Attention! Reliability and life of the product are provided not only by the quality of product itself, but also by the compliance with operating modes and conditions, therefore, this document requirements is mandatory

"Lun-11" (mod.5, 6)
GSM/3G Wireless Communication Link Control Panel

Operating Manual

$C\epsilon$

<table>
<tr><td rowspan="5">ortus
ORTUS Group</td><td colspan="3">Product Compatibility Table</td></tr>
<tr><td>Control Panel</td><td>Lun-11</td><td>Version mod.5, 6</td></tr>
<tr><td>Detectors</td><td>According to two- wire or four-wire connection circuit</td><td>Version</td></tr>
<tr><td>Control Panel Configuration Software</td><td>Configurator 11</td><td>Version</td></tr>
<tr><td>Central Monitoring Station</td><td>Orlan</td><td>Version</td></tr>
</table>

Contents

1. Purpose

"Lun-11" (mod.5 and mod.6) Control Panel (CP) are designed to monitor the status of alarm and fire system zones with two-wire or four-wire circuit, to monitor the status of wireless detectors, as well as to control strobes and/or sounders and transmit announcements to the "Orlan" or "Ritm" central monitoring station (CMS) or work in stand-alone mode – events are sent to the user's monitoring center «Phoenix-Web» (registered user's Internet-based page) or to the preselected mobile phones via SMS.

The modifications difference is determined by used mobile networks:

Lun-11 mod.5	Lun-11 mod.6
• GSM (850/900/1800/1900 MHz)	•3G (WCDMA 900/2100 MHz, HSDPA, HSUPA) •GSM (850/900/1800/1900 MHz)

Control Panel includes the master unit and one or several Indication and Control Devices (ICD). The following devices can be used as ICD (shipped separately):

- "**Lind-11**" ICD – multifunctional LCD keypad;
- "**Lind-11TM**" ICD – TouchMemory key (DS1990A-F5) reader;
- "**Lind-11LED**" ICD – multifunctional LED-keypad;
- "**Lind-9M3**" ICD – multifunctional keypads;
- "**Lind-EM**" – RFID-card reader;
- "**Lind-15**"/"**Lind-29**" – multifunctional keypad with touch LCD.
- Any third party TouchMemory Anti-vandal Key Reader can be used for CP arming/disarming. In this case can be used an ordinary TouchMemory keys (DS1990A-F5) or copy protected keys (DS1961S-F5).

Control Panel can be enhanced with the following Functionality Expansion Modules (EM):

- "**Lun-11E**" EM (adds 10 alarm zones, mounted inside a Control Panel housing);
- "**Lun-11H**" EM (adds 10 alarm zones, 2 PGM outputs and 1 BELL output, can be completed with the network supply unit);
- "**LanCom**" Ethernet-communicator (**rev.14** or **rev.15**);
- "**TK-17**" Telephone Communicator;
- Relay outputs module **"MPB-8M"** for 8 configurable isolated relay outputs;
- "**AM-11**" Address Module (allows for connection of up to 31 devices to TAN address bus, each modules adds 3 alarm zones);
- "**Dozor**" Alarm Photo-proof Module (make photo of the configured events from up to four analog cameras);
- "**P433**" Radio Receiver for Visonic®, Roiscok®, Rielta® wireless detectors/keyfobs;
- "**P433M**" Radio Receiver for Jablotron® wireless detectors/keyfobs;
- "**MCR-300**" Visonic® Radio Module for Visonic® wireless detectors/keyfobs;
- "**Astra-RI-M**" or "**Astra-RI-M RR**" Radio Module or "**P433A**" for "Astra"® wireless detectors/keyfobs;
- "**Crow-Lun-11 Adapter**" Radio Module for "Crow"® wireless detectors/keyfobs;
- Ajax Radio Receiver "**RR-108**" or "**uartBridge**" for "Ajax"® wireless detectors/keyfobs.

Control Panel uses AES-128 communication protocol encryption for communication with "Orlan" CMS.

We declare that this control panel is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

It should be installed by qualified professionals who will inform you about the principles of its operation and provide regular maintenance and testing.

This product can be used in all EU member states.

> **Attention! Product is not equipped with built-in cameras and microphones, devices and units for hidden video and audio recording.**

2. Safety Precautions

Only the employees, familiar with the Control Panel configuration, instructed on the safety arrangements, and having the permit to work with electrical installations with the capacity of up to 1000 V shall be allowed to install, routinely maintain and repair the Control Panel.

> **Attention! The Control Panel has open live parts posing the electrical shock hazard. The Control Panel has safety ground, termination point of which is indicated and placed in the network terminal block.**

Control Panel is designed for permanent connection to a single-phase AC mains 100…240V. An easily accessible bipolar switch must be provided to full disconnect Control Panel from the AC mains. This bipolar switch must be placed in the room where the Control Panel is installed.

3. Technical characteristics

Control Panel has the following technical characteristics (Table 1):

Table 1. Control Panel's basic technical parameters

Parameter name	Value
Number of wired zones	8
Maximum number of groups	16
Maximum number of NC detectors in the zone	32
Current in the fire zone for "normal" status, maximum, mA (for circuit with NC detectors)	8
Number of the controlled outputs (PGM)	4
Number of "Lun-11E"/"Lun-11H" EM connected	12
Number of "Lind-11"/"Lind-11LED" ICD connected	16
Number of "Lind-11TM" ICD connected	24
Total number of binded wireless zones/sirens *	48/16
Number of wireless sirens connected (Crow wireless system)	16
Number of "AM-11" address modules connected	31
Number of wired zones of "AM-11" address module	3
Number of RFID tags Readers of EM-Marine "Lind-EM" standard	14
Connection of TouchMemory Anti-vandal Electronic Key Reader	available
Time-out for detection of wireless detector connection failure, min	10**…1450
Availability of integrated Battery Charge Controller	+
Output current +S12V, A, max	0,5
Output current +12F1, A, max	1
Output current +12F2, A, max	1
Output current Bell, A, max	0,5
Leakage impedance, between zone wires, kOhm, min	50
Resistance of zone wires, Ohm, max	100
Zone response time in the normal mode, ms max	350
Zone response time in the Instant mode, ms max	20
Failure detection time, seconds, max	300

Control Panel power voltage, V	14.0...16.5
Absorbed current consumption of the Control Panel board and "Lind-11/11TM" (without peripheral equipment and battery charge current), mA, max	500
Absorbed current of the armed Control Panel board***, mA, max	160
Absorbed current of "Dozor" module with no cameras, maximum/armed, mA	150/120
Absorbed current of "P433" radio receiver, maximum/armed, mA	70/65
Absorbed current of "AM-11" address module, maximum, mA	3
Allowable joint current for +12F1, +12F2, S12V, Bell outputs including consumption of Control Panel board, A, max	1.2
Resistance of wired zone end-of-line resistor (see app. 2), kOhm	2±5%
AC mains power voltage, V	100...240
AC mains absorbed current, A, max	0,74
Battery power voltage, V	11.5...14.0
Battery absorbed current, exclusive of peripheral equipment, mA, max	500
Battery cut-off voltage, V, min	10,9
Battery voltage, when "Low battery" event is generated, V, min	11.2
Battery voltage, when "Normal charge" event is generated, V, min	12.5
Charging rate, mA, max	700
Charging rate cut-off, mA, max	900
Output voltage +S12V (active state), V	10...14.0
Bell output commutation voltage, V, max	18.0
Output ripple, mV, max	300
Battery and recharger fault location time, max, sec	300
Time of delay of mains supply failure message, sec	60
Recommended battery parameters**** (gel maintenance-free sealed lead battery, for example CSB GB1272F2), voltage, V/capacity, Ah	12 / 7.2
Rated current of input wire fuse (FU1), A	1.0
Rated current of battery short circuit protection wire fuse (FU2), A	2.5
The capacity of non-volatile event log	16384
The size of non-volatile event queue	128
Number of remote control functions in "voice" mode (DTMF)	8
Number of remote control functions in GPRS mode	14
Housing dimensions, WxHxD, mm	300x240x91
Dimensions when packed, WxHxD, mm	325x255x100
Device weight, net/gross, kg, max	1.5 / 1.7

* – The actual total number of binded wireless devices (by its types too) is limited by the capacity of the wireless system and may be less than indicated in the table – for details, refer to the documentation of the manufacturer of the wireless system.

** – The minimum possible timeout value depends on the wireless system type.

*** – The estimated operating time of the control panel from the full charged recommended battery with the Lind-11 ICD and 3 wired motion sensors connected to the main board (1 SIM card, GPRS channel, test period sets to 10 minutes) – up to 45 hours.

**** – Battery is outside the scope of supply, but it can be supplied on demand.

> **Attention! The maximum current consumed from power supply unit shall not exceed 1.2 A! Safety ground for the power supply unit is required!**

An example of calculation of the required battery capacity:

Absorbed current of the armed Control Panel, max	**160 mA**
Absorbed current of the armed "Lind-11", max	**30 mA**
detectors current	**~10 mA**

Total battery capacity required to provide one-day work is **(0.16+0.03+0.01)*24=4.8 Ah.**

It is also required to provide one hour of the alarmed mode (additional current consumption of **100 mA**), which will require **0.3 Ah**.

Total capacity will be **(4.8+0.3)=5.1 Ah.**

The nearest larger value of the battery capacity equals **7.2 Ah** shall be selected.

4. Detectors selecting

Control Panel allows the connection to both the burglar alarm and fire zones of any detectors with **normally open** or **normally closed** contacts only in accordance with the **two or four-wire connection circuit**. Each zone type and its response time (see. Section 6.3) may be selected during Control Panel configuration process.

The possible detector connection circuits are shown in section 25.

5. Device appearance and functions of its terminals

Layout of Control Panel components in the housing is shown in Figure 1.
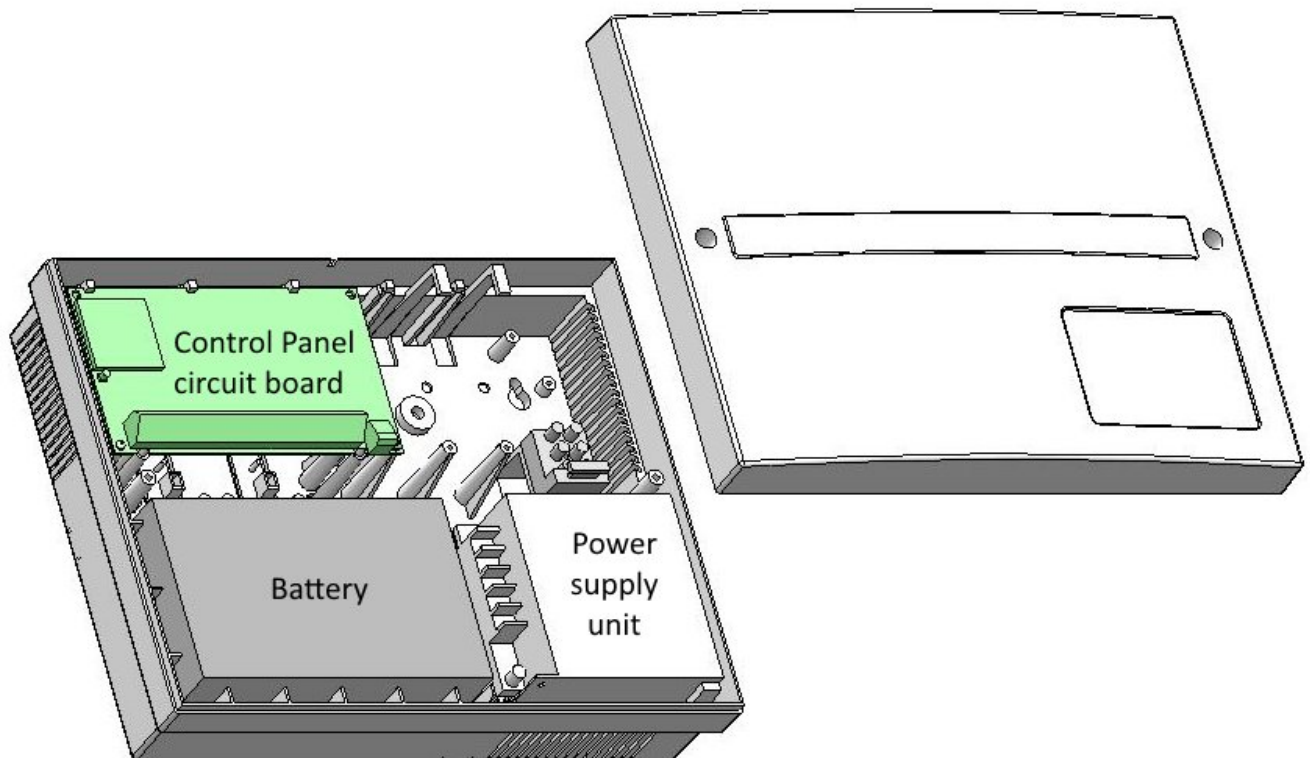
Figure 1. Control Panel components in its housing (upper cover open)

The housing overall dimensions are given in Figure 2, mounting dimensions – in Figure 3.

Control Panel's housing should be installed on a solid, reliable, flat vertical plane (for example, on a concrete wall). The orientation of the housing must correspond to the instructions in the figure 2. The reverse side of the enclosure should be completely located on the surface where it is installed.

The wires/cables must be inserted into the housing through the special places provided for this purpose – the holes on the back or on every side walls (remove thin decorative plastic cover previously). More see in "Lun-11 mounting at B004 housing", available for download from www.lun.ortus.io site.

Figure 2. Control Panel housing overall dimensions

Back side; dimensions - mm

Figure 3. Control Panel housing mounting dimensions

The appearance of Control Panel circuit board and functions of some of its components are shown in Figure 4.

Control Panel circuit board contains the following terminals (Table 2):

Table 2. Control Panel terminals functions

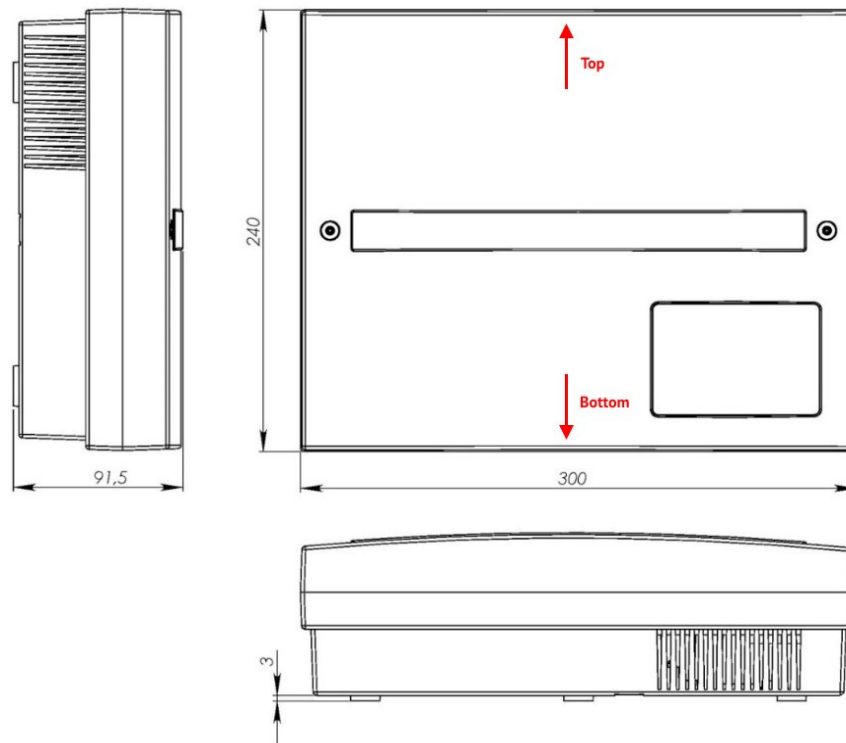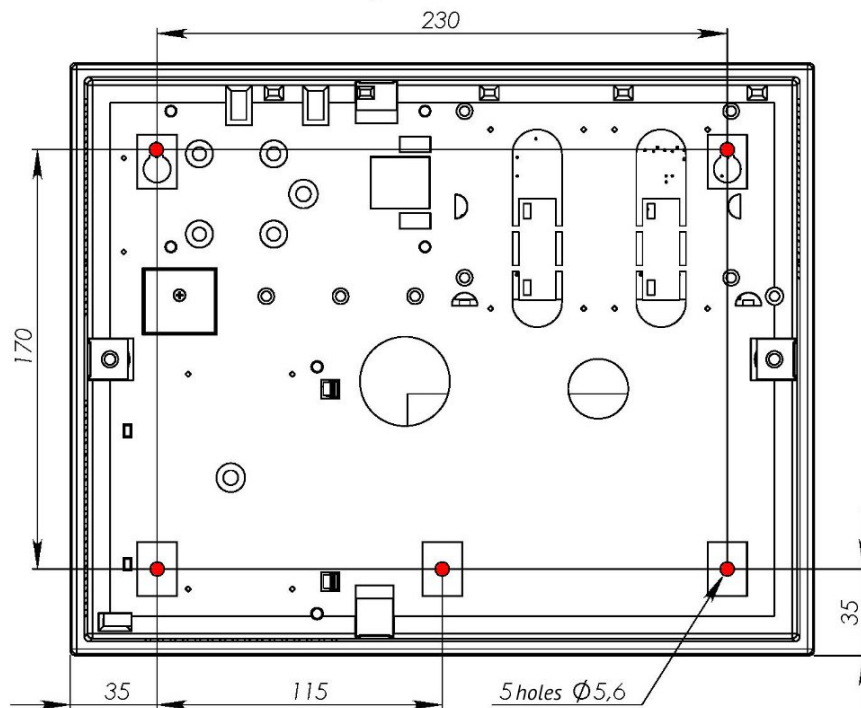| Terminal marking	Function
Z1...Z8*	Connection of zones 1...8
GND	Common terminal (−) of Control Panel
MON	Interface for the connection of "Lind-11"/"Lind-11LED" ICD, "Lun-11E"/"Lun-11N" EM, "MPB-8M" relay output module
TAN	Interface for the connection of "Lind-11TM" ICD, "Lind-EM" RFID readers, "AM-11" address modules, or TouchMemory anti-vandal electronic key reader
GND	Common terminal (−) of Control Panel
PGM1**	Programmable output 1 (−) of "Open collector" type
12F1	Output for power-up (+) of "Lind-11", "Lind-11TM" ICD and siren with limited SC current
BELL	Contact (−) of siren with limited SC current
PGM2**	Programmable output 2 (−) of "Open collector" type
12F2	Output of power-up (+) of active detectors with limited SC current
PGM3**	Programmable output 3 (−) of "Open collector" type
GND	Common terminal (−) of Control Panel
S12V	Remote controlled (with CMS and keypad) power-up output (+) of active detectors with limited SC current
PGM4**	Programmable output 3 (−) of "Open collector" type
TAMP	Input for connection of tamper for housing opening and tamper for shifting of housing from the place of installation
+14V	Power-up input (+) of Control Panel
GND	Common terminal (−) of Control Panel

* – "fire" or "burglar alarm" type of zone shall be set with the help of "Configurator 11" software, and they differ in detector connection.

** – function of each of PGM1...PGM4 controlled outputs shall be set with the help of "Configurator 11" software (see "Configurator 11" Guide). Commutation current shall not exceed 0.5A (with voltage not exceeding 15V).

> **Attention! To connect any devices to MON or TAN buses the foiled twisted pair, e.g. FTP CAT5/5e cable, shall be applied with connection of the shield wire to GND contacts at both ends – in Control Panel and connecting device.**

> **The interface cable's total length connected to the MON (or TAN) bus depending on the number of ICD in alarm system shall not exceed:**
> **150m   for up to 5   "Lind-11/11LED/15" ("Lind-11TM/EM") ICDs;**
> **100m   for up to 10 "Lind-11/11LED/15" ("Lind-11TM/EM") ICDs;**
> **50m   for up to 15 "Lind-11/11LED/15" ("Lind-11TM/EM") ICDs.**
> **30m   anti-vandal reader and ordinary keys (DS1990A-F5).**
> **5m   anti-vandal reader and copy protected keys (DS1961S-F5).**

To connect alarm zones, a straight-through cable, e.g. ALARM 6x0.22, can be used.

The connection circuits of detectors depends of the of the Control Panel zones configuration (fire or burglar alarm – see section 25).

The backup power source (battery) should be connected via the PCB wires with terminals.

> **Be careful! The black wire should be connected to the negative terminal of the battery, the red wire – to the positive terminal of the battery.**

The battery is the replaceable part and with a reduction in its capacity is subject to replacement. It is recommended to replace the battery once a year.

To replace the battery, turn off the main power supply then disconnect the battery terminals and remove battery from the Control Panel housing. A new battery of the same type, size and model must be installed in the reverse order with mandatory polarity.

If the Control Panel is planned to be turned off for a long time (more than 24 hours) or when it is taken out of service, disconnect both battery terminals.
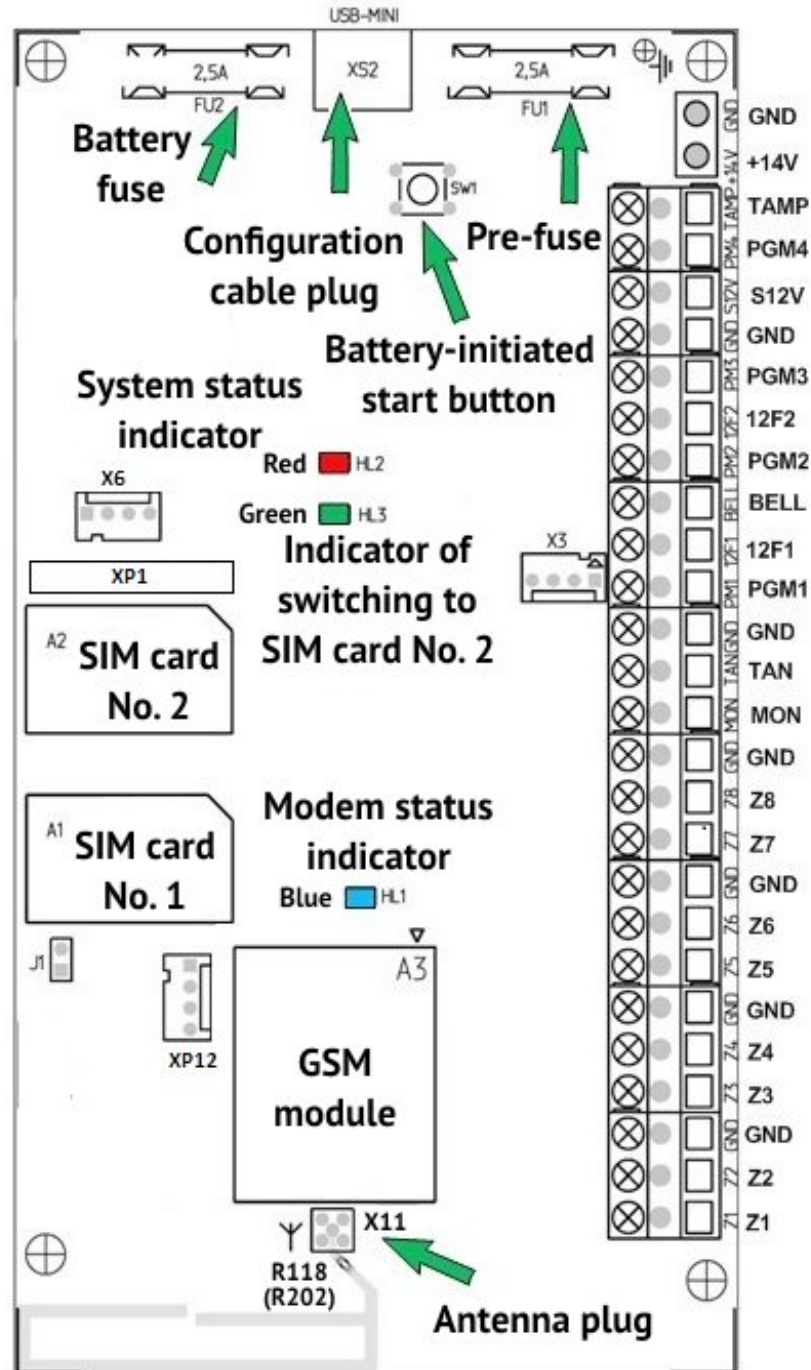

Figure 4. Control Panel circuit board appearance

It is allowed to use an additional power supply unit (PSU) to power the detectors/sirens. In this case, the minus wire (-Vout) of the Panel's built-in PSU and the minus wire (-Vout) of the additional PSU must be securely connected.

For the reliable operation, when the Panel wiring, make sure that all the twisted wires have been soldered.

6. Control Panel features

Control Panel has a few operating algorithms in GSM network depending on the communication channel used. The device allow to select a number of mobile network providers (1 or 2), transmission channels (only GPRS, only Voice channel, both GPRS+Voice), and operation with "LanCom" Ethernet communicator (rev.15 or rev.14) or WiFi module and "TK-17" telephone communicator. The Control Panel also supports the control via mobile phones of the responsible persons of the facility.

All the parameters, including channel priorities, are configured using "Configurator 11" software and stored in Control Panel non-volatile memory.

Attention! Control Panel support the remote control via GPRS, Voice, and Ethernet/Wifi. "Phoenix-4" software automatically determines the list of available commands depending on the communication channel used.

All events are automatically recorded in the nonvolatile event log with its date and time, as well as the event code. Event log can be accessed (for reading or full erasing) from the "Configurator 11" software when connecting to a computer with a USB cable.

6.1. Operating mode selecting

Control Panel send events and test messages to CMS (owned by security company) or can work in stand-alone mode – events are sent to the user's monitoring center «Phoenix-Web» (registered user's Internet-based page) or are sent to user's preselected cell phone numbers via SMS.

Operating mode selecting is carried out when configuring Control Panel in the "Configurator 11" software on the "**CMS**" tab – in "**Mode**" drop-down list (Figure 5). Depending on the configuration, the transmission of events to the CMS can be accompanied by calling to owners (to the preselected cell phone numbers, similar to that described in sections 6.1.4, 6.1.5).

6.1.1. Orlan CMS mode

If the value "**Phoenix – CMS**" selected, then Control Panel will work with the security company CMS (this is default mode used by "Orlan" CMS and controlled by "Phoenix" software).

For correct logging (matching the date and time) should turn on "**Time synchronization by CMS**" parameter and set the "**Offset of the time zone relatively to CMS**" value in the Control Panel configuration. Then set the check-box "**Synchronize time on the control panels with the CMS**" in the Phoenix 4 Control Center software settings.

If you plan to use the "**Phoenix-MK**" application, the **IP-address** and **port** of the server in the application should be set by security company data.

6.1.2. Ritm CMS mode

If the CMS used equipment "Ritm", you should select the "**Ritm – CMS**" value (and be sure to set an eight digits password and Ritm transmitted number in the window bottom part).

Time synchronization can not be used in this mode.

6.1.3. Standalone Web mode

To work with the user's monitoring center «Phoenix-Web», should select the "**Web**" value. Then all events will be transmitted to the user's monitoring center and displayed at the registered user's Internet-based page.

Only registered user can view the events, set up the Control Panel, zones, events, and other options (including for multiple security objects) – for its own security system(s) only.

> **Attention! Using the «Web-CMS" mode did not provide the service in the security company! This is a stand-alone mode (including for multiple security objects) with a convenient network interface!**

Setting parameters to Control Panel in "Web-CMS" mode differs – you should set IP-address *lun.ortus.io* and port *8089* on the "**GPRS**" tab for each SIM-card with the *Internet* **network type**. If you are using a WiFi communication channel, the above parameters (IP-address and port) should be set on "**Lan/WiFi**" tab. The Ethernet channel **can not be used** in this mode.

You will need the information contained in the "**IMEI**" field (Figure 5) for receive events from Control Panel setting on user's Internet-based page "Phoenix-Web" – click on "**Read IMEI**" button and write the number in the next field appears.

Web-based access is performed in any browser access page – www.lun.ortus.io. To enter you must specify the **e-mail address** and **password** – you can register the mailbox on the Internet previously, and then sign up for the online service www.lun.ortus.io. E-mail address will also be used to activate your account – you need to go to the link in the confirmation letter you get.

User's Monitoring Center settings and operation manual are described in the online help that is available after logging in to the page – the "**?**" button or in the document "Phoenix-web_User-Manual", available for download from www.lun.ortus.io site.

For correct logging (matching the date and time) should turn on "**Time synchronization by SNTP server**" parameter and set the "**Offset of the time zone**" value in the Control Panel configuration.

> **You should set the server IP-address *lun.ortus.io* and port *8087* in the "Phoenix-MK" application settings.**

6.1.4. Standalone mode via SMS

To work in stand alone mode by SMS, you need to select "**SMS**" value (Figure 5). Then all events and test messages will be sent as an SMS to a preselected cell phone numbers. The Control Panel sends SMS using the most priority SIM-card, and in case of impossibility to send messages from it – uses a second SIM-card. It is necessary to set "**Test period for SMS**" and "**SMS lower balance limit**", and on the tab "**SMS**" set mobile phone numbers and the types of events for each of them.

The "**SMS balance lower limit**" is set for warning exhaustion of the SIM-card balance and therefore it is necessity top up your balance for further work.

After transmission of any SMS to the owner, CMS requests SIM-card balance. If it is decreasing below the specified limit by the "**SMS balance lower limit**" parameter, the Control Panel sends a message with the contents (for example account balance 19.75):

<div align="center">

"Low SIM balance = 19.75"

</div>

Repeated reminders are not sent until balance refilled above the set limit.

To control the balance state you should specify the correct "**Request balance verification**" parameter for every SIM-card you used on the "**SIM card**" page as a USSD-request code.

> **Attention! To find out the correct USSD-request code you should refer to the mobile communication carrier (see carrier's site on the Internet).**

USSD-request example for the Kyivstar (Ukraine) carrier: **✶111#**

If USSD-request code is not specified or is incorrect or unable to check the balance, the CMS sends an SMS with a warning:

"Can't check SIM balance (USSD-query is not valid?)"

SMS is **always** sent to phone numbers with the "**SMS**" checkbox selected, in any Control Panel operating mode besides "Ritm CMS".

For correct logging (matching the date and time) should turn on "**Time synchronization by SNTP server**" parameter and set the "**Offset of the time zone**" value in the Control Panel configuration.

> **The mobile application "Phoenix-MK" can't be used in SMS mode.**
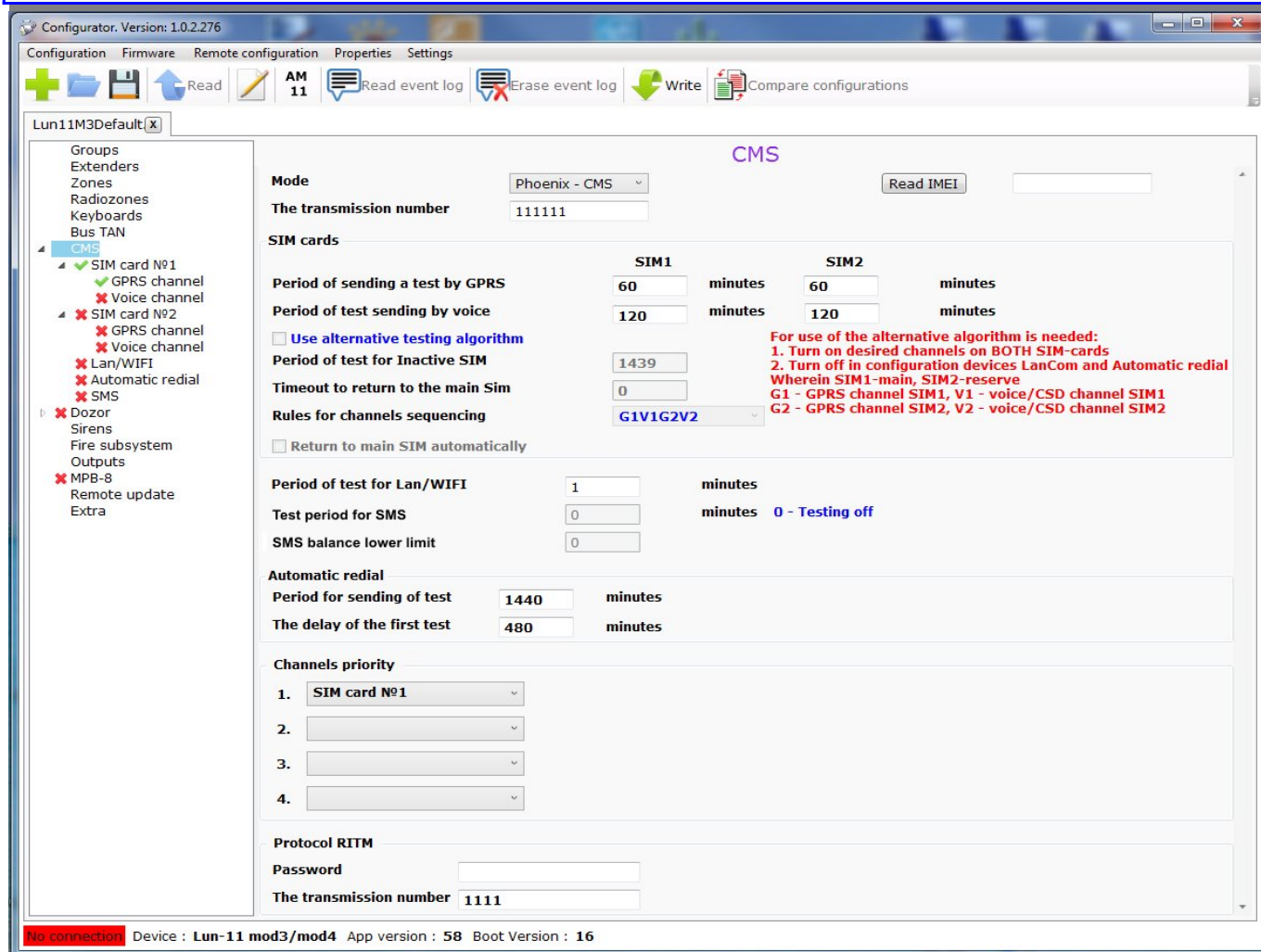
Figure 5. Communication channels and priorities setting

6.1.5. Calling to owner

If "**Calling**" is checked, then the Control Panel performs phone call to the correspondent owner phone numbers, to attract their attention. Don't answer the call. If the "**Only Alarm**" is checked, the call is performed only for alarm events. Calls to alarm events are accompanied by an audible "*Alarm*" message when the handset is picked up.

> **If the multiple alarm events sequential occur, the phone will be call for the events with more than 5 minutes interval.**

For **SMS mode** the Control Panel will be call to owners after all SMS in queue according applying event filters was transmitted.

In **other operation modes** the Control Panel will be call to owners without any event filters.

To make a call, you must enable the voice channel for the SIM card in use.

Call to the owner can be skipped when the mobile network problems occurred (for example, when the network is busy).

6.2. Message transmission and testing

When an event occurs, Control Panel tries to transmit it to CMS (or User monitoring center "Phoenix-Web" – depending on the settings) in accordance with the configuration of transmission channels and their priorities, starting from the highest priority channel and ending with the lowest priority channel (Figure 5).

Each communication channel used by Control Panel is tested independently. For each channel a periodic testing interval is specified. So the test messages are transmitted to CMS via specific channel in accordance with its testing interval. This is the basic algorithm for generating and transmitting tests. It can operate with any combination of communication channels.

If both the communication channels for a one SIM-card switched on, the Voice channel testing is not performed as long as the GPRS channel is workable (test messages successfully are sent).

If a new event occurs during the transmission of a test, the event is transmitted via the same channel as the test message. If the event occurred after the successful completion of the test transmission (i.e., a successful delivery receipt has been received from CMS), this new event is transmitted in accordance with the priorities of the channels.

If unable to transmit events on any of the channels, they are stored in the event queue until such time as the transfer will be possible again. If the event queue is full, the last event recorded as "**Event queue is full**". The next events are not queued up until the queue is cleared (fully or partially).

You can use an alternative test transmission algorithm. This algorithm works only with two SIM-cards used (all another communication channels must be disabled).

In this algorithm, the SIM-card №1 always has the highest priority (the **Main SIM-card** for events transfer) and you can choose the channels sequencing rules for data sent – GPRS1-Voice1-GPRS2-Voice2 or GPRS1-GPRS2-Voice2-Voice1 (digits indicate SIM-card number).

Parameters in the "SIM1" column are used to set the test intervals for the **Main SIM-card** – rows "Period of sending a test" by voice and GPRS channels respectively.

SIM-card №2 is a backup (**Inactive SIM**) and during normal operation (when all the channels works) is used for tests sent to verify SIM-card and the communication channel operability only. The test period for the inactive SIM is used from "**Period of test for Inactive SIM**" parameter.

Channel sequencing rule is used if all attempts to send the event or test by the current communication channel failed.

In this case Control Panel switched to the communication channel that is next in the sequencing rule list and tries to sent event through it. If this channel placed on another SIM-card (for example, the SIM2) and the event/test sent successfully, the Control Panel will use this SIM-card and this communication channel for further events sent. The current SIM-card sets as **Active SIM** with automatic test transmission period change for the current SIM-card number (i.e. from SIM2 column for the above example). Returning to the **Main SIM-card** will occur at the first successful test for inactive SIM (it is now the SIM-card №1 in this example) or the parameter "**Timeout to return to the main SIM**" (whichever comes first).

Events are always sent by the **Main SIM-card**, as long as it is available for communication. Otherwise, the event will be sent by backup SIM-card up to the first successful test for the **Main SIM-card** or by timeout ends.

If the check-box "**Return to main SIM automatically"** set and communication on both SIM-cards work, then the switching to the main SIM-card will be immediately after the backup SIM-card test to reduce the time of readiness to sending events.

6.3. Control panel zone types

Control Panel operates with the following types of zones (Table 3):

Table 3. Available zone types

Zone type	Description
"Delayed"	Type of zone, violation (both in entrance and in exit) of which is caused by the time delay. For example, touch-sensitive magnetic contact of entrance door.
"Interior delayed"	Type of zone, violation of which is always caused by the time delay in the exit, and in in the entrance it is affected by the time delay only if the delayed zone has already been violated. For example, motion detector in walk-through corridors. Also, this type of zone is not analyzed in the Stay-Home Mode.
"Instant"	Standard type of zone that operates in the Armed Mode of Control Panel. This zone will only be activated when the Control Panel is armed. For example, window-mounted detectors.
"24hour"	Type of zone, which is always activated regardless of the Control Panel status (whether it is armed or not). For example, the alarm button.
"Arming"	Type of zone, violation of which disarms the group and recovery arms it.
"24h Fire"	Type of zone to operate with smoke detectors according to 2 or 4 connection circuit.
"Arm Stay"	Zones of this type are not analyzed, if the Control Panel is in the armed Stay-Home Mode. In this case, people can stay in the premise without causing an alarm, but violation of other zone types will cause a corresponding reaction of the Control Panel (e.g., glass brake will lead to the transmission of an alarm signal to CMS) – more see Chapter 6.10
"General Alarm"	Type of zone, violation of which causes transmission of the general alarm code to CMS. It is applied in the case, when the facility uses a central operating via telephone line, and "Lun-11" Control Panel is used as a back-up one.
"Delayed/Instant"	Type of zone identical to "Delayed" zone in the Armed Mode and to "Instant" zone in the Stay-Home Mode.
"Interior delayed/ Instant"	Type of zone identical to "Interior delayed" zone in the Armed Mode and to "Instant" zone in the Stay-Home Mode
"Arming by pulse"	Trigger type of zone: short violation of the zone (0.5...2 s) switches the device status (whether it is armed or not) to the opposite one.

The "**Silent**" parameter can also be set for each zone. If a zone with the preset "Silent" parameter is violated, the siren will be disabled.

Zones response time can be switched when Control Panel configuring.

"**Instant response**" mode should be used for the vibration detectors only (for example, M5-Adj Ebelco type). For other detectors types you should choose the normal response time ("**Instant response**" check-box is unchecked).

6.4. Groups

In the process of configuration, the zones connected to the Control Panel can be logically combined into groups, which allows to operate all the zones of each group as a one unit.

The allowed types of groups:

- **Instant** – the most common type;
- With "**Logic AND**" depending;
- With "**Logic OR**" depending;
- "**Grif**".

The group type is selected in the process of configuration.

The instant group can be either independent, or it can be one of the master groups for one (and only one) dependent group. The interaction of several master groups in relation to the dependent one is described by the logical function AND/OR of this dependent group.

An example of work of dependent groups, if groups 1, 2, 3 are common, controlled by passwords, and group 4 is dependent on groups 1, 2, 3.

The "Logic AND" depending group:

In this case, "Group 4" is armed as soon as all the groups – **1 AND 2 And 3** – are armed. "Group 4" is disarmed, if at least one of the groups – 1 or 2 or 3 – is disarmed.

If at least one zone of the dependent **AND** group (group 4) is violated, and some of the master groups (e.g., groups 1, 3) are already armed, the last master group (group 2) will not be armed until all the zones of the dependent group are recovered.

The "Logic OR" depending group:

"Group 4" will be armed, if at least one of the groups – **1 OR 2 OR 3** – is armed. "Group 4" will be disarmed, if all the groups – 1 and 2 and 3 – are disarmed.

If at least one zone of the dependent **OR** group (group 4 in this example) is violated, none of the master groups will be armed until all the zones of the dependent group are recovered.

"Configurator 11" assigns every key (for readers) and every password (for "Lind" ICD) to some group (see Configurator 11 Guide). It is allowed to use any key/password for several groups.

If "Configurator 11" allows to use the same passwords for several groups, these passwords can be used to arm/disarm a few groups at a time (except the dependent ones).

It is possible to allow/restrict the remote disarming using CMS for each group.

Any specific group can be remotely armed using CMS.

"**Grif**" group is used to organize object patrols and can replace the existing check order of service device "Grif" by simpler and cheaper software implementation.

Group "Grif" can contain up to 128 wire loops/zones (connected to the Control Panel main board, to expanders "Lun-11E" and "Lun-11H", to address modules "AM-11"). Every zone is a non-contact detector, placed on a protected area in predetermined locations – check points.

Zones type for "Grief" group is limited – can only be selected the next types of zones:

- "**Instant**" – the main zone type for this group;
- "**Arming**" – can be used for patrol mode turn on/off;
- "**Not used**" – zone not used in patrol mode.

Since the "Grif" group patrol mode turn on (by the same way as arming), security personnel must periodically get territory and violate and restore "Grif" zones one by one in group's numerical order. Each "Grif" zone has two timing parameters – "**Time to push**" and "**Time to beep**".

"**Time to push**" – time to security personnel to walk away from the previous check point to the current check point. This parameter is determined by the checkpoint location by way timing, time for rest and other possible factors.

"Time to beep" – the time remaining until the alarm occurrence due to lack of violation of the current zone (event "**Violation of checkpoint monitoring**"). This timeout accompanied by short beeps of siren to remind you to touch the next checkpoint zone detector by the key.

Checkpoints order violation, the absence of a violation of the next checkpoint zone detector in the expected time period – cause alarm with the "**Violation of checkpoint monitoring**" description. To cancel the alarm you should to violate the next checkpoint zone detector or turn off (same to disarm) the group "Grif".

6.5. Programmable outputs

The Control Panel has four programmable outputs (of open collector type) – PM1...PM4. The function of each of them is set when configuring the Control Panel. One of the following functions for each output can be selected:

- **Armed** – as an output signal about arming (in any mode) of **all** groups where this output is assigned;
- **24h Fire** – as a fire output signal;
- **Fault** – as a fault output signal (main and backup power supply troubles, troubles at MON/TAN buses);
- **Readiness** – as an output signal of being prepared to arming;
- **Zone repeater** – as an output signal – repeater of the status of the selected zone;
- **Control from CMS or by user** – as an output, enabling/disabling of which is controlled using CMS;
- **Remote LED*** – output signal for connecting an external LED, which:
    - ◆ **switched on** – if at least one group where it is assigned is armed;
    - ◆ **flashes slowly** (1 time per second) – until the arming is not confirmed from CMS;
- **Network appliance power** – is used as power sink of LanCom rev.6;
- **Zone repeater, blinking** – violation of the selected zone is accompanied by discontinuous signal;
- **Alarm in the group, blinking** – alarm of the selected groups will be accompanied by discontinuous signal until the disarming code/key is entered in the alarmed group;
- **Siren*** – as an output for additional siren (including the acknowledgment of arming/disarming when using a keyfob);
- **Remote LED + alarm*** – as an external LED for main board, which:
    - ◆ **switched on** – if at least one group where it is assigned is armed;
    - ◆ **flashes slowly** (1 time per second) – until the arming is not confirmed from CMS;
    - ◆ **flashes frequently** (5 times per second) up to group disarming – if group was alarmed;
- **By force** – output is activated when the disarming is made by "under duress" code. The output is switched off when entering the "normal" code or by legal key touching;
- **Fault (for "24h fire" mode)*** – output signal of the malfunction in accordance with requirements of fire safety standards (active when a malfunction occurs, including when the device is turned off);
- **Disarmed** – as a disarming output signal;

- **Remote LED with delay*** – as an external LED, which:
    - ◆ **switched on** – if at least one group where it is assigned is armed;
    - ◆ **flashes slowly** (1 time per second) – until the arming is not confirmed from CMS and exit delay is not over;
- **Remote LED with delay + alarm*** – as an external LED for main board, which:
    - ◆ **switched on** – if at least one group where it is assigned is armed;
    - ◆ **flashes slowly** (1 time per second) – until the arming is not confirmed from CMS and exit delay is not over;
    - ◆ **flashes frequently** (5 times per second) up to group disarming – if group was alarmed;
- **Armed (stay home)** – switched on if **all** groups where it is assigned are armed in the "**stay home**" mode;
- **"Fire Exit" indicator** – it light on while there is no fire alarm and blinks (every second) if the fire alarm is registered. The "Fire Reset" command will restore the continuous indication.

You can set the **power-on delay** and the **operating time** for every output (except marked with *). If the event ends before any of the parameters, then the output will be turned off (ie, short events can turn off the output before the **operating time** ends or the output don't turned on at all). When the value is set to "0", the corresponding parameter is not used (i.e., "*no delay*" or "*the output works while an event operates*").

If you tried to group arm while some zone 1…8 is violated the **remote LED** output will show this zone number by corresponding short flashes. If the number of flashes is 9, this means that the zone with number 9 or more is violated. If the several zones are violated, the flashes always indicate the zone with the lowest number.

If the output for **remote LED** connection is assigned to several groups, then when the next group disarming, the LED turns off for 3s and then continues to display the status for other groups where it is assigned.

6.6. Antenna connection

Control Panel has a built-in antenna, so prior to installation it is necessary to check the GSM/3G signal strength at the installation place. The communication shall be steady, the voice during a phone conversation shall not be echoed and distorted.

If the GSM/3G signal strength is pure, you can use an external antenna. To do this:

- On revision 19 PCB – with a sharp knife, remove the entire narrow wire located **AFTER** the external antenna connector **X11** (next a wide built-in antenna begins, Figure 6);
- On another revision PCB – cut the **R118/R202** resistor (depends of PCB revision) with side cutters (Figure 4);
- Connect the external antenna to **X11** connector (MMCX connector type, see Figure 4). The external antenna with the required cable length (2.5m, 5m, 10m, 15m) is available on request. The antenna cable shall be completely pulled out of the Control Panel housing.
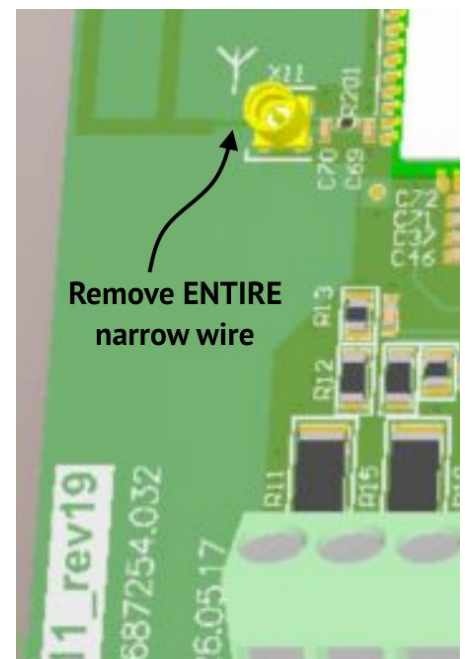

Remove ENTIRE narrow wire

Figure 6. How to prepare the PCB rev.19 for connecting an external antenna

If you need to install several Control Panels with GSM/3G modules, it is recommended to place its external antennas at least of 0.5m from each other. The external antenna shall be located 1m from the detector with active electronic elements and at least of 30cm from the Control Panel housing.

It is not recommended to put the antenna cable into one cable channel (box) with zone wires and power supply circuits.

Do not install the antenna on a metal surface.

6.7. Control of fire detector false alarms

In the Control Panel There are three different signal processing modes of fire alarm detectors:
1. "By the first alarm";
2. "By repeating alarm in the system";
3. "By the alarm of 2 or more detectors in the zone".

> **When working in a mode "Alarm on first alarm" in case of fire in protected area – "Fire" event will be immediately transmitted to the CMS.**

Control Panel can filter the false fire zones in modes 2 and 3.

The function is activated when configuring the Control Panel in "Configurator 11" by setting "**By repeating alarm in the system**" in the "*Fire Detection*" parameter and input parameters:
- "*Timeout for detector reset*";
- "*Time of expectation readiness*";
- "*Time of expectation for the repeat drawdown*".

> **When working in the "By repeating alarm in the system" algorithm and alarm occurrence on a fire zone, the Control Panel first turns off all detectors power for time specified in "*Timeout for detector reset*", and "Probably the fire alarm" event is transmitted to CMS.**

> **Then detectors are powered on, but during "*Time of expectation readiness*" Control Panel does not respond to the fire zones state.**

> **After this time the Control Panel expects re-triggering of the fire alarm in any zone within the "*Time of expectation for the repeat drawdown*" and in case of alarm in this period – "Fire" event is transmitted to CMS**

> **Attention! All timing parameters of "Fire after the second response" option are configured in "Configurator 11", and apply to all fire zones, including the zone expansion modules.**

"**Repeating alarm in the system**" mode allows you to connect to the Control Panel two detectors in a single zone, and recognizes the activation of one and both of them, when "*Recognize the second detector in the same fire loop*" option is set (characteristics of connecting zones in this mode refer to Table 10). Upon detection of such a situation, the device sends a "**The massive fire**" event to CMS.

> **"*Recognize the second detector at the same fire loop*" option applies to all fire zones, including the zone expansion modules.**

> **When working in "By the alarm of 2 or more detectors in the zone" mode and alarm occurrence in a zone – "Probable fire alarm" event is transmitted to CMS. In the event of the next alarm from a fire detector in the same zone – "Fire" event is transmitted to the CMS.**

6.8. Arming

1. To arm the facility, you shall shut all the doors and windows equipped with detectors.

> **If at least one detector (zone) is alarmed, the facility shall not be armed.**

In case the reader is in the area of coverage of the optical detector, you shall stop and stand still until the detector is in the normal state.

2. When all zones are in a normal state, you shall touch Touch Memory key reader with the correct authorized electronic key or bring the RFID-card closer to "Lind-EM" reader – it depends of reader type used or enter the user's regular code from the keyboard. If the key/card recognized, the reader emits a short beep. If the key/card/keyfob/code is not registered in the Control Panel's configuration, a specific sound will be played but arming will not starts.

If only an anti-vandal TouchMemory key reader is installed to system, there are no zones status displayed, and the external LED should be used to armed mode display.

> **Trying to arm the partition with the zones violated will fail and accompanied by short, quick flashes of remote LED – their number equal to the number of the first violated zone 1…8. If the number of violated zone more than 8, the number of flashes will always be equal to 9.**

If the "Lind-11TM", "Lind-29/15/11/9M3" ICD is used then it displays zone violation by its ZONE LEDs. If the number of violated zone is 9/17 and more (it depends of ICD type) and you try to arming, then all zone LEDs will flash thrice and group will not arming.

If the "Lind-29/15/11/9M3" ICD is used for arming, then the preliminary registered "ordinary" 4-digits user code should be entered. User codes can be set at initial system configuration or added/changed later. The violated zones of the group (first 16 zones) are displayed as lighting LEDs of zones 1…16, failed zones are displayed as blinking LEDs.

If all zones are in the normal state, the arming process starts with countdown beeps (up to timeout ends). "ARMED" LED and remote LED begins to flash evenly (frequency ~1Hz) till arming event not sent to the CMS. At the same time, a repeated beeps used to remind to leave the premises. Immediately after the "ARMED" LED and the remote LED start flashing, you should leave the house/object (until the end of the "exit delay" in Control Panel's configuration).

> **"ARMED" ICD LED displays the status of that group the ICD was assigned to.**

Any violated zone types of "Delayed", "Interior Delayed" and "Arm Stay" will be ignored up to the end of the "exit delay" countdown. You can control the arming process by watching the remote LED outside the house/object.

> **If you did not leave the house/object before the "exit delay" countdown ends, and the siren was turned on, you shall touch the reader with the authorized electronic key or enter the user's regular code from keyboard. The siren will turn off and arming will be canceled. "ARMED" LED will turn off. Arming process can be repeated in a few seconds.**

3. If "ARMED" LED and remote LED are constantly lit, it shall mean the following:
   1. Group has been armed.
   2. Arming message was sent to CMS and the confirmation from CMS is received.

> **ARMED LED and remote LED shall not flash within more than 180 seconds. If this time is exceeded or LEDs are not lit, this means that the facility was not armed for some reasons.**

If arming failed, the following shall be checked by installer:
1. Signal strength at the Control Panel's remote antenna installation place.
2. CMS connection configuration settings.

The dependent groups can be armed if its master groups are armed. If the dependent group is not ready to arm then its last master group can't be armed too.

Some group can be armed automatically after it was disarmed if the "**Automatic arming**" is checked for this group in Control Panel configuration and all zones are restored. You should set the "**Arming delay**" and "**Alarm delay**" time out values too.

6.9. Mobile phone control

The Control Panel can be controlled by calls from mobile phones by entering commands from the mobile phone keypad. Each group allows up to 8 phone numbers, which can be stored in the Control Panel configuration using "Configurator 11" software.

The numbers shall be entered in the international format without "+" sign, e.g., Ukrainian numbers: **380671234567** (12 digits); Russian numbers: **79011234567** (11 digits).

> **The voice channel must be enabled in the Control Panel configuration in order to use a mobile phone for arming/disarming.**

To control the device from a mobile phone, the following shall be done:
1. Call the number of Control Panel. The device will answered to the incoming call from the preprogrammed phone numbers only;
2. Enter *<group number>* on the mobile phone keypad;
3. Press ✱ ;
4. Enter *<command>*;
5. Press # .

> **The next remote control commands are supported:**
> **1 – Arming;**
> **2 – Disarming;**
> **3 – Status poll (armed   – 1 tone beep is answered,**
> **   disarmed   – 2 tone beeps is answered);**
> **5 – Forced disarming;**
> **8 – Arming in "Stay Home" mode;**
> **9 1 1 – Alarm. This code can be entered without group number, "✱" and "#", at any time after the device has answered the call. Can be used in "Orlan CMS" mode only.**

Execution of a command is accompanied with the corresponding beep:
● Successful execution – long single beep.
● Impossibility of execution – a series of 5 short tone beeps ("trill").

If some zones are violated, the correspondent group cannot be armed with "trill" sound. If your mobile phone number is not assign to some group then the arming/disarming command will not be executed with "trill" sound.

Control Panel shall stay connected until:
● Connection is closed by the phone user command;
● Under timeout (idle time) within 5 seconds;
● Under global timeout of 30 seconds (maximum communication session).

6.10. "Stay Home" mode

This mode is intended for cases when the owner needs to stay inside the protected area, but to arm the "perimeter zones".

The "**Stay Home**" mode can be activated if "**Arm Stay**" and "*Delayed*" or "*Delayed/Instant*" zones is presented in Control Panel's configuration.

The "**Stay Home**" mode will be activated, if the "Delayed" or "Delayed/Instant" zones not violated while arming (timeout for exit) process **OR** the "**Stay Home**" key ("Lind-15/9M3" ICD) or "**Shield**" ("Lind-11/11LED") key was pressed before the user's password entered on.

In this mode the **"Arm Stay"** and **"Interior delayed"** zones are not analyzed.

6.11. Disarming

1. In order to disarm you should go in the arming house/object through the front door. Since the opening of the front door to trigger the alarm has a time interval "entrance delay" (time interval configurable).
2. During this time, should have time to go to the ICD and touch/bring to it by key/card/keyfob (allowed for a certain group) or enter the user's regular code from keyboard. At key/card/keyfob recognition a short beep will emit. If the key/card/keyfob/code registered in the Control Panel configuration, the group will be disarmed with a series of short beeps, and the "ARMED" LED and remote LED will turn off.

    If the key/card/keyfob/code is not registered in the Control Panel's configuration, then disarming it will not be execute. Beeper emits long intermittent signal.

> **If you did not have time to disarm the house/object within the "entrance delay" time allowed and the siren was turned on, you should touch/bring to the reader with the authorized key/card/keyfob or enter the user's regular code from keyboard. The siren will turn off.**

> **In the case of invasion into the room not through the front door (for example, in the case of a door lock failure) alarm and siren will instantly turn on. To turn off the siren and disarming the house/object you should touch/bring to reader by authorized key/card/keyfob or enter the user's regular code from keyboard (allowed for a certain group). The siren will turn off.**

> **If the "forced" password ("Lind-15/11/9M3") is used to disarm, then the group disarming and the panic event is transmitted to CMS simultaneously.**

6.12. Schedule

The Control Panel can be armed and disarmed automatically, according to a predetermined schedule.

To do this, you need to specify the time for arming and disarming for every day of the week (in the Control Panel configuration "**Schedule**" tab). Each group can use its own schedule. Control panel time synchronization must be enabled (via CMS or SNTP) for the schedule to work correctly.

> **Note: SNTP time synchronization works only in the open Internet via GPRS/WiFi communication channels.**

> **When the Control Panel works with the "Orlan" CMS, an additional schedule in the "Phoenix 4" software can be used. Each schedule operates independently.**

6.13. TAN bus devices operation features

TAN bus is designed for connection of the following peripheral equipment:
- "Lind-11TM" ICD (TM reader);
- "Lind-EM" ID card/keyfob non-contact reader;
- "AM-11" address modules;
- Any third party TouchMemory anti-vandal key readers.

> **Any device operating on TAN bus shall have its own unique address (assigned by the engineer when configuring the system). The only exception is the anti-vandal reader, which has no address.**

> **Attention! It is only possible to connect either third party TM anti-vandal key readers, or "Lind-11TM", "Lind-EM", or "AM-11" devices.**

> **It is prohibited to connect these devices simultaneously because of different bus voltage required for different devices!**
> **Connection of TM anti-vandal key reader with the configured "Lind-11"/"Lind-11LED"/ "Lind-9M3" shall result in the immediate breakdown of any TouchMemory key when it touches the reader!**

In case of connection of "Lind-11TM", "Lind-EM", or "AM-11" devices the maximum length of the bus is limited (see Table 2). Connection shall be carried out using the foiled twisted pair.

6.14. Zone expansion with "AM-11" address modules

Expansion in the number of the security system zones can be provided with either "Lun-11E"/"Lun-11N" expansion modules (which are fully-featured Control Panels having 10 zones each), or "AM-11" compact address modules (Figure 7) with 3 additional zones. An example of use of the modules is shown in Figure 42.
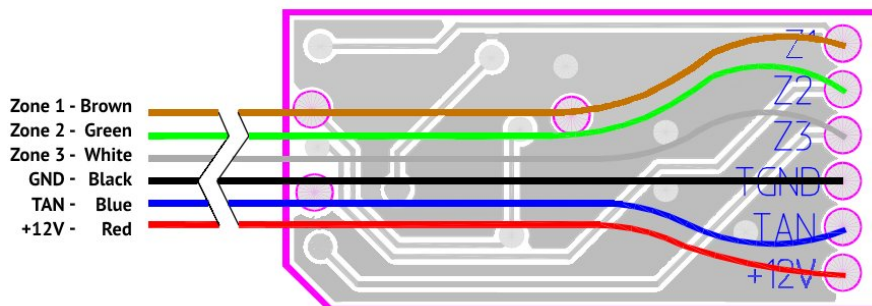

Figure 7. Appearance and functions of the hard-wired zone of "AM-11" address module

> **"AM-11" has 3 zones, in such case you can select the "normally open" or "normally closed" line type, and any type of zone, except the "fire" one.**

The total wired zones count is always the same – 144.

> **"AM-11" modules are connected to TAN bus; each module shall have its unique address (address 1 is preset). Configuring of modules (address assignment, see Figure 9) and zones applying by modules is carried out using "Configurator 11" software.**

The configuration details you can see in "Configurator 11 Guide" at www.ortus.io.

To connect "AM-11" modules to a computer in the configuration process, "Config-AM11" adapter is required (Figure 8).
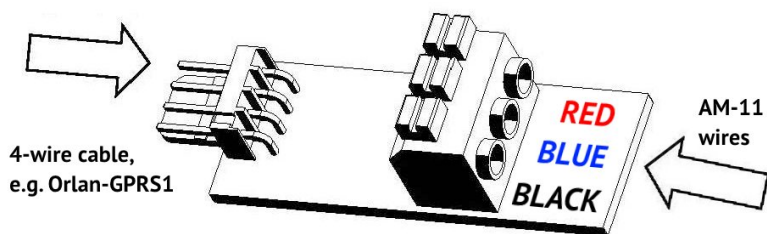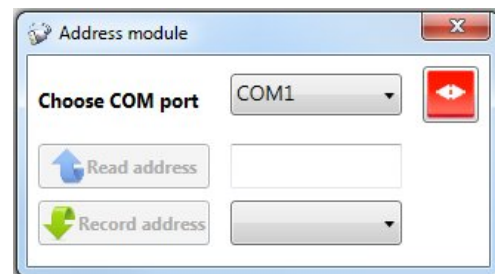
Figure 8. "Config-AM11" adapter appearance

Figure 9. Configuring of "AM-11"

A 4-wire cable "Orlan-GPRS" is connected to **XP1** plug, and "AM-11" module is connected to **XS2** terminals in accordance with the wire colors specified (to fix the wire in the terminal, you shall push the corresponding fixing lug, insert the wire and then release the fixing lug).

6.15. Arming acknowledgment by siren

The Control Panel has the function of acknowledgment of arming using a short (about 0.5s) siren beep. This function is available for keyfob arming and for the "Arming" type zones; it is enabled by selecting the corresponding check-box in "Configurator 11" software.

6.16. Detection of cellular signal jamming

If Control Panel use GSM(3G) communication channels, the build-in modem detect cellular signal jamming automatically. Information about the signal lost is displayed on "Lind-11" ICD, and is also sent to the CMS over an available communication channel (if the check-box "**Detect GSM jamming**» set on the "**Extra**" tab in the "Configurator 11" software). In arming mode the Control Panel siren will turn on if jamming detect for more then 5s and the check-box "**Siren ON when GSM jamming**» set (on the "**Extra**" tab in the "Configurator 11" software).

7. LED indicators in the Control Panel circuit board

The Control Panel has indicators of three types – red, blue and green (see Figure 4).

<u>**Red**</u> **– system status indicator**;

<u>**Blue**</u> **– modem status indicator**;

<u>**Green**</u> **– indicator of operation with backup SIM** (displayed with continuous light).

System status indicator (red LED) operation modes:

- <u>Twice per second flash</u> – Control Panel is in the configuring mode (wired or remote) or at the Control Panel starts (after its switching on);
- <u>Blinks in series of 3 flashes</u> – the firmware update mode (wired or remote) – **do not turn off the Control Panel power until the end**;
- <u>Continuous flashes with short pause</u> – Control Panel operates in its normal mode and has the events, which have not been transmitted to CMS yet. The indicator often flashes in the course of session;
- <u>Short flashes with long pause</u> – Control Panel operates in its normal mode and all the events have already been transmitted to CMS;
- <u>No light and no flashes</u> – Control Panel is not configured, not powered, or out of service.

Modem status indicator (blue LED) operation modes:

- <u>Triple per second flashes</u> – modem has been successfully registered in GPRS network;
- <u>Twice per second flashes</u> – modem has been successfully registered in GSM network;
- <u>Flashes every two seconds</u> – modem is in the network registration process;
- <u>No light and no flashes</u> – modem is not powered or out of service.

8. Key readers

Control Panel allows for connection of the following readers:

- "Lind-11TM" indication and control devices (TM key reader);
- "Lind-EM" RFID card reader;
- Any third party TM anti-vandal key reader.

8.1. "Lind-11TM" indication and control device

"Lind-11TM" ICD is designed to display the Control Panel's group arming status, its first 8 zones state, and system failures. This device allows to arm and disarm Control Panel's preselected group using TouchMemory iButton keys, as well as to reset the fire alarm.

The appearance of "Lind-11TM" is shown in Figures 10, 11. The connection and use of the device shall be carried out in strict accordance with its Operation Manual (see "Lind-11TM" Indication and Control Device. Operation Manual" at www.ortus.io). An example of ICD connection is shown in Figure 41.

Figure 10. "Lind-11TM" ICD front view
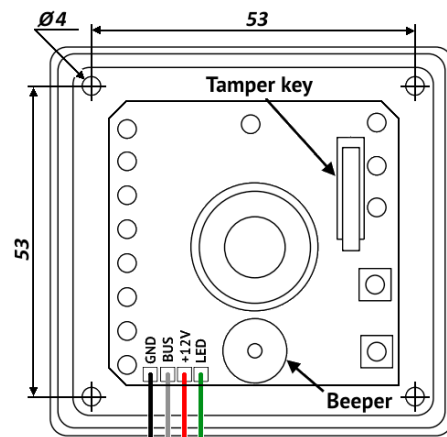
Figure 11. "Lind-11TM" ICD without cover

"Lind-11TM" ICD is connected to TAN expansion bus. Each device operating on the bus shall have its unique address. Address is assigned with RESET and TROUBLE buttons prior to connection of BUS conductor to TAN bus. The selected with the buttons address shall coincide with the address selected in "Configurator 11" software.

Attention! Arming/disarming and their indication with the help of "Lind-11TM" shall be carried out only for the group to which the specific ICD is assigned.

8.2. "Lind-EM" RFID-card reader

"Lind-EM" reader (Figure 12) is a non-contact reader of cards/RFID markings of EM-Marine type. The device operates at the frequency of 125 kHz at the approach of a card/RFID marking at the distance of 3...8 cm.

> **The reader carries out arming/disarming and their indication only for the group, to which it is assigned.**
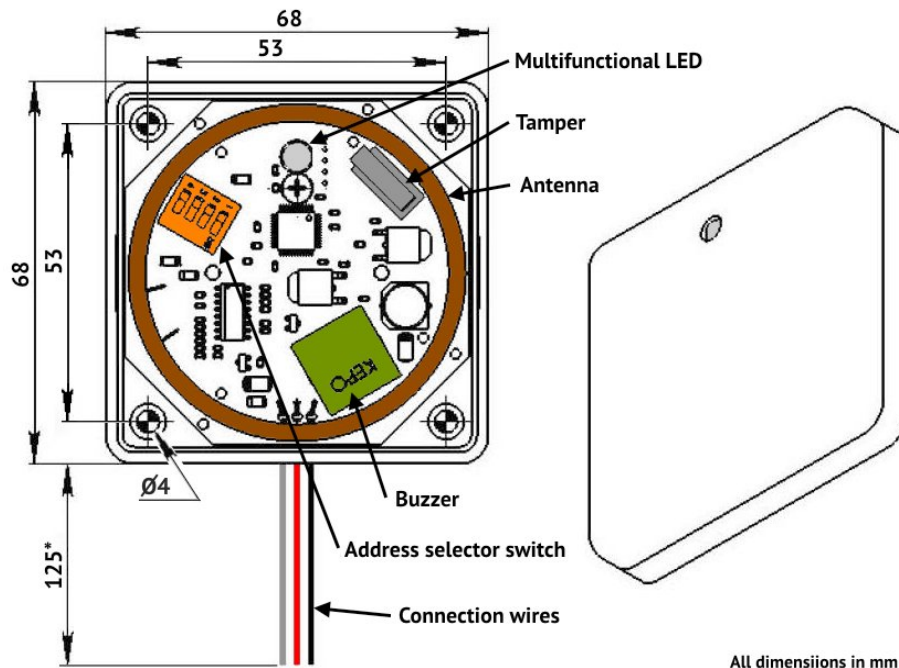

Figure 12. Appearance and arrangement of "Lind-EM" ICD

> **"Lind-EM" reader is connected to TAN expansion bus. Each device operating on the bus shall have its unique address. Address is assigned with DIP-switch prior to connection of BUS conductor to TAN bus. The selected with the switch address shall coincide with the address selected in "Configurator 11" software.**

The connection and use of the device shall be carried out in strict accordance with its Operation Manual (see "Lind-EM" non-contact ID cards reader. Operation Manual" at www.ortus.io).

8.3. Anti-vandal reader

Control Panel allows to connect any standard or third party TouchMemory electronic key reader. It is connected to TAN bus, see the details in section 6.13. Remember, if you connected the anti-vandal key reader, other devices can not be connected to the TAN bus.

You can use either the ordinary TouchMemory keys (DS1990A-F5) either copy protected keys (DS1961S-F5). You should check the "**Protected keys**" checkbox in the appropriating group for copy protected keys using.

> **Attention! If the copy protected key is using, the arming/disarming is performed for all groups, when this key assigned (including groups, where "Protected keys" checkbox is not checked).**
>
> **If the ordinary key using and "Protected keys" checkbox is checked in the some groups where this key is assigned – no one group (including groups, where this checkbox is cleared) will not be armed/disarmed.**

9. Indication and control devices (keypads)

9.1. "Lind-29"

Figure 13. Appearance of the "Lind-29" ICD

"Lind-29" ICD is designed to control and indicate the Control Panel's status (Figure 13). When using ICD all management functions are available, namely:

- Arming and disarming of the group (including the "stay at home" mode);
- View the first 16 zone status of the selected group (including intrusion and zone fault) and activate or deactivate the zone bypass;
- Display group armed state, "Fire" state and reset the "Fire" state;
- Display all system failures;
- Display GSM signal strength;
- Manage of the user's passwords/keys, passwords of administrator and fire subsystem for each group;
- Enrolling of the wireless detectors and checking of their signal level.

ICD must be connected and used in strict accordance with its instruction manual. An example of connecting ICD is shown in Figure 44.

"Lind-29" ICD is connected to MON expansion bus. Each device operating on the bus shall have its unique address. The address is set by the keys of the ICD keypad (while the BUS terminal disconnected) in accordance with its instruction manual at www.ortus.io. The selected address shall coincide with the address selected in "Configurator 11" software.

Arming/disarming process and arming state indication is carried out just for group, where the specific ICD is assigned to.

9.2. "Lind-15"

Figure 14. Appearance of the "Lind-15" ICD

"Lind-15" ICD is designed to control and indicate the Control Panel's status (Figure 14). When using ICD all management functions are available, namely:

- Arming and disarming of the group (including the "stay at home" mode);
- View the zone status of the selected group (including intrusion and zone fault) and activate or deactivate the zone bypass;
- Display group armed state, "Fire" state and reset the "Fire" state;
- Display all system failures;
- Display GSM signal strength;
- Manage of the user's passwords/keys, passwords of administrator and fire subsystem for each group;
- Enrolling of the wireless detectors and checking of their signal level.

The ICD must be connected and used in strict accordance with its instruction manual. An example of connecting ICD is shown in Figure 31.

> **"Lind-15" ICD is connected to MON expansion bus. Each device operating on the bus shall have its unique address. The address is set by the keys of the ICD keypad (while the BUS terminal disconnected) in accordance with its instruction manual (available at www.ortus.io). The selected address shall coincide with the address selected in "Configurator 11" software.**

> **Arming/disarming process and arming state indication is carried out just for group, where the specific ICD is assigned to.**

9.3. "Lind-11", "Lind-11LED"

"Lind-11" ICD (Figure 15) and "Lind-11LED" ICD (Figure 16) are designed to manage of Control Panel and indicate its status.

Figure 15. "Lind-11" ICD with open cover

Figure 16. "Lind-11LED" ICD with open cover

"Lind-11" ICD has the full functional of control over the Control Panel.

"Lind-11LED" ICD is its simplified analogue: it indicates the status of only first 16 zones of the group; it does not allow for arming/disarming of several groups at a time, registration of wireless detectors, and looking through troubles of the device tampers.

"Lind-11" and "Lind-11LED" ICDs are connected to MON expansion bus. Each device operating on the bus shall have its unique address. Address is assigned after the simultaneous pressing of # and F4 buttons. The selected with the buttons address shall coincide with the address selected in "Configurator 11" software.

The connection and use of the devices shall be carried out in strict accordance with their Operation Manuals (see "Lind-11" Indication and Control Device. Operation Manual", "Lind-11LED" Indication and Control Device. Operation Manual", "Lind-9M3" Indication and Control Device. Operation Manual" at www.ortus.io).

Table 4. ICD terminals functions

Terminal marking	Function
GND	Common terminal (–)
BUS/MON	Interface for the Control Panel communication (foiled twisted pair with overall length of up to 150 m)
+12V	Power-up input (+)

9.4. "Lind-9M3", "Lind-9M4"

ICD (16 zones red LEDs, Figure 17) is designed to control the main functions of Control Panel and indication of its status.
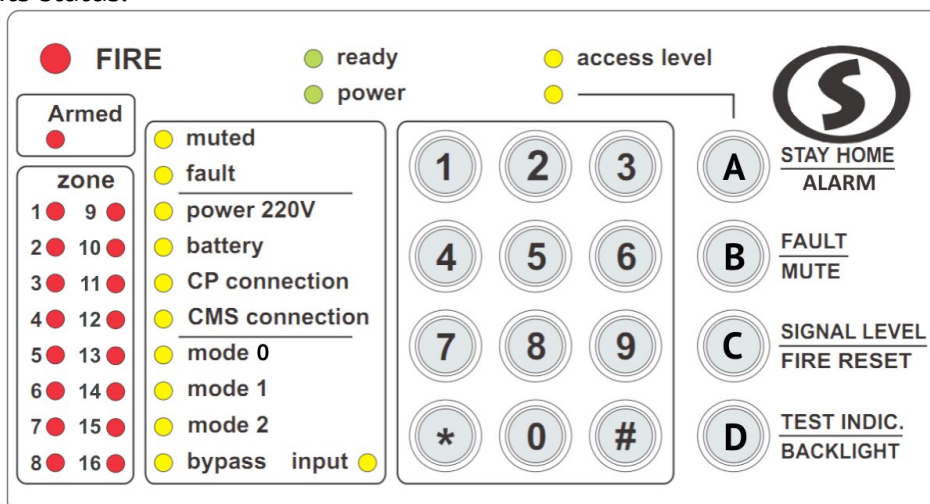
Figure 17. Appearance of "Lind-9M4" ICD

ICD allows to control the main functions of the Control Panel.

ICD is connected to MON expansion bus. Each device operating on the bus shall have its unique address. Address can be set after the simultaneous pressing of `#` and `1` buttons. The selected with the buttons address shall coincide with the address selected in "Configurator 11" software.

Remember that the ICD hasn't built-in zone and you can't use the alarm buttons (fire and burglar). This should be considered when configuring the security system in the "Configurator 11" software.

10. "MPB-8M" relay output module

"MPB-8M" relay output module is designed to expand the functionality of the facility fire and security alarms based on the "Lun-11" Control Panel, and allows to turn on and turn off the equipment at the facility, as well as to duplicate zone statuses or events that occurred using isolated eight built-in relays.

The module should be installed in the Control Panel housing according to figure 18.
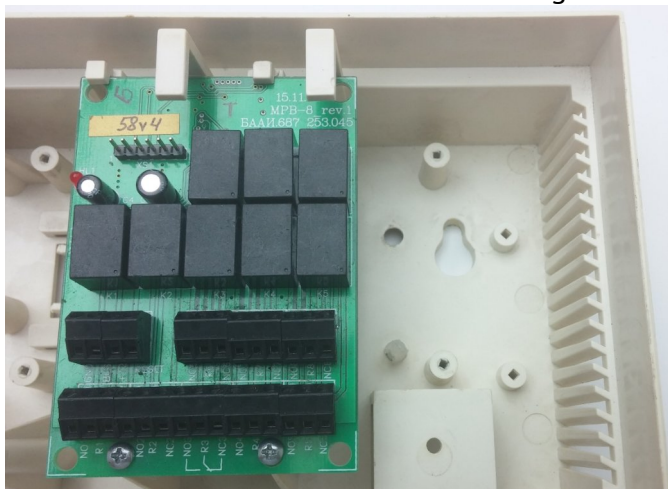
Figure 18. "MPB-8M" module in the housing

> **Only one "MPB-8M" module can be connected to Control Panel, module address is assigned by the manufacturer and it cannot be changed. The connection shall be carried out according to MON interface using the foiled twisted pair.**

The function of each module (relay) output is set independently when configuring Control Panel using "Configurator 11" software.

Table 5."MPB-8M" module terminal functions

Terminal marking	Function
GND	Common terminal (−)
BUS	Interface to Control Panel MON bus, (foiled twisted pair with overall length of up to 150 m)
+12	Power-up input (+)

The following functions for each relay output are supported:
- Not used;
- Armed – as an arming output signal;
- Fire – as a fire output signal;
- Fault – as a fault output signal (main and backup power supply troubles, troubles at MON/TAN buses);
- Preparedness – as an output signal of being prepared to arming;
- Zone repeater – as an output signal – repeater of the status of the selected zone;
- CMS control – as an output remotely controlled using CMS;
- Remote LED indicator – LED is lit, if at least one of the groups it is assigned to is armed;
- Zone repeater, flashing – as an output flashing when the selected zone is violated;
- Group alarm, flashing – as an output flashing when there is alarm in the group;
- Siren – as an output for additional siren;
- Disarmed – as a disarming output signal.

11. Wireless system

11.1. General information

Radio receiver connected to the Control Panel board provides operation of the wireless detectors. The summary table of radio systems acceptable for use in this Control System and radio receivers for them is given below.

Table 6. Wireless systems and radio receivers supported by Control Panel

Wireless system manufacturer	Radio receiver required	Frequency range, MHz	Radio receiver manufacturer
Visonic	«MCR-300» (with "Visonic-Lun11" cable)	433	Visonic
Ajax	«Ajax RR-108» (with "Ajax RR108-Lun11 Adapter" cable)	868	"Ajax Systems Inc."
Astra	◆ «Astra-RI-M» (with «Astra-Lun11» adapting board); ◆ or «Astra-RI-M RR» (with «Rielta-Lun» adapting board);	433	"Teko"
Rielta	◆ or «R433A» ◆ «R433» / «L25_R433» ◆ or «Lun RKI» rev.3 (with "Ajax RR108-Lun11 Adapter" cable) ◆ or «Lun RKI» rev.3.3		ORTUS Group
Roiscok	«R433»		
Jablotron	«R433M»		
Crow	◆ "CROW–Lun-11" Adapter ◆ or "L25_CROW_rev3" Adapter ◆ or "L25–CROW B" Adapter	868	
ORTUS	Lun-R	433	

Radio receiver shall be installed in the device housing as shown in Figures 20, 23, 25, 26, 30 and then a hardwired zone/cable from the radio receiver shall be connected to **X3** connector on the Control Panel board.

The type of the installed radio receiver, number of wireless zones, their types and assigning to groups carried out using "Configurator 11" software, shall be specified in the configuration of Control Panel.

Finally, turning the unit into operation mode (I.e. disconnected from the computer) should to register the wireless detectors into 145…192 zones using "Lind-11" ICD from the "engineer" access level.

> **Attention! All wireless detectors used in one Control Panel shall be of the same product range of the same manufacturer.**

> **Supported wireless detectors types for each radio system and their registration sequence written in section 27.**

11.2. Lun-R radio receiver

"Lun-R" radio receiver allows to connect of **ORTUS** wireless devices (total up to 31 wireless devices).

The radio receiver is installed in the housing, as shown in Figure 19, and connected with its own wire loop to the **X3** connector on the control panel board.
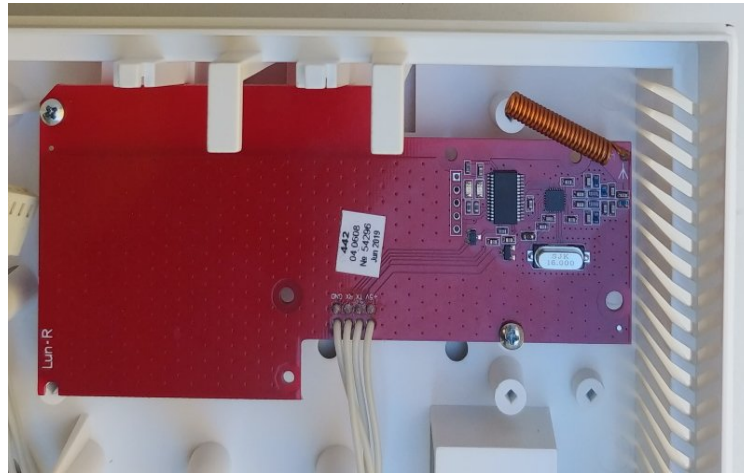

Figure 19."Lun-R" radio receiver in the device housing

11.3. R433, R433M, R433A radio receivers

R433 radio receiver allows to connect of **Roiscok** wireless detectors/keyfobs and **Rielta**.

R433M radio receiver allows to connect of **Jablotron** wireless detectors/keyfobs JA-60 Series.

R433A radio receiver allows to connect of **Astra** wireless detectors/keyfobs.

All modules have the same dimensions and is installed in housing under Control Panel, as shown in Figure 20 (to do this, two destructive housing elements shall be broken out previously). Then it is connected via its own cable to **X3** connector on the Control Panel board.

The modules have two LEDs:

• **"Radio" (HL2)** - flashes in the process of radio exchanging with detectors;

• **"Alarm" (HL1)** - flashes in the case of any detector alarm.

R433 module has **XP2** connector used to change the network of Rielta wireless system.
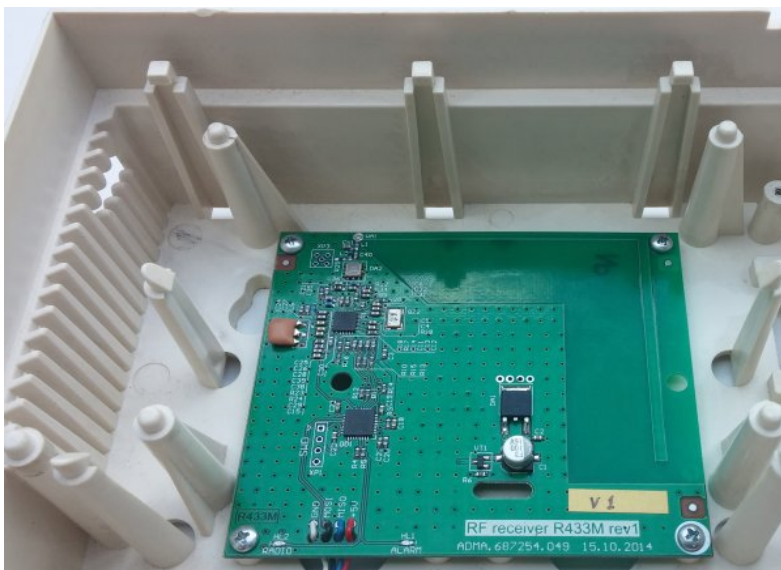
Figure 20. "R433"/"R433M" radio receiver in the device housing

Figure 21."R433" rev. 4 radio receiver in the device housing

When shipped, the antenna is folded. When installing the radio receiver of this revision the following shall be done:

1. Line up the antenna in the plane of radio receiver board and direct it perpendicular to the board edge, near which the antenna is located;
2. Drill a hole in the device housing as shown in Figure 22, and install the radio receiver board as shown in Figure 21;
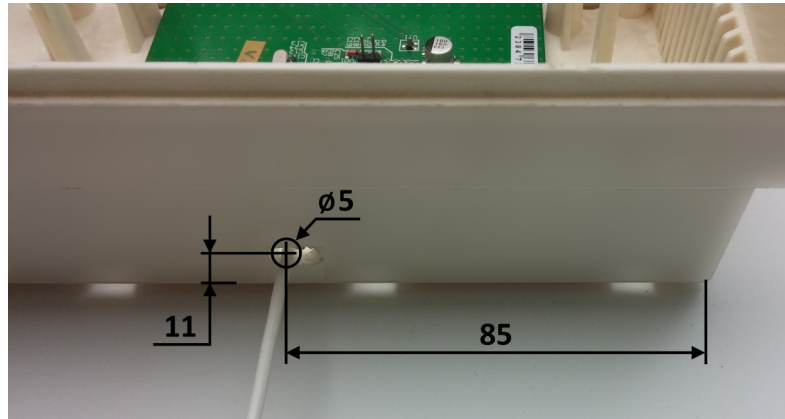3. Connect the radio receiver zone as described above.

Figure 22. Hole in the housing for the antenna of "R433" rev.4 radio receiver

11.4. "MCR-300" Visonic radio receiver

"MCR-300" Visonic radio receiver is used to operate with wireless detectors / keyfobs manufactured by Visonic. The radio receiver is installed in the Control Panel housing (Figure 23) and connected using a special cable "Visonic-Lun11" (manufactured by ORTUS Group, Figure 24) to **X3** connector on the Control Panel board.
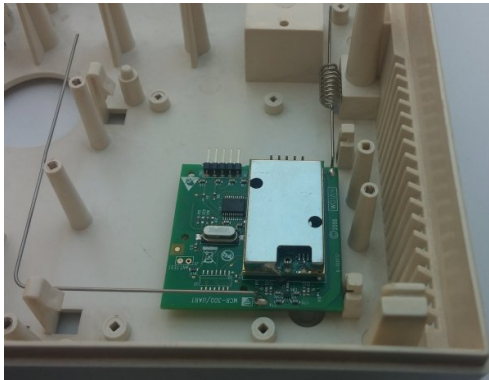
Figure 23. "MCR-300" Visonic radio receiver in the device housing
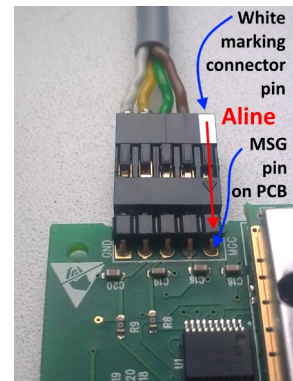
Figure 24. MCR-300 cable connecting

11.5. "L25_R433", "L25_R433A", "L25_R433M" radio receivers

This radio receivers are used instead of correspondent R433, R433M, R433A radio receivers (see section 11.3).

This receivers are installed in the device housing on a piece of 3M double-sided adhesive tape alike Figure 24. Any radio receiver is connected in the same way (see section 11.3).

11.6. Lun RKI v.3 radio receiver

This radio receiver is used to work with Rielta wireless devices made on a red PCB.

This receiver is installed in the device housing on a piece of 3M double-sided adhesive tape alike Figure 24 and it is connected via "Ajax RR108-Lun11 Adapter" cable to **X3** connector on the Control panel's PCB.

11.7. "Lun RKI" rev.3.3 radio receiver

Radio receiver is used to operate with wireless detectors / keyfobs manufactured by Rielta. It should be installed in the Control Panel housing like as shown in Figure Ошибка: источник перекрёстной ссылки не найден. This receiver should be connected by built-in cable to Control Panel **X3** connector.

11.8. Astra radio system

"Astra" wireless detectors/keyfobs operate via **one** of the next radio receivers:
◆ "**R433A**" radio receiver;
◆ "**Astra-RI-M** radio receiver" peripheral retransmitter connected to Control Panel via "Astra-Lun 11" adapter;
◆ "**Astra-RI-M RR** radio receiver" peripheral retransmitter connected to Control Panel via "Astra RR-Lun 11" adapter.

> **Attention! Prior to the retransmitter connection to the Control Panel, all "Astra" wireless detectors/keyfobs shall be registered according to the retransmitter operation manual. The wireless detectors registration priority sequence in "Astra-RI-M radio receiver" shall correspond to wireless zones sequence in Control Panel.**

"Astra-Lun11"/"Astra RR-Lun11" adapter shall be installed in the Control Panel housing as shown in Figure 25, and connected to **X3** connector and **12F1** terminal of Control Panel's board.
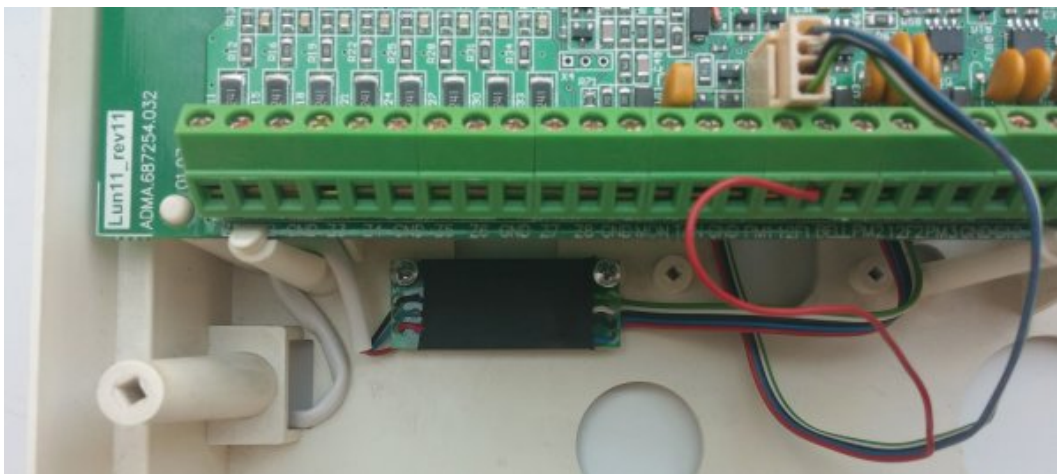

Figure 25. Installation and connection of "Astra-Lun11" adapter

After registration of wireless detectors, "Astra-RI-M radio receiver" shall be connected to "Astra-Lun11" adapter (using the cable of this adapter) according to the diagram given in section 26 (Figure 45).

"Astra-RI-M RR radio receiver" shall be connected to "Astra RR-Lun11" adapter (using the cable of this adapter) as shown in section 26 (Figure 46).

"R433A" radio receiver installation and connecting described in section 11.3.

11.9. Crow radio receiver

To provide the operation of Control Panel with the Crow wireless devices, one of the radio receiver shall be used and connected to **X3** connector of the Control Panel board:

- "**CROW−Lun-11**" Adapter – should be installed into the device housing (Figure 26);
- "**L25_CROW_rev3**" Adapter – prepare a place for adapter (Figure 28) then install the adapter with double-sided tape (Figure 29);
- "**L25_CROW_rev4**" Adapter – should be installed into the device housing (Figure 27);
- "**L25−CROW B**" Adapter – should be installed outside the device housing (it has its own case), in a place where the wireless detectors signals are received good. This adapter includes a cable (5m long) to connection to the CP. The free side of the cable is connected to the adapter terminals as shown on the Figure 47. The cable free side can be cut off for best fitting.
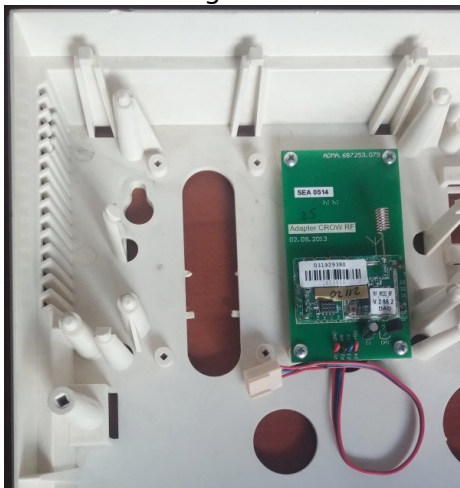
Figure 26. "Crow-Lun-11" adapter in the device housing
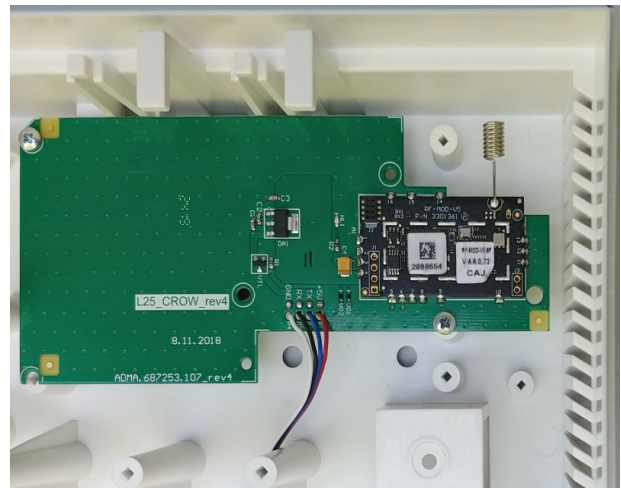
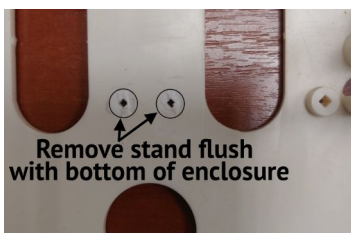*Figure 27. Adapter «L25_Crow_rev4» in the device housing*

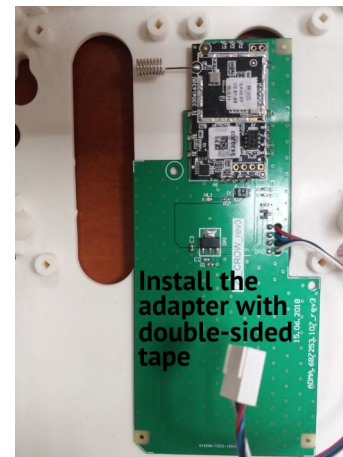*Figure 28. Preparing the device housing for the adapter "L25_Crow_rev3"*

Figure 29. Adapter «L25_Crow_rev3» in the device housing

11.10. Ajax radio receiver

To provide the operation of Control Panel with Ajax wireless detectors, "Ajax RR-108" or "uartBridge" radio receiver shall be installed in the housing as shown in Figure 30 or Figure 31 respectively. Following that, it shall be connected to **X3** connector on the Control Panel board using "Ajax RR108-Lun11 Adapter" cable (manufactured by ORTUS Group).
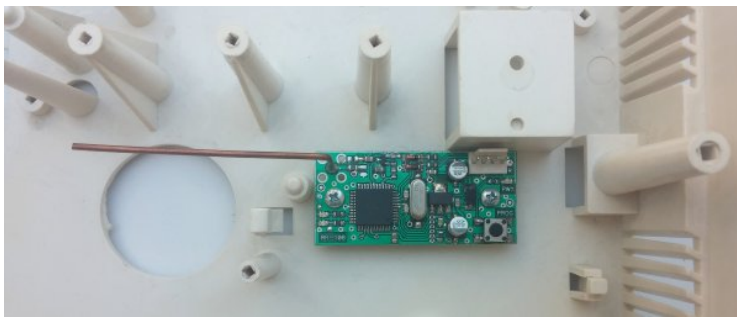
Figure 30. Ajax "RR-108" radio receiver in the device housing

Figure 31. Ajax "uartBridge" radio receiver in the device housing

11.11. Wireless detectors registration

Prior to registration of wireless detectors, the type of radio system shall be selected, number and type of zones shall be specified in the Control Panel configuration (at the stage of the device configuring using "Configurator 11" software).

Attention! Prior to registration of wireless detectors, the group to be changed shall be disarmed.

Registration management can be performed via "Lind-29/15/11/9M3" ICDs as follows:

"Lind-29":

◆ Press ✱ , *group number*, ✱ to go to the desired group and make sure that it is disarmed.

◆ Press # + 7 , *installer_password* to access to the wireless detectors control mode. Zones LEDs in **red** indicate the radiozones numbers with binded wireless sensors, and the **green** ones indicate free radiozones.

◆ Enter **radiozone number 1...16** and confirm by ✱ . It will flash in **red**.

◆ Select action:

  ▪ A , ✱ – **delete** wireless sensor;

  ▪ B , ✱ – **add** wireless sensor.

  ▪ C – sensor signal level (bar by zones LEDs 1...3) in the last communication session.

The button # – to exit the mode.

"Lind-15":

◆ Go to the right group by touching its number on the ICD upper level screen and make sure that it is disarmed.

◆ Touching the "**Wireless system**" button and then entering the *installer_password*, go into the wireless detectors control mode – the "**Wireless zones**" button.

◆ Then the available wireless zones will be displayed as a table. Touch the line with the desired zone number. If the wireless detector has not yet been registered in this zone (the remaining columns in this line contain dashes), then to switch the Control Panel into the binding mode, touch the "**Add**" button. If the selected zone already contains a wireless detector, you must delete its data first – click the "**Delete**" button.
If the wireless detector was previously bound in another zone of this Control Panel, then you need to delete its binding first.

◆ Initiate the transmission of the binding signal by the wireless detector depending on the type of wireless system and the type of wireless detector – see section 27. Successful registration is accompanied by a beeping sound "trill".

The button # – to exit the mode.

"Lind-11":

◆ Press ✱ , *group number*, ✱ to go to the desired group and make sure that it is disarmed.

◆ Select the menu item "**Wireless zones**", enter the *installer_password* to access to the wireless detectors control mode.

◆ Select the free (with a blank "**ID detector**" field in the first line of ICD display) wireless zone via < and > buttons. If the selected zone already has a wireless detector, you need to delete this data first (press **F2** button). If the wireless detector was previously bound in another zone of this Control Panel, then you need to delete its binding first;

◆ Switch the Control Panel to the wireless detector binding signal waiting mode (press **F1** button).

◆ Initiate the transmission of the binding signal by the wireless detector depending on the type of wireless system and the type of wireless detector – see section 27. Successful registration is accompanied by a beeping sound "trill".

The button # – to exit the mode.

"Lind-9M3":

◆ Press ✱ , *group number*, ✱ to go to the desired group and make sure that it is disarmed.

◆ Press # + 7 , *installer_password* to access to the wireless detectors control mode (**MODE 0** LED is lit). Be sure the **MODE 1** LED is <u>turned off</u> (if it is lit, press TEST INDIC. once). You can bind up to 16 wireless detectors for each group with this ICD. Available wireless zones is displayed via red ZONE LEDs (wireless zone #1 in the current group corresponds to ZONE_1 LED):

▪ If some wireless zone contains a detector then the corresponding ZONE LED *is lit*.
▪ If the some wireless zone is free then the corresponding ZONE LED *is flashing*.
▪ All unavailable wireless zones are displayed as *turned off* ZONE LEDs.

◆ Select wireless zone you need by entering its number (1...16) and press ✱ to confirm. Another ZONE LEDs will turned off.

◆ Then you can do the next in depends of the wireless zone current binding state:

1. Press FAULT/MUTE – to switch the Control Panel to the wireless detector binding signal waiting mode (if the wireless zone is free). Then you need to initiate the transmission of the binding signal by the wireless detector depending on the type of wireless system and the type of wireless detector – see section 27. Successful registration is accompanied by a beeping sound "trill".

2. Press STAY HOME – to delete the existing binding (if the wireless zone is occupied).

3. Press and hold SIGNAL LEVEL – to check the occupied wireless zone detector signal strength. It is displayed by the **ZONE 1...3** LEDs. A greater number of luminous LEDs corresponds to a higher signal level.

The button # – to exit the mode (**MODE 0** LED turns off).

> **Attention! After registration or deletion of wireless detectors, the Control Panel shall be automatically rebooted for all the changes made to apply.**

Upon assignment of the wireless detectors, their operation shall be controlled by the events occurring in case of violation/recovery of wireless detector zones in the "Zone status" menu of the corresponding group on ICD display, or by the event codes sent by the Control Panel to "Orlan" CMS.

11.12. Wireless sirens registration

Prior to registration of wireless detectors, the type of radio system shall be selected, number and type of zones shall be specified in the Control Panel configuration (at the stage of the device configuring using "Configurator 11" software).

> **Attention! Prior to registration of wireless detectors, the group to be changed shall be disarmed.**

Registration management can be performed via "Lind-29"/"Lind-15"/"Lind-11"/"Lind-9M3" ICDs as follows:

"Lind-29":

- ◆ Press ✶ , *group number*, ✶ to go to the desired group and make sure that it is disarmed.
- ◆ Press # + 9 , *installer_password* to access to the wireless sirens control mode. Zones LEDs in **red** indicate the radiosirens numbers with binded wireless sirens, and the **green** ones indicate free radiosirens.
- ◆ Enter **radiosiren number 1…16** and confirm by ✶ . It will flash in **red**.
- ◆ Select action:
    - ▪ A , ✶ – **delete** wireless siren;
    - ▪ B , ✶ – **add** wireless siren.
    - ▪ C – siren signal level (bar by zones LEDs 1…3) in the last communication session.

The button # – to exit the mode.

"Lind-15":

- ◆ Go to the right group by touching its number on the ICD upper level screen and make sure that it is disarmed.
- ◆ Touching the "**Wireless system**" button and then entering the *installer_password*, go into the wireless sirens control mode – the "**Wireless sirens**" button.
- ◆ Then the available wireless sirens will be displayed as a table. Touch the line with the desired siren number. If the wireless siren is not yet registered (the remaining columns in this line contain dashes), then to switch the Control Panel into the binding mode, touch the "**Add**" button. If the selected siren already registered, you must delete its data first – click the "**Delete**" button.
  If the wireless siren was previously registered in another siren number of this Control Panel, then you need to delete its binding first.
- ◆ Initiate the transmission of the binding signal by the wireless siren depending on the type of wireless system and the type of wireless siren – see section 27. Successful registration is accompanied by a beeping sound "trill".

The button # – to exit the mode.

"Lind-11":

- ◆ Press ✶ , *group number*, ✶ to go to the desired group and make sure that it is disarmed.
- ◆ Select the menu item "**Wireless sirens**", enter the *installer_password* to access to the wireless sirens control mode.
- ◆ Select the free (with a blank "**ID siren**" field in the first line of ICD display) wireless siren via < and > buttons. If the selected siren already registered, you need to delete this

data first (press **F2** button). If the wireless siren was previously bound in another siren number of this Control Panel, then you need to delete its binding first;

◆ Switch the Control Panel to the wireless siren binding signal waiting mode (press **F1** button).

◆ Initiate the transmission of the binding signal by the wireless siren depending on the type of wireless system and the type of wireless siren – see section 27. Successful registration is accompanied by a beeping sound "trill".

The button │ **#** │ – to exit the mode.

"Lind-9M3":

◆ Press │ ✶ │, *group number*, │ ✶ │ to go to the desired group and make sure that it is disarmed.

◆ Press │ **#** │+│ **7** │, *installer_password* to access to the wireless detectors/sirens control mode (**MODE 0** LED will be lit). Be sure the **MODE 1** LED <u>is lit</u> (if no then press │ **TEST INDIC.** │ once). You can bind up to 16 wireless sirens for each group with this ICD. Available wireless sirens is displayed via red **ZONE** LEDs (wireless siren #1 in the current group corresponds to **ZONE 1** LED):

▪ If some wireless siren contains a device then the corresponding **ZONE** LED *is lit*.
▪ If the some wireless siren is free then the corresponding **ZONE** LED *is flashing*.
▪ All unavailable wireless sirens are displayed as *turned off* **ZONE** LEDs.

◆ Select wireless siren you need by entering its number (1...16) and press │ ✶ │ to confirm. Another **ZONE** LEDs will turned off.

◆ Then you can do the next in depends of the wireless siren current binding state:

1. Press │ **FAULT/MUTE** │ – to switch the Control Panel to the wireless siren binding signal waiting mode (if the wireless siren is free). Then you need to initiate the transmission of the binding signal by the wireless siren depending on the type of wireless system and the type of wireless siren – see section 27. Successful registration is accompanied by a beeping sound "trill".

2. Press │ **STAY HOME** │ – to delete the existing binding (if the wireless siren is occupied).

3. Press and hold │ **SIGNAL LEVEL** │ – to check the occupied wireless siren signal strength. It is displayed by the **ZONE 1...3** LEDs. A greater number of luminous LEDs corresponds to a higher signal level.

The button │ **#** │ – to exit the mode (**MODE 0** LED turns off).

12. Communicators

Control Panel allows for transmission of events to "Orlan' CMS via Ethernet using "LanCom" Ethernet-communicator (rev.14 or rev.15), or via wired phone line using TK-17 phone communicator.
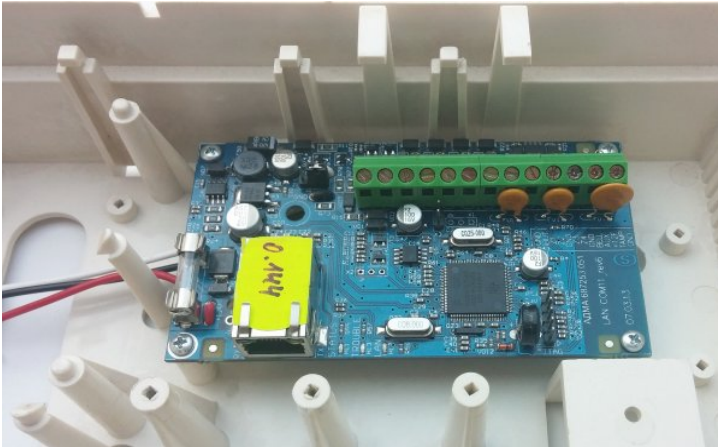

Figure 32. "LanCom" rev.6/rev.15 communicator in the device housing
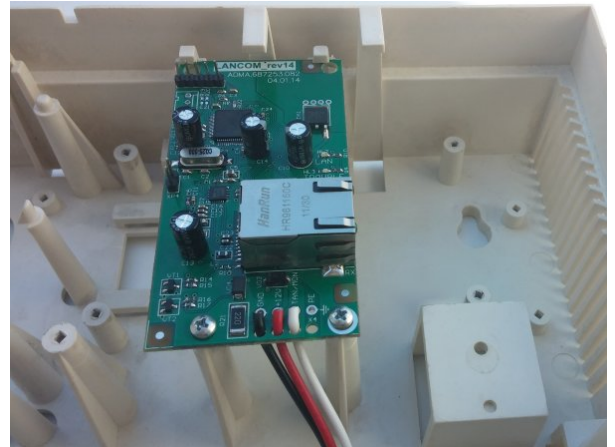

Figure 33. "LanCom" rev.14 communicator in the device housing

12.1. "LanCom" rev.15 Ethernet-communicator

To connect the communicator to the Control Panel the following shall be done:
1. Place the communicator into the housing (Figure 32) and connect it with the Control Panel board according to the schematic diagram in Figure 43;
2. Switch the communicator to the "Lun-11" mode (using built-in Web-configurator on page "Control Panel type", "Lun-11" option shall be selected);
3. Enable and configure the communication parameters and channels priority in the Control Panel configuration ("Configurator 11" software).

More see in "LanCom rev.15 Operating Manual" available at www.ortus.io.

12.2. "LanCom11" rev.14 Ethernet-communicator

To connect the communicator to the Control Panel the following shall be done:
1. Place the communicator into the housing (Figure 33) and connect with the Control Panel board according to the diagram in Figure 43;
2. Switch the communicator to the "Lun-11" mode (using "Configurator" software, "Connected to Lun-11" option shall be selected);
3. Enable and configure the communication parameters via the communicator and priority of communication channels in the configuration of Control Panel (using "Configurator 11" software).

The detailed description of the communicator can be found in "LanCom rev.14 Operating Manual" available at www.ortus.io.

12.3. "TK-17" phone communicator

To connect the communicator to the Control Panel the following shall be done:

1. Place the communicator into the housing (Figure 34) and connect with the Control Panel board according to the diagram in "TK-17 phone communicator. Installation Guide" available at www.ortus.io;

2. Switch the communicator to the "Lun-11" mode (using "Configurator" software, "Connected to Lun-11" option shall be selected);

3. Enable and configure the communication parameters via the communicator and priority of communication channels in the configuration of Control Panel (using "Configurator 11" software);

4. Connect the wires to the telephone line and telephone (if required).

The detailed description of "TK-17" phone communicator can be found in "TK-17 phone communicator. Installation Guide" available at www.ortus.io.
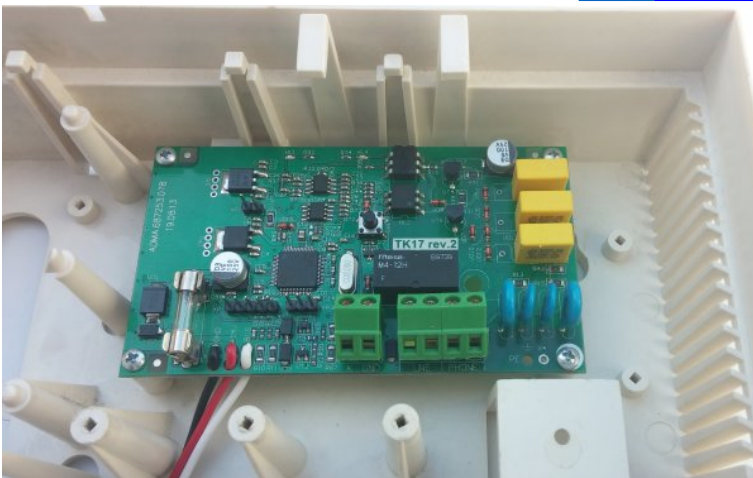
Figure 34. "TK-17" communicator installation
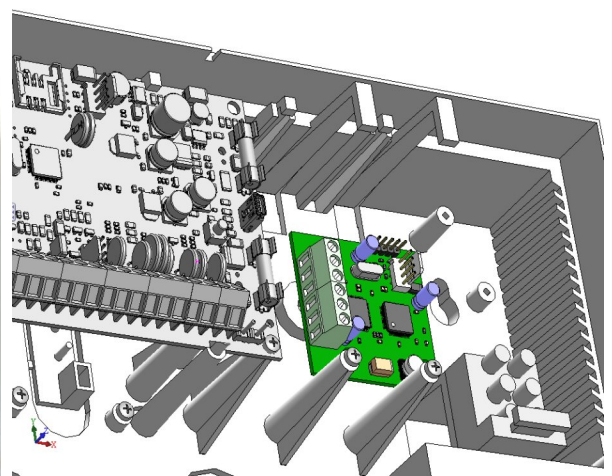
Figure 35. Installation of "Dozor" module

13. "Dozor" alarm photo-proof module

The expansion module is designed for visual confirmation of alarms using photos of the protected facility. "Dozor" photo-proof module is installed in the housing of Control Panel, and connected to it; it supports up to 4 analog cameras.

Photos (one or more taken at the specified interval) made by the module cameras according to the specified events through are transmitted by the device via 3G/GPRS/WiFi channels to "Orlan" CMS (through the open Internet or "Orlan-Video" module).

Photos are stored in the CMS database and are available for viewing at any time.

The main characteristics of "Dozor" module are given in Table 7.

Table 7. "Dozor" module characteristics

Characteristic	Value/Implication
Number of inputs for cameras	4
Type of cameras connected	Analog, Pal standard
Photo, pixel resolution	360x288; 720x576
Motion detector	n/a
Events for which photoshoot is conducted	Zone alarm; group alarm; arming; disarming; group fire

Cameras shall be connected to the terminals of "Dozor" module only with the foiled pair (UTP, CAT5/5e) of the maximum length of 40 meters.

Terminal functions shown in Table 8.

Table 8. "Dozor" module terminal functions

Terminal marking	Function
V1...V4	cameras 1...4 video signal
GND	COM (-)

The module shall be installed in the device housing as shown in Figure 35. To connect it to the Control Panel board (to **X6** connector), the supplied cable shall be used. The connection diagram is given in section 26.

14. Using a WiFi connection channel
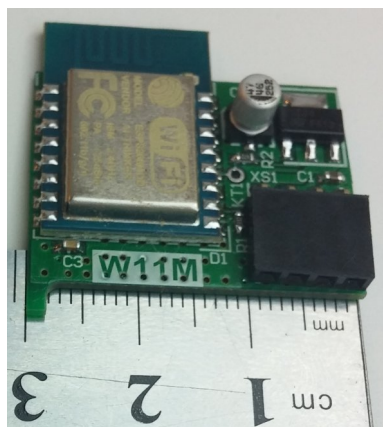
Figure 36. "W11M" module

Wireless communication can be used as an additional channel of communication with the CMS. Communication through this channel provides an additional module «W11M».

Module «W11M» (see. Figure 36) is a device that connects to the Control Panel's PCB via integrated connector (no cables or wires uses) and provides two-way communication over the wireless link at a frequency of 2.4 GHz 802.11b/g/n with protection according to the WPA2 PSK.

Control Panel with «W11M» module connected to the CMS through the pre-selected WiFi access point and Internet connection. This channel provides the transmission of all events, tests and control signals to/from the CMS.

"W11M" module can be used **instead** of any of the Ethernet-communicators, because all of them use the same "open Internet" communication channel.

Attention! Do not connect "W11M" WiFi module and any Ethernet-communicator simultaneously!

One of the Control Panel's PCB connectors – **X3** (wireless radio receiver connector – see Figure 37) or **X6** ("Dozor" module connector – see Figure 38) is used to install the WiFi "W11M" module.
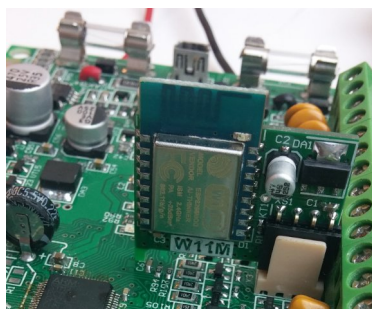

Figure 37. Installing "W11M" to X3 connector

Figure 38. Installing «W11M» to X6 connector

So can not be used or any wireless wireless detector's subsystem or "Dozor" module in the alarm system. As the installing connector for "W11M" module selected (depending on the required components of the security system) is necessary to record this selection in the configuration by using the "Configurator 11" software (available on the www.ortus.io website).

15. Control Panel configuring

Attention! After the Control Panel is mounted, it shall be configured using "Configurator 11" software. To do this, the Control Panel shall be connected to PC with USB/mini-USB cable.

You should use **XS2** connector (see Figure 4) on the Control Panel board and mini-USB cable.

The details of connection and configuring process can be found in "Configurator 11" Guide" available at www.ortus.io.

Attention! "Configurator 11" software runs only on PC with MS Windows 7 operating system or higher.

After the "initial" configuring of the device carried out using USB/mini-USB cable, the further configuring of the device installed at the facility shall be carried out remotely using 3G/GPRS channel (this channel shall be activated and configured in advance).

To configure the Control Panel remotely, the same "Configurator 11" software is used. The configured FTP-server is also required. The details of use of "Configurator 11" software are available at www.ortus.io.

16. Firmware update

Firmware update made in order to increase functionality or correct possible errors.

Control Panel supports firmware update locally (performed by cable USB/mini-USB, plug-in as described in section 15), or remotely (performed via 3G/GPRS connection or WiFi; main power and battery power are required).

"Configurator 11" software commands are used for local updating. Remote update is performed by "Phoenix 4" software (by CMS operator command) or by commands from the "Lind-15" ICD (group menu – **Settings** – **Info** – **Update system**) or "Lind-11" ICD (menu "**Update software**") or "Lind-11LED» (press keys **F5**, **0**, *installer_password*).

Note: After installing the security system to the object, as well as the existing system expansion with additional devices (for example, extenders or ICD – except for the wireless detectors), it is strongly recommended to firmware update of whole system.

The new firmware is checked for compatibility before it's loading. If a newer version is not compatible with currently installed, then the loader program (boot) required to update first. The bootloader is updated remotely – automatically, immediately after updating the main firmware (there is only one attempt to update the bootloader) or locally – manually, using the Configurator 11 program.

Immediately after locally boot updating you should update the main firmware locally.

During the update process, the red LED blinks in series of 3 flashes – do not turn off the Control Panel's power to avoid damage of the firmware.

17. Control Panel remote control

The remote control is available from CMS using "Phoenix-4" software, as well as from a mobile phone (from the configured numbers) – see section 6.9.

Control Panel supports remote control via mobile applications «Phoenix-MK» (WiFi or GPRS/3G channel should be turn on) is available for devices on Android OS and iOS.

18. Battery monitoring

The battery monitoring function in Control Panel is enabled by default and runs automatically. You can switch off battery monitoring for any Expansion Module by "Configurator 11" software.

If necessary, replace the battery in accordance with the instructions in section 5.

19. Main power supply monitoring

The main power supply monitoring function in Control Panel is enabled by default and runs automatically. The main power supply loss message is generated with delay (see Table 1). The main power supply recovery message is generated with no delay.

To ensure proper Control Panel start-up you should make 10s pause before it turns on!

20. Maintenance

The Control Panel does not require any maintenance.

21. Operating conditions

The Control Panel shall be used at the temperature of −5°C to +40°C and relative humidity of 5% to 85%.

22. Storage

1. Storage temperature shall be of -50°C...+40°C at the relative humidity of 5% up to 98%.
2. During handling operations, transportation and storage in warehouses, boxes with the product shall not be exposed to sharp bows. Stacking and fixing of the boxes to the transporter shall not include their movement.
3. Product shall be stored in the manufacturer's package.

23. Transportation

1. Product transportation shall be carried out in the manufacturer's package.
2. Product is allowed to be transported by all types of enclosed transporters, subject to observing the shipping rules applicable for each type of transport.
3. Transportation temperature shall be of -50°C to +50°C at the relative humidity of 5% up to 98%.
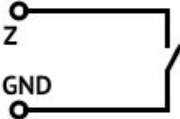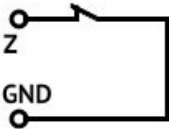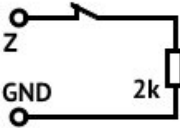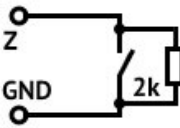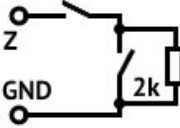
24. Disposal

Product disposal shall be carried out according to electronic household appliance disposal rules established by the legislation of the State, where the product is operated.

25. Appendix 1. Control Panel zones types

The physical type of a zone (line) (i.e. to which type of event it responds) is configured using "Configurator 11" software. The details of use of "Configurator 11" can be found in "Configurator 11" Guide".
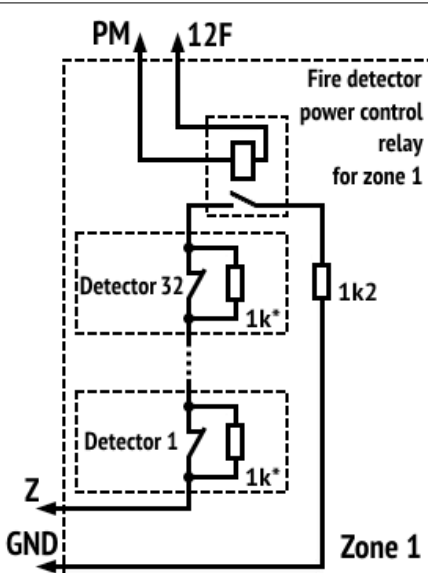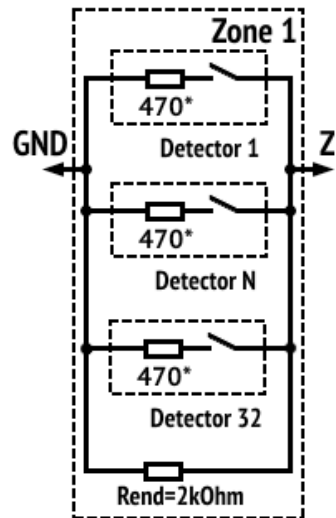
See the types of protective zones and events generated in case of their violation, in Table 9.

Table 9. Protective zones types

Connection circuit	Short circuit-generated event	Disconnection-generated event
1. Zone type – "Normally open"		
	alarm	norm
2. Zone type – "Normally closed"		
	norm	**alarm**
3. Zone type – "Termination resistor, alarm upon disconnection"		
	zone fault	**alarm**
4. Zone type – "Termination resistor, alarm upon short circuit"		
	alarm	*zone fault*
5. Zone type – "Termination resistor, alarm upon disconnection and short circuit"		
	alarm	**alarm**

The types of fire zones and events generated in case of their violation see in Table 10.

Table 10. Fire zones types

| Connection circuit	Short circuit-generated event	Disconnection-generated event
6. Zone type – "Normally closed, 2 resistors"		
	zone fault	*zone fault*
* – To recognize second detector in the zone, the resistance of the additional resistor for each detector should be **1 kOhm**	**detector circuit break – alarm**	
7. Zone type – "Normally open, 2 resistors"		
	zone fault	*zone fault*
* – To recognize second detector in the zone, the resistance of the additional resistor for each detector should be **820 Ohm**	**closing of detector circuit – alarm**	
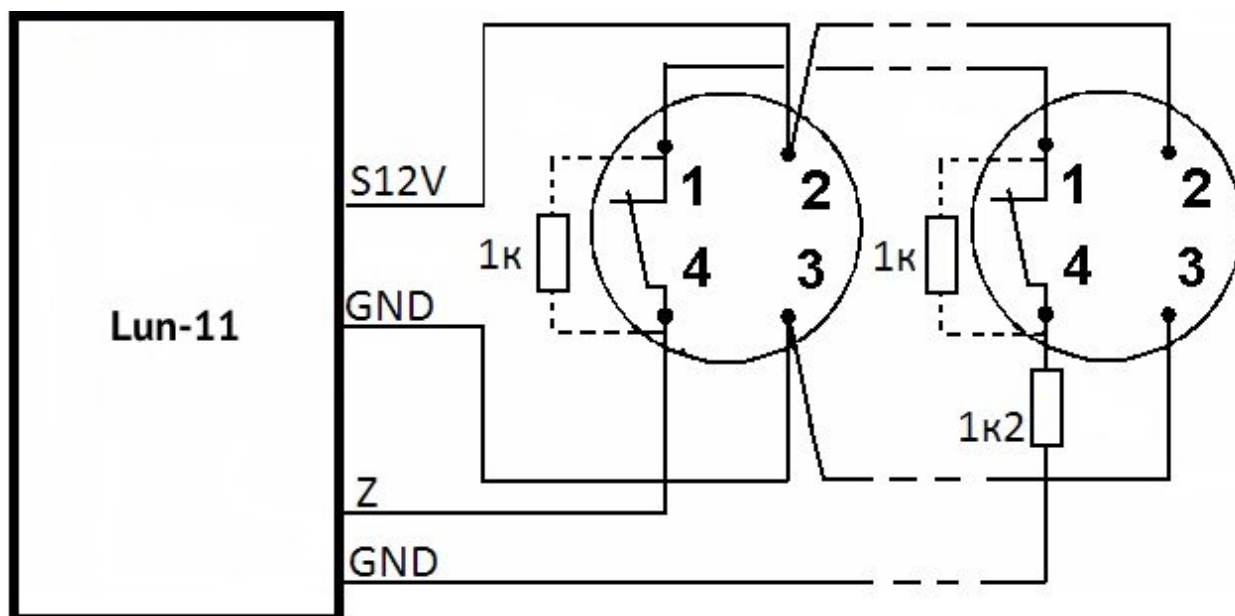
Figure 39. Fire detector connection diagram according to four-wire circuit
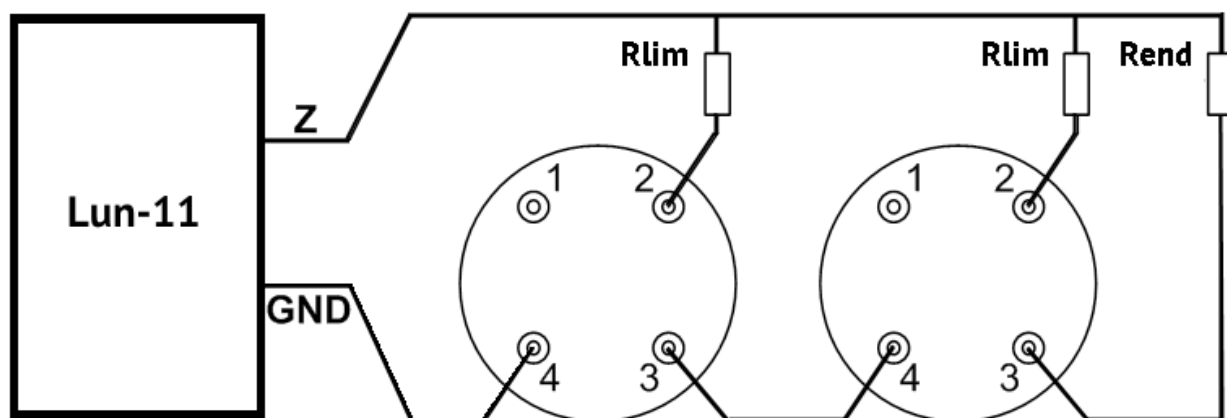

Figure 40. Diagram of connection of detectors to fire zone according to two-wire circuit

Table 11. An example of Rlim calculation

Detector type	Rlim nominal value
IPK-8	200 Ohm
SPD-3	470 Ohm
Any other detector	Rlim is calculated by the formula: **Rlim=800 Ohm – Rdet**, Where Rdet is detector resistance in the "Fire" state, Ohm

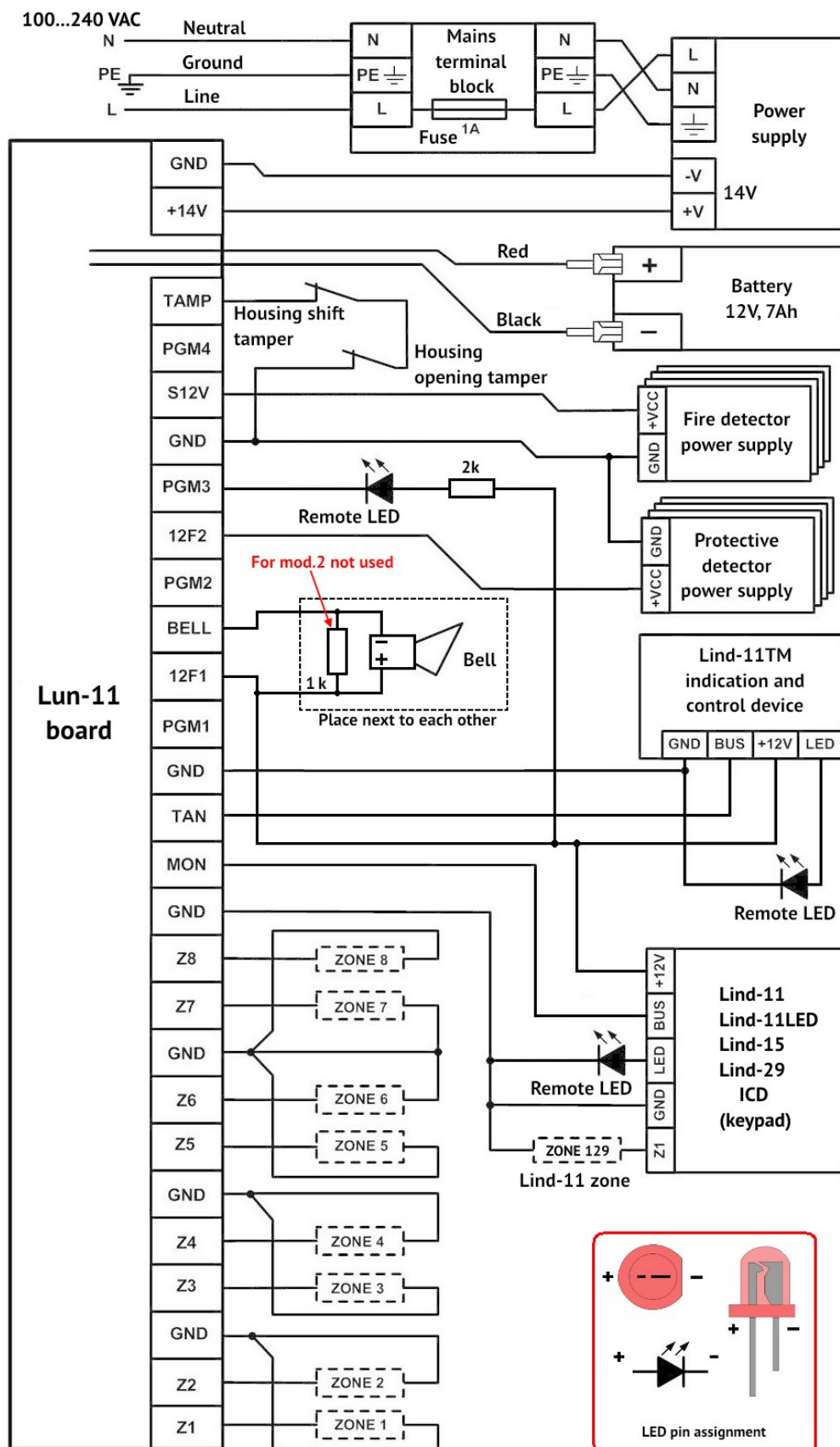# 26. Appendix 2. Control Panel connection diagram

Figure 41. Control Panel connection diagram

> **Attention!** Adherence to this connection diagram is mandatory. Failure to comply with this requirement can lead to breakdown of the device, and consequently, to impossibility of performance of the warranty liabilities.
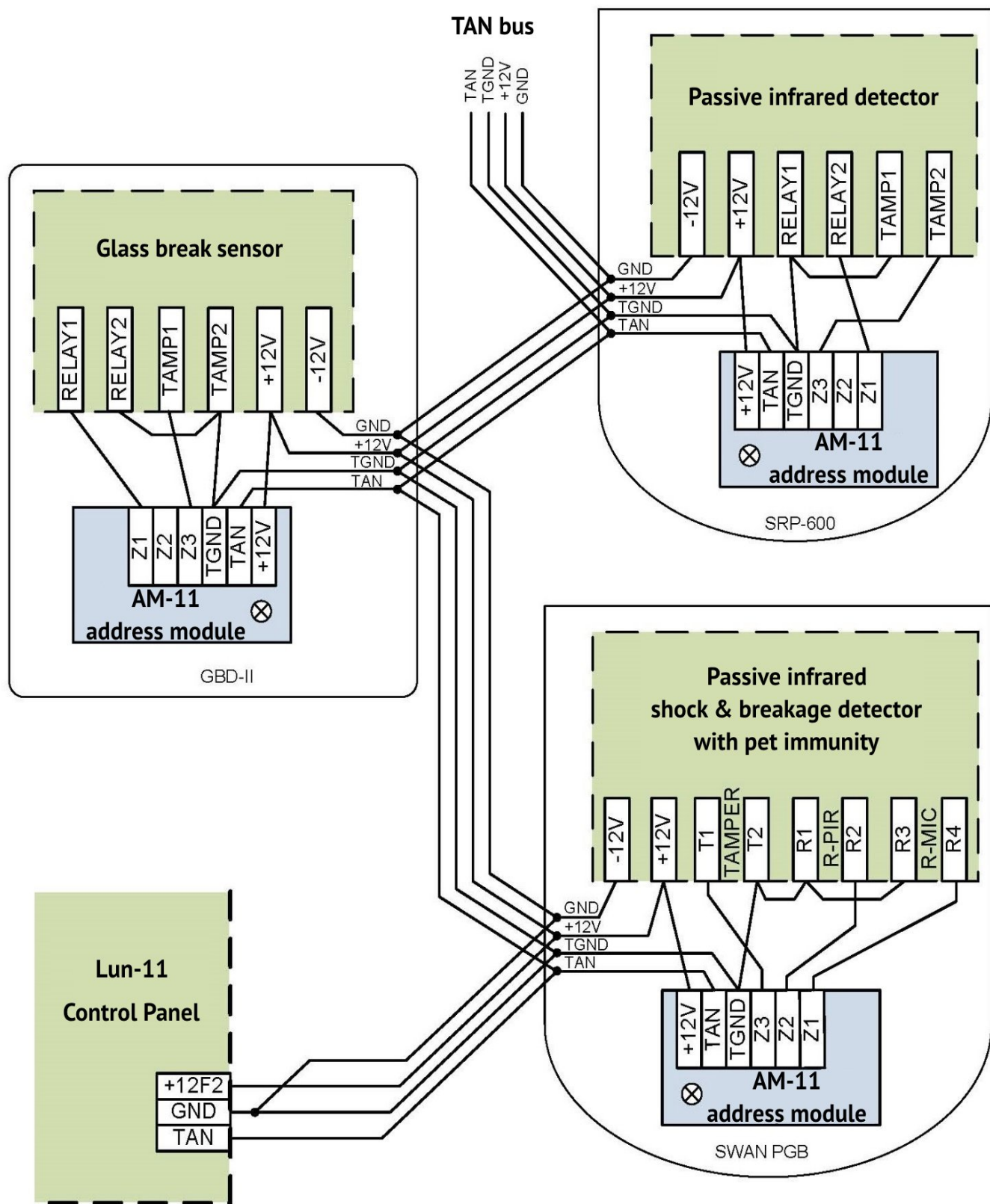
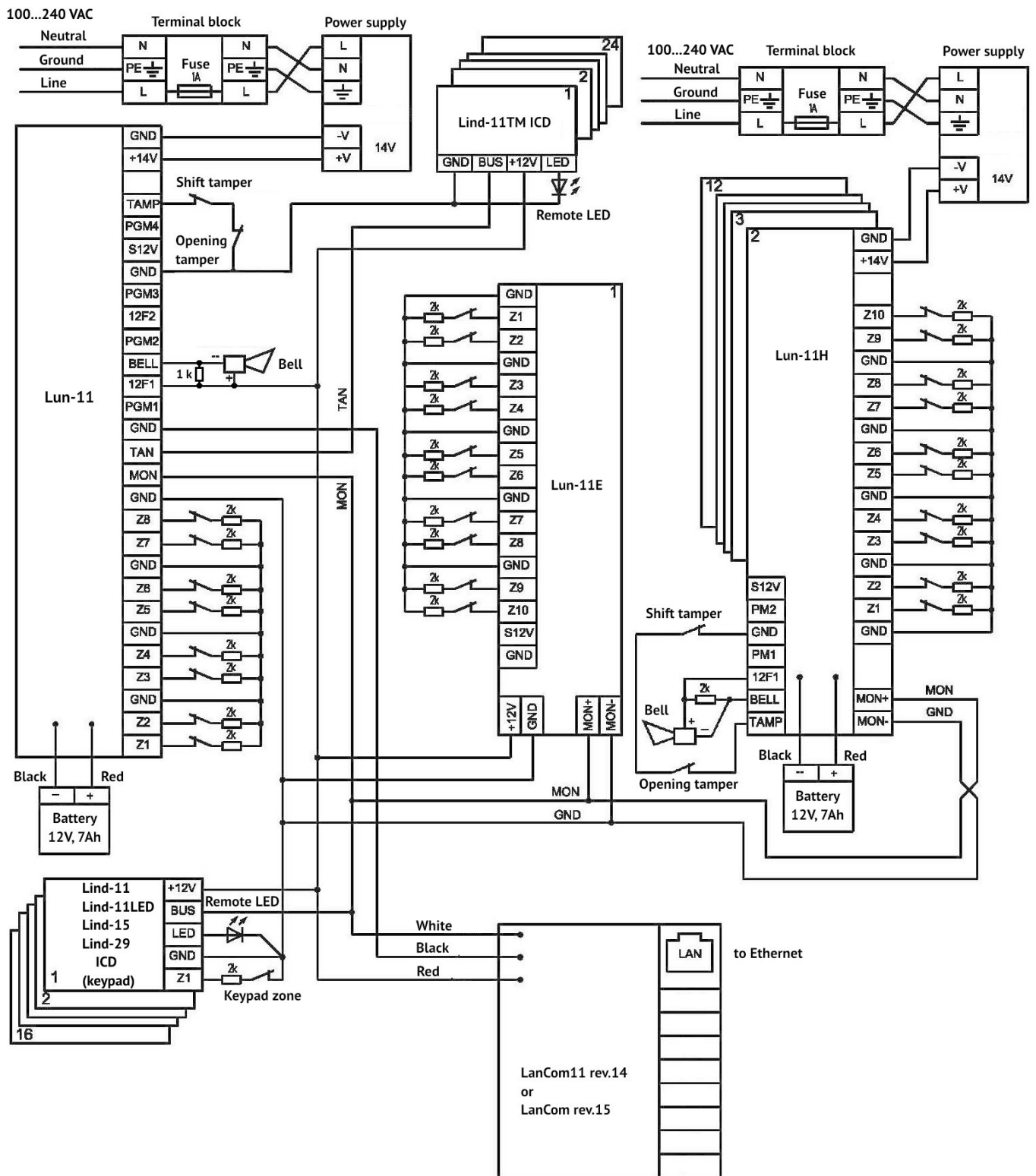*Figure 42. An example of use of "AM-11" address modules*
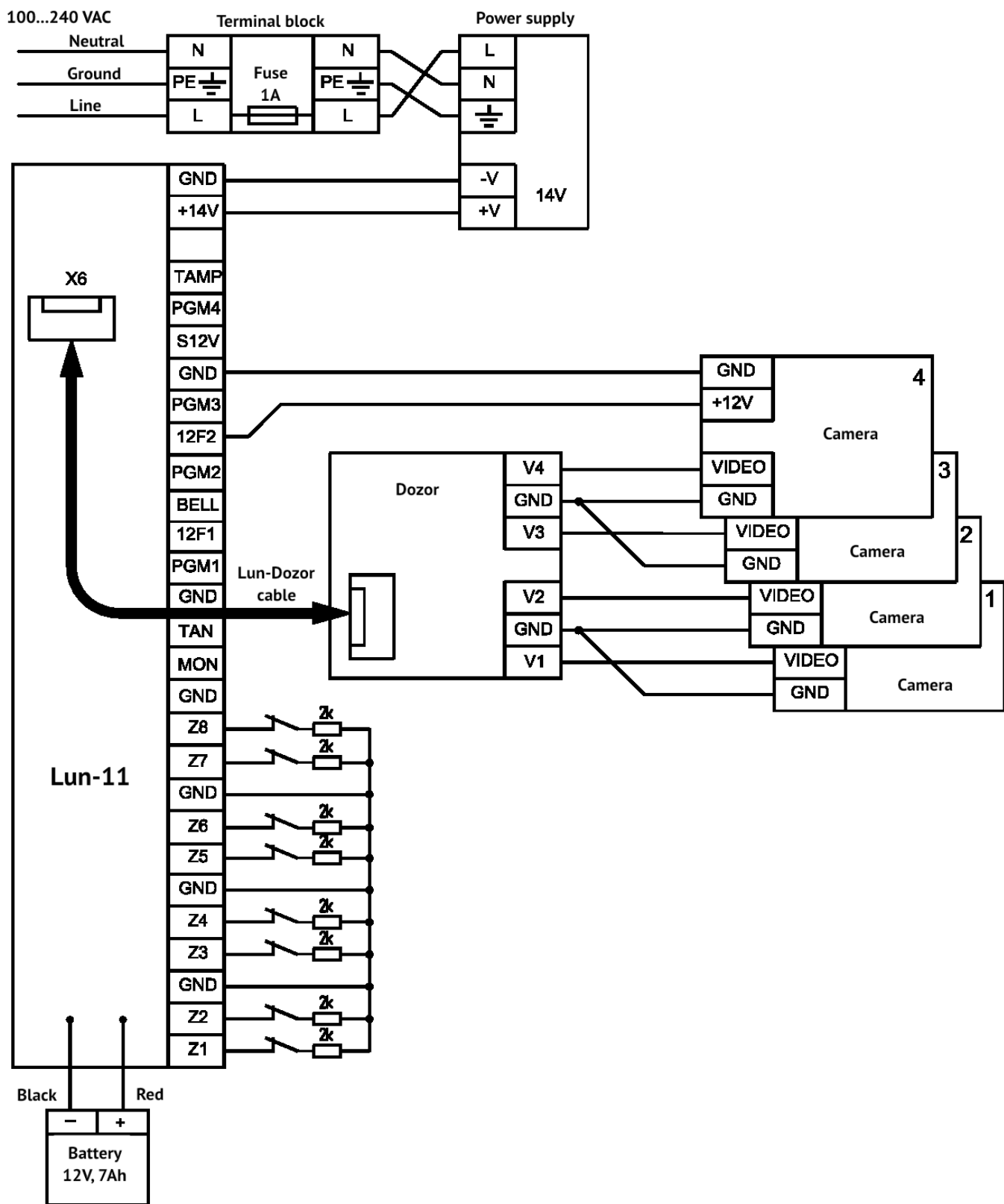
Figure 43. Network device connection diagram

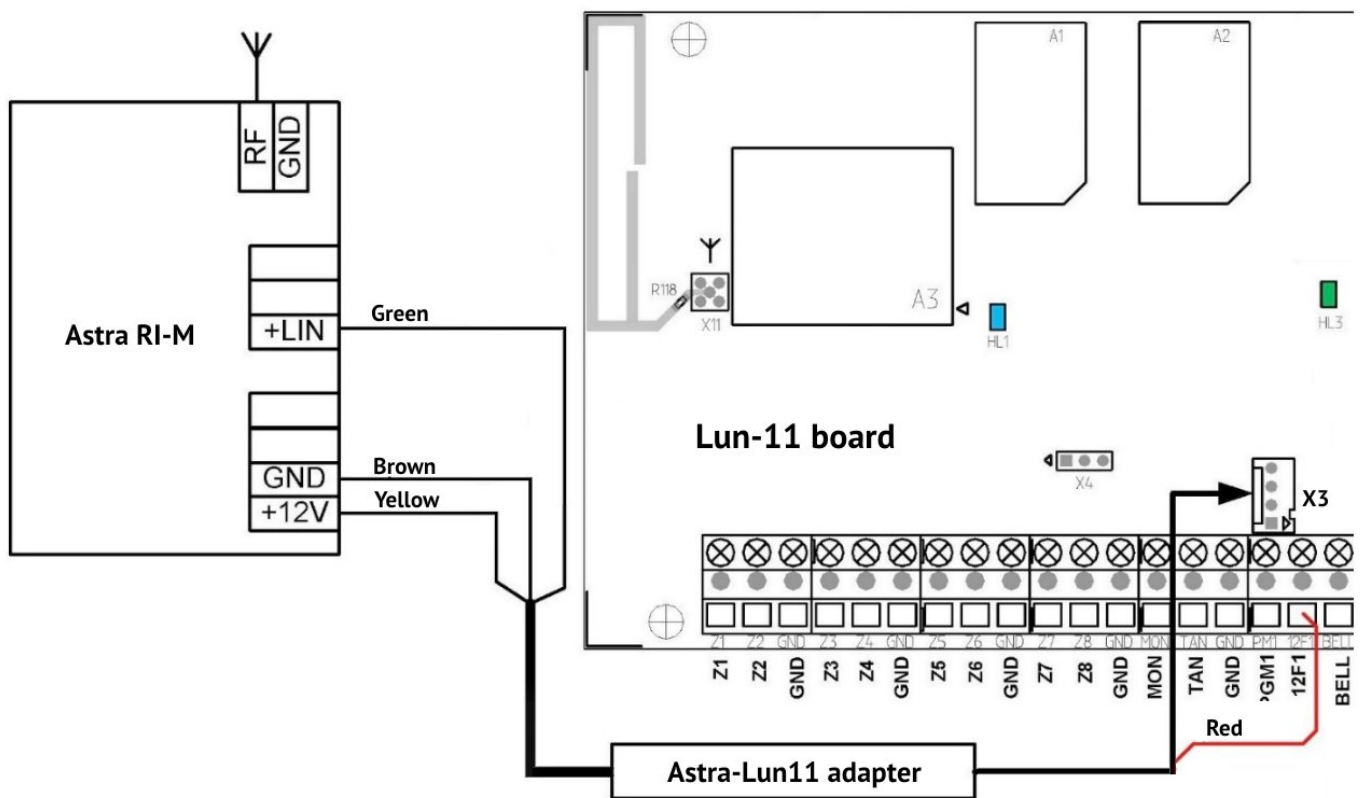*Figure 44. Connection diagram for "Dozor" alarm photo-proof module*

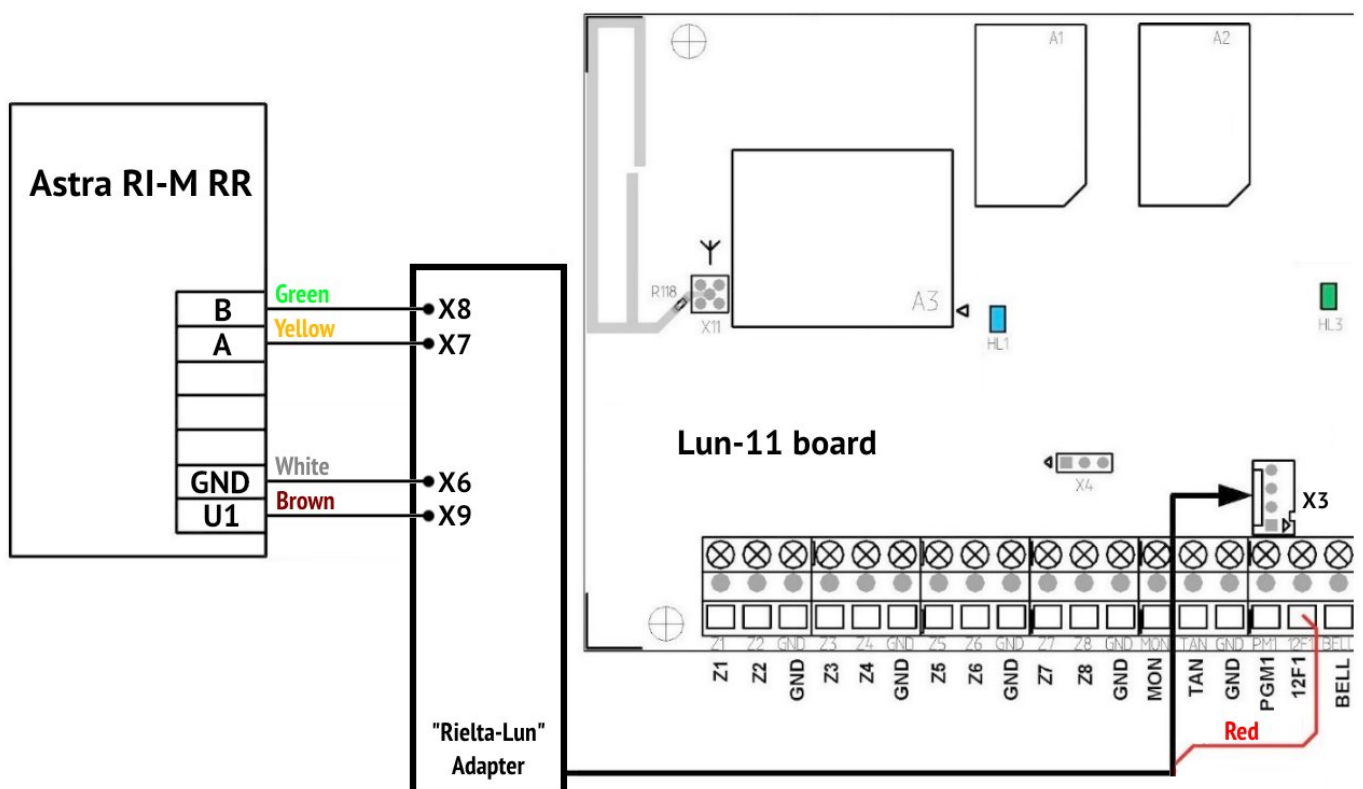*Figure 45.* "*Astra RI-M" radio receiver connection diagram*

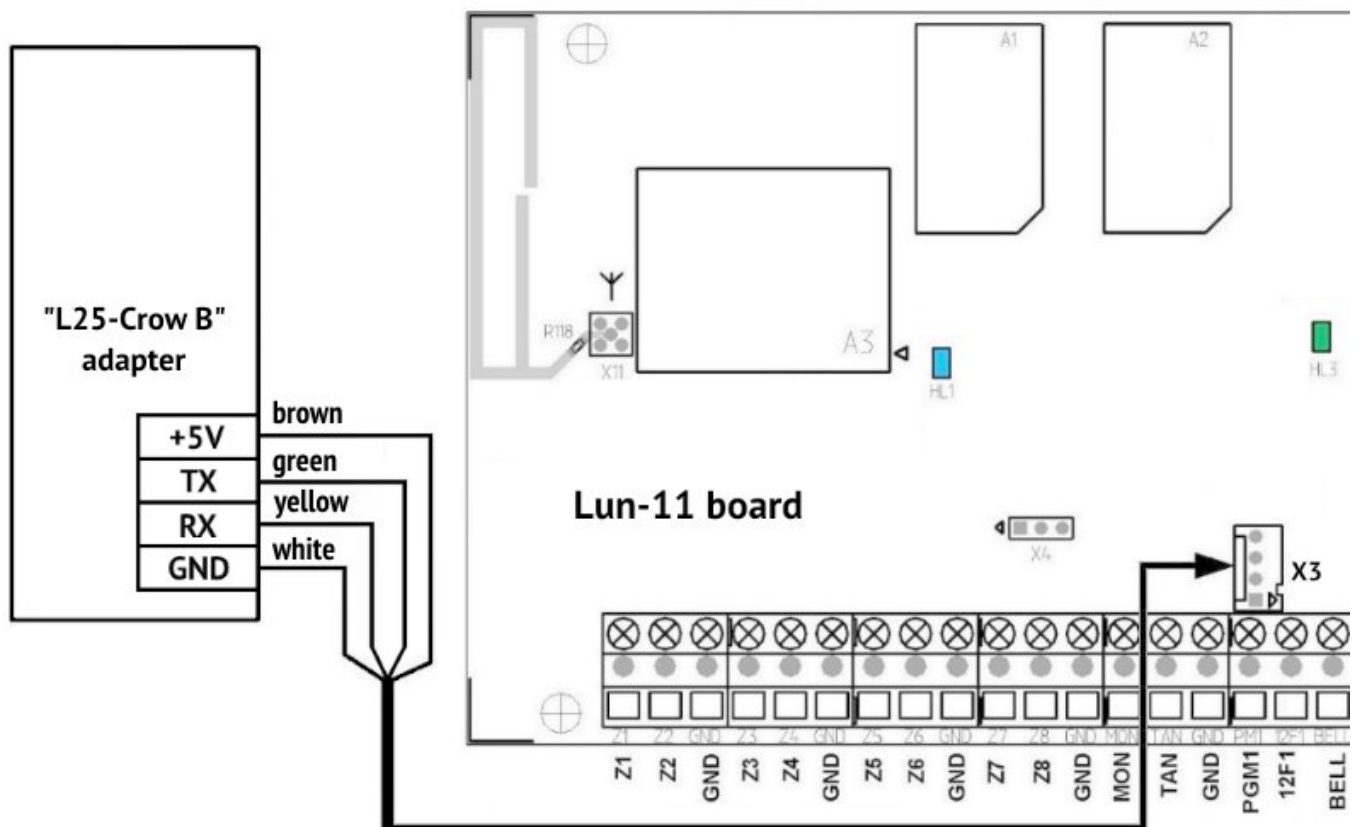*Figure 46. Astra RI-M RR" radio receiver connection diagram*

Figure 47. Adapter "L25-Crow B" connection diagram

27. Appendix 3. Wireless devices handling

27.1. Lun-R

The Control Panel supports the next Lun-R wireless detectors:
- **Button-R**" – Keyfob;
- "**Keypad-R**" – Keypad;
- "**Magnet-R**" – Magnetic contact security detector;
- "**PIR-R**" – Passive infrared detector;
- "**Flood-R**" – Flood detector;
- "**PIROUT-R**" – Security passive infrared wide-angle detector for open areas;
- "**SMOKE-R**" – Smoke detector;
- "**PIR-CR**" – Curtain PIR detector;
- "**GBD-R**" – Glass break detector;
- "**Button-VR**" – Keyfob with vibration response;
- "**Repeater-R**" – Signal repeater;
- "**Socket-R**" – Controlled socket;c
- "**Relay-R**" – Controlled relay;
- "**Siren-R**" – Indoor siren.

The "Lun-R" radio receiver should be set in the Control Panel configuration.

To register (bind) one Lun-R wireless detector the following shall be done:
- Remove battery from the wireless detector;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Install batteries to the wireless device (for repeater – battery only), then switch the wireless device to the binding mode (this is accompanied by flashing green LED):
  - ◆ **Repeater** – close the **START** pins for device start from battery – up to red-green flashing. When the red-green flashing ends close the START again for 2…3 seconds – up to green flashing;
  - ◆ **Detector, relay** – close **RESET** pins shortly;
  - ◆ **Socket** – hold down the button until the indicator blinks green;
  - ◆ **Keyfob** – press any key (for rebinding – press all keys for 3 seconds simultaneously);
  - ◆ **Siren** – close the terminal "**4**" to **minus pole** of any battery (MAIN / BACKUP) for 3 sec.
- Make sure the wireless detector is registered by red flash of his LED and control panel's sound trill. Control panel waits a binding signal up to 40 seconds, if a binding fails the process ends with a long beep.

27.2. Jablotron

The Control Panel supports some Jablotron wireless detectors (Table 12).

Table 12. Jablotron wireless detectors

Wireless detector type	Description	Operation mode
JA-60N	Wireless magnetic contact detector	instant
JA-60V	External infrared motion detector	delay
JA-60P	Infrared motion detector	delay
JA-60B	Wireless glass break detector	delay
JA-60G	Wireless gas leak detector	MEM=OFF
JA-63S	Wireless fire detector	instant
RC-60	Wireless controller (use "RC-60" zone in the device)	MODE= as you need
RC-11	Two-button wireless keyfob	–
RC-86K	Wireless keyfob	17, each pair of buttons – for separate group

Attention! Jablotron wireless detector shall be registered not using its tamper, but only by installing of its battery tamper (if any) shall be violated in this case.

Adequate operation of the device is only possible if the corresponding detector is set in the mode specified in Table 12, zone type should be set to "24h Fire" for all fire detectors.

A zone of "RC-60" type shall be used for Jablotron RC-60 wireless detector. In this case, the wireless detector is processed as a keyfob (as RC-11), but also taking account of the tamper present, as of the common wireless detector, and processing of the connection loss signal.

The minimum timeout of loss of connection with Jablotron wireless detectors is 45 minutes.

To register (bind) one Jablotron wireless detector the following shall be done:
- Remove battery from the wireless detector;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Install the power supply unit in the wireless detector;
- Visually monitor the wireless detector registration.

27.3. Visonic

The device can operate with the following Visonic wireless detectors:
- MCT-302N – magnet contact with PowerCode transmitter;
- MCT-234 – wireless (CodeSecure) button micro-transmitter;
- MCT-501 – wireless sound glass break detector;
- NEXT MCW – wireless passive electrooptical infrared detector;
- NEXT K9-85 MCW – wireless PowerCode Pet-Immune PIR Detector;
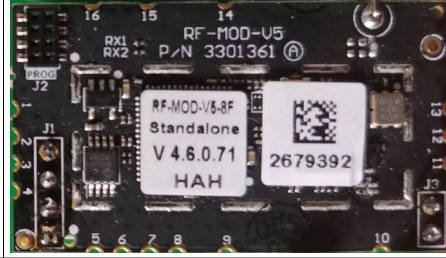- MCT-426 – Wireless Smoke Detector.

To register (bind) one Visonic wireless detector the following shall be done:
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Change its status – violate/recover the tamper or set the alarm/normal mode;
- Visually monitor the wireless detector registration.

27.4. Crow

Depending on the installed Crow module, the Control Panel supports of the following Crow wireless devices (see Table 13).

Table 13. Crow wireless devices

Receiver based...	...on RF UART 0034638 module	...on RF EFM 32 V5 module
Wireless device **Model No.**		
FW2-MAG-8F – magnet contact	0034590 0034895	0034895
FW2-RMT-8F – keyfob	0022012 (release date earlier 5016 with the receiver version **2.66 only**; release date 0916 and higher with receiver version **2.67 and higher**)	0022012
FW2-Panic Button – panic button	0022540	0022540
FW2-NEO-8F– infrared detector	0034770 0035690	0035690
FW2-SMK-8F – smoke and heat detector	0024160	0024160
FW2-FLOOD-8F – flood detector	0046496 0034898	0034898
FW2-EDS3000-8F – outdoor PIR AM detector	0034710	0034710
FW2-ICON-KP-8F – user control keypad	0035420 (with receiver version **2.67 and higher**)	---
FW2-VESTA-8F – indoor siren	0020580 (release date **1018 and higher** with the receiver **version 2.67 and higher**)	---
FW2-SIREN-8F – outdoor siren	002366X	0035750
FW2-RPTR-8F – repeater module	0034360	0059360
SH-MAG-8F – magnet contact	---	0059580
SH-PIR-8F– infrared detector	---	0059910
SH-CRT-8F– infrared detector	---	0059930
SH-FLOOD-8F – flood detector	---	0059970
SH-GBD-8F – glass break detector	0034970	0059260
SH-KP-8F – user control keypad	---	0059280

If the receiver was replaced, or the wireless sensors settings was switched from "External" to "Internal" and vice versa, each registered wireless sensor in the system should be repowered after the Control Panel has started to work in normal mode (i.e. is not in update/configuration mode).

To register (bind) one Crow wireless detector the following shall be done:
- Remove battery from the wireless detector;
- Switch the Control Panel to the binding mode (chapter 11.11);
- To register:
    1. **Wireless detector** – install the wireless detector battery, wait until the two-color LED stops flashing, change the status of its tamper – violate it and then recover it;
    2. **Keyfob** – delete the previous registration by pressing the ② and ③ buttons simultaneously. Registration – press ③ and ④ buttons simultaneously (see Figure 48);
    3. **Keypad ICON** – delete previous registration – **C**, **0000**, **SOS**+**SOS** to 🔧 off; then press any key to new binding.
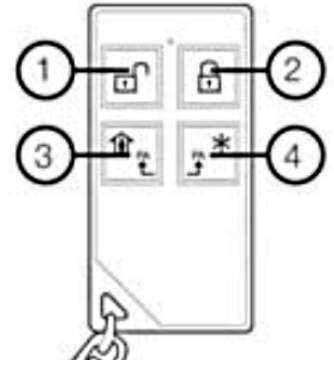- Visually monitor the wireless detector registration.

Figure 48. Keyfob Crow FW2-RMT-8F

To register (bind) one Crow wireless siren the following shall be done:
- Turn off the wireless siren battery;
- Remove the previous binding from wireless siren – <u>press and hold</u> **LEARN** key then turn on wireless siren battery. Wait until the LED flashing starts then release the key;
- Switch the Control Panel to the binding mode (see chapter 11.12);
- Start the transfer of the wireless siren binding signal by short press **LEARN** key;
- Visually monitor the wireless siren registration.

To register (bind) one Crow wireless repeater the following shall be done:
- The wireless zone type for the repeater in the Control Panel configuration should be set to "**Radio keyfob**";
- Open the cover of the repeater housing and disconnect the backup battery cable;
- After 30 seconds, turn on the repeater's battery cable, close the cover of its housing;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Insert the repeater plug into the mains socket for automatic binding. It occurs when the repeater indicator stops flashing.

27.4.1. SH-KP keypad

The keyboard is registered by its serial number – it should be entered in the "DeviceID" field of the corresponding wireless zone in the "Configurator 11" program. Keyboard batteries must be installed after recording the configuration and turning on the Control Panel.

By default, the keypad controls the group where it is assigned to in the Control Panel configuration. For arming in the "**Stay at Home**" mode, you must enter a password (or attach a key), and then press the button ⌂ . For arming into **normal** mode, enter the password (or attach a key), and then press the button ↟⌂ for example:

<div align="center">2145   ↟⌂</div>

– group armed in the normal mode with password **2145**.

For disarming, enter the password (or attach a key), and then press the **Enter** button (↵) for example:

<div align="center">2145   ↵</div>

– group disarming with password **2145**.

The keypad allows you to arm and disarm other groups. To do this, before entering the user's password, you must enter a group number of two digits, for example:

<div align="center">032964   ⌂</div>

– group **3** armed in the "Stay home" mode with password **2964**.

The Control Panel's passwords/keys can be edited by this keypad in the next manner.

> SH-KP supports keys compliant with ISO 15693 (13.56 MHz frequency) only.

A sequence of 3 commands is used to manage passwords/keys:

1)   **NNNAAAA**   **Enter**   (⌂ **flashes once by green to accept**)

there **NNN** – is a group number where the user password/key is registered;
    AAAA – this group's administrator password.

2)   **KMXXX**   **Enter**   (⌂ **flashes once by green to accept**)

there **K** – command to manage the password/key:
      3 – user's "**normal**" password management;
      4 – user's "**under duress**" password management;
      6 – user's **keys** management.
    M – command modification:
      0 – **delete** the existing password/key;
      1 – **add** a new password/key into free cell.
    XXXX – password/key number.

3)   **YYYY**   **Enter**   (⌂ **flashes once by green to accept**)

there **YYYY** – new password or attached key.

If the password/key is accepted in this step, the ⌂ icon is briefly turned on **red** and then **GREEN**, followed by a beep.

If the command declined on the any step, the ⌂ icon flashed once in **RED**.

For example the next commands sequence –

0010000 ⏎

31007 ⏎

7475 ⏎

– will add the **7475** code as a password **#7** in the group **#1** (by administrator password **0000**).

If the new password/key is not accepted then you can repeat the command 3) right away – for example to enter another password (attach key).

If the whole commands sequence 1)+2)+3) is performed then the keypad will return to normal mode immediately. If the entering the commands 2) or 3) is not completed then the keypad will re- turn to normal mode automatically over 30 seconds after the last command was sent to the Control Panel (a command is sent by the ⏎ is pressed).

If the 1) command was performed then you can switch to another group right away – while the 2) command is not entered yet.

You can't to assign the users to some group by keypad – do it previously by "Configurator 11" software.

27.5. Rielta

The device can operate with the following Crow wireless detectors:
- Ladoga IPR-RK – wireless channel manual fire detector;
- Ladoga KTS-RK – wireless channel manual burglar alarm detector;
- Ladoga MK-RK – wireless channel magnet contact burglar alarm detector;
- Ladoga PD-RK – electrooptical smoke detector;
- Steklo-3RK – wireless channel sound surface burglar alarm detector;
- Foton-12-RK – wireless channel electrooptical burglar alarm detector;
- Foton-SH – electrooptical surface burglar alarm detector;
- Foton SH2-RK – electrooptical surface burglar alarm detector.

Depending on the design of the wireless sensors used and the wireless receiver, the appropriate receiver type should be set in the Control Panel configuration:
- Rielta – RKI New – for devices with an optimized radio channel (see manufacturer's instructions) made on the red PCB;
- Rielta – RKI – for devices made on the green PCB.

To register (bind) one Rielta wireless detector the following shall be done:
- Remove battery from the wireless detector;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Install battery to wireless detector, set the registration mode by short closing of "RESET" jumper (accompanied by green flashing of LED);
- To register:
  1. Wireless detector – runs automatically;
  2. Keyfob – press the test detection button until LED lights up green; press this very button until LED lights up red; press any button to complete the registration.
- Visually monitor the wireless detector registration.

Potential problems:
1. One of wireless detectors does not send signals or does it rarely. "Radio" (HL2) LED on the receiver lights up for a few seconds or is constantly lit.
   Solution: This can occur, when a new wireless detector has been registered, but the previous wireless detector registered in the same wireless zone, has not been disabled. This previous conflicting wireless detector shall be found and disabled. In extreme case, the radio network address can be changed and the wireless detectors can be re-registered.
2. Radio receiver cannot be turned on. Both LEDs of the radio receiver flash at the same time at 1 sec intervals.
   Solution: The conflict of radio network addresses is present. The network address shall be changed in the Control Panel configuration. If any wireless detectors have been previously registered, they shall be bound once more.
3. Board failure. Both LEDs are lit at the same time.
   Solution: The board shall be changed and wireless detectors shall be re-registered.
4. Radio receiver firmware error. The LEDs flash alternately.
   Solution: Update the radio receiver firmware or replace the radio receiver.

27.6. Astra

The device can operate with the following Crow wireless detectors:
- Astra-3321 – wireless channel magnet contact addressable burglar alarm detector;
- Astra-5131 – wireless channel passive electrooptical burglar alarm detector;
- Astra-5121 – wireless channel passive electrooptical space violation burglar alarm detector;
- Astra-421 – wireless channel electrooptical smoke detector;
- Astra-4511 – wireless channel manual fire detector;
- RPDK Astra-RI-M – mobile wireless channel electric contact addressable burglar alarm detector (keyfob).

Information concerning the registered wireless detectors is stored in the "Astra" radio receiver and is not available for reading. In "detector ID" field is stored conventional wireless detector type and detector's index only. Those, value in this field should be considered as a unique sign of the registered detector presence in this area rather than as really existing code or serial number of the wireless detector.

Attention! When replacing radio receiver "Astra" (for example, because of its failure) is required to re-register all the wireless detectors in the new receiver (you should remove them in the ICD with the "F2" key previously).

If you want to change the zone number for the already registered wireless detector, you must first remove its registration in the "Astra" radio receiver and in the Control Panel, and then to register it in another zone. Searching detector to remove is recommended to focus on the previously applied to the wireless detector sticker/label with its zone number (you should apply this sticker/label on every new registration of each wireless detector). In other words, do not focus on the "detector ID" field value – it is not tied to a real wireless detector in the Control Panel!

27.6.1. Wireless detectors registration in the "Astra-RI-M" radio receiver

"Astra" wireless detectors/keyfobs shall be registered in "Astra-RI-M radio receiver" transmission unit according to the Guide attached to the transmission unit. Priority of wireless detectors registration in "Astra-RI-M radio receiver" shall correspond with the wireless zones functions in the Control Panel.

"Astra-RI-M radio receiver" transmission unit shall operate off-line (**F1, F2, F3** jumpers shall be dismounted, **F10** jumper shall be installed).

Only one "Astra-RI-M" radio receiver unit can be used.

To register wireless detectors the following shall be done:
1. **Turn off** the transmission unit, set the registration mode (F2 jumper shall be installed);
2. Prepare all the wireless detectors – open their housings and dismount their power supply units (or dismount their power-on jumpers – that depends on the wireless detector used; see the Operation Manual for this specific wireless detector);
3. **Power on** "Astra-RI-M radio receiver", **green** and **red** LEDs shall light up for 1 sec;
4. If all previously registered wireless detectors are to be deleted from the radio receiver memory (which is mandatory for the first use), S1 shall be pressed and hold within 5...6 sec until **red** LED lights up;
5. Shortly press **S1**, and the radio receiver will switch to the mode of wireless detector waiting mode (for 45 sec);

6. Power on the wireless detector being registered according to the zone order of "Lun-11" Control Panel (for "Astra-421" and "Astra-4511", shortly close **F1** plug (if it exist) on the wireless detector board, then press tamper button for 1sec and release it);

7. **Both** LEDs on the radio receiver board will go out, and in case of successful registration, in 2…3 sec **red** indicator of the radio receiver shall flash twice a second within 5 sec. In case of other indication, the registration has failed and it shall be repeated starting from step 5;

8. Register the remaining wireless detectors by repeating the steps starting from the 5th one.

9. Turn off the radio receiver, dismount **F2** jumper;

10. If required, install the required **F4…F8** jumpers;

11. Connect the radio receiver to the Control Panel.

27.6.2. Wireless detectors registration in the "Astra-RI-M RR" or "R433A" radio receivers

Only one "Astra-RI-M RR" radio receiver unit can be used.

Make sure that the "Astra-RI-M RR" receiver operates in the "system" mode and that jumpers F1…F4 are removed. Astra RI-M RR firmware version – **Rrs-rim-av3_0.tsk**.

If a repeater is used in the radio system, then it must work in the "repeater" mode, jumpers F1…F4 – should be removed, firmware version – **RRa-rim-av3_0.tsk**. All wireless detectors are registered through the receiver. The repeater must be registered first of all wireless detectors. While detectors is registering, the repeater must be turned on. If the repeater is not needed, it should be deleted in the Control Panel configuration, and the wireless detectors that worked through it should be deleted and re-registered.

The software version of the radio receiving module both in the "Astra-RI-M RR" and in the repeater is **Rpp2r-av3_2.tsk**.

Depending on the radio channel mode used in wireless sensors (see manufacturer's instructions), select the appropriate type of receiver in the Control Panel configuration:

- Mode 1 – P433A / Astra-RI-M RR;
- Mode 2 – P433A / Astra-RI-M RR New.

If at least one of the wireless detectors does not support "mode 2", then all wireless detectors and a radio receiver must be configured to operate in "mode 1".

If all wireless detectors support "mode 2", then during setup you can set any of the operating modes (1 or 2), and this mode should be the same for all wireless devices.

All wireless devices in the system must operate with the same operating frequency.

To register wireless detectors the following shall be done:

- Remove battery from the wireless detector;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Install battery to wireless detector, then place "On/Off" jumper (if it is provided wireless detector design). After that, registration is automatic (for "Astra-421" and "Astra 4511" briefly close the F1 plug on wireless detector board, and then click on 1s and release the tamper);
- Visually monitor the wireless detector registration.

27.7. Ajax

27.7.1. Ajax "RR-108" radio receiver using

The Control Panel can operate with the following Ajax wireless detectors:
- WS-401 – door/window opening detector;
- WS-301 – motion detector;
- WS-601 – glass break detector;
- WS-502 – smoke detector;
- WS-101 – keyfob.

To register (bind) one Ajax wireless detector the following shall be done:
- Switch the Control Panel to the binding mode (see chapter 11.11);
- To register the detector, press **"TEST"** button on the detector; registration process takes 3...5 sec;
- Visually monitor the wireless detector registration.

All wireless detectors of this series sent tamper alarm as wireless detector housing opening but **tamper restore are not sent** (at the close of the case). Therefore, as tamper alarm received from the wireless detector, the Control Panel report transmitted to the CMS, and then after 1...3 seconds CP automatically generates a tamper recovery and also sends it to the monitoring station. This occurs regardless of the actual state of the wireless detector tamper.

27.7.2. Ajax "uartBridge" radio receiver using

The Control Panel can operate with the following Ajax wireless detectors:
- Ajax DoorProtect – wireless reed magnet contact detector;
- Ajax MotionProtect / Ajax MotionProtect Plus – wireless passive infrared / microwave motion detectors;
- Ajax GlassProtect – wireless glass break detector;
- Ajax CombiProtect – wireless glass break and passive infrared motion detector;
- Ajax Space Control – keyfob;
- Ajax FireProtect / Ajax FireProtect Plus – wireless smoke / smoke+CO detectors;
- Ajax LeaksProtect – wireless flooding detector.

To register (bind) one Ajax wireless detector the following shall be done:
- Turn the wireless detector power switch **OFF** (located on the back of the wireless detector housing);
- Switch the Control Panel to the binding mode (see chapter 11.11);
- To register the detector, turn the detector power switch **ON**; registration process takes 3... 5 sec. For remote control, press the buttons ⭕ and ⏻ at the same time;
- Visually monitor the wireless detector registration.

> **Attention! When replacing radio receiver Ajax "uartBridge" (for example, because of its failure) is required to re-register all the wireless detectors in the new receiver (you should remove them in the ICD with the "F2" key previously).**

If you want to change the zone number for the already registered wireless detector, you must first remove its registration in the Ajax radio receiver and in the Control Panel, and then to register it in another zone. Searching detector to remove is recommended to focus on the previously applied to the wireless detector sticker/label with its zone number (you should apply this sticker/label on every new registration of each wireless detector). In other words, do not focus on the "detector ID" field value – it is not tied to a real wireless detector in the Control Panel!

After wireless detectors registration – during installation – it is recommended to check the level of the signal from each wireless detector – select "**Wireless Zone**" menu item at "Lind-11" ICD, then select wireless detector number and press «**F3**». After 3...120 seconds, the system turn on a signal strength indicator for the current wireless detector and then continuously measures the signal level and displays it by the wireless detector blinking LED:

- Lights permanently with very short off pulses (0.1...0.2 seconds) every 2 seconds – Level 3, **excellent**;
- Flashes quickly – Level 2, **good**;
- Periodically turn on for 1 second, then off for 1 second – level 1, **bad**;
- The rare short bursts (0.1...0.2 seconds) every 2 seconds – the level of 0, there is **no connection**.

During the signal level check, you can move the wireless detector from place to place, picking up his position to get a better connection.

Exit from this mode – after **10 minutes**, or by pressing the **#** key on ICD "Lind-11" keyboard.

You can check the detection area and change the sensitivity for **MotionProtect/Plus**, **GlassProtect** and **CombiProtect** wireless detectors – select "**Wireless Zone**" menu item at "Lind-11" ICD, then select wireless detector number and press «**F4**». After 3...120 seconds, wireless detector switches to detection area test mode for **10 minutes**, and the screen displays the current sensitivity value – **1** (**minimum**), **2** (**medium**) or **3** (**maximum**). You can change the sensitivity value by ICD numeric keys if necessary. If you change the sensitivity, the wireless detector switches to settings mode (to apply the new values), and then returns to the detection area test mode again. During the switching, the display shows the message "*Wait...*".

Other types of wireless detectors can not switch to detection area test mode.

Exit from the detection area test – by pressing the **#** key on your ICD keyboard.

All wireless detectors of this series sent tamper alarm as wireless detector housing opening and tamper restore as the wireless detector housing close.

The system supports of additional wire detectors for the wireless detectors, which provide such ability (for example, the main **DoorProtect** wireless detector). Wired detector must be assigned to a free wireless zone when configuring wireless zones (via "Configurator 11" software) and set the zone type, line type (normally closed or normally open) and the group number.

The additional wired zone is not displayed at "Lind-11" ICD while the wireless detectors be registering and any wireless detector can't register in them – it sets automatically when wireless detector is registering in the main radio zone.

> **Additional zone type can be selected from the list while configuring. Additional zone type can not be set as "Keyfob" or "24h Fire". If the main wireless zone isn't a "24-hour" type, then don't set the additional <u>wire-based</u> zone type as the "24-hour" too.**

The **CombiProtect** detector should be configured as 2 wireless zones – main (motion detector) and additional (glass breakage detector). The signals from these wireless zones are processed separately, depending on the settings in the Control Panel configuration. The additional wireless zone type for this wireless detector can be set **regardless** of the main wireless zone type.

27.8. Roiscok

The device can operate with the following Roiscok wireless detectors:
- iDo105 – wireless reed magnet contact detector;
- iDo302DW – wireless passive infrared motion detector with bottom protective zone;
- iDo303DRW – wireless digital electrooptical passive motion detector;
- RK2000W – wireless ceiling electrooptical passive motion detector.

To register (bind) one Roiscok wireless detector the following shall be done:
- Remove battery from the wireless detector;
- Set the wireless detector switch with "WriteCode" marking to "Closed" position;
- Install battery to wireless detector observing the polarity;
- Switch the Control Panel to the binding mode (see chapter 11.11);
- Press and release the tamper button of the wireless detector. In this case, the wireless detector transmits the registration signal;
- After dismounting of the power supply unit, set the wireless detector switch with "WriteCode" marking to "Open" position;
- Visually monitor the wireless detector registration.