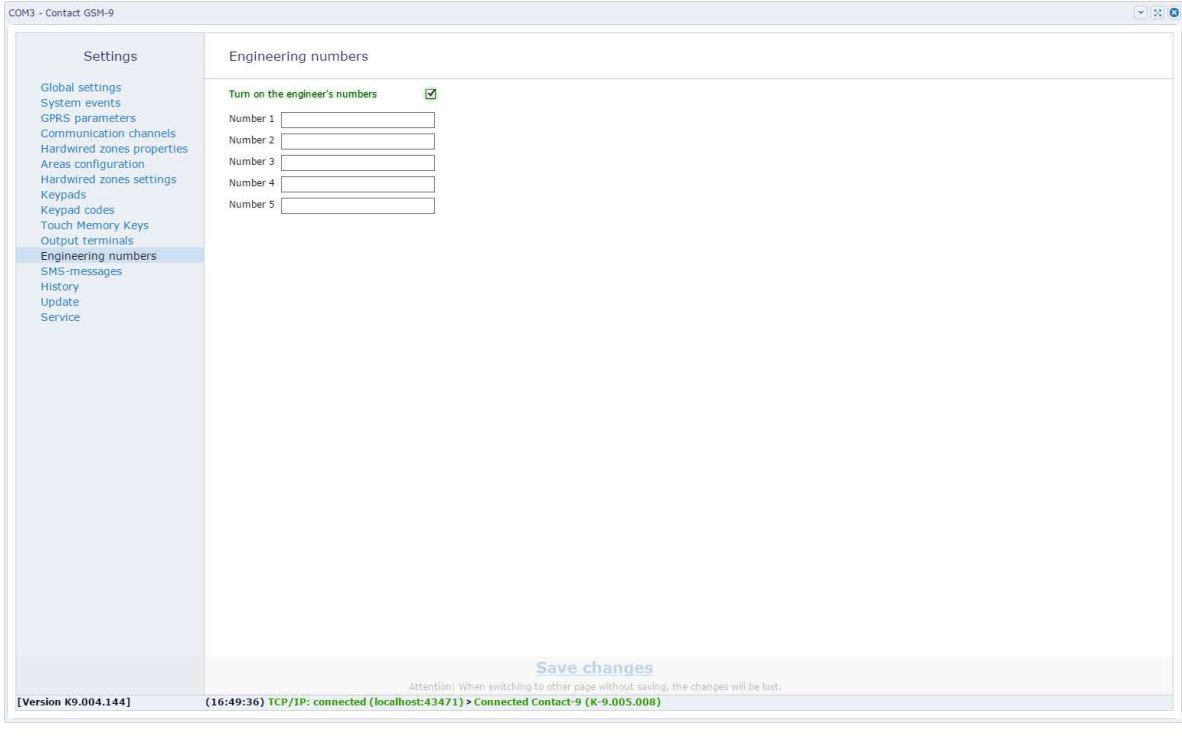

Figure 33. Engineering Numbers section

SMS-messages

When using the **SMS SIM1 (SIM2)** communication channel it is necessary to use a rule of changing the standard machine readable ContactID message into a human readable text.

The message 1234181402010017 is hard to decipher, therefore it should be brought into the form "Disarming area 1 using the key 2".

The manufacturer settings allow using SMS for the user without additional setup. If an event needs to be clarified, pick it from the list and type a new message. To apply the changes click **Save changes**.

The **Download SMS values by default** link resets the added values with those preconfigured at the manufacturer.

Language of the default values depends on chosen language of configuration software.

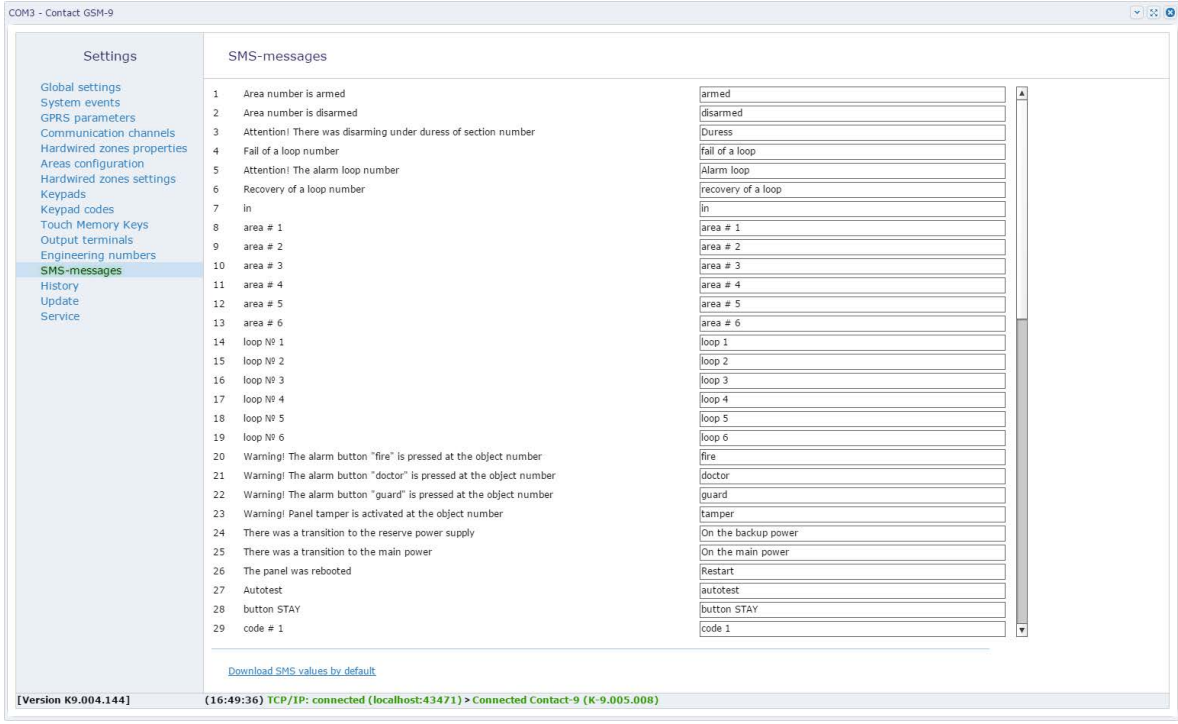

Figure 34. “SMS-messages” section

History

This section (fig. 35) is intended to view history stored in the panel.

Each page can host 20 entries.

The total number of events which can be stored in the history is 65535.

For every event this section shows the following information:

- **#** is an index number of the event (the numbering is consecutive);
- **Time** is date and time of the event in accordance with the built-in clock;

Contact GSM-9K synchronise the time at starting. So when you restart the device (for example, exit the configuration program) the first formed event will be recorded in history with date and time "01.01.2000 00:00:00". The rule applies only in the case installed serviceable battery.

- **Object #** is a number of a guarded facility where the event has been generated (specified on page "Global Settings");
- **Code** is a ContactID event code;
- **A\R** is a type of the event (alarm or recovery);
- **Event** — shows the description of an event;
- **Area** is the number of the area in which the event has been generated;
- **Hardwured zone or TM** — is the number of a hardwired (zone) / user code . TM key involved in the event;
- **Package** — is an event in the form of a ContactID code;
- **CRC** shows whether the checksum is correct;
- **Sent** indicates the information on whether the message was transferred to the necessary directions;
- **Directions** is information about the communication channels which were being used to transmit the event.

The color of the number illustrates which channels from various directions were successfully used to send the events.

- ***Red** are the channels where events were not transmitted;*
- ***Green** are the channels which were successfully used to send the events.*

To update the information click the **Update page** link.

Exporting history entries

The table with the history can be saved on a local computer in the txt format.

To do that specify the number of entries and read them clicking the **Read the records** link.

After that click the link **Export of the read history to txt**.

Deleting history

To delete the history from the memory click **Clear history**.

When deleting history the data is deleted from the panel, the history still remains in the monitoring software.

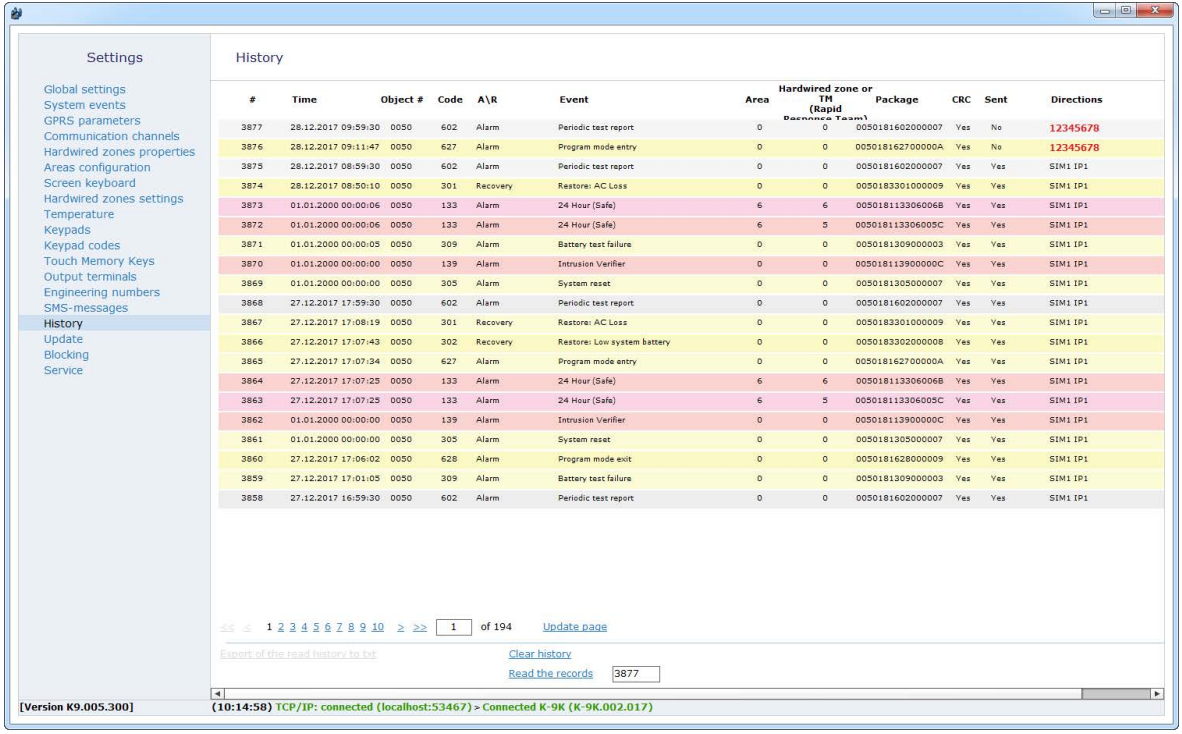

Figure 35. History section

Update

This section enables installation of available panel firmware updates (fig. 36).

Install new versions of the software consistently. Before installing the latest update version download and install all previous versions.

To update the panel software, follow the following steps:

1. Select a firmware version to update.
2. Click “Start updating” to begin downloading the software to the panel.

The panel restarts automatically after firmware installation is completed.

To download the list of available updates into the configuration software, the local PC should have an access to the Internet.

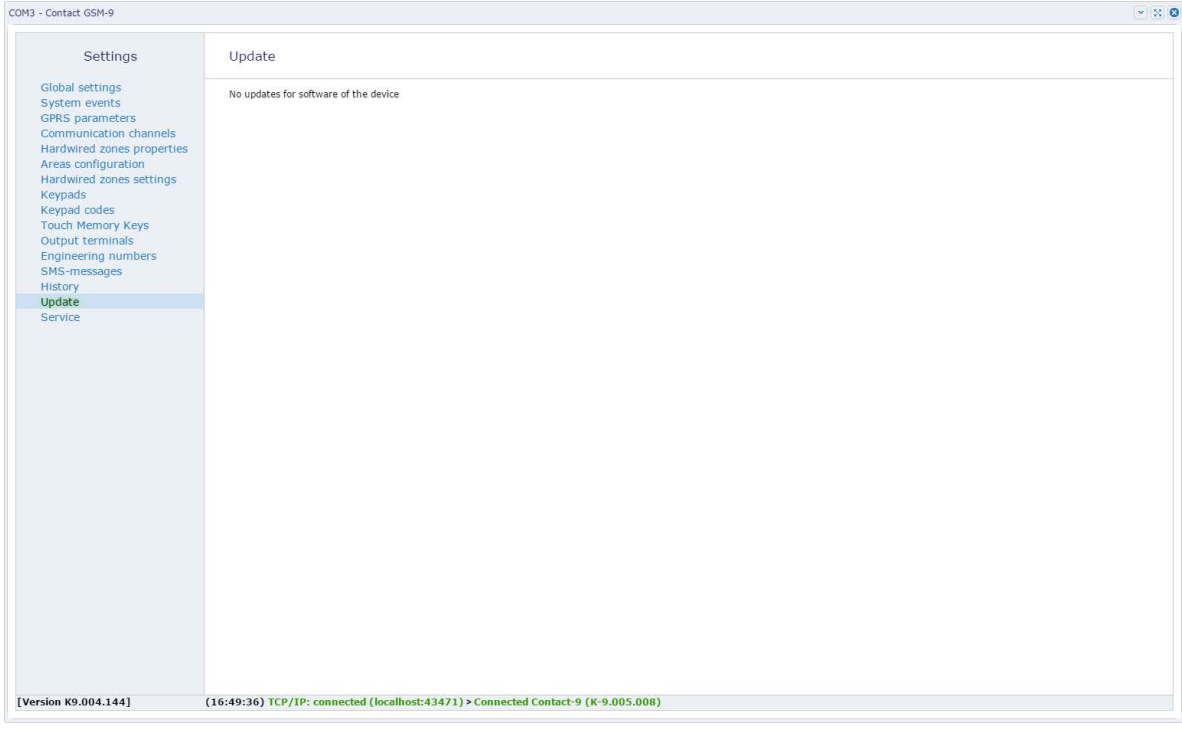

Figure 36. Updates Section

Blocking

This section allows to disable changes of communication channels (fig. 37).

Enabling “**Device blocking for guard service provider**” option disables changes in the “Communication channels” and “GPRS parameters” sections.

To enable or disable blocking you can use the GEO.RITM monitoring software and Ritm-Link only. To enable or disable blocking you can not use third party monitoring software.

This option allows to prevent stealing panels to switch them on other security providers.

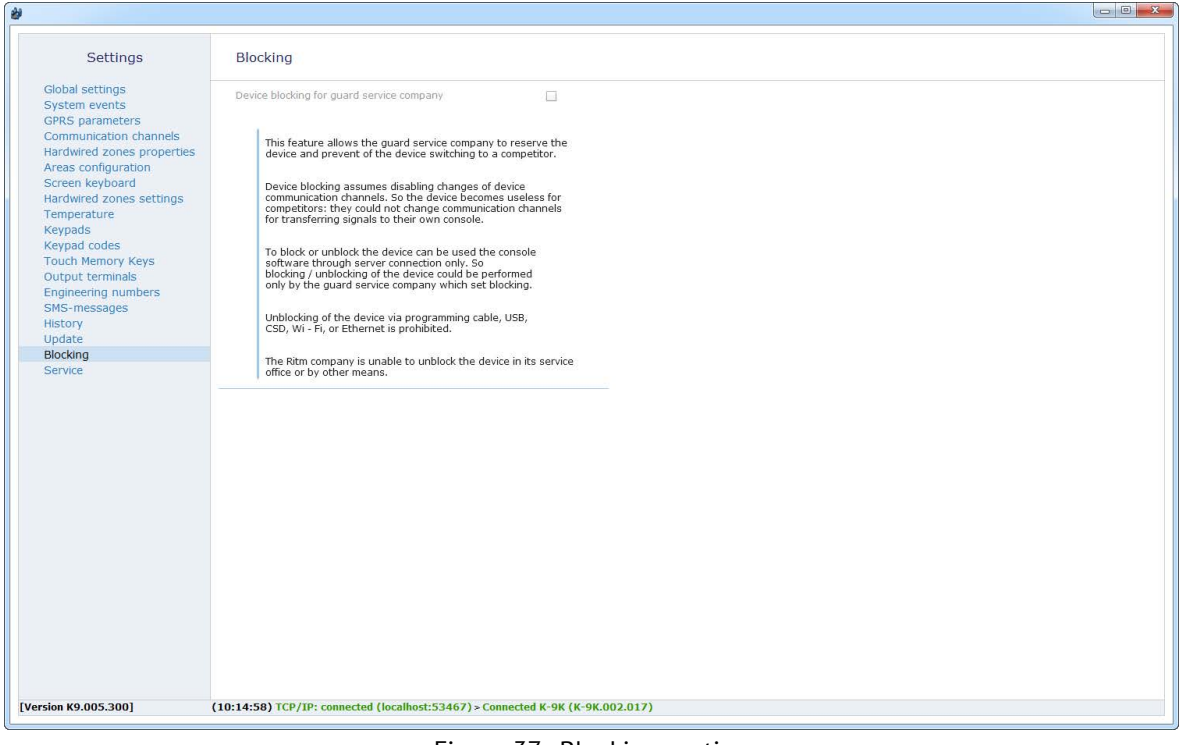

Figure 37. Blocking section

Service

This section (fig. 38) is used to load the panel settings from a file and to save the settings into a file.

Save settings into a file

To create a settings file click the **Read settings from the device** link and wait for the loading to finish. After this click the **Save settings into the file** link and specify where you wish to save the file.

Use the settings file to accelerate setup of a large number of panels or to backup specified settings.

Load settings from the file

To load the settings into the panel from a previously created file use the link and use the path to the settings file.

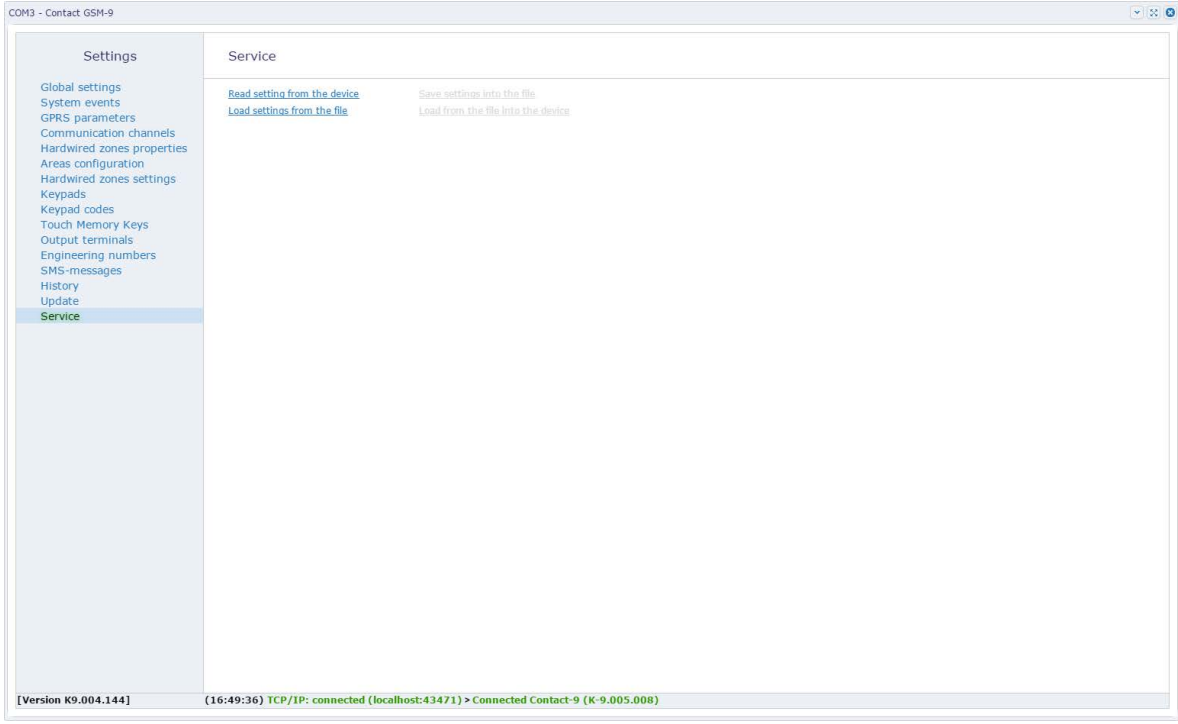

Figure 38. Service Section

Adding to GEO.RITM

Go to eu.ritm.ru or another URL provided by your monitoring service provider.

To add the panel to the account you must enter IMEI of the built-in GSM modem. IMEI is indicated on the GSM modem enclosure and in the section "Global Settings".

If you do not yet have a user account, perform the registration procedure by following the “**Registration**” hyperlink.

Follow the wizard hints during the registration procedure. In case of questions, please refer to “GEO.RITM” document. User Manual.

Log into your account. In the main menu select the “Stationary Objects” section. Click “**Add an object**” (Fig. 39).

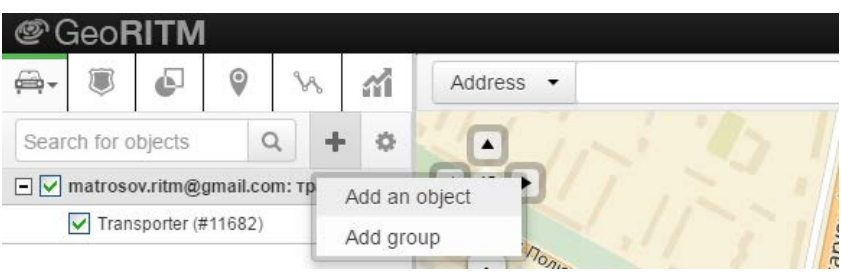

Figure 39. "Add an object" button

Follow the instructions given by the Configuration Wizard. After you finish the add object procedure the new object appears in the “Stationary Objects” section of the main menu.

To show the object on the map please select “Set objects coordinates” and enter the necessary coordinates, or use the mouse to indicate the position of the device on the map. The panel will be shown on the map.

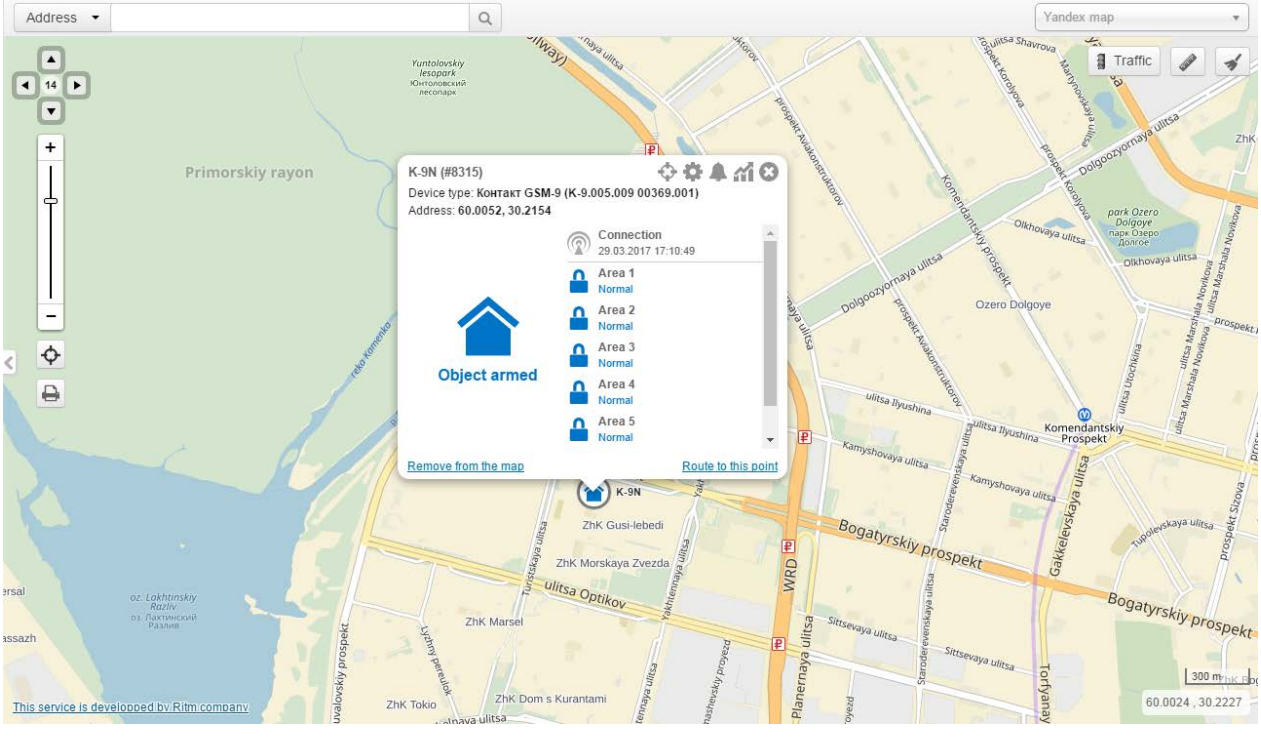

Figure 40. GEO.RITM Service

Maintenance

At least once per month check SIM card accounts for funds.

At least twice per year visually inspect the panel for enclosure or connector damages. Clean the terminals if you find it necessary.

Transportation and Storage

The panel should be transported in packaging in closed vehicles. Storage conditions should conform to those listed in 1K1 under EN 60721-3-1. Transportation conditions should conform to those listed in 1K1 under EN 60721-3-2. Storage premises should be free of current-conducting dust, acid and alkaline fumes, corrosive gases and gases harmful to insulation.

Manufacturer's Warranties

The manufacturer guarantees that the panel complies to requirements of the technical specifications, provided the client ensures compliances to conditions of transportation, storage, installation and operation.

Although the warranty exploitation period is 12 months from the commissioning date, it may not exceed 18 months from the production date.

The warranty storage period is 6 months from the production date.

The manufacturer shall not be responsible for quality of data links provided by GSM operators and Internet service providers.

The manufacturer reserves the right for modification of the panel in any way that does not degrade its functional characteristics without prior notice.

Contact Details

Main office:
Saint Petersburg, Russia, 195248
pr. Energetikov, 30, bld 8.
+7 (812) 325-01-02

Moscow office:
Moscow, Russia, 127051
2 Kolobovskiy per, 13/14
+7 (495) 609-03-32

www.ritm.ru info@ritm.ru

Disposal Note

The panel does not contain precious metals, dangerous or toxic substances possible to harm to health or environment. and does not pose a hazard to life, health or environment after expiration of term of service.

Therefore panel disposal may be performed in accordance with the disposal considerations for general purpose industrial waste.

	Note: Although this product does not contain any harmful materials, we suggest you return the product to the dealer, distributer or directly to the manufacturer after use.

Change history

Revision	Revision date	Description
1.0	25.04.2017	Full revision of document
1.1	31.04.2017	Signs, Product Liability Act, Usual care and caution, Warnings for installation personnel, Safety tips
1.2	28.12.2017	Sections Temperature, Screen keyboard and Blocking were added