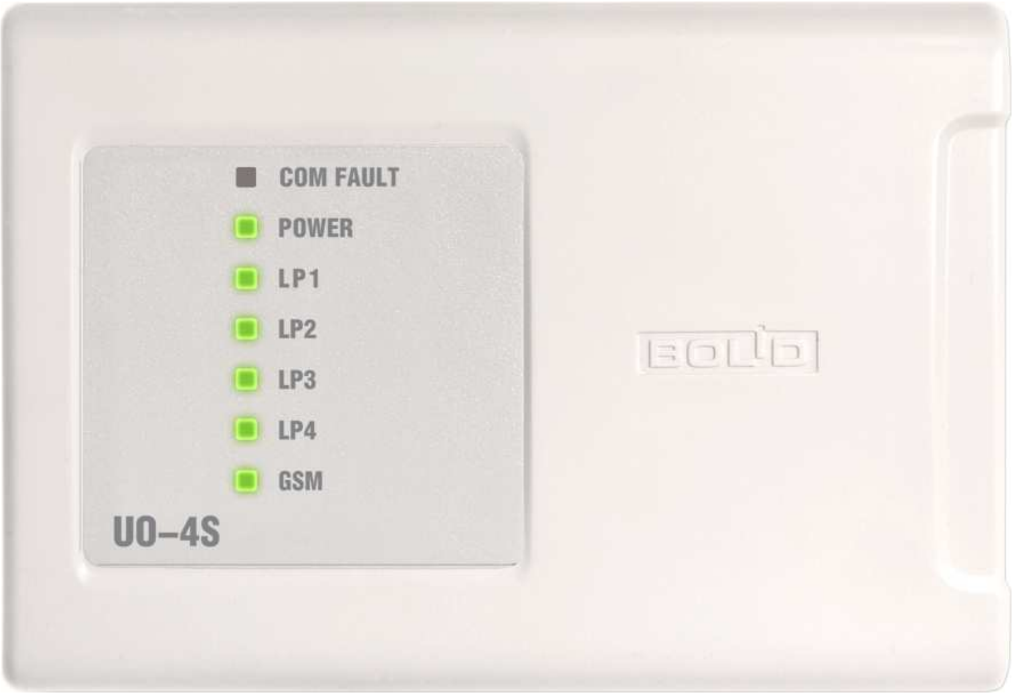
Orion ISS



GSM Four-Input Alarm Panel

ИСО 9001

UO-4S Rev.02

User's Manual

The Bolid Company, Russia; 4 Pionerskaya Str., Korolev, Moscow Region 141070

Tel./Fax: +7 (495) 775-71-55 (PBX), 777-40-20, 516-93-72

E-mail: info@bolid.ru, http://bolid.ru

This User’s Manual is intended to help for studying operability and maintenance principles of **UO-4S Revision 02 GSM Four-Input Alarm Panel**.

⚠ ***Please read the instructions from this manual completely before connecting, adjusting, operating, or maintaining this device***

The following terms are used throughout the Manual:

Alarm Loop: The electrical circuit with non-addressable fire or intrusion detectors (or other non-addressable devices) included. Actuation of a single detector brought in an alarm loop causes activation of the loop as a whole, so the actuated detector can be located only with the accuracy of an alarm loop.

Zone: A minimum part of the security and safety installation that can be monitored and controlled independently. Depending on the context, the term “zone” in an Orion ISS can be understood as an alarm loop, an addressable detector, a monitored circuit of an input module etc.

Partition: A number of zones that can be controlled by user as a whole. As a rule, zones are combined into partitions depending on their locations (e.g., one partition can involve all zones in a single premise)

Arm/Disarm: This action means activation or termination of monitoring of defense zones and triggering alarms

Integration Time: A time interval during which alterations of loop resistance are not considered as loop’s being activated and the alarm loop doesn’t proceed to an alarm status

Network Address (Address): A unique number of the device (from 1 to 127) within a local RS-485 Orion ISS Network

Table of Contents

GENERAL

UO-4S Revision 02 GSM Four-Input Alarm Panel (hereinafter referred to as the UO-4S or the panel) is designed to be used in centralized and standalone intrusion and fire alarm systems for industrial, business, and residential premises (enterprises, banks, offices, hospitals, shops, warehouses, residential buildings, etc.).

The UO-4S can operate both in standalone mode and as part of an Orion integrated security system as a device transmitting notifications through GSM cellular communication channels.

In accordance with classification of Russian Standard ГОСТ Р 53325-2012 the UO-4S rev.02 panel can be used as:

1. An object terminal device;
2. A module in a modular control and indicating equipment consisting of S2000M Monitoring and Control Panel, S2000-SP1 Executive Relay Module, and UO-4S Revision 02 Four-Input GSM Alarm Panel.

For both the applications the UO-4S must be powered by an external battery backed power supply which meets the requirements of ГОСТ Р 53325-2012.

It is not allowed to use relay outputs of the UO-4S to control actuators of automatic fire-fighting equipment.

There are no potential hazard circuits within the panel.

The design of the panel meets the requirements of electric and fire safety in line with Russian Standards ГОСТ 12.2.007.0-75 and ГОСТ 12.1.004-91.

The panel is designed to provide its fire safety while emergency operating and on violations of operation rules in accordance with Russian Standard ГОСТ 12.1.004-91.

Do SHUT OFF power from the panel before mounting, installing, and maintaining this one.

Mounting and maintenance of the panel should be carried out by persons with the second or higher electric safety qualification level.

SPECIFICATIONS

Alarm Inputs (Alarm Loops)	**4 Initiating Device Circuits**
Input voltage in the quiescent mode	6 to 12 V
Integration Time	300 ms
Max current drawing through an alarm loop	12 mA
Max resistance of wires without regards to termination resistance	1 kOhm for intrusion alarm loops, 100 Ohm for fire alarm loops
Min leakage resistance between the alarm loop wires or between each wire and the earth	20 kOhm for intrusion alarm loops, 50 kOhm for fire alarm loops
Outputs	**3 Relay Outputs**
Max Switched Current	1 A dc 0.5 A ac
Max Switched Voltage	24 V dc 100 V ac
Max Switched Power	10 W
External Reader	**Dallas iButton Reader**
Max number of readers connected in parallel	4
Max number of light indicators to be connected to the LED terminal	1
Distance between the UO-4S and the reader	100 m max at wire diameter at least 0.5 mm
Credential Memory Capacity	16 codes
Communication Port	**RS-485**
Protocol	Orion
Non-volatile Event Log	128 events for transmission via GSM channel 60 events for transmission over RS-485 interface
Input Power	**An external uninterrupted power supply**
Rated Voltage	10.2 V to 15 V
Consumed Current	Max values: 150 mA in the quiescent mode 200 mA when sending a notification 1 A is the peak consumed current
Resistance to Climatic Effects	**Category 03 in line with OCT 25 1099-83**
Operating Temperatures	Minus 30°C to +50°C
Relative Humidity	Up to 98% at +25°C
Ingress Protection Rating	IP20
Overall Dimensions	**156 mm × 107 mm × 39 mm**
Weight	About 0.3 kg

STANDARD DELIVERY

Item	Q-ty
UO-4S Revision 02 GSM Four-Input Alarm Panel	1 pc.
Antenna	1 pc.
Installation Manual	1 pc.
Datasheet	1 pc.
iButton	1 pc.
Half-round head woods screw 3×25	3 pcs.
Wall plug 6x30 S	3 pcs.
DIN 7982 flat head tapping screw with cross drive 2.2×6.5	1 pc.
Resistor MF 1/2W-8K2-5%	4 pcs.
UO-4S-to-PC connecting cable	1 pc.

If an external antenna should be installed with the device then the one of the following products can be provided in addition:

Product	Description
Antenna ANT GSM ADA-0071-SMA	GSM dual-band magnetic mount antenna. Gain: 4 dB. Cable length: 2.5 meters.
Antenna ANT GSM ADA-0062-SMA	GSM dual-band glass mount antenna. Gain: 2.5 dB. Cable length: 2.5 meters.
Antenna ANT GSM ADA-0070-SMA	GSM dual-band magnetic mount antenna. Gain: 2 dB. Cable length: 2.5 meters.

The device is not designed to be used in aggressive or dust environments or in explosion hazardous premises. The ingress protection rating is IP20 in line with Russian Standard ГОСТ 14254.

As to resistance to mechanical attacks the device falls into the 03 placement category in accordance with Russian Standard ОСТ 25 1099-83.

As to electromagnetic emission and resistance to industrial radio interference the panel meets the requirements of at least third severity level in line with Russian Standards ГОСТ Р 50009, ГОСТ 30804.4.2, ГОСТ Р 51317.4.3.

The mean time between failures of the device in quiescent mode should be at least 35000 hours which is equivalent to the probability of no failure 0.97 within 1000 hours.

The probability of a failure which can trigger a false alarm response of the device is no more than 0.01 per 1000 hours.

The average lifetime of the device is 10 years.

The content of precious materials: no need to account for the storage, disposal and recycling.

UO-4S rev.02 User’s Manual can be downloaded from the company site http://bolid.ru in the section PRODUCTS at the page of UO-4S rev.02.

OPERATION PRINCIPLES

GENERAL LAYOUT AND MAIN FUNCTIONS

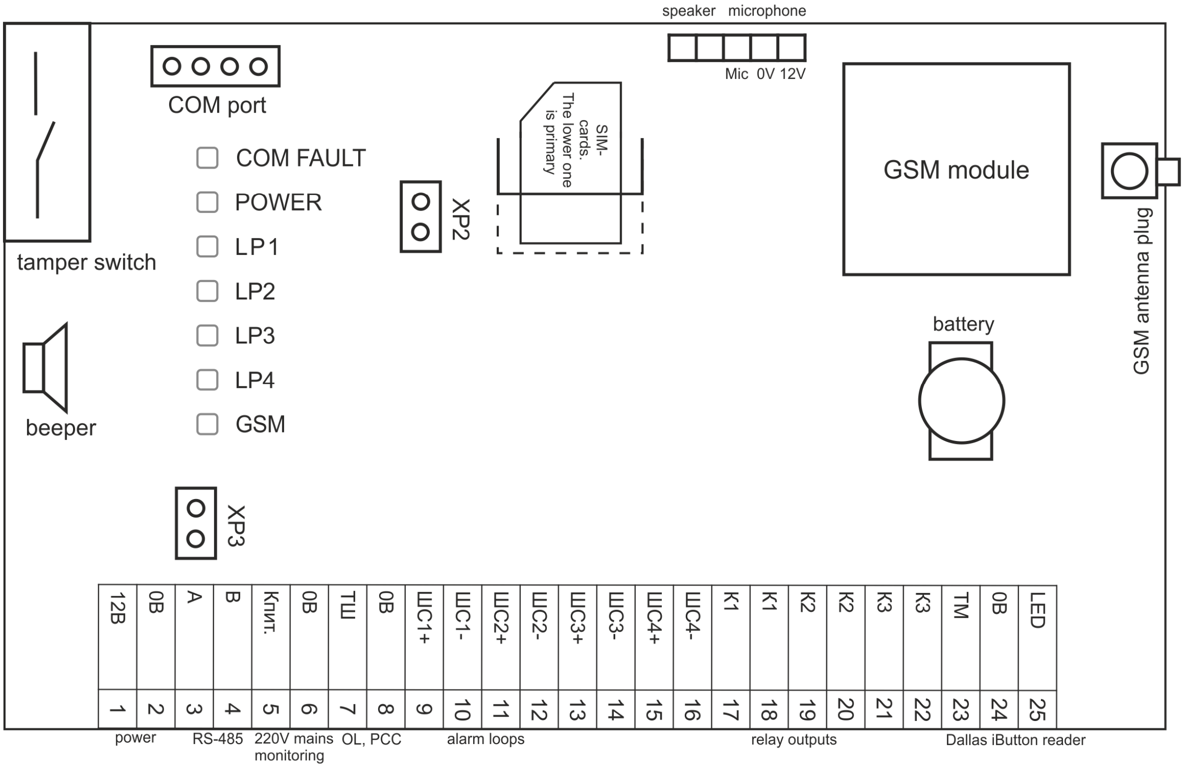


Figure 1. UO-4S Layout

The UO-4S comprises the following hardware elements:

- Tamper switch;
- Beeper;
- Seven information LEDs;
- XP2 Mode Select jumper;
- XP3 620 Ohm pull-up resistor jumper;
- Two slots for primary (the lower one) and backup SIM cards;
- 25-input terminal block for connecting a power supply, RS-485 interface bus, a 220V monitoring circuit, an operating loop, four alarm loops, three actuation devices, and a reader for reading iButtons or Proximity cards;
- Terminal blocks for connecting a microphone/speaker.

The main functions of the UO-4S are:

- Monitors conditions of four inputs (alarm loops).
- Monitors for 220 V mains power conditions (closing the contacts 5 (“Кпит”) and 6 (“0 В”) means a mains failure while opening of these contacts means restoring power conditions).
- Controls three relay outputs depending on conditions of alarm loops and communication channel.
- Provides arming and disarming by means of iButtons or Proximity cards.

- Transmits notifications through GSM 900/1800 cellular communication channels providing backup operation (the second SIM card).
- Provides transmitting to five phone numbers with programming the following notification types for every phone number:
  - Contact ID (ADEMCO),
  - User SMS,
  - Egida-2 SMS,
  - Egida-3 SMS,
  - CSD,
  - CSD (DC-09),
  - GPRS (DC-09)
  - Voice Message,
  - Phone Call.
- Provides filtering messages to be transmitted based on the programmable notification filter.
- Polls Orion system devices and transmits messages from these devices:
  - Under an S2000/S2000M control console or Orion Pro Workstation (Slave 1 and Slave 2 modes),
  - Without a control panel (Master mode).
- Enables remote controlling by received SMS messages:
  - Arming/disarming own alarm loops,
  - Arming/disarming partitions (Slave 1 and Slave 2 modes),
  - Requesting for partition states (Slave 1 and Slave 2 modes),
  - Switching the relay outputs on/off,
  - Changing phone numbers for subscribers,
  - Changing Object Number.
- Provides light and sound indication of conditions of its own alarm loops, power supplies and communication channel; this indication can be disabled.
- Provides sending test messages for link control.
- Provides automatic (and on-request) checking of the balance on the SIM cards.
- Provides protection against reading out the configuration.
- Transmits events about lost/restoring of communication channels with subscribers to the S2000M control panel and to directions for transmission.

OPERATION MODES

The UO-4S provides operation in the following operation modes:

Standalone

This mode is intended for standalone use of the panel. In this mode the UO-4S does not communicate data over the RS-485 interface.

- The UO-4S monitors and transmits only its own states of alarm loops, power conditions, and communication conditions.
- Alarm loops are armed and disarmed by means of a credential, an operating alarm loop, or remotely via GSM channel.

Slave 1, Slave 2

This mode is in use when the UO-4S operates as part of Orion integrated security system under an S2000 or S2000M monitoring and control panel.

Transmitting notifications via UO-4S is supported by S2000 panels of versions 1.12+ and all versions of S2000M panels.

To transmit notifications from an S2000/S2000M panel through the UO-4S, the S2000/S2000M panel should be programmed with the help of ***PProg*** *utility – see the panel's manual.*

The Slave 1 operation mode is to be selected when panels S2000 or S2000M of versions 2.01-2.03 are in use.

For control panels S2000M of versions 2.05 and higher and Orion Pro software 1.11 SP2 and higher the operation mode Slave 2 must be selected.

The UO-4S transmits not physical numbers of zones but unique Contact ID numbers of zones, readers, relays, and state zones of devices which are assigned to these objects in PProg for S2000M control panels of versions 2.04 and higher or added to the UO-4S configuration on Zones and Partitions tab for control panels of lower versions. Numbering of Contact ID zones (relays, device states) in the control panel configuration (in PProg.exe) must be continuous.

When the UO-4S operates in one of the slave modes all the credentials should be enrolled in the control panel (up to control panel version 3.0.3), otherwise all messages about arming and disarming are transmitted without a user number.

When the UO-4S operates in the Slave 1 / Slave 2 operation mode:

- The maximum number of partitions is 99;
- The maximum number of zones is 128;
- The maximum number of user credentials is 255.

Master

This mode is intended for transmitting notifications from such Orion devices as S2000-4, S2000-KDL, Signal-20, Signal-20M, Signal-20P, Signal-10, S2000-ASPT in a system without an S2000/S2000M control panel or Orion Pro workstation.

When the UO-4S operates in the Master operation mode:

- The maximum number of partitions is 99;
- The maximum number of zones is 128;
- The maximum number of user credentials is 255;
- There cannot be two or more UO-4S in the Master mode used in the same network. Also no UO-4S in the Master mode can be used in one network together with a control panel.
- The XP2 jumper (see Figure 1) must be removed (open) for the Master mode. For all other modes (Standalone, Slave 1, Slave 2) the jumper must be put on (closed).

When the UO-4S operates in the Master mode the numbers of all the alarm loops and readers and the addresses of the devices must be enrolled on the Zones and Partitions tab of UProg. Every string number of this tab is considered as the Contact ID number of the zone, reader, or device which is described in this string. The credentials for the connected devices must also be enrolled on the tab Credentials – Global.

If the UO-4S was connected to the PC over the RS-232 interface for programming by means of UProg.exe then for the panel to operate in the modes Master, Slave 1 and Slave 2 the connection cable must be disconnected from the relevant UO-4S port after completing programming.

INDICATION

The UO-4S indicates its conditions in quiescent mode as follows:

Table 1. LED Indication

<table>
<tr><th colspan="2">Conditions</th><th>Indicator Performance</th></tr>
<tr><td colspan="3"><b>COM FAULT LED:</b> Indicates communication conditions for GSM channel and RS-485 interface</td></tr>
<tr><td colspan="2">Normal communications</td><td>Off</td></tr>
<tr><td colspan="2">RS-485 communication fault</td><td>Amber</td></tr>
<tr><td colspan="2">One of the subscribers is not available; no SIM card is present, or the SIM card is not registered on network</td><td>Flashes with amber twice per second</td></tr>
<tr><td colspan="3"><b>POWER LED</b>: Indicates conditions of the power supply</td></tr>
<tr><td colspan="2">Norm</td><td>Green</td></tr>
<tr><td colspan="2">12 V Power Failure</td><td>Flashes with amber twice per second</td></tr>
<tr><td colspan="2">220 V Power Failure</td><td>Flashes with amber once per two seconds</td></tr>
<tr><td colspan="3"><b>LP1÷LP4 LEDs</b>: Indicate states of the relevant alarm loops</td></tr>
<tr><td colspan="2">Disarmed</td><td>Off</td></tr>
<tr><td colspan="2">Armed</td><td>Green</td></tr>
<tr><td colspan="2">Intrusion/Panic/Entrance Alarm[2]</td><td>Flashes with red four times per second</td></tr>
<tr><td colspan="2">Fire Alarm</td><td>Flashes with red twice per second</td></tr>
<tr><td colspan="2">Arming Failed</td><td>Flashes with green once per second</td></tr>
<tr><td rowspan="2">Arming Delay</td><td>Alarm loop is activated</td><td>Illuminating with green flashing with red twice per second</td></tr>
<tr><td>Alarm loop is OK</td><td>Illuminating with green flashing with red once per two seconds</td></tr>
<tr><td colspan="2">Short/Open Circuit Failure</td><td>Flashes with amber once per two seconds</td></tr>
<tr><td colspan="3"><b>GSM LED</b>: Indicates status of the GSM communication channel</td></tr>
<tr><td colspan="2">Normal communications</td><td>Flashes once per four seconds</td></tr>
<tr><td colspan="2">Communication lost</td><td>Flashes 5-8 times every 10 seconds</td></tr>
</table>

Alarm Loop Indicators continue indicating alarms also within two minutes after the relevant alarm loops are disarmed

Table 2. Internal Beeper

Event (Condition)	Beeper Performance
Norm	Off
Alarm, Fire	Interrupted sound *(Can be enabled / disabled via UProg)*
Short/Open Circuit Failure	Beeps once per second
Arming	Two beeps upon arming *(Can be enabled/disabled by means of UProg)*
Disarming	Turns off (if it was on) and then beeps once *(Can be enabled/disabled by means of UProg)*
Arming Delay	Beeps once per two seconds Within 15 seconds before the end of the delay the beeper starts beeping twice per second
Arming Failed	A beep
An unknown credential is presented	A long sound
Saving configuration to the device by means of UProg	A beep
Entering the mode of programming credentials	Three pairs of beeps
Communication Fault*	Beeps once per two seconds
Test is run remotely from the S2000M panel	A long sound

* - *The internal sounder can be disabled for communication line faults in UProg.*

Table 3. Indicators of Reader and Patrol Check Circuit

Event (Conditions)	Indicator Performance
Disarmed (All intrusion alarm loops are disarmed)	Off
Armed (One or more intrusion alarm loops are armed)	Illuminates when power is in norm, otherwise flashes once per two seconds)
Alarm (One or more alarm loops are in Intrusion Alarm, Fire Alarm, Entrance Alarm)	Flashes four times per second
Arming Failed (One or more alarm loops are in the Arming Failed status)	
Arming Delay (One of the alarm loops of the Entrance type is in the Arming Delay status)	Flashes ones per two seconds
Fault (One or more alarm loops are in the Short/Open Circuit Failure status)	Flashes twice per second
12 V Power Failure	Flashes ones per two seconds
First touch by the credential in the quiescent mode (see Note below)	Switches on for a short time three times and then indicates the current state of the alarm loops associated with the current credential (only for reader LED)
Disarming is performed after the second touch by the credential	The indicator is switched off
Arming is performed after the second touch by the credential	The indicator is switched on
Patrol Check	Patrol Check Circuit indicator flashes twice with three flashes
Unknown credential is presented	Indicator of the reader flips its state for 1 s
Programming mode	The indicator is switched off
Master Key Programming mode	The reader indicator is on
Note: *After a single touch by the credential the indicator of the reader within 30 seconds indicates the status of a group of alarm loops associated with this credential. Arming and disarming is performed after a second touch of the reader by the same credential within 30 seconds.*	

The parameter Disable Device Indication in UProg provides disabling of almost all UO-4S indication except for the GSM indicator. If this parameter is set on then the panel regardless of its operation mode doesn’t indicate by sound or by light conditions of its own alarm loops, communication conditions, power conditions, and reading iButtons. Only GSM indicator is active. The parameter has not an effect on reader indication.

ALARM LOOPS

The main configuration parameter of an alarm loop which defines how the alarm loop will be monitored and what kind of initiating devices can be brought into the alarm loop is **Loop Type**:

- **Fire**: A loop of the Fire type is always armed. If a fire detector in the alarm loop kicks in then a ***Fire Alarm notification*** is generated. In case of a short or open circuit failure in the alarm loop a ***Short Circuit*** or ***Open Circuit notification*** is generated respectively. On restoring the alarm loop an ***Armed notification*** is generated. *For a fire alarm loop the parameter Auto Arming After Failures is always applied.*
- **Intrusion**: The alarm loop can be armed and disarmed. If the alarm loop is armed then on activation of this one (in case of short or open circuit failure) an ***Intrusion Alarm notification*** is generated immediately.
- **Panic**: The alarm loop is permanently armed. If the alarm loop is activated (a short/open circuit failure has occurred) a ***Panic Alarm notification*** is generated.
- **Entrance**: The intrusion alarm loop which is armed and disarmed with entrance and exit delay.
- **Operating**: A short circuit failure of this alarm loop results in disarming (an open circuit failure results in arming) of intrusion and entrance alarm loops linked with this loop. Only one alarm loop from the five ones (including LP0) can be of Operating loop type.
- **Patrol Check Circuit**: In case of a short circuit in this loop a ***Patrol Check notification*** is generated (This alarm loop type can be given only for LP0).
- **Phone Call**: The short circuit in the loop results in a phone call.

Auto Arming:

The intrusion types of alarm loops (Intrusion, Entrance, Panic) provide arming the alarm loops after being in alarm and after failures automatically. A procedure of auto arming is performed on expire of a delay programmed in the UO-4S configuration. To reset the status of a fire alarm loop after activation also the parameter of auto arming after alarms should be set on.

Protecting Common Areas

To protect common areas, the alarm loops can be combined into an operating group:

- All the operating alarm loops are armed -> the operated alarm loops are armed
- If at least one of operating alarm loops is disarmed -> the operated alarm loops are disarmed

Table 4 shows how resistance values of the alarm loops match their states for alarm loops of various types.

Table 4

Loop Type	**Loop State Depending on the Loop Resistance**			
	OK	Activated	Open Failure	Short Failure
Fire	2÷14 k	17 k÷50 k 500 Ω÷1,6 k	>50 k	<200 Ω
Intrusion, Panic, Entrance	2÷14 k	<1.6 k >17 k	------------	----------------

For the purpose of protection against sabotage, after the intrusion alarm loops are armed they are monitored for changes their resistance with time. If the alarm loop resistance jumps more than 10% then the alarm loop is considered to be activated.

RELAY CONTROL

The UO-4S supports eight tactics of controlling its relays (see Table 5). For all the tactics apart from **Remote Control** and **Communication Failure** operation of a relay depends on the selected control tactics and states of the alarm loops associated with this relay. For all the tactics except for Lamp, Communication Failure, and Switch Off upon Arming* a time in the range of 1 to 254 seconds must be defined for which the relay will be switched on or the relay will be operated permanently until the state of the related inputs (alarm loops) changes; the Lamp tactics regardless of the given time is always applied until input’s state changes. For all the tactics of control excluding Remote Control it is necessary to tick the alarm loops associated with this relay.

Table 5. Relay Control Tactics

Tactics «Lamp»*	
All the alarm loops are disarmed	Off
There is an alarm loop armed	On
Fire Alarm	On/Off with a period of 0.25 s
Intrusion Alarm Entrance Alarm Arming Failed	On/Off with a period of 0.5 s
Loop open circuit failure Loop short circuit failure	On/Off (0.25 s on, 1.75 s off)
Tactics «Confirmation»	
All the alarm loops are disarmed	Off
Waiting for a confirmation	On/Off with a period of 2 s
A confirmation is received	On
Fire Alarm	On/Off with a period of 0.25 s
Intrusion Alarm Entrance Alarm Arming Failed	On/Off with a period of 0.5 s
Loop open/short circuit failure	On/Off (0.25 s on, 1.75 s off)
Tactics «Siren»	
The loop(s) in Fire Alarm	On/Off (1.5 s on, 0.5 s off)
The loop(s) in Alarm	On
Other states	Off
Tactics «Lock Control»	
A short circuit of the disarmed alarm loop	On, after opening the alarm loop the relay is turned off in 4s
Disarming of the alarm loop(s)	The relay is turned on for 4 s

Table 5 (continued)

Tactics «Alarm Output» **	
All the alarm loops are armed	On
Otherwise	Off
Tactics «Switch Off upon Arming»***	
A command to arm the alarm loop is given	The relay is turned off for a time
Otherwise	The relay is turned on
Tactics «Remote Control»	
An SMS-command to turn the relay on has been received	The relay is turned on for a given time; if no time is given then the relay is on steady
An SMS-command to turn the relay off has been received	The relay is turned off
Tactics «Communication Failure»****	
Normal communication with subscribers	Off
Loss of communication at least with one subscriber	On

* *When the tactics «Lamp» is used with fire and panic alarm loops the relay is turned off when the alarm loop is OK because fire and panic alarm loops are always armed.*

** *Tactics «Alarm Output» doesn't operate with fire alarm loops, i.e. the relay changes its state neither in case of a fire nor in case of an open/short circuit failure of the alarm loops.*

*** *The time for which the relay will be turned off can be set in the limits of 1 to 80 conventional units provided that one conventional unit of the parameters is equal to 0.125 s. For example, in order to give time for the relay to be turned off to 5 seconds the value of 40 should be entered (for a fire alarm loop the relay can be turns off only on being armed by iButton from such state as Disarmed or Fire Alarm credential to perform power-on reset for the detector).*

**** *Tactics «Communication Failure» may not work is the subscriber uses Who Called service of similar. Also the tactics is not operable in case of using SMS-protocols.*

For tactics «Switch Off upon Arming» and «Lock Control» the relay can be linked only with a single alarm loop.

CREDENTIAL PROGRAMMING MODE

The UO-4S can operate partitions by means of credentials. The panel can be programmed for using credentials by means of UProg or immediately in the mode of programming credentials. To switch the UO-4S to the credential programming mode, the Master Key should be used.

In the process of programming the Master Key all previously saved credential data are cleared.

The Master Key is not designed for arming and disarming.

Programming the Master Key:

1. Disarm all alarm loops assigned with the Intrusion and Entrance types.
2. Power off the UO-4S.
3. Use a piece of wire to couple the contacts of the UO-4S reader and keep the contacts coupled.
4. Power up the UO-4S.
5. Wait until the panel issues the Master Key Programming signal (***two short double beeps and then one long sound***).
6. Open the contacts of the reader of the UO-4S and then quickly, within no more than 10 seconds briefly touch the UO-4S reader by the iButton. The panel beeper issues **a beep**. It means that the Master Key is written to the UO-4S memory.

7. Quitting the mode of programming the Master Key is performed by short closing the reader contacts for 4 seconds or automatically in 30 seconds after completing configuring operation. In this case **the panel issues one beep and then one long sound signal**. Quitting can also be performed by shutting the power off.

Programming credentials for arming and disarming alarm loops without using a PC:

1. Disarm all the alarm loops with the types Intrusion and Entrance.
2. Enter the mode of programming credentials by touching the UO-4S reader by the Master Key; the UO-4S shall issue the signal of proceeding to the programming mode **(three pairs of double beeps**).
3. Briefly touch the UO-4S reader by another iButton. The iButton code shall be entitled in the UO-4S memory and the beeper **beeps twice.**
4. Light indicators LP1÷LP4 show the number of programmed credential in binary code (see Table 6) and then after two seconds they show the states of the related alarm loops.

Notes:

– *If the credential code has already been in the panel memory then the beeper issues a **short Confirmation sound**.*

– *If the credential memory is full (16 credentials has already been enrolled) then the beeper issues a **long Error signal**.*

5. Define the match between the credential and the alarm loop(s) by brief closing of the relevant alarm loop. If the LED related to the alarm loop illuminates it means that the alarm loop can be operated by this credential.
6. To confirm programming, briefly touch the UO-4S readers by the same credential. The credential authorized to arm and disarm will be saved in the device memory.
7. To program the panel for using other credentials, repeat steps 3–5.
8. To quit the mode of programming credentials, close the reader terminals for 4 seconds, or the panel quits this mode automatically in 30 seconds after last operation. **The beeper beeps once**. Quitting can also be performed by shutting the power off.

Table 6. Indicating User Number by Alarm Loop LEDs

#	LP1	LP2	LP3	LP4	#	LP1	LP2	LP3	LP4
1	●	○	○	○	9	●	○	○	●
2	○	●	○	○	10	○	●	○	●
3	●	●	○	○	11	●	●	○	●
4	○	○	●	○	12	○	○	●	●
5	●	○	●	○	13	●	○	●	●
6	○	●	●	○	14	○	●	●	●
7	●	●	●	○	15	●	●	●	●
8	○	○	○	●					

Deleting Arming / Disarming Credentials

1. Disarm all the Entrance and Intrusion alarm loops.
2. Enter the mode of programming credentials by touching the UO-4S reader by the Master Key. The panel shall issue the signal of proceeding to the programming mode (three pairs of double beeps).

3. Holding the Master Key touched to the reader press the tamper switch (see Figure 1) down for a short time (no longer than 0.5 s) and then remove the Master Key. POWER LED shall flicker periodically (two times per second with pauses of 1 second) indicating the mode of deleting credentials.
4. By short presses on the tamper switch select the number of the credential. Indicators LP1÷LP4 shall show the number of the credential.
5. Press the tamper switch and hold it pressed for 5-8 seconds. When the credential descriptor is deleted from the panel memory the beeper will issue **two beeps and then one long sound**. If there is no credential with such number in the panel memory then the panel issues the Error signal (**single long sound**).
6. To delete another credential descriptor, repeat the procedure starting with the step 4.
7. To quit the mode of programming credentials, close the reader terminals for 4 seconds, or the panel quits this mode automatically in 30 seconds after last operation. **The beeper beeps once**. Quitting can also be performed by shutting the power off.

ARMING AND DISARMING BY MEANS OF DALLAS IBUTTONS

To arm and disarm an alarm loop or a partition by means of an iButton, a double touch tactics is used.

First Touch

Within 30 s after the first touch the indicator of iButton reader indicates status of the alarm loops or partitions associated with this credential (см. Table 3. *Indicators of Reader and Patrol Check Circuit*).

Second Touch

The second touch should be performed within no longer than 30 s after the first touch.

Credential with Authorities to Arm/Disarm

- If all the alarm loops associated with the credential are disarmed or in the **Arming Failed** state then a process of arming is started.
- If at least one alarm loop associated with the credential is armed or in the **Alarm** state then a process of disarming is started (a process of arming will be started upon next touching).

Credential with Authority to Arm

- If at least one alarm loop associated with the credential is in the state **Disarmed**, **Arming Failed**, **Alarm** then a process of arming is started.

Credential with Authority to Disarm

- If at least one alarm loop associated with this credential is in such state as **Alarm, Arming Failed, Armed** then the process of disarming will be started.

Fire and panic alarm loops are always armed, so the rules mentioned above are not applicable to them.

CONTROLLING UO-4S REMOTELY BY SMS

To control the UO-4S remotely it is necessary to send an SMS with a relevant command to the UO-4S phone number (the phone number of the currently active SIM card) – see Table 7.

Table 7. Remote Control Commands

Commands	SMS Messages
Request for Armed Loops The response will be one of the following: – If there are armed alarm loops: S,S **Armed** – If no alarm loop is armed: **Disarmed**	PXXXXX**q**
Request for Partition Status Maximum 8 partitions in a single request	PXXXXX**qpP,P**
Arm (to arm the specified local alarm loops of the UO-4S)	PXXXXX**a**SS…
Disarm (to disarm the specified local alarm loops of the UO-4S)	**P**XXXXX**d**SS…
Arm Partition (only for Slave 1 / Slave 2 modes)	**P**XXXXX**ap**C…
Disarm Partition (only for Slave 1 / Slave 2 modes)	**P**XXXXX**dp**C…
Activate Relay (to switch the relay on for a time, to switch the relay off) Only a relay of the Remote Control type can be activated remotely	**P**XXXXX**r**NY**t**Z
Confirmation (the response from a central monitoring station for an arming SMS)	**P**XXXXX**k**
Set Time (if necessary to correct the time)	**P**XXXXX**t**hhmm
Set Time and Date	**P**XXXXX**t**hhmm**d**DDMM
Set Object Number	**P**XXXXX**n**IIII
Check Balance (to receive the status of the balance on the active SIM card of the UO-4S)	**P**XXXXX**m** <carrier's code>
Check Balance (to receive the status of the balance on the specified SIM card of the UO-4S)	**P**XXXXX**b**Q <carrier's code>
Change Phone Number (to change the specified phone number)	**P**XXXXX**cn**K<phone number>
Change Phone Number (to change the own phone number)	**P**XXXXX**c**<phone number>

Where:

- **XXXXX** stands for a five-digit user's password
- **P** stands for a partition number
- **S** stands for a number of an alarm loop (1 to 4)
- **C** stands for a partition number (1-99)
- **Y** can take a value "1" for "switch on" or "0" for "switch off"
- **N** stands for a relay number (1-3)
- **Q** stands for a sequential number of a SIM card (1-2)
- **K** stands for a subscriber sequential number (1-5)
- **IIII** stands for an object number (4 digits)
- **Z** stands for a time in seconds. The maximum value is 255 (in no time is defined or the time is equal to zero then activation time is not limited)
- **P**, **a**, **m, d**, **q**, **r**, **k**, **t, c, b, n** are the characters typed from the keypad
- **hhmm** means the hours and minutes while **DDMM** designates the day and the month
- **<carrier's code>** is the code of the carrier to check the account balance, for example *100# or *102#, it should be specified for a particular carrier in a particular region, for example P12345m*100#. The bal-

ance can be checked among others also for post-paid cards (in this case and answer can be received in two parts namely as a USSD message about receiving a request and an SMS with the balance status).

If no response has been received for account balance requests then you need to change SMS notification service to USSD.

Examples of the commands:

P12345**a**14 is the command to arm the alarm loops 1 and 4 of the UO-4S, the user password is 12345
P34563**d**134 is the command to disarm the alarm loops 1 and 3 of the UO-4S, the user password is 34563
P12345**ap**12 is the command to arm the 12th partition;
P45321**r**11**t**10 is the command to switch the relay 1 on for 10 seconds, the user password is 45321
P45321**r**10t0 is the command to switch the 1st relay off, the user password is 45321
P12345**b2*100#** is the command to request the balance on the 2nd SIM card of the MTC carrier
P12345**n**1234 is the command to set the object number
P12345**t**1345**d**1304 is the command to set the time and date (the 13th of April, 13:45)
P12345cn3+123456789 is the command to change the phone number of the 3rd subscriber for the number +123456789
P12345cn3123456789 is the command to change the phone number of the 3rd subscriber for the number 123456789
P12345c123456789 is the command to change the own phone number for the number 123456789
P12345qp12,34,56,78 is the command to request for status of the partitions 12, 34, 56, 78

Table 8. Responses for Control Commands

Responses	In Cyrillic Characters	In Latin Characters
Relay N Activated	Реле включено N Реле выкл. N	Relay is on Relay is off
Time Set	Уст. времени	Time set
Time and Date Set	Уст. времени	Time set
Object Number Set	Номер изменен	Set number
Phone Number Changed	Замена номера	Phone set
Confirmation	Квитирование	Receipt
Wrong Password	Неверный код	Wrong password
Command Failed (an unknown phone number, a parameter error of the command in the SMS)	Нет доступа	No access
Relay Control Denied	Нет доступа	No access

* – *A response to a request for partition status comes in the Egida-3 SMS protocol (for example, F99I0255S241P10) and is intended for operation in Egida-3 Central Monitoring Station software)*

** – *The response is generated in Latin symbols if extended character set is not in use by the panel (that is there are no Cyrillic characters in parameter and event descriptions)*

INSPECTING PANEL OPERATION IN THE TEST MODE

In the Test mode the panel inspects operation of its light indicators and beeper. The panel can be switched to the Test mode only from the menu of the control panel and only for S2000M of versions 3.0 and higher (for more information please refer to S2000M User’s Manual).

After the panel has entered the test mode:

- The panel beeps;
- The indicators COM FAULT, POWER, LP1 - LP4
    1. *Illuminate with amber, then*
    2. *Illuminate with green, then*
    3. *Illuminate with red, then*
    4. *One-by-one turns on with green, and finally*
    5. *One-by-one turns on with red.*

After the test has been completed the panel automatically exits the self-diagnostic mode and returns to quiescent mode.

TRANSMITTING NOTIFICATIONS

Notification Formats

The UO-4S can transmit notifications to five phone numbers and for each number a notification format can be programmed individually:

- Contact ID (ADEMCO) – Appendix A;
- User SMS – Appendix B;
- Egida-2 SMS – Appendix C;
- Egida-3 SMS – Appendix D;
- Voice Message – Appendix E;
- Phone Call;
- CSD;
- CSD (DC-09).

Contact ID (ADEMCO)

This notification type is used to transmit events via voice channels to central monitoring stations. The list and format of notifications is shown in Appendix A. An UOP-3 GSM can be used as a receiving device.

User SMS

The panel supports transmitting user messages both in Cyrillic and Latin characters and provides editing them by means of UProg (using Latin character provides more cost-effective way to send SMS).

Depending on the mode the device operates in the data transmitted in user SMS vary in follow aspects:

Standalone Mode: messages are sent with specifying alarm loop numbers:

Object Name, DD-MM (optionally) HH:MM, Event, LP, Zone Description (optionally)

Object Name, DD-MM (optionally) HH:MM, Event, User Number, User Description (optionally)

Slave 1, Slave 2, Master Mode: messages are sent with specifying numbers of partitions and zones:

Object Name, DD-MM (optionally) HH:MM, Event, Partition Number, Zone Number, Zone Description (optional)
Object Name, DD-MM (optionally) HH:MM, Event, Partition Number, User Number, User Description (optional)

The list of messages is shown in Appendix B.

SMS (Egida-2), SMS (Egida-3)

Transmitting SMS to a central monitoring station with Egida rev.02 or Egida rev.03 software respectively. Notification formats are shown in Appendix C and Appendix D. Receivers can be an UOP-3 GSM and a GSM modem. Description of SMS for the protocols Egida-2 and Egida-3 is not available for editing by user.

Voice Messages

All voice messages begin with the phrase “Attention, the message from the object number…” followed by the code of the object and the text of the message itself. The panel cannot synthesize object descriptions by voice, so the messages contain only the numbers of partitions, zones, and users (credentials).

⚠ *A voice message for a current direction is considered to be delivered if it has been heard in full including the given number of message repeats. Otherwise the UO-4S will try to establish communication once more and to transmit the notification so many times as defined for the voice message notifications.**

*** If the Who Called option (or similar) is activated for the subscriber then the number will not be called repeatedly.*

Phone Call

For this notification type the UO-4S dials to the subscriber and hangs up; this type of notification is used to inform the subscriber that an event has happened without describing the event.

CSD (DC-05)/CSD(DC-09)

If this type of notifications is selected then data are transmitted via GSM network over the fax-data channel in digital form with the rate of 9.6 Kbit/s. A receiver can be UOP3-GSM or GSM modem for CSD (DC09).

⚠ *Many carriers can transmit and receive data via CSD only after special connecting of this service.*

GPRS (DC09)

Notifications are transmitted using GPRS in the protocol «DC-09» to a specified IP address and port. Data can be received on a PC immediately (without panels) provided that Egida-3 Central Monitoring Station software or other software supporting this protocol is installed on the PC.

If the transmission over GPRS is enabled it is of the highest priority in its group. While operating via GPRS, by default data are encrypted using the default key (encryption keys are adjusted in UProg.exe and Egida-3) provided that encryption can be disabled when necessary.

Filtering

To minimize data to be transmitted and to provide receiving only the required information, an event filter can be adjusted for every subscriber number. The filter criteria are alarm loop numbers (for the standalone mode) and types of event.

Grouping

To provide redundancy, phone numbers can be combined into groups. If a group number is the same for all phone numbers then the panel will transmit notifications only to one number from the group, namely the first number which the panel has reached. If group numbers are different then the UO-4S will consistently transmit notifications for all phone numbers assigned with different group numbers.

Testing Communication Channel

Test notifications are intended for testing current operability of the communication channel and can be applied for phone 1 and phone 2. A Test notification can be either SMS (a transmission period in hours should be specified) or a phone call (a call period can be set in minutes or in hours or a time for calls once or twice a day should be specified).

Test notifications must comply with notification type selected for the relevant subscriber. That is, if User SMS are in use then Test notifications should also be SMS while if voice calls, ID Contact, and CSD are in use then Test notifications should be phone calls. Phone calls are also permitted to be used as Test notifications for operation with Egida-3 Central Monitoring Station using Egida-3 SMS notification type.*

** If the Who Called (or similar) service is active for the subscriber then the panel will consider a test call as successful and this can affect the results of testing the quality of communication channel with the relevant subscriber.*

Apart from the option “Phone call at a specified time”, Test Transmission Period starts to be counted since the moment of last transmission of any notification to the relevant phone.

In the mode of phone calls on receiving a Test notification a subscriber takes the call. This confirms for the UO-4S that the notification is received and the panel releases the phone line. *The call time doesn’t exceed two seconds and as a rule is not charged by the carrier.*

If at the time of sending a test notification the subscriber is not available or no answer is received from the server while operating via GPRS the panel generates the event of communication loss for this channel and transmits this event to other subscribers and to the S2000M control panel (while operating in a slave mode).

MOUNTING THE DEVICE

Figure 2 shows the appearance and overall and mounting dimensions of the UO-4S panel. The panel is to be mounted on walls or other structures in the premises at places protected against atmospheric fallouts, mechanical damage, and unauthorized access.

Wiring of connecting lines is to be carried out as shown in Figure 5 (“UO-4S Connection Diagram”).

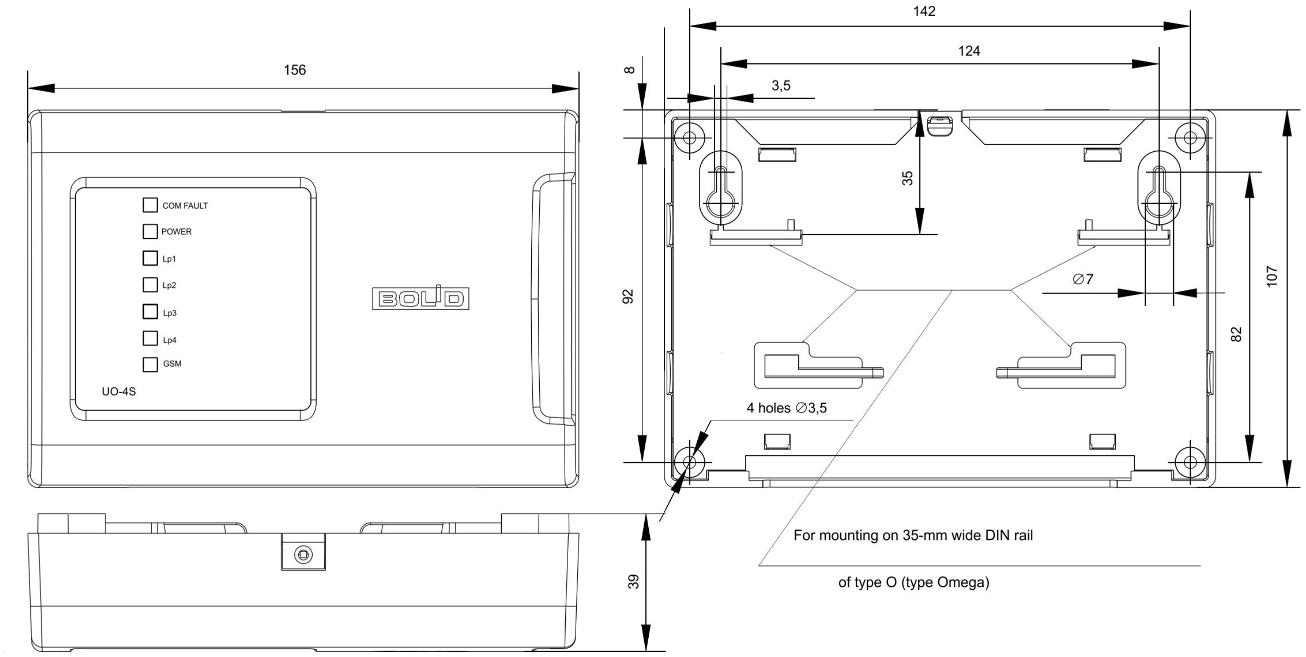


Figure 2. Overall and Mounting Dimensions

The UO-4C should be mounted in line with the Russian regulatory document РД.78.145-92 “Rules of Work Arrangement and Commissioning. Installations of intrusion and fire alarm systems”. The panel should be attached at a height where it is convenient to operate and maintain the device.

Mounting on a Wall

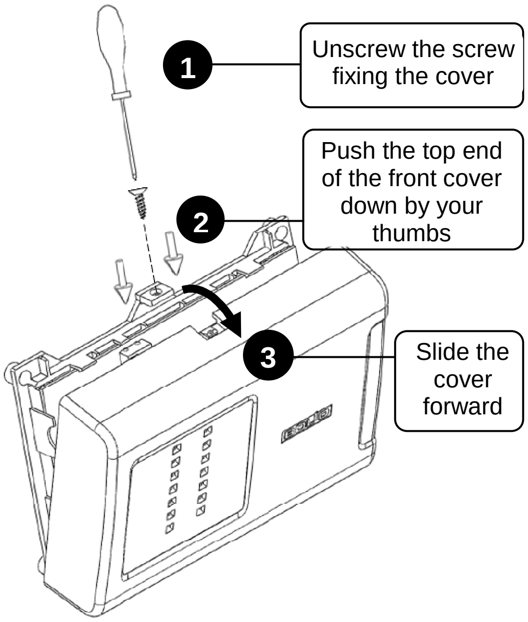

1
Unscrew the screw fixing the cover
2
Push the top end of the front cover down by your thumbs
3
Slide the cover forward

Figure 3. How to Remove the Cover

1. Please ensure that the wall the device is to be mounted on is solid, flat, clean, and dry.
2. Mark places for three mounting holes on the wall (for two upper holes and one of the bottom ones) in accordance with the mounting pattern for the panel.
3. Drill the holes, insert wall plugs into them and screw provided woodscrews into the two upper holes so that the distance between a screw head and the wall is about 7 mm.
4. Remove the front cover from the panel as shown in Figure 3).
5. Hang the device on the two screws. Screw the next woodscrew into the bottom mounting hole and tighten it up until bumping to fasten the device to the wall.

Mounting on a DIN Rail

1. Select the mounting location where free access to the tapping screw at the upper end of the device front cover is provided.
2. Install the device on the DIN rail as shown in Figure 4.
3. Remove the device front cover as shown in Figure 3.

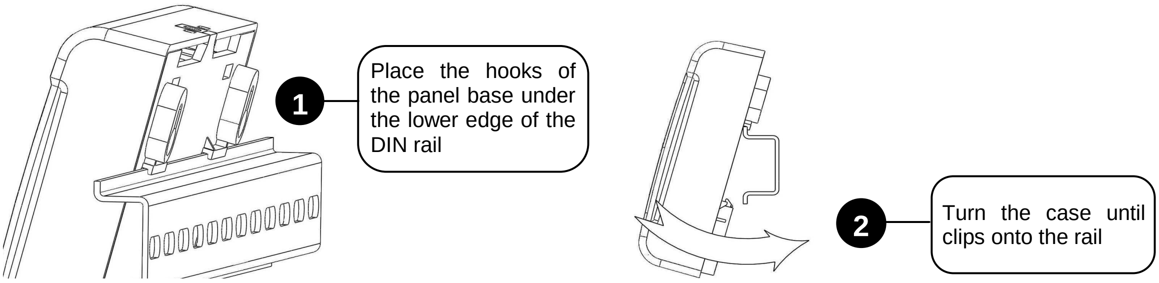

1
Place the hooks of the panel base under the lower edge of the DIN rail
2
Turn the case until clips onto the rail

Figure 4. Mounting the Panel on a DIN Rail

Connection

Mounting of connecting and communication lines is carried out in accordance with Figure 5 (“UO-4S Connection Diagram”).

RS-485 Interface Bus

When the UO-4S is used as part of an Orion integrated security system:

1. Connect the terminals RS-485A and RS-485B to the lines A and B of the RS-485 interface bus respectively.

2. Connect the “0 B” circuit of the panel to the similar circuit of the preceding and the subsequent devices on the RS-485 trunk (if the devices are powered by the same power supply this doesn’t have to be done).

3. If the panel is neither the last nor the first device on the RS-485 interface bus then remove the XT3 jumper which is situated closely to A and B contacts on the PCB.

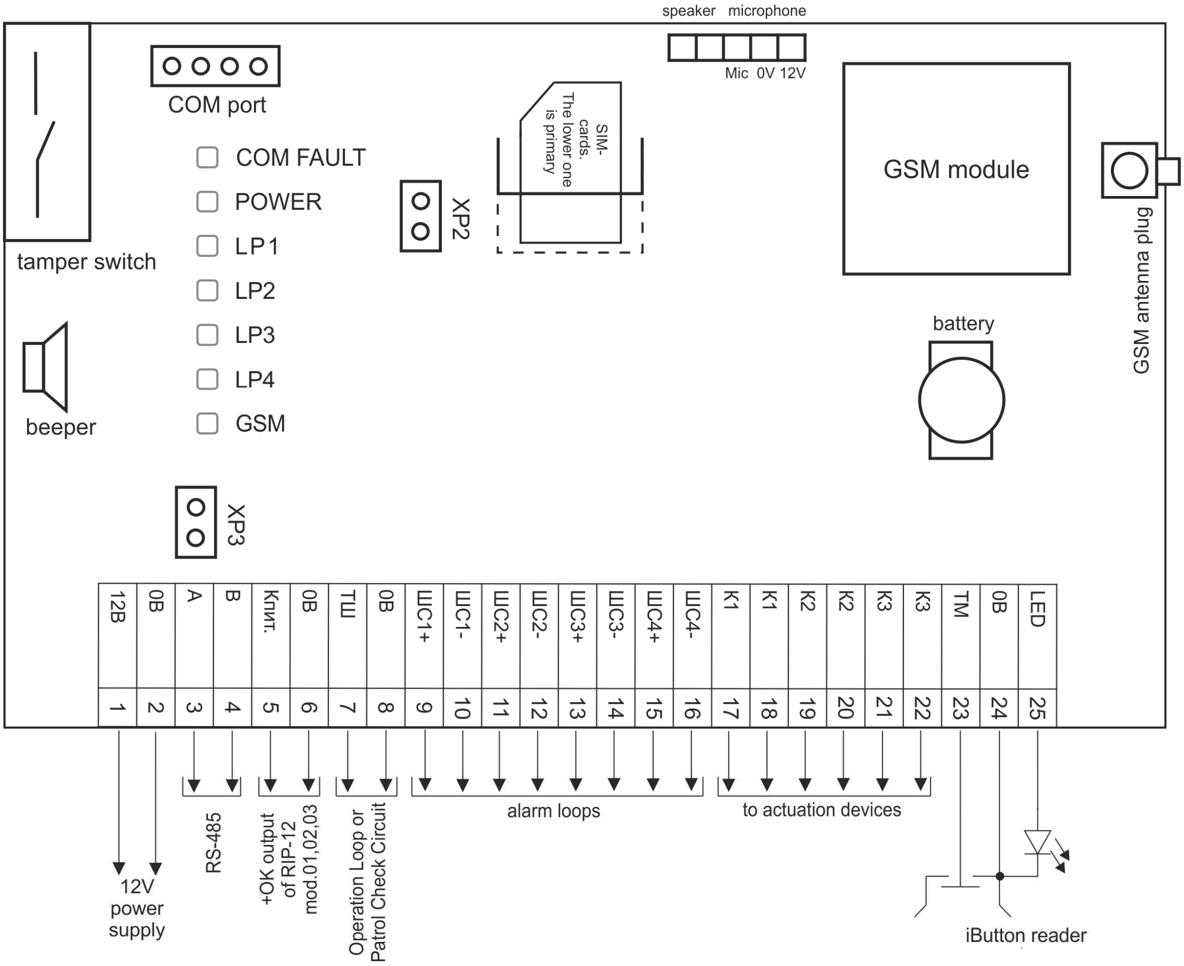


Figure 5. UO-4S Connection Diagram

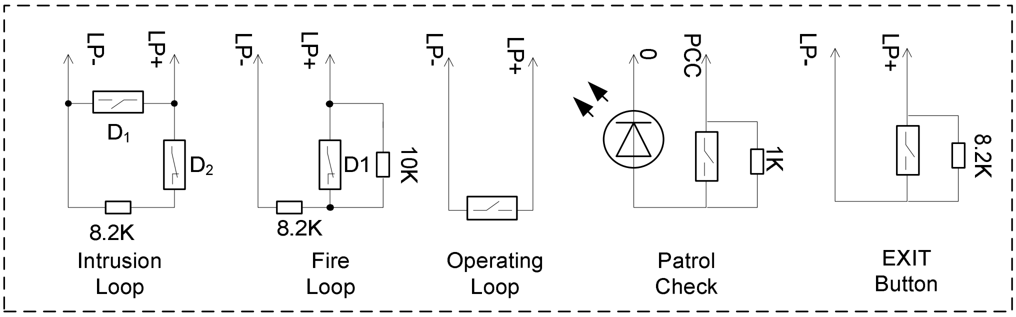


Figure 6. Connecting Alarm Loops and Operating Loop

Four-wire detectors (with external powering) should be used as fire detectors. After receiving a Fire event it is necessary to reset power of the relevant detector; for doing so one of the panel relay outputs can be used (the tactics «Switch Off upon Arming»).

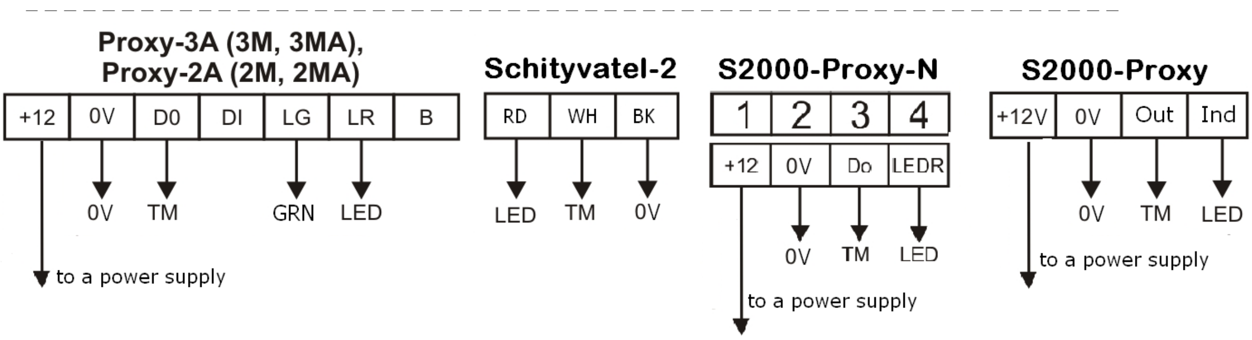


Figure 7. Connecting Readers

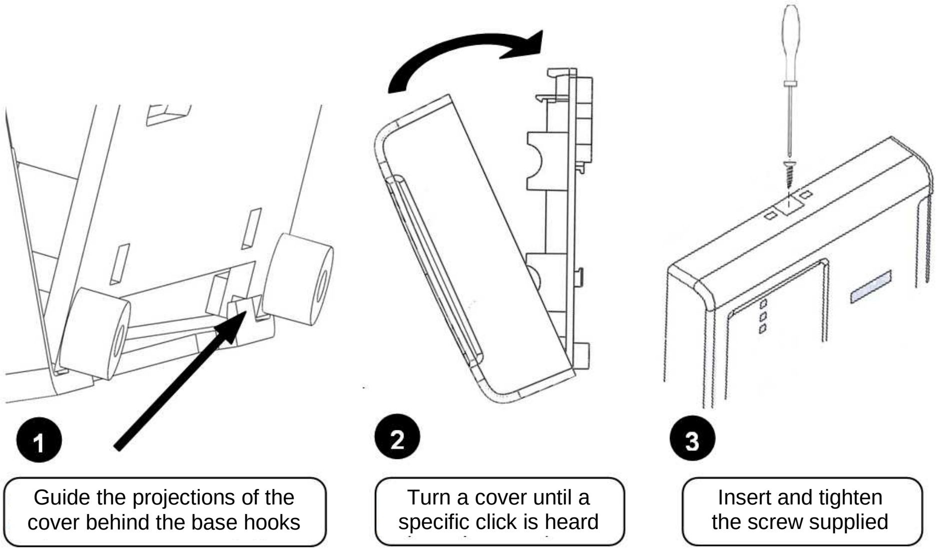
Inserting SIM Cards

SIM cards are to be installed into the panel after the panel has been programmed.

Prior to inserting SIM cards into the UO-4S it is preferable to turn off asking PIN codes for them by means of a cell phone. If it is required to use SIM card protected by asking PIN then digit PINs of the primary and backup SIM cards should be specified in SIM card settings in UProg (tab “Device”).

The primary SIM card is to be inserted into the lower slot (which is closer to the panel’s PCB), and the backup SIM card is to be inserted into the upper slot (under the metal plate).

Closing Cover



Guide the projections of the cover behind the base hooks

Turn a cover until a specific click is heard

Insert and tighten the screw supplied

Figure 8. How to Close the Cover

PROGRAMMING UO-4S

The UO-4S parameters are configured with the help of **UProg** (of version 4.1.0.51 and higher).

While programming the UO-4S it is recommended to use the last version of UProg which can be downloaded from
https://bolid.ru/files/373/566/InstallUProg_411.zip

https://bolid.ru/support/download/?groupsID=3&tagsID=0&q=Uprog

Configuring

To configure the UO-4S parameters, connect the panel to a power supply and to a PC with **UProg.exe** Device Configuration Tool installed via the adapter cable provided or via one of the Bolid manufactured interface converters (PI-GR, S2000-PI, S2000-USB, or USB-RS-485).

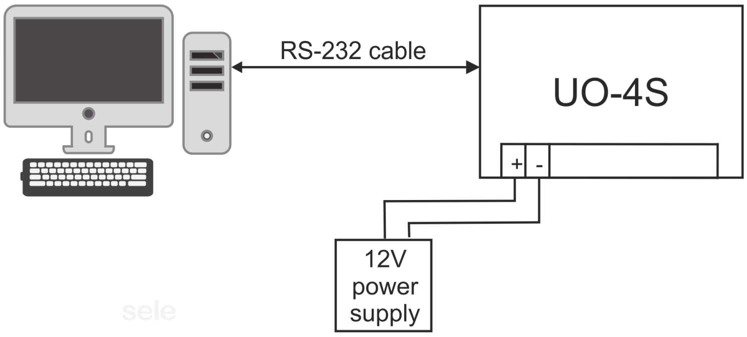


Figure 9. Connecting the UO-4S to a PC via the Adapter Cable

If the UO-4S is connected to the PC over the RS-232 cable for programming then for the panel can operate in the modes Master, Slave 1 and Slave 2 the connection cable must be disconnected from the relevant UO-4S port after configuring.

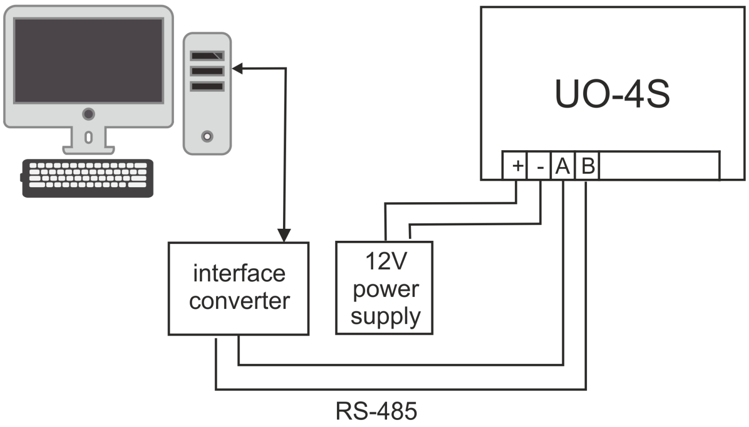


Figure 10. Connecting the UO-4S to a PC via an Interface Converter

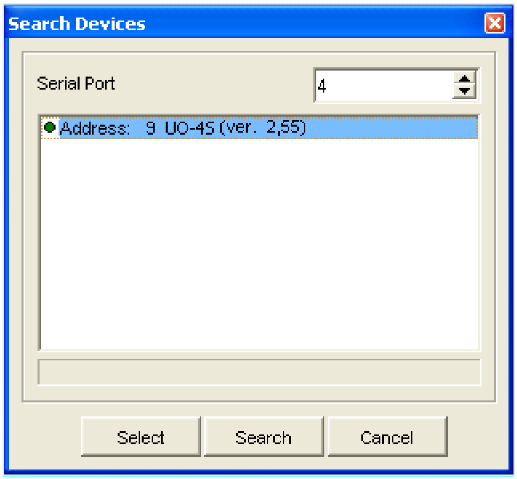
Please remove SIM-cards from the UO-4S while programming the panel parameters. The XP2 jumper (see Figure 5) must be closed during programming.

RUNNING CONFIGURATION TOOL

Run **UProg**.

Load configuration from the device memory:
Menu ***Device*** → ***Read Device Configuration***

The window for searching devices connected to the computer appears on the PC display. In the Serial Port field enter the logical number of the COM port the UO-4S is connected to. Then the Search Devices procedure is started.



Search Devices

Serial Port: 4

● Address: 9 UO-4S (ver. 2,55)

Figure 11

On completing the search procedure UProg displays the list of all the devices connected to the selected COM port, with address and version numbers being specified for each device. Select the device that is to be programmed.

Change Panel Address

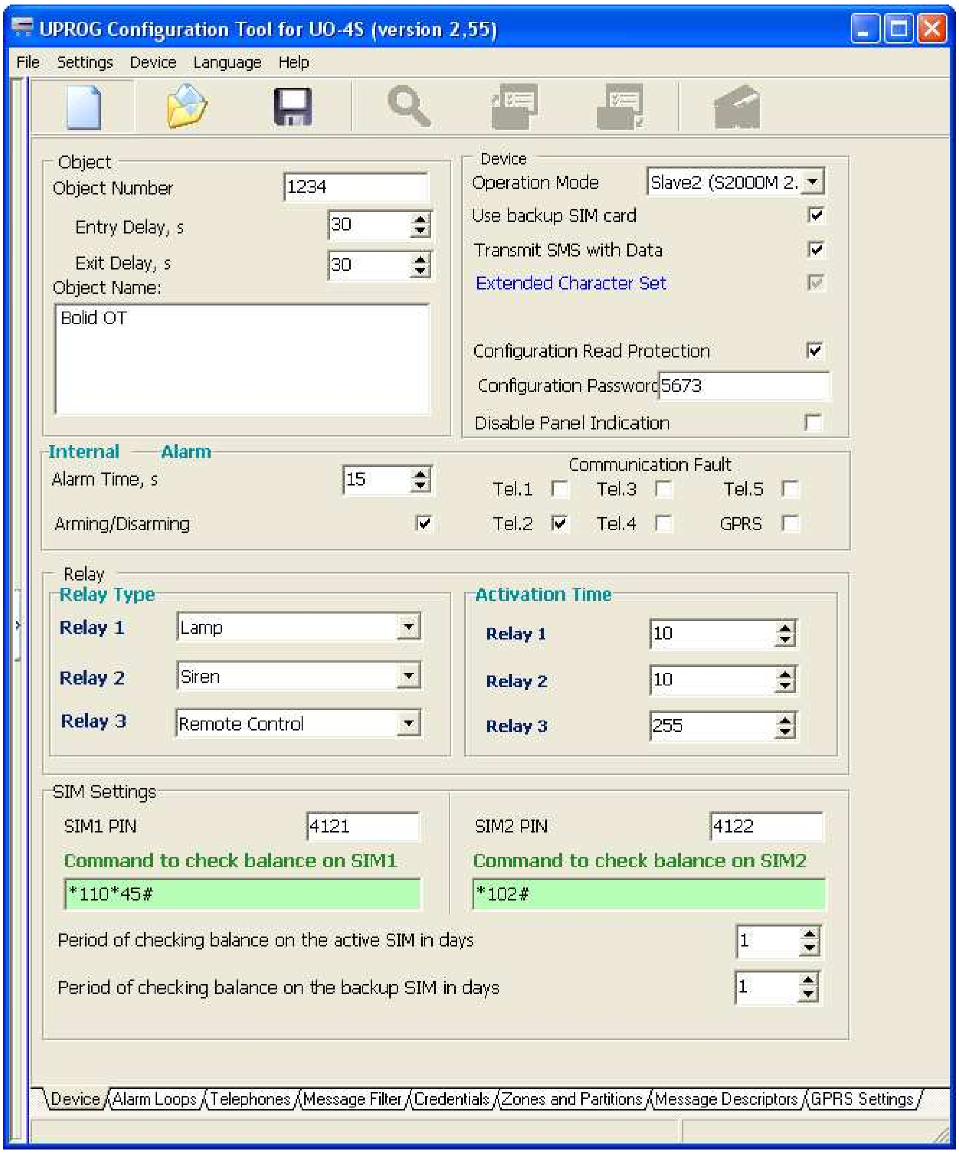
The panel's RS-485 network address can be changed by means of the UProg menu command **Device → Change Device Address.**

In a slave mode the UO-4S address is recommended to be set to 127 while addresses of the devices connected to the UO-4S should be set to values from 1 and higher.

Saving Configuration

To write configuration to the UO-4S memory, please click the Write Configuration to Device button and exit the program. The UO-4S shall confirm writing the new configuration by sounding of the built-in beeper.

Tab «Device»


UPROG Configuration Tool for UO-4S (version 2,55)
File Settings Device Language Help
Device / Alarm Loops / Telephones / Message Filter / Credentials / Zones and Partitions / Message Descriptors / GPRS Settings

Object
Object Number 1234
Entry Delay, s 30
Exit Delay, s 30
Object Name:
Bolid OT

Device
Operation Mode Slave2 (S2000M 2.
Use backup SIM card ☑
Transmit SMS with Data ☑
Extended Character Set ☑
Configuration Read Protection ☑
Configuration Password 5673
Disable Panel Indication □

Internal Alarm
Alarm Time, s 15
Arming/Disarming ☑
Communication Fault
Tel.1 □ Tel.3 □ Tel.5 □
Tel.2 ☑ Tel.4 □ GPRS □

Relay

Relay Type		Activation Time	
Relay 1	Lamp	Relay 1	10
Relay 2	Siren	Relay 2	10
Relay 3	Remote Control	Relay 3	255

SIM Settings
SIM1 PIN 4121
Command to check balance on SIM1
*110*45#
SIM2 PIN 4122
Command to check balance on SIM2
*102#
Period of checking balance on the active SIM in days 1
Period of checking balance on the backup SIM in days 1

Figure 12. UProg for UO-4S

Object

- **Object number** is composed of four digits 1 to 9.
- **Object Name** can comprise maximum 64 Latin characters including spaces or 32 characters including spaces if Cyrillic characters are in use (used in case of transmitting user SMS).
- **Entry Delay** is the delay for alarm loop’s proceeding from an Entrance Alarm state to the Intrusion Alarm state.
- **Exit Delay** is the delay of arming an alarm loop.

Internal Alarm

- **Alarm Time** is the time is seconds for which the internal beeper sounds upon receiving such alarms as Intrusion Alarm, Fire Alarm, Short Circuit, and Open Circuit from the alarm loops linked to the beeper.
- **Arming/Disarming**: If this parameter is set on then the panel beeper will sound when alarm loops of the panel are armed and disarmed.
- **Communication Fault**: If this parameter is set on then the panel beeper will sound in case of loss of communication in specified channel.

Device

- **Operation Mode:** This parameter provides selecting the mode of panel operation.

> *The required operation mode must be obligatory selected prior to proceeding to **setting parameters of credentials, zones, and partitions**.*

- **Use Backup SIM Card**: If a second (backup) SIM card is installed into the UO-4S then when a notification cannot be transmitted over the primary notification channel (poor communication quality, zero or negative account balance) this one will be transmitted over the backup communication channel (both cards are equivalent and the panel returns to operation with the primary card only when transmitting data using the backup card fails or after power-on reset).
- **Extended Character Set**: The parameter informs that notifications are transmitted using Unicode extended character set (the UO-4S starts transmitting SMS in Unicode if the object name or User SMS contain Cyrillic characters).
- **Transmit SMS with Data**: If this parameter is set on then the UO-4S transmits User SMS with the data, not only with the time.
- **Configuration Read Protection**: This parameter can be set on / off when a password against unauthorized programming of the panel is given. If the parameter is set on then in case of an attempt to read configuration after 30 seconds since last programming UProg will ask the password.

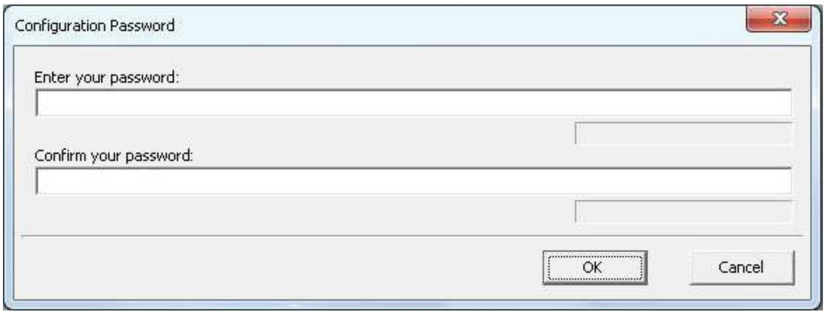
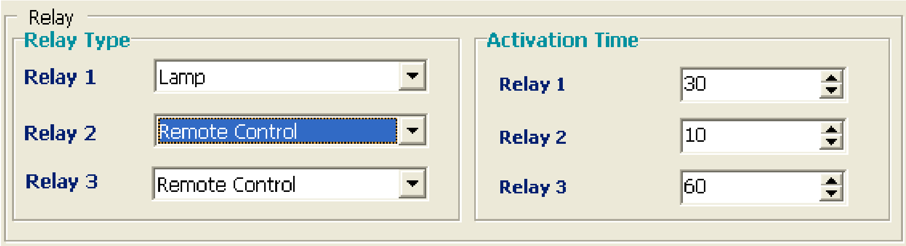


Figure 13. The Dialog Window to Enter Configuration Password

> *Configuration Password can be discarded upon panel's entering the programming mode without presenting Master Key (on powering the panel up with closed terminals of the reader). Then panel's configuration should be read and password should be changed or discarded.*

- **Disable Panel Indication**: If this parameter is set on then the panel indicates events neither by lighting nor by sounding except for GSM LED and reader indication. Indication can be suppressed only when the tamper switch of the panel is closed.

Relay Outputs



Relay

Relay Type

Relay 1: Lamp

Relay 2: Remote Control

Relay 3: Remote Control

Activation Time

Relay 1: 30

Relay 2: 10

Relay 3: 60

To program relays it is necessary to select Relay Type, to give Activation Time during which every relay is activated in accordance with the defined control tactics, and to select the alarm loops linked with every relay.

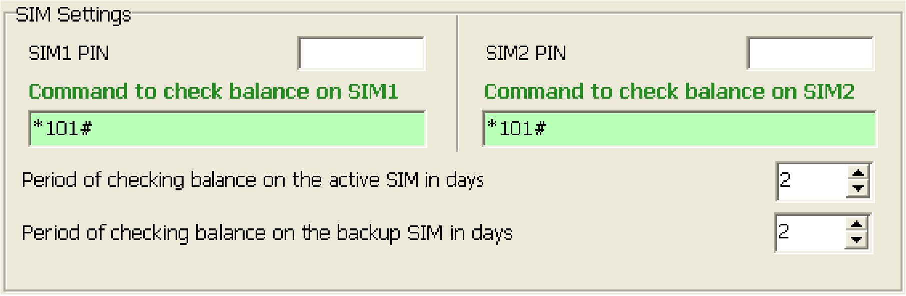
The parameter Activation Time for the relay tactics **Switch Off upon Arming** can be set to a value which corresponds to a time in the range of 1 to 10 seconds, with one unit of the parameter being equal to 0.125 s.

- Activation Time = 0 – The relay will not be activated.
- Activation Time = 255 – The relay will operate in accordance with the selected tactics until linked inputs change their state.

The Activation Time parameter is not applicable to a relay if the relay is assigned with one of such tactics as Lamp, Communication Failure, and Remote Control. Such relay always operates in accordance with given tactics until the linked inputs change their state.

When the relay control tactics «Switch Off upon Arming» and «Lock Control» are in use the relay can be linked only with a single alarm loop.

SIM Card Settings



SIM Settings

SIM1 PIN:

Command to check balance on SIM1: *101#

SIM2 PIN:

Command to check balance on SIM2: *101#

Period of checking balance on the active SIM in days: 2

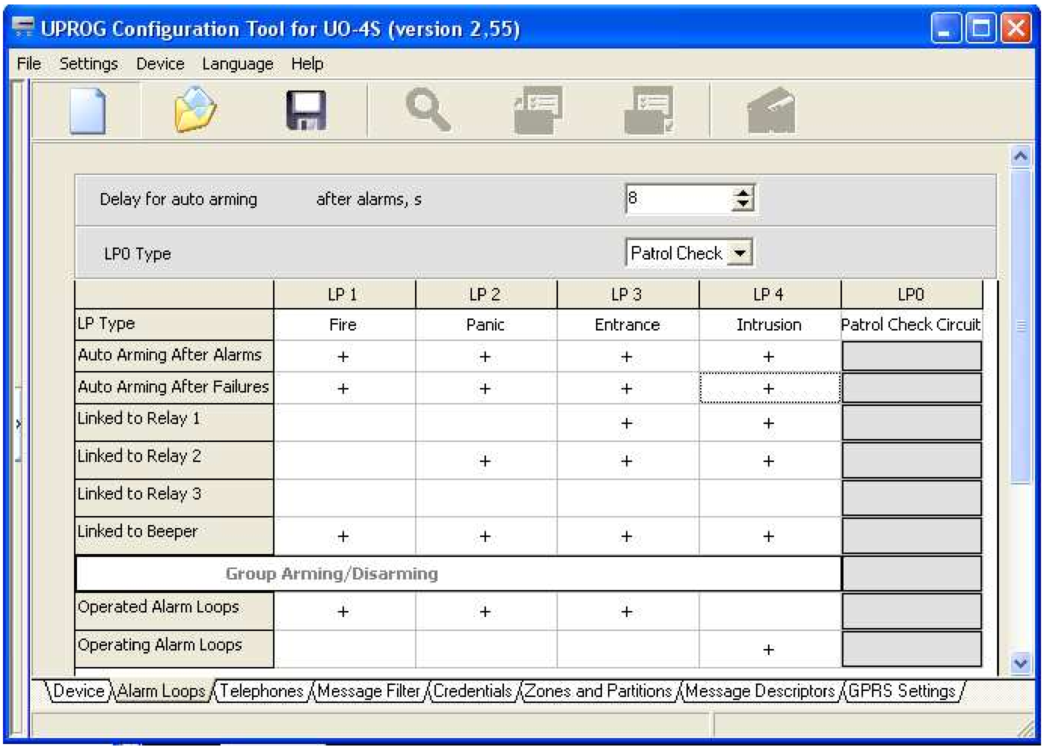
Period of checking balance on the backup SIM in days: 2

While using SIM cards it is recommended previously to turn their PIN codes off. However, if it is required to work with cards for which PIN codes are asked then it is necessary to specify these codes in the relevant fields for the primary and backup SIM cards.

If it is necessary to ask the balance automatically then the balance request codes should be typed in the relevant fields of SIM1/SIM2 and the relevant period for automatic checking in days should be selected.

To turn a PIN off in the device settings switch the panel to the programming mode without presenting the Master Key (power the panel up closing the reader terminals)

Tab «Alarm Loops»



Delay for auto arming after alarms, s 8

LP0 Type Patrol Check

	LP 1	LP 2	LP 3	LP 4	LP0
LP Type	Fire	Panic	Entrance	Intrusion	Patrol Check Circuit
Auto Arming After Alarms	+	+	+	+	
Auto Arming After Failures	+	+	+	+	
Linked to Relay 1			+	+	
Linked to Relay 2		+	+	+	
Linked to Relay 3					
Linked to Beeper	+	+	+	+	
Group Arming/Disarming					
Operated Alarm Loops	+	+	+		
Operating Alarm Loops				+	

Figure 14. Alarm Loops Tab

Auto Arming Delay: This parameter means a time in which an alarm loop will be armed when it has been repaired after being in alarm. The value can be set in the range of 1 to 255.

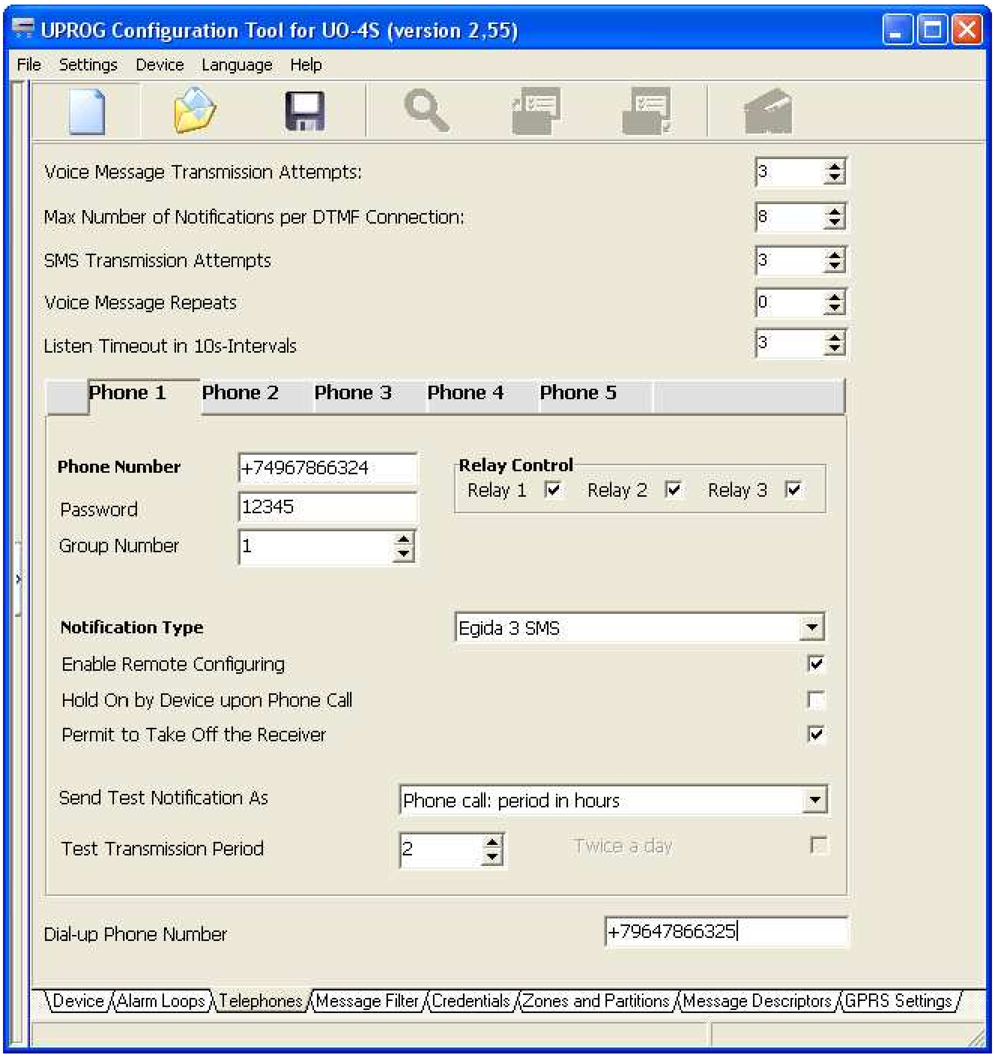
For an alarm loop of the Entrance type Auto Arming Delay must exceed Entry Delay.

- **LP Type**: Selecting the type of an alarm loop for LP0-LP4.
- **LP0 Type**: The way to use the input “0B-ТШ” on the device PCB, namely Patrol Check Circuit, Operating Loop, or Phone Call. If a Patrol Check button is used then select the type Patrol Check Circuit; if a common alarm loop is used which operates other UO-4S inputs then select Operating Loop; and if activation of zeroth alarm loop should lead in a phone call to a dial-up phone number then select the Phone Call type.
- **Auto Arming After Alarms/Failures**: Intrusion types of the alarm loops (Intrusion, Entrance, Panic) support automatic arming them after being in alarms or in the Arming Failed status. An auto arming procedure is started on expire of a programmable delay defined in configuration; the parameters of auto arming are defined for every internal alarm loop individually.

The parameter Auto Arming After Failures is always applied for fire alarm loops (regardless of whether this flag is set on or off).

- **Linked to Relay…**: Tick the alarm loops linked with the relevant relay.
- **Linked to Beeper**: If the parameter is set on then activation of this alarm loop causes the panel to indicate this event by sounding.
- **Group Arming / Disarming**: Operated alarm loops are armed upon arming of all operating alarm loops. Operated alarm loops are disarmed upon disarming of any operating alarm loop. Both operated and operating alarm loops must be marked with a plus character.

Tab «Telephones»



Voice Message Transmission Attempts: 3

Max Number of Notifications per DTMF Connection: 8

SMS Transmission Attempts 3

Voice Message Repeats 0

Listen Timeout in 10s-Intervals 3

Phone Number +74967866324

Password 12345

Group Number 1

Relay Control: Relay 1 ☑ Relay 2 ☑ Relay 3 ☑

Notification Type Egida 3 SMS

Enable Remote Configuring ☑

Hold On by Device upon Phone Call □

Permit to Take Off the Receiver ☑

Send Test Notification As Phone call: period in hours

Test Transmission Period 2 Twice a day □

Dial-up Phone Number +79647866325

Figure 15. Telephones Tab

Voice Message Transmission Attempts

A communication attempt can fail due to subscriber on the receiving side being busy or poor link quality or a communication failure. After a specified number of attempts the panel proceeds to a next subscriber and enter the communication fault mode for the current subscriber. The parameter is applicable to voice messages and transmission in the Contact ID protocol.

The number of attempts should not be equal to zero, it is advised to be set to 2 – 3 attempts or more.

Max Number of Notifications per DTMF Connection

The maximum number of notifications per a single Phone Call used while operating with the Contact ID protocol. *It is advised to set this value to 5-8 notifications (to be corrected experimentally).*

SMS Transmission Attempts

The number of attempts to transmit an SMS after which the panel switches to a next subscriber and enter the communication fault mode for the current subscriber. *It is recommended to specify 2-3 attempts or more.*

Voice Message Repeats

It is advised to set at least one and no more than three times the voice messages will be repeated (if the number of repeats is set to zero then voice messages will be spoken once). On repeating the object number is not spoken.

Listen Timeout in 10 s-Intervals (*10)

It is the time after expiry of which the panel terminates the connection established upon activation of an alarm loop of the Phone Call type.

Phone Number

A phone number should be entered completely including the country/area code (the prefix «+» can be used).

Password

To provide a possibility to control the panel from the cell phone, a five-digit password must be set in this field.

To operate partitions in a slave mode, in the configuration of the control panel (in PProg.exe) the phone number must be entered as a credential with the relevant access level to operate partitions. The phone number should be entered in the control panel configuration along with the country and area codes (with «8» or «7» without the «+» sign) as well as it is entered in the UO-4S itself.

Group Number

To create backup communication channels, phone numbers are combined into groups. If a notification cannot be delivered to a first phone in the group it is transmitted to a next number. If a notification is supposed to be sent to every phone number then the group values should be set different for every number.

Communication Fault messages are not transmitted between the groups (directions) apart from the GPRS channel.

Notification Type

To transmit events, one of the following notification types can be selected:

- Contact ID (ADEMCO);
- User SMS;
- Egida-2 SMS;
- Egida-3 SMS;
- Voice Message;
- Phone Call;
- CSD (DC-05/DC-09)

One phone number can be used to transmit notifications of various types to it. For doing so, the phone number should be added twice to the panel configuration with different notification types. The two phones are to be combined in a group, thus the second notification type will be the backup one.

Enable Remote Configuring

If this parameter is set on for a subscriber then this subscriber can remotely (by SMS commands) change Object Number, request for the balance, change the data and time, and change its phone number. In addition, the subscriber can remotely change also the number of another subscriber if it specifies this number in the command (after changing the number a confirmation command from the UO-4S about changing the number is arrived to the new number).

Send Test Notification As

Test notifications are used to check operability of communication channels and can be sent to Phone 1 and Phone 2. A Test can be sent either as an SMS (sending period is set in hours) or as a phone call provided that a period of calling can be set in minutes or hours or calls can be given at the set time (once or twice a day).

The field Test Transmission Period can take a value ranging or from 1 to 59 if the period is set in minutes, or from 1 to 24 if the period is set in hours or at a specified time, or from 1 to 12 when the Twice a Day flag is set on.

Apart from the mode of phone call at a specified time the period of sending Test message is counted starting at the moment of last transmission of any message (including response messages to the balance request and SMS control commands) to the relevant cell phone.

In the mode of a phone call on receiving the test notification the subscriber takes a call and this is a confirmation for the UO-4S that the notification is taken. Then the UO-4S clears the line. *The call time doesn't exceed two seconds and as a rule is not charged by a communication operator.*

If a Test notification is sent in one direction then it will not be transmitted to other directions.
SMS-notification "Test" can be used only with SMS notification types (User SMS, Egida-2 SMS, Egida-3 SMS)

Dial-up Phone Number

This is a number of the telephone where dial-up is made when an alarm loop with the Phone Call type is activated. This phone number must be entered in full, including the area code. When a call is made from this number the UO-4S picks up the handset to broadcast the signal from the microphone.

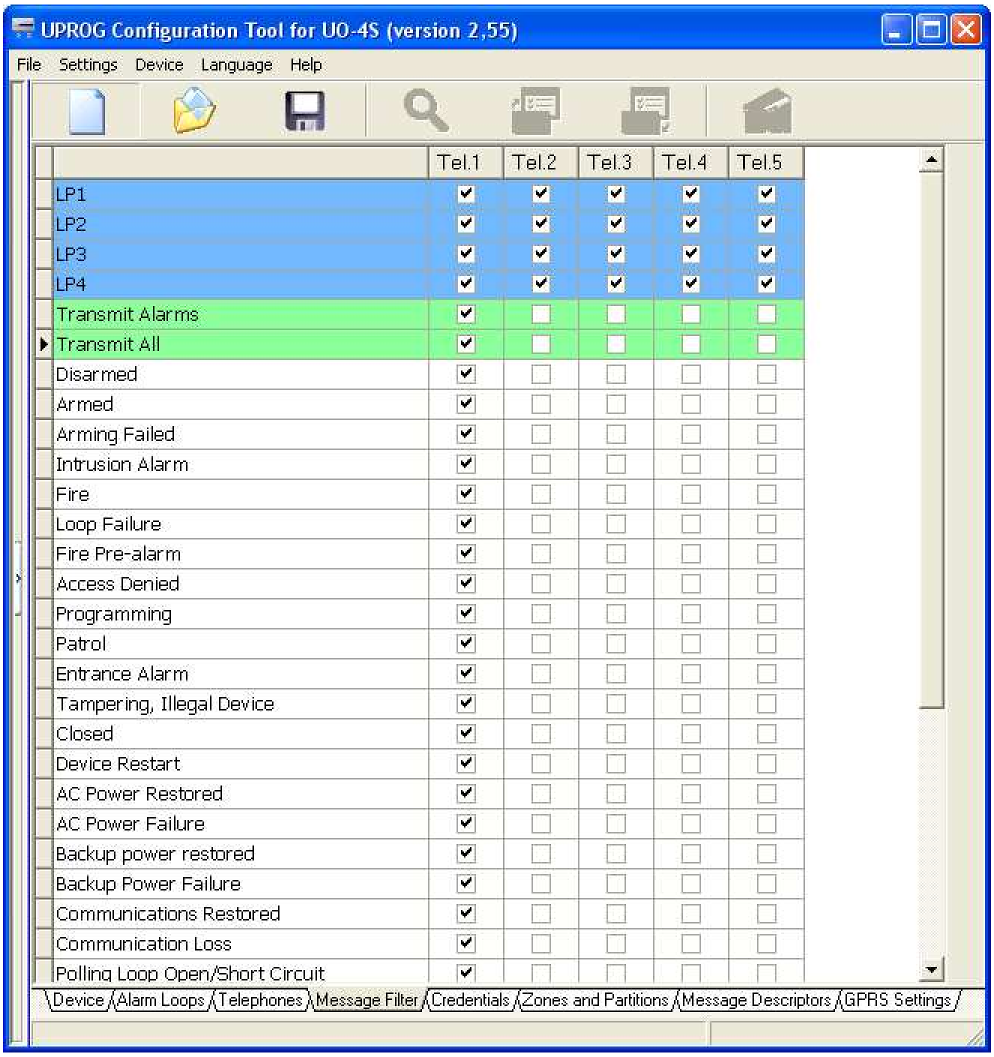
Permit to Take Off the Receiver

When called from the phone number for dialing, the panel turns on the microphone and speaker (if they are connected to the corresponding terminals) for the specified listening time in 10 seconds intervals.

Phone Call Hold

If at the moment of translation the panel is ringed up, the panel doesn't hang up.

Tab «Message Filter»



	Tel.1	Tel.2	Tel.3	Tel.4	Tel.5
LP1	☑	☑	☑	☑	☑
LP2	☑	☑	☑	☑	☑
LP3	☑	☑	☑	☑	☑
LP4	☑	☑	☑	☑	☑
Transmit Alarms	☑	□	□	□	□
Transmit All	☑	□	□	□	□
Disarmed	☑	□	□	□	□
Armed	☑	□	□	□	□
Arming Failed	☑	□	□	□	□
Intrusion Alarm	☑	□	□	□	□
Fire	☑	□	□	□	□
Loop Failure	☑	□	□	□	□
Fire Pre-alarm	☑	□	□	□	□
Access Denied	☑	□	□	□	□
Programming	☑	□	□	□	□
Patrol	☑	□	□	□	□
Entrance Alarm	☑	□	□	□	□
Tampering, Illegal Device	☑	□	□	□	□
Closed	☑	□	□	□	□
Device Restart	☑	□	□	□	□
AC Power Restored	☑	□	□	□	□
AC Power Failure	☑	□	□	□	□
Backup power restored	☑	□	□	□	□
Backup Power Failure	☑	□	□	□	□
Communications Restored	☑	□	□	□	□
Communication Loss	☑	□	□	□	□
Polling Loop Open/Short Circuit	☑	□	□	□	□

Figure 16. Message Filter

Message Filter provides adjusting a list of events and local alarm loops for which notifications will be sent to a specified phone.

A tick in the Message Filter table means transmitting the relevant messages to the relevant phone while a blank cell means that the events will not be transmitted. The filter is applied both to standalone operation of the UO-4S and to cooperation of the UO-4S with Orion system devices.

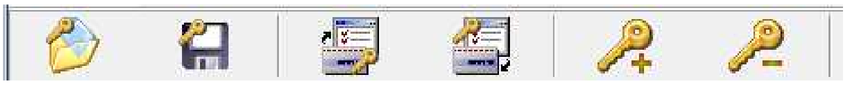
Every filter can comprise several events falling under this group. The table below shows the examples of the events falling under the filters.

The filter for alarm loops of the UO-4S (LP1 – LP4) is applicable only when the panel operates in the Standalone or Master mode. If the UO-4S operates under the control panel the filter related to the internal alarm loops of the UO-4S is ignored.

Filter Name	Events
Armed	Partition is armed, a leakage is repaired
Alarm	Intrusion alarm, panic alarm, leakage (flood detector alarm)
Fire	Fire, Fire2
Loop Failure	Alarm loop short circuit failure, alarm loop open circuit failure, fire protection equipment failure, service required, loop configuration error, temperature sensor fault, noise
Communications Restored	Communication with the device/subscriber is restored
Communication Loss	Loss of communications with a device, loss of connection with a subscriber
PL Open/Short Circuit	Polling loop short circuit failure, polling loop open circuit failure, PL communication error, PL unstable communication
Output Circuit Failure	Output open circuit failure, output short circuit failure, actuator failure, actuator error
Off / On	An alarm loop is disconnected, and alarm loop is connected, and output is disabled, an output is enabled, a pump is on, a pump is off, an actuator is in initial position, an actuator is in operation position, auto mode is off, auto mode is on
Temperature	High temperature, low temperature, normal temperature
Level	High level, low level, too high level, too low level, normal level
Auxiliary Loop	Auxiliary loop alarm, auxiliary loop restored, activation of a second auxiliary alarm loop
Batteries	Low battery, low backup battery, backup battery restored, battery failure, battery restored, battery test error
Charger	Power supply overload, overload repaired, RIP charger failed, RIP charger restored
Equipment	Discharge of extinguishing agent, voice announcement activated and other events not included in the filters
Doors	A door is forced open, a door is propped open, a door is closed (after being forced/propped open), wrong code

Tab «Credentials»

To work with credentials and their operating authorities there is an additional toolbar in the UProg with the tools as follows.



	Load credentials from a file		Write credentials to the device
	Save credentials to a file		Load credentials from the panel memory
	Add a new credential descriptor		Read a credential
	Delete the selected credential descriptor from the panel memory		

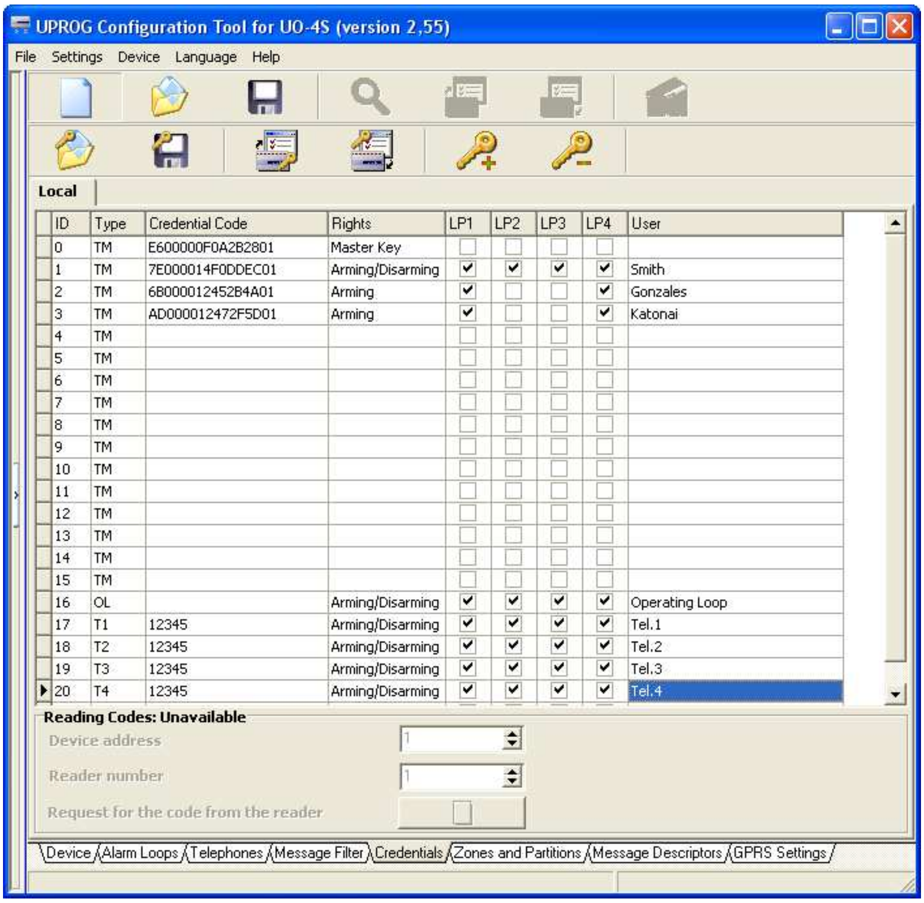
Prior to enrolling credentials ensure that the Operation Mode parameter on the Device tab is set to a proper value.

Enrolling Credentials by means of an iButton Reader

To enroll credential codes by means of an iButton reader, the iButton reader should be connected to the UO-4S terminals 23, 24, and 25 (see Figure 5).

1. Load the panel configuration by means of UProg. Go to the Credentials tab. When the Credential tab has been open the device descriptors start being read from the panel memory automatically.
2. Add a new credential descriptor on the Credential tab by clicking 🔑.
3. Then read the credential code ▣. If the credential code is read successfully the panel beeps and a unique code appears in the relevant Credential Code cell.
4. Next, define the credential rights by ticking the boxes in the cells of the alarm loops which can be operated by the credential. Then save the credential to the panel memory by activating the tool ☑, «Write credentials to the device».
5. To delete a credential descriptor from the panel memory use the button 🔑.

Setting Local Credentials



ID	Type	Credential Code	Rights	LP1	LP2	LP3	LP4	User
0	TM	E600000F0A2B2801	Master Key	□	□	□	□	
1	TM	7E000014F0DDEC01	Arming/Disarming	☑	☑	☑	☑	Smith
2	TM	6B000012452B4A01	Arming	☑	□	□	☑	Gonzales
3	TM	AD000012472F5D01	Arming	☑	□	□	☑	Katonai
4	TM			□	□	□	□	
5	TM			□	□	□	□	
6	TM			□	□	□	□	
7	TM			□	□	□	□	
8	TM			□	□	□	□	
9	TM			□	□	□	□	
10	TM			□	□	□	□	
11	TM			□	□	□	□	
12	TM			□	□	□	□	
13	TM			□	□	□	□	
14	TM			□	□	□	□	
15	TM			□	□	□	□	
16	OL		Arming/Disarming	☑	☑	☑	☑	Operating Loop
17	T1	12345	Arming/Disarming	☑	☑	☑	☑	Tel.1
18	T2	12345	Arming/Disarming	☑	☑	☑	☑	Tel.2
19	T3	12345	Arming/Disarming	☑	☑	☑	☑	Tel.3
20	T4	12345	Arming/Disarming	☑	☑	☑	☑	Tel.4

Reading Codes: Unavailable

Device address: 1

Reader number: 1

Request for the code from the reader

Figure 17. Local Credentials

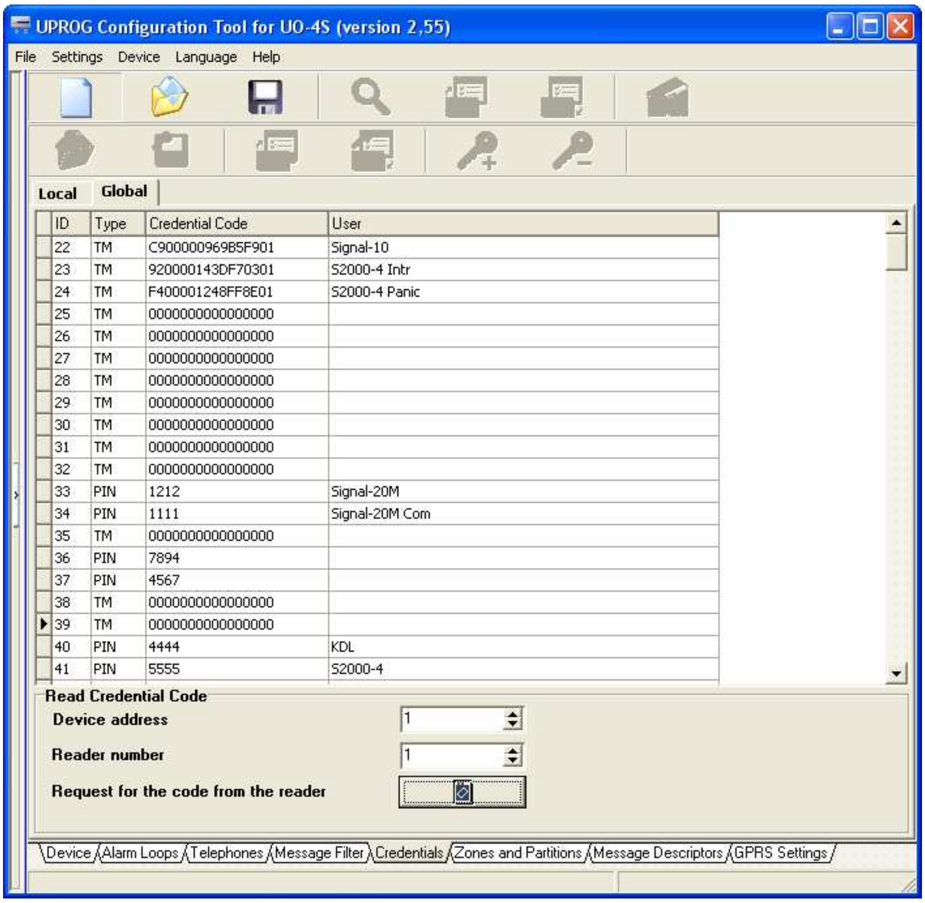
- Type: The type of the credential. The value of Type can be one of iButton (TM), Operating Loop (OL), Telephone (T1, T2, T3, T4, T5), or PIN code (PIN).
- Credential Code: For iButtons their codes are read by means of the iButton reader and for telephones the code is entered using the keyboard (5 digits).
- Rights: Operating authorities of the credentials (Arming, Disarming, Arming / Disarming).
- LP1 – LP4: The numbers of the alarm loops which can be operated by the credentials.

The credential with ID 0 is the system Master Key which is used for programming user credentials for the UO-4S without UProg and cannot be used for arming / disarming.

In the modes Slave 1 and Slave 2 all the credentials including local ones must be enrolled in the control panel. Messages about arming and disarming the UO-4S contain ID (the sequential number) of the user in accordance as they are numbered in the control panel while the match between ID and the user name is defined in Global credential settings

Setting Global Credentials in the Master Mode

To transmit User ID and User Name while arming and disarming zones/partitions the Global Credentials table is used.



UPROG Configuration Tool for UO-4S (version 2,55)
File Settings Device Language Help
Local Global
Device Alarm Loops Telephones Message Filter Credentials Zones and Partitions Message Descriptors GPRS Settings

ID	Type	Credential Code	User
22	TM	C900000969B5F901	Signal-10
23	TM	920000143DF70301	S2000-4 Intr
24	TM	F400001248FF8E01	S2000-4 Panic
25	TM	0000000000000000	
26	TM	0000000000000000	
27	TM	0000000000000000	
28	TM	0000000000000000	
29	TM	0000000000000000	
30	TM	0000000000000000	
31	TM	0000000000000000	
32	TM	0000000000000000	
33	PIN	1212	Signal-20M
34	PIN	1111	Signal-20M Com
35	TM	0000000000000000	
36	PIN	7894	
37	PIN	4567	
38	TM	0000000000000000	
39	TM	0000000000000000	
40	PIN	4444	KDL
41	PIN	5555	S2000-4

Read Credential Code

Device address: 1

Reader number: 1

Request for the code from the reader

Figure 18. Global Credentials, Master Mode

Global credentials can be enrolled using the reader or the keyboard (credentials of the PIN type).

In the Master mode the UO-4S cannot control the slave devices and the credentials are enrolled only for the possibility to transmit credential ID and User Name. So, the same credentials must be locally enrolled in the devices.

Setting Global Credentials in the Slave 1 or Slave 2 Mode

When the UO-4S operates under the control panel all the credentials including local ones must be enrolled in the memory of the control panel as described in the control panel’s manual. In this case the sequence number of a credential will be transmitted by the control panel as a user number (ID). The match between ID and user names is described in the UO-4S on the tab Credential – Global.

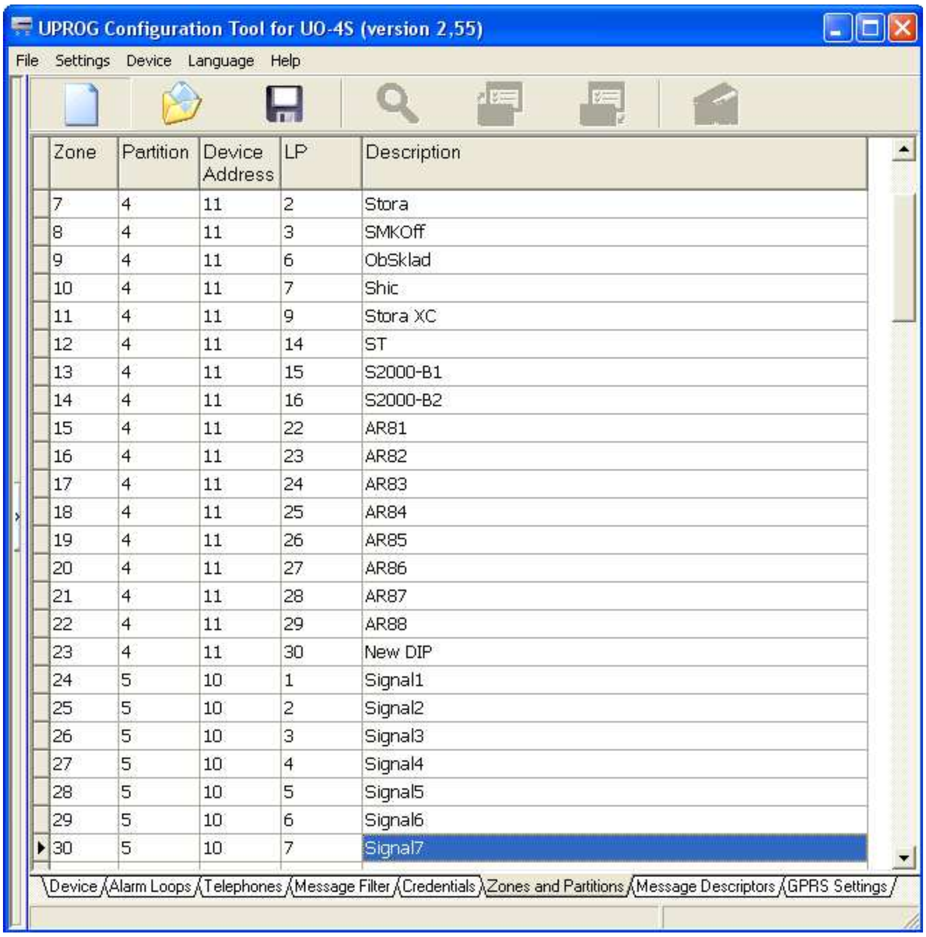
Tab «Zones and Partitions»

Standalone Mode: The match between the zones and partitions is given in the UO-4S. A Zone Number means the number of an ID Contact Zone (in the Standalone mode this tab can be not filled in).

Master Mode: The match between device addresses, zones, and partitions is described in the UO-4S. A string number in this case is the number of the ID Contact Zone.

Slave 1 Mode: The match between device addresses, zones, and partitions is described in the UO-4S. To receive events from the devices the UO-4S configuration must contains status zones of the devices where the alarm loop number is specified as zero (“0”) and the number of this string will mean the ID Contact number of the device state.

Slave 2 Mode: Numbers of zones and partitions are transmitted from the control panel; only textual description of the zone can be added in the UO-4S. For the Slave 2 mode, assign in the control panel configuration (using PProg.exe) the ID Contact numbers of all the zones, readers, panel status zones, and relays which events are to be transmitted to the UO-4S. A test description of a zone in this case is typed opposite the number of the string which matches to the zone ID Contact number in the configuration of the control panel.



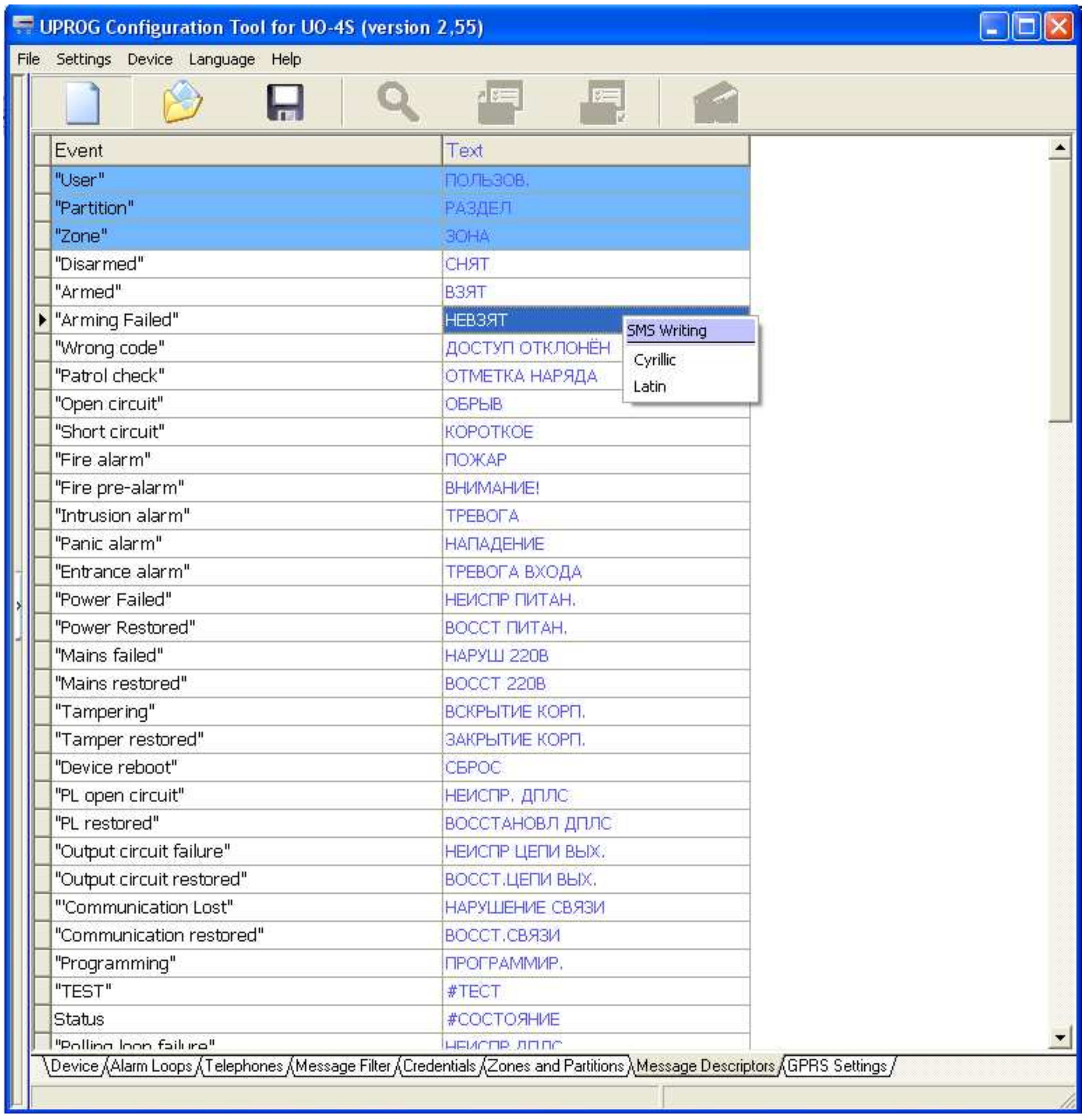
Zone	Partition	Device Address	LP	Description
7	4	11	2	Stora
8	4	11	3	SMKOff
9	4	11	6	ObSklad
10	4	11	7	Shic
11	4	11	9	Stora XC
12	4	11	14	ST
13	4	11	15	S2000-B1
14	4	11	16	S2000-B2
15	4	11	22	AR81
16	4	11	23	AR82
17	4	11	24	AR83
18	4	11	25	AR84
19	4	11	26	AR85
20	4	11	27	AR86
21	4	11	28	AR87
22	4	11	29	AR88
23	4	11	30	New DIP
24	5	10	1	Signal1
25	5	10	2	Signal2
26	5	10	3	Signal3
27	5	10	4	Signal4
28	5	10	5	Signal5
29	5	10	6	Signal6
30	5	10	7	Signal7

Figure 19. Zones and Partitions. Master Mode

The UO-4S doesn’t support partition descriptions so only partition numbers are specified for user SMS.

When the UO-4S operates together with the control panel in Slave 1 or Slave 2 operation modes, local alarm loops must be enrolled in the control panel database

Tab «Message Descriptors»

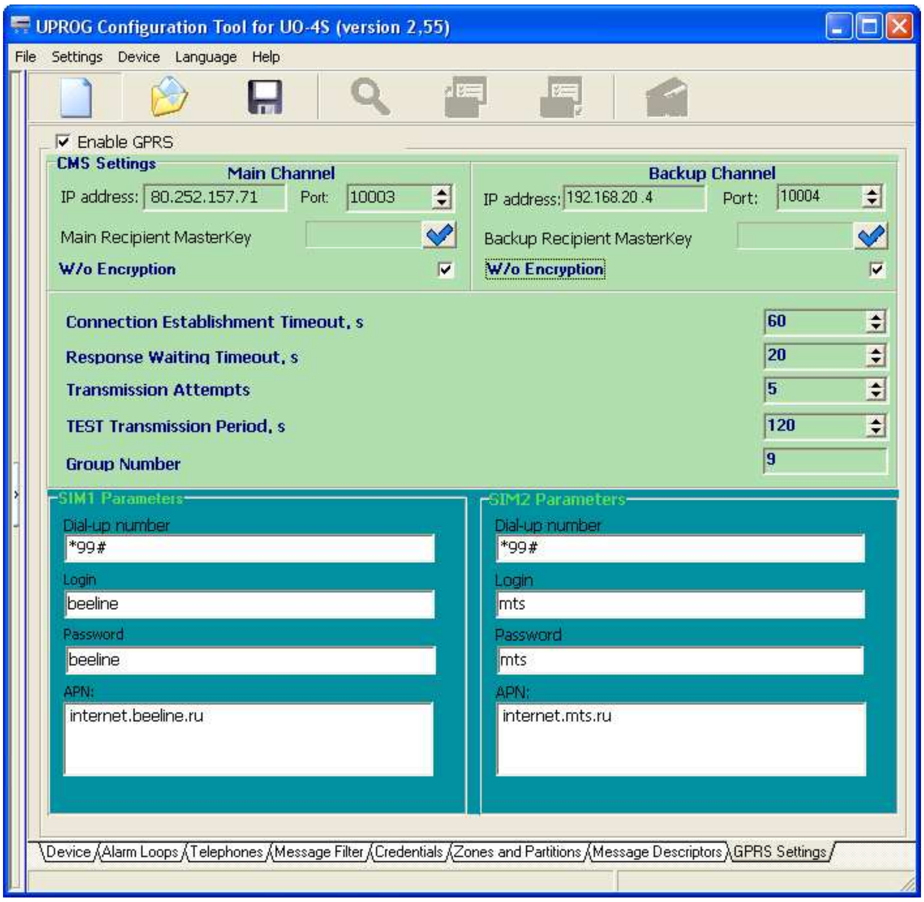


Event	Text
"User"	ПОЛЬЗОВ.
"Partition"	РАЗДЕЛ
"Zone"	ЗОНА
"Disarmed"	СНЯТ
"Armed"	ВЗЯТ
"Arming Failed"	НЕВЗЯТ
"Wrong code"	ДОСТУП ОТКЛОНЁН
"Patrol check"	ОТМЕТКА НАРЯДА
"Open circuit"	ОБРЫВ
"Short circuit"	КОРОТКОЕ
"Fire alarm"	ПОЖАР
"Fire pre-alarm"	ВНИМАНИЕ!
"Intrusion alarm"	ТРЕВОГА
"Panic alarm"	НАПАДЕНИЕ
"Entrance alarm"	ТРЕВОГА ВХОДА
"Power Failed"	НЕИСПР ПИТАН.
"Power Restored"	ВОССТ ПИТАН.
"Mains failed"	НАРУШ 220В
"Mains restored"	ВОССТ 220В
"Tampering"	ВСКРЫТИЕ КОРП.
"Tamper restored"	ЗАКРЫТИЕ КОРП.
"Device reboot"	СБРОС
"PL open circuit"	НЕИСПР. ДПЛС
"PL restored"	ВОССТАНОВЛ ДПЛС
"Output circuit failure"	НЕИСПР ЦЕПИ ВЫХ.
"Output circuit restored"	ВОССТ.ЦЕПИ ВЫХ.
"'Communication Lost"	НАРУШЕНИЕ СВЯЗИ
"Communication restored"	ВОССТ.СВЯЗИ
"Programming"	ПРОГРАММИР.
"TEST"	#ТЕСТ
Status	#СОСТОЯНИЕ
"Polling loop failure"	НЕИСПР ДПЛС

Figure 20. Message Descriptors

This tab is intended to edit texts of user SMS if necessary. Symbols in Latin or Cyrillic scripts can be used. The SMS writing system can be selected from the context menu by right clicking on a text string.

Tab «GPRS Settings»



UPROG Configuration Tool for UO-4S (version 2,55)

☑ Enable GPRS

CMS Settings

	Main Channel	Backup Channel
IP address:	80.252.157.71	192.168.20.4
Port:	10003	10004
Main/Backup Recipient MasterKey	✓	✓
W/o Encryption	☑	☑

Connection Establishment Timeout, s	60
Response Waiting Timeout, s	20
Transmission Attempts	5
TEST Transmission Period, s	120
Group Number	9

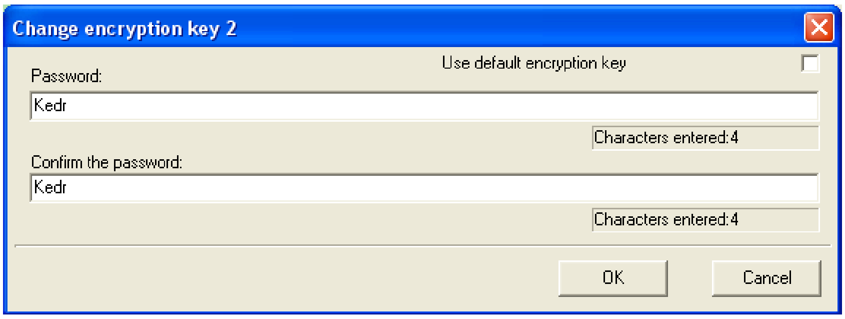
	SIM1 Parameters	SIM2 Parameters
Dial-up number	*99#	*99#
Login	beeline	mts
Password	beeline	mts
APN:	internet.beeline.ru	internet.mts.ru

Figure 21. GPRS Settings

Enable GPRS: The flag enables sending data over the GPRS channel.

For the main and backup receiver the following parameters must be set individually:

- IP Address (Static IP address of the host with Egida rev.3 Central Monitoring Station)
- Port (the number of the UDP port open for receiving messages over Internet on the host with Egida rev.3 Central Monitoring Station)
- MasterKey (encryption key). This key is used for encrypted transmitting of events to Egida rev.3 Central Monitoring Station. To specify a key, open the relevant dialog window by clicking the check mark at the right part of the MasterKey field (see Figure 22). To use the default encryption key, tick the relevant box at the right top part of the window.



Change encryption key 2

Use default encryption key □

Password: Kedr

Characters entered:4

Confirm the password: Kedr

Characters entered:4

Figure 22. Changing Encryption Key

Also your own encryption key can be generated by the program automatically using the typed passphrase. For doing so, enter a password in Latin script into the Password field, then confirm it, and finally save changes by clicking OK. For Egida 3 Central Monitoring Station the same password must be entered in GPRS settings for this UO-4S to provide decoding of the notifications.

W/o Encryption: If this flag is set on then the UO-4S sends DC09 notifications without encrypting them. *(This parameter is recommended to be set on for networks with low GPRS channel throughput and high density of events sent from the UO-4S to the CMS (Central Monitoring Station).*

If backup channel is not in use then there must be all zeros in the IP Address and Port fields.

Common settings are the following:

- Connection Establishment Timeout (60 seconds is recommended)
- Response Waiting Timeout (20 seconds)
- Transmission Attempts (the minimum recommended value is 2-3 attempts)
- TEST Transmission Period (60 to 250 seconds); *this time must be longer than call setup time*
- Group Number (the number of the group in which GPRS-transmission is included)

Carrier settings, to be set individually for SIM1 and SIM2:

- Login (the login (account name to access GPRS service of the carrier. For every carrier its specific login must be used, for example “mts” for the “MTC” carrier, “beeline” for the “Beeline” carrier, and “megaphone” for the “Мегафон” carrier)
- Password (the password to access GPRS service of the carrier. For every carrier its specific password must be entered, for example “mts” for the “MTC” carrier, “beeline” for the “Beeline” carrier, and “megaphone” for the “Мегафон” carrier)

Access point name APN (the name of the GPRS/3G gateway for your carrier, for example “internet.beeline.ru” for “Beeline”, “internet.mts.ru” for “MTC:, and “internet.megafone.ru” for “Мегафон”).

The UO-4S must be maintained at least annually by electricians with the third or higher electric safety qualification level.

To maintain the panel, do the following:

a) Ensure the panel enclosure is not damaged and is mounted securely; ensure the wire terminals are fastened properly;

b) Remove dust, debris, and corrosion from the contact connections and the panel enclosure;

c) Inspect panel operability by testing panel indication in accordance with Table 1 and panel sounder performance in accordance with Table 2.

Table 9. Troubleshooting

Problem	Possible Cause	Solution
POWER LED is off when the UO-4S is switched on	No power is applied	Check power voltage to be applied to the UO-4S
POWER LED flashes with amber two times per second	Input power voltage is exceeding 15 V or is below 10 V	Check the level of the supply voltage
COM FAULT LED illuminates with amber	No communication with the devices or the control panel over the RS-485 interface	For a slave mode check the operation mode of the control panel. For the Master mode check the XT2 jumper to be open
GSM LED doesn’t illuminate	SIM card not inserted or failed	Check the SIM card
	SIM card is locked to ask PIN or extra options (such as SimToolKit) are activated for it	Turn off asking the PIN and extra options for the SIM card by means of a mobile phone or the carrier
COM FAULT LED pulses with amber two times per second	• SIM card cannot register in the mobile network • No connection with the subscriber (message failed to be delivered) • No connection with the central station • Wrong phone number of the SMS center is entered • Account balance is lower than a minimum value	• Make sure the SIM card is inserted into the relevant slot • Check the antenna or connect an external one • Check the signal level at the mounting location of the UO-4S by means of a mobile phone • Enroll the phone number of the SMS center into the SIM card as described in the phone manual (use a cell phone to setup) • Eliminate the financial debt
POWER LED flashes with amber once per two seconds	Mains power applied to the RIP has failed (signal from contacts 5 and 6)	Repair mains power of the RIP

STORAGE, TRANSPORTATION, AND WARRANTY

STORAGE

The UO-4S in the consumer packing must be stored in line with Storage Ambients 1 of Russian Standard ГОСТ 15150-69.

The premises where the UO-4S is stored must be free from any acid fumes, alkaline fumes and other aggressive gases and harmful impurities which can cause corrosion.

TRANSPORTATION

The packed UO-4S should be transported by any covered vehicles in accordance with requirements of transport organizations.

The transportation terms and conditions for the UO-4S must be the same as Storage Ambients 5 of Russian Standard ГОСТ 15150-69.

WARRANTY

The manufacturer warrants the UO-4S to conform its technical specifications if the consumer meets the rules of transportation, storage, mounting, and operation.

The warranty period is 18 months since putting the panel into operation, but no more than 24 months since the acceptance date.

In case of difficulties in programming or operating the product, please contact Technical Support by calling +7 495 775-71-55 (multichannel) or by emailing support@bolid.ru.

APPENDIX A. CONTACT ID PROTOCOL

Notification	Contact ID Protocol Messages					
	Serial Number *4 symbols*	*ID*	*Qualifier*	*Event Code*	*Partition Number* *2 symbols*	*Zone Number (Z), User ID* *3 symbols*
Disarmed	XXXX	18	1	401	P	User
Armed	XXXX	18	3	401	P	User
Arming Failed	XXXX	18	1	454	P	Z
Guessing	XXXX	18	1	406	P	Z
Patrol Check	XXXX	18	1	999	P	Z
Fire Loop Failure	XXXX	18	1	373	P	Z
Fire Alarm	XXXX	18	1	110	P	Z
Fire Prealarm (Orion)	XXXX	18	1	118	P	Z
Intrusion Alarm	XXXX	18	1	132	P	Z
Panic Alarm	XXXX	18	1	122	P	Z
Entrance Alarm	XXXX	18	1	134	P	Z
Alarm Loop Open Circuit Failure	XXXX	18	1	371	P	Z
Alarm Loop Short Circuit Failure	XXXX	18	1	372	P	Z
Loop Repaired After Open Failure	XXXX	18	3	371	P	Z
Loop Repaired After Short Failure	XXXX	18	3	372	P	Z
Power Failed *(power voltage is below 11 V or above 15 V)*	XXXX	18	1	302	P	Z
Power Restored	XXXX	18	3	302	P	Z
AC Power Failed *(longer than 20 seconds)*	XXXX	18	1	301	P	Z
AC Power Restored *(longer than 20 seconds)*	XXXX	18	3	301	P	Z
Tamper Alarm	XXXX	18	1	383	P	Z
Tamper Restored	XXXX	18	3	383	P	Z
Device Restart	XXXX	18	1	305	P	Z
Polling Loop Failure *(Orion)*	XXXX	18	1	331	P	Z
Polling Loop Restored *(Orion)*	XXXX	18	3	331	P	Z
Output Circuit Failure *(Orion)*	XXXX	18	1	320	P	Z
Output Circuit Restored *(Orion)*	XXXX	18	3	320	P	Z
Device Disconnected *(Orion)*	XXXX	18	1	350	P	Z
Device Connected *(Orion)*	XXXX	18	3	350	P	Z
Starting Programming Mode	XXXX	18	1	627	P	Z
PL Short Circuit *(Orion)*	XXXX	18	1	332	P	Z
Disabled *(Orion)*	XXXX	18	1	382	P	Z
Enabled *(Orion)*	XXXX	18	3	382	P	Z
High Temperature *(Orion)*	XXXX	18	1	158	P	Z
Low Temperature *(Orion)*	XXXX	18	1	159	P	Z
High Level *(Orion)*	XXXX	18	1	166	P	Z
Low Level *(Orion)*	XXXX	18	1	167	P	Z
Two High Level *(Orion)*	XXXX	18	1	168	P	Z
Too Low Level *(Orion)*	XXXX	18	1	169	P	Z
Normal Level *(Orion)*	XXXX	18	3	166	P	Z

Notification	Contact ID Protocol Messages					
	Serial Number *4 symbols*	*ID*	*Qualifier*	*Event Code*	*Partition Number* *2 symbols*	*Zone Number (Z), User ID* *3 symbols*
Auxiliary Loop Alarm *(Orion)*	XXXX	18	1	150	P	Z
Auxiliary Loop Restored *(Orion)*	XXXX	18	3	150	P	Z
Low Battery *(Orion)*	XXXX	18	1	302	P	Z
Battery Restored *(Orion)*	XXXX	18	3	311	P	Z
Battery Failed *(Orion)*	XXXX	18	1	311	P	Z
Battery Test Error *(Orion)*	XXXX	18	1	309	P	Z
Overvoltage *(Orion)*	XXXX	18	1	312	P	Z
Power Restored *(Orion)*	XXXX	18	3	312	P	Z
Charger Failed *(Orion)*	XXXX	18	1	319	P	Z
Charger Restored *(Orion)*	XXXX	18	3	319	P	Z
Fire Equipment Failed *(Orion)*	XXXX	18	1	380	P	Z
Fire Equipment Restored *(Orion)*	XXXX	18	3	380	P	Z
Pump On *(Orion)*	XXXX	18	1	205	P	Z
Pump Off *(Orion)*	XXXX	18	3	205	P	Z
Service Required *(Orion)*	XXXX	18	1	393	P	Z
Fire Equipment Test *(Orion)*	XXXX	18	1	607	P	Z
Test Quitted *(Orion)*	XXXX	18	3	607	P	Z
Substitution *(Orion)*	XXXX	18	1	339	P	Z
Door Forced Open *(Orion)*	XXXX	18	1	426	P	Z
Door Restored *(Orion)*	XXXX	18	3	426	P	Z
Door Held Open *(Orion)*	XXXX	18	1	426	P	Z
Test Error *(Orion)*	XXXX	18	1	343	P	Z
Alarm Test *(Orion)*	XXXX	18	1	611	P	Z
Subscriber Communication Fault *(Orion)*	XXXX	18	1	351	P	Z
Communication Restored *(Orion)*	XXXX	18	3	351	P	Z
Leak Alarm *(Orion)*	XXXX	18	1	154	P	Z
Leakage Repaired *(Orion)*	XXXX	18	3	154	P	Z
Auto On *(Orion)*	XXXX	18	1	221	P	Z
Auto Off *(Orion)*	XXXX	18	3	221	P	Z
Discharge *(Orion)*	XXXX	18	1	222	P	Z
No-Pulse Release *(Orion)*	XXXX	18	1	223	P	Z
Release Failed *(Orion)*	XXXX	18	1	225	P	Z
Inhibited *(Orion)*	XXXX	18	1	226	P	Z
Abort *(Orion)*	XXXX	18	1	227	P	Z
Pressure Switch Failed *(Orion)*	XXXX	18	1	230	P	Z
Pressure Signal *(Orion)*	XXXX	18	1	224	P	Z
Pre-Discharge Delay *(Orion)*	XXXX	18	1	229	P	Z
Released *(Orion)*	XXXX	18	1	228	P	Z
Fire 2 Alarm *(Orion)*	XXXX	18	1	119	P	Z
Voice Alarm Activated *(Orion)*	XXXX	18	1	231	P	Z
Voice Alarm Stopped *(Orion)*	XXXX	18	3	231	P	Z
Noise *(Orion)*	XXXX	18	1	394	P	Z
Noise Removed *(Orion)*	XXXX	18	3	394	P	Z
Actuator Failed *(Orion)*	XXXX	18	1	165	P	Z
Actuator Error *(Orion)*	XXXX	18	1	170	P	Z
Actuator in Initial Position *(Orion)*	XXXX	18	3	164	P	Z
Actuator in Operating Position *(Orion)*	XXXX	18	1	164	P	Z
Manual Test *(Orion)*	XXXX	18	1	614	P	Z

APPENDIX B. USER’S SMS

Default Notification List

Notification	In Latin	In Cyrillic
Disarmed	DISARMED	СНЯТ
Armed	ARMED	ВЗЯТ
Arming Failed	FAULT	НЕВЗЯТ
Wrong Code (is generated after presenting three unknown credentials)	REFUSE	ДОСТУП ОТКЛОНЕН
Patrol Check	DETAIL	ОТМЕТКА НАРЯДА
Alarm Loop Open Circuit Failure	BREAK	ОБРЫВ
Alarm Loop Short Circuit Failure	SHORT	КОРОТКОЕ ЗАМЫКАНИЕ
Fire Alarm	FIRE	ПОЖАР
Fire Prealarm (Orion)	ATTENTION	ВНИМАНИЕ!
Intrusion Alarm	ALARM	ТРЕВОГА
Panic Alarm	PANIC	НАПАДЕНИЕ
Entrance Alarm	ENTRY ALARM	ТРЕВОГА ВХОДА
Power Failure (below 11 V or above 16 V)	DC TROUBLE	НЕИСПР ПИТАН
Power Restored	DC OK	ПИТАНИЕ В НОРМЕ
AC Power Failed	AC LOW	НАРУШ ОСН ПИТАН
AC Power Restored	AC OK	ВОССТ ОСН ПИТАН
Tamper Alarm	OPEN	ВСКРЫТИЕ КОРПУСА
Tamper Restored	CLOSE	ЗАКРЫТИЕ КОРПУСА
Device Restart	RESET	СБРОС
Polling Loop Failure (Orion)	TROUBLE 2WIRE	НЕИСПРАВНОСТЬ ДПЛС
Polling Loop Restored (Orion)	RESET 2WIRE	ВОССТАНОВЛ ДПЛС
Output Circuit Failure (Orion)	RELEY TROUBLE	НЕИСПР ЦЕПИ ВЫХ
Output Circuit Restored (Orion)	RELEY RESET	ВОССТАН ЦЕПИ ВЫХ
Device Disconnected (Orion)	DISCONNECT	НАРУШЕНИЕ СВЯЗИ
Device Found (Orion)	CONNECT	ВОССТАНОВЛ СВЯЗИ
Programming Started	PROG PART	ПРОГРАММИРОВАНИЕ
TEST (only states of own alarm loops are transmitted in the notification)	TEST STATUS ARMED or STATUS DISARMED	ТЕСТ СОСТОЯНИЕ ВЗЯТ or СОСТОЯНИЕ СНЯТ
Alarm Loop State (is generated as a response to a Request Armed command)	STATUS ARMED or STATUS DISARMED	СОСТОЯНИЕ ВЗЯТ or СОСТОЯНИЕ СНЯТ

In the Standalone Mode the events are transmitted with the number of an alarm loop:

– *Object Name, DD-MM (optional) HH:MM, Event, Alarm Loop, Object Description (optional)*

– *Object Name, DD-MM (optional) HH:MM, Event, User Number, User Description (optional)*

For the modes Slave 1, Slave 2, Master the notifications are transmitted with the number of partition and the number of zone:

– *Object Name, DD-MM (optional) HH:MM, Event, Partition, Zone, Object Description (optional)*

– *Object Name, DD-MM (optional) HH:MM, Event, Partition, User Number, User Description (optional)*

APPENDIX C. EGIDA-2 SMS

Notification	Egida-2 Local Mode	Egida-2 Slave 1/2, Master Mode
Disarmed	DISARMED **S** USER N	DISARMED PART **P** USER **N**
Armed	ARMED **S** USER **N**	ARMED PART **P** USER **N**
Arming Failed	FAULT **S**	FAULT PART **P** ZONA **Z**
Wrong Code (is generated after presenting three unknown credentials)	REFUSE	-
Patrol Check	DETAIL	DETAIL
Alarm Loop Open Circuit Failure	TRUBLE **S**	TROUBLE PART **P** ZONA **Z**
Alarm Loop Short Circuit Failure	TRUBLE **S**	TROUBLE PART **P** ZONA **Z**
Fire Alarm	FIRE **S**	FIRE PART **P** ZONA **Z**
Fire Prealarm (Orion)	-	ATTENTION PART **P** ZONA **Z**
Intrusion Alarm	ALARM **S**	ALARM PART **P** ZONA **Z**
Panic Alarm	PANIC **S**	PANIC PART **P** ZONA **Z**
Entrance Alarm	ENTRY ALARM **S**	ENTRY ALARM PART **P** ZONE **Z**
Power Failed (below 11V or above 16 V)	DC LOW	DC LOW PART **P** ZONE **Z**
Power Restored	DC OK	DC OK PART **P** ZONE **Z**
AC Power Failed	AC LOW	AC LOW PART **P** ZONE **Z**
AC Power Restored	AC OK	AC OK PART **P** ZONE **Z**
Tamper Alarm	OPEN	OPEN PART **P** ZONE **Z**
Tamper Restored	CLOSE	CLOSE PART **P** ZONE **Z**
Device Restart	RESET	RESET PART **P** ZONE **Z**
Polling Loop Failure (Orion)	-	TROUBLE 2WIRE PART **P**
Polling Loop Restored (Orion)	-	RESET 2WIRE PART **P**
Output Circuit Failure (Orion)	-	RELEY TROUBLE PART **P**
Output Circuit Restored (Orion)	-	RELEY RESET PART **P**
Device Disconnected (Orion)	-	DISCONNECT PART **P**
Device Found (Orion)	-	CONNECT PART **P**
Programming Started	PROG	PROG PART **P**
TEST (only states of own alarm loops are transmitted in the notification)	-	TEST STATUS ARMED **Z** or STATUS DISARMED
Alarm Loop State (is generated as a response to a Request Armed command)	-	STATUS ARMED ZONE **Z** or STATUS DISARMED

Where:

- **S** is for the number of the alarm loop
- **P** is for the number of the partition
- **D** is for the address of the device
- **Z** is for the number of the zone

APPENDIX D. EGIDA-3 SMS

Notification	SMS	Event Source
Disarmed	F99 IXXXX M242	Partition/UO-4S Internal Alarm Loop
Armed	F99 IXXXX M241	Partition/UO-4S Internal Alarm Loop
Arming Failed	F99 IXXXX M17	Zone/UO-4S Internal Alarm Loop
Wrong Code	F99 IXXXX M26	Reader
Patrol Check	F99 IXXXX M223	UO-4S
Open Circuit Failure	F99 IXXXX M45	Zone/UO-4S Internal Alarm Loop
Short Circuit Failure	F99 IXXXX M214	Zone/UO-4S Internal Alarm Loop
Fire Alarm	F99 IXXXX M37	Zone/UO-4S Internal Alarm Loop
Fire Prealarm (Orion)	F99 IXXXX M44	Zone
Intrusion Alarm	F99 IXXXX M3	Zone/UO-4S Internal Alarm Loop
Panic Alarm	F99 IXXXX M58	Zone/UO-4S Internal Alarm Loop
Entrance Alarm	F99 IXXXX M118	Zone/UO-4S Internal Alarm Loop
Power Failed	F99 IXXXX M198	Zone / Device
Power Restored	F99 IXXXX M199	Zone / Device
AC Power Failed	F99 IXXXX M2	Zone / Device
AC Power Restored	F99 IXXXX M1	Zone / Device
Tamper Alarm	F99 IXXXX M149	Zone / Device
Tamper Restored	F99 IXXXX M152	Zone / Device
Device Restart	F99 IXXXX M203	Device
Polling Loop Failure (Orion) (increased polling loop voltage)	F99 IXXXX M222	Device
Polling Loop Restored (Orion)	F99 IXXXX M47	Device
Output Open Circuit Failure	F99 IXXXX M112	Zone
Output Short Circuit Failure	F99 IXXXX M122	Zone
Output Circuit Restored	F99 IXXXX M123	Zone
Device Disconnected (Orion)	F99 IXXXX M250	Device
Device Connected (Orion)	F99 IXXXX M251	Device
Starting Programming Mode	F99 IXXXX M84	Device
RS-485 Communication Fault	F99 IXXXX M217	Device
RS-485 Communication Restored	F99 IXXXX M218	Device
Polling Loop Short Circuit Failure	F99 IXXXX M215	Device
Alarm Loop Disconnected	F99 IXXXX M187	Zone
Alarm Loop Connected	F99 IXXXX M188	Zone
Output Disconnected	F99 IXXXX M126	Zone
Output Connected	F99 IXXXX M127	Zone
High Temperature	F99 IXXXX M76	Zone
Low Temperature	F99 IXXXX M206	Zone

Notification	SMS	Event Source
Normal Temperature	F99 IXXXX M78	Zone
High Level	F99 IXXXX M74	Zone
Low Level	F99 IXXXX M71	Zone
Too High Level	F99 IXXXX M75	Zone
Too Low Level	F99 IXXXX M77	Zone
Normal Level	F99 IXXXX M72	Zone
Auxiliary Input Alarm	F99 IXXXX M35	Zone
Auxiliary Input Restored	F99 IXXXX M36	Zone
Low Battery	F99 IXXXX M211	Device / Zone
Battery Failed	F99 IXXXX M202	Device / Zone
Battery Restored	F99 IXXXX M200	Device / Zone
Battery Test Error	F99 IXXXX M205	Device / Zone
Power Supply Overload	F99 IXXXX M194	Device / Zone
Overload Repaired	F99 IXXXX M195	Device / Zone
Charger Failed	F99 IXXXX M196	Device / Zone
Charger Restored	F99 IXXXX M197	Device / Zone
Fire Equipment Failed	F99 IXXXX M41	Device / Zone
Fire Equipment Restored	F99 IXXXX M39	Zone
Pump On	F99 IXXXX M130	Zone / Output
Pump Off	F99 IXXXX M131	Zone / Output
Service Required	F99 IXXXX M204	Zone / Output
Alarm Test	F99 IXXXX M19	Zone
Fire Equipment Test Started	F99 IXXXX M20	Device / Zone
Test Quitted	F99 IXXXX M21	Device / Zone
Configuration Error	F99 IXXXX M165	Zone
Door Forced Open	F99 IXXXX M27	Reader
Door Restored	F99 IXXXX M31	Reader
Door Held Open	F99 IXXXX M33	Reader
Access Denied	F99 IXXXX M29	Reader
Test	F99 IXXXX M255	Device
Subscriber Communication Fault *(Orion)*	F99 IXXXX M90	Subscriber
Communication Restored *(Orion)*	F99 IXXXX M91	Subscriber
Leak Alarm *(Orion)*	F99 IXXXX M79	Zone
Leakage Repaired *(Orion)*	F99 IXXXX M80	Zone
Auto On *(Orion)*	F99 IXXXX M148	Zone
Auto Off *(Orion)*	F99 IXXXX M142	Zone
Discharge *(Orion)*	F99 IXXXX M146	Zone
No-Pulse Error *(Orion)*	F99 IXXXX M145	Zone
Release Failed *(Orion)*	F99 IXXXX M139	Zone

Notification	SMS	Event Source
Inhibited *(Orion)*	F99 IXXXX M147	Zone
Abort *(Orion)*	F99 IXXXX M143	Zone
Pressure Switch Failed *(Orion)*	F99 IXXXX M221	Zone
Pressure Signal *(Orion)*	F99 IXXXX M220	Zone
Pre-Discharge Delay *(Orion)*	F99 IXXXX M141	Zone
Released *(Orion)*	F99 IXXXX M144	Zone
Fire 2 Alarm *(Orion)*	F99 IXXXX M40	Zone
Voice Alarm Activated *(Orion)*	F99 IXXXX M150	Zone
Voice Alarm Stopped *(Orion)*	F99 IXXXX M151	Zone
Noise *(Orion)*	F99 IXXXX M4	Zone
Noise Removed *(Orion)*	F99 IXXXX M6	Zone
Actuator Failed *(Orion)*	F99 IXXXX M155	Zone
Actuator Error *(Orion)*	F99 IXXXX M156	Zone
Actuator in Initial Position *(Orion)*	F99 IXXXX M154	Zone
Actuator in Operating Position *(Orion)*	F99 IXXXX M153	Zone
Manual Test *(Orion)*	F99 IXXXX M140	Zone

APPENDIX E. VOICE MESSAGES

List of Default Voice Messages

Notification	Voice Message
Disarmed	Снят с охраны раздел P пользователь N
Armed	Взятие под охрану раздел P пользователь N
Arming Failed	Не взятие раздел P зона Z [пользователь N]
Wrong Code (generated after three presenting of unknown credentials)	Доступ отклонен прибор D
Patrol Check	Отметка наряда прибор D
Open Circuit Failure	Обрыв раздел P зона Z
Short Circuit Failure	Короткое замыкание раздел P зона Z
Fire Alarm	Пожар раздел P зона Z
Fire Prealarm (Orion)	Опасность пожара раздел P зона Z
Intrusion Alarm	Тревога раздел P зона Z
Panic Alarm	Нападение раздел P зона Z
Entrance Alarm	Тревога входа раздел P зона Z
Power Failed (is below 11 V or exceeds 16 V)	Неисправность питания раздел P зона Z
Power Restored	Восстановление резервного питания прибор D
AC Power Failed	Нарушение основного питания раздел P зона Z
AC Power Restored	Восстановление основного питания раздел P зона Z
Tamper Alarm	Взлом корпуса раздел P зона Z
Tamper Restored	Закрытие корпуса раздел P зона Z
Device Reset	Сброс раздел P зона Z
Polling Loop Failure (Orion)	Нарушение ДПЛС раздел P зона Z
Polling Loop Restored (Orion)	Восстановление ДПЛС раздел P зона Z
Output Circuit Failure (Orion)	Нарушение выхода раздел P зона Z
Output Circuit Restored (Orion)	Восстановление выхода раздел P зона Z
Communication Fault (Orion)	Нарушение связи раздел P зона Z
Communication Restored (Orion)	Восстановление связи раздел P зона Z
Programming Started	Программирование раздел P зона Z [пользователь N]
TEST (only states of own alarm loops are transmitted in the notification)	--------------
Alarm Loop State (is generated as a response to a Request Armed command)	--------------

Where:

- **P** is for the number of the partition
- **D** is for the address of the device
- **Z** is for the number of the zone
- **N** is for the user number

MANUFACTURER DATA

Made by the Bolid Company, Russia.

4 Pionerskaya Str., Korolev, Moscow Oblast, 141070, Russia

Tel./Fax: +7 (495) 775-71-55 (multichannel), 777-40-20, 516-93-72

E-mail: info@bolid.ru, http://bolid.ru.
Technical Support: support@bolid.ru.