


**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.9) Wireless Communication Link Control Panel**

### **Operating Manual**

	Product Compatibility Table		
	Control Panel	Lun-11	Version mod.9
	Detectors	Two- wire or four-wire connection circuit	Version
	Control Panel Configuration Software	Configurator 11	Version
	Central Monitoring Station	Orlan	Version

# Contents

1. Purpose.....	4
2. Safety Precautions.....	5
3. Technical characteristics.....	5
4. Detectors selecting.....	7
5. Device appearance and functions of its terminals.....	7
6. Control Panel features.....	10
6.1. Operating mode selecting.....	10
6.1.1. Orlan CMS mode.....	10
6.1.2. Ritm CMS mode.....	11
6.1.3. Standalone Web mode.....	11
6.1.4. Standalone mode via SMS.....	11
6.1.5. Calling to owner.....	12
6.2. Message transmission and testing.....	12
6.3. Control panel zone types.....	14
6.4. Groups.....	15
6.5. Programmable outputs.....	16
6.6. External antenna.....	17
6.7. Control of fire detector false alarms.....	18
6.8. Arming.....	19
6.9. “Stay Home” mode.....	20
6.10. Disarming.....	20
6.11. Schedule.....	21
6.12. Arming confirmation by Siren.....	21
7. Connect to interface buses.....	21
7.1. Operation features for MON/RS-485 devices.....	22
7.2. TAN bus devices operation features.....	22
7.3. Zone expansion with “AM-11” address modules.....	23
8. LED indicators.....	24
9. Indication and control devices.....	25
9.1. “Lind-15”.....	25
9.2. “Lind-9M4”.....	26
9.3. “Lind-29”.....	27
9.4. “Lind-11”, “Lind-11LED”.....	28
9.5. “Lind-11TM”.....	29
9.6. “Lind-EM”.....	30
9.7. Anti-vandal reader.....	30
10. “MPB-8M” relay output module.....	31
11. Wireless system.....	32
11.1. General information.....	32
11.2. Lun-R, Lun-R 868 radio receivers.....	33
11.3. R433 radio receiver.....	33

11.4. “L25_R433” radio receiver.....	34
11.5. “Lun RKI” rev.3.3 radio receiver.....	34
11.6. Crow radio receiver.....	34
11.7. Ajax radio receiver.....	35
11.8. Wireless devices binding.....	35
12. Additional communication channels.....	36
12.1. “LanCom rev.15” Ethernet-communicator.....	36
12.2. “LanCom23” Ethernet-communicator.....	36
12.3. “W11M” WiFi module.....	37
12.4. “TK-17” phone communicator.....	38
13. “Dozor” alarm photo-proof module.....	38
14. Control Panel configuring.....	39
15. Firmware update.....	39
16. Control Panel remote control.....	40
17. Battery monitoring.....	40
18. Main power supply monitoring.....	40
19. Maintenance.....	40
20. Operating conditions.....	40
21. Storage.....	40
22. Transportation.....	40
23. Disposal.....	40
24. Appendix 1. Control Panel zones types.....	41
25. Appendix 2. Control Panel connection diagram.....	44
26. Appendix 3. Wireless devices handling.....	50
26.1. Lun-R.....	50
26.2. Crow.....	51
26.2.1. SH-KP keypad.....	52
26.3. Rielta.....	54
26.4. Ajax “uartBridge” .....	56

# 1. Purpose

"Lun-11" mod.9 Control Panel (further called as "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. It transmits announcements to the "Orlan" or "Ritm" central monitoring station (further called as "CMS") or works 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.

CP uses 4G/GSM cellular networks for transmitting events and receiving commands.

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" – multifunctional LCD keypad;
- "Lind-11TM" – TouchMemory key (DS1990A-F5) reader;
- "Lind-11LED" – multifunctional LED-keypad;
- "Lind-15", "Lind-29" – multifunctional keypads with touch control;
- "Lind-9M4" – multifunctional keypad;
- "Lind-EM" – RFID-card reader.
- Any third party TouchMemory Anti-vandal Key Reader for 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" (adds 10 alarm zones, mounted inside a Control Panel housing);
- "Lun-11H" (adds 10 alarm zones, 2 PGM outputs and 1 BELL output, can be completed with the network supply unit);
- "LanCom rev.15" or "LanCom23" Ethernet-communicators;
- "W11M" WiFi 802.11b/g/n (2.4GHz band) communicator;
- "TK-17" wired phone line communicator;
- "MPB-8M" relay outputs module – 8 configurable isolated relay outputs;
- "AM-11" address module (allows for connection of up to 31 devices to TAN interface bus, each modules adds 3 alarm zones);
- "Dozor" Alarm Photo-proof Module (make photo of the configured events from up to four analog cameras);
- "Lun-R" or "Lun-R 868" Radio Receiver for "ORTUS Group" wireless detectors/keyfobs;
- "Crow-Lun-11 Adapter" Radio Module for "Crow"® wireless detectors/keyfobs;
- "P433" or "Lun RKL v.3.3" Radio Receiver for Rielta® wireless detectors/keyfobs;
- "uartBridge" Radio Receiver for "Ajax"® wireless detectors/keyfobs.

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

**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 wired zones (with expansion modules)	144
Maximum number of groups (partitions)	16
Maximum number of NC detectors in the zone	32
Maximum current in the fire zone for "normal" state, mA (for circuit with NO detectors)	8
Number of the controlled outputs (PGM)	4
Total number of "Lun-11E" and/or "Lun-11H" expansion modules connected	12
Total number of "Lind-11"/"Lind-11LED"/"Lind-15"/"Lind-29"/"Lind-9M4" ICD connected	16
Total number of "Lind-11TM" ICD connected	24
Total number of bound wireless zones/sirens/outputs *	48/16/16
Number of "AM-11" address modules connected	31
Number of "Lind-EM" EM-Marine standard RFID tags Readers	14
Maximum number of users (freely appointed by groups)	512
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 for S12 output, A, max	0,5
Output current for 12F1 output, A, max	1
Output current for 12F2 output, A, max	1
Output current for Bell output, 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
Total current for 12F1, 12F2, S12, Bell outputs including consumption of Control Panel board, A, max	1.2

Resistance of wired zone end-of-line resistor (see Section 24.), kOhm	2±5%
AC mains power voltage, V	100...242
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 S12 (active state), V	10...14.0
Bell output commutation voltage, V, max	18.0
Outputs ripple, mV, max	300
Battery and charger fault detection time, max, sec	300
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
Non-volatile event queue size	128
ATS category (EN 50136-1:2014)	SP5
Security grade (EN 50131-1:2014)	Grade 2
ATS performance criteria for 4G/GPRS communication channel (ATS/D/M/T/S/I)	ATS5/D4/M4/T6/S2/I3
Housing dimensions, W*H*D, mm	300*240*91
Dimensions when packed, W*H*D, mm	325*255*100
Device weight, net/gross, kg, max	1.5 / 1.7

\* – The actual total number of bound wireless devices (and by its types) is limited by the capacity of the wireless system and may be less than the table shows – 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	<b>160 mA</b>
Absorbed current of the armed "Lind-11", max	<b>30 mA</b>
detectors current	<b>~10 mA</b>

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.

Table 2. Frequencies and emitted power

Communication Mode	Band	Emitted power
GSM	900MHz	up to 2W (EGSM900) up to 0.5W (EGSM900 8-PSK)
	1800MHz	up to 1W (DCS1800) up to 0.4W (DCS1800 8-PSK)
WCDMA	850/900/2100 MHz	up to 0.25W
LTE-FDD	B1/B3/B5/B7/B8/B20/B28	up to 0.2W
LTE-TDD	B38/B40/B41	

## 4. Detectors selecting

Control Panel allows the connection to both the burglar alarm and fire zones of any detectors with **normally opened** or **normally closed** contacts with the **two-wire 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 24..

## 5. Device appearance and functions of its terminals

Layout of Control Panel components in the housing is shown in Figure 1.

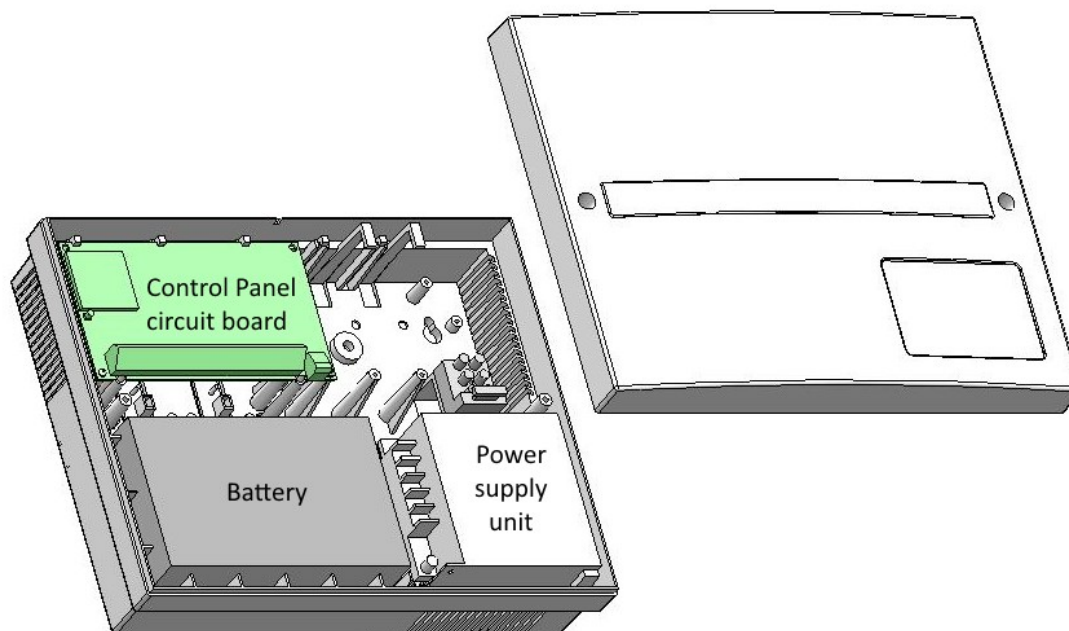


Figure 1. Control Panel components in its housing (upper cover open)

The housing overall dimensions are shown 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 housing orientation is shown 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 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](http://www.lun.ortus.io) site.

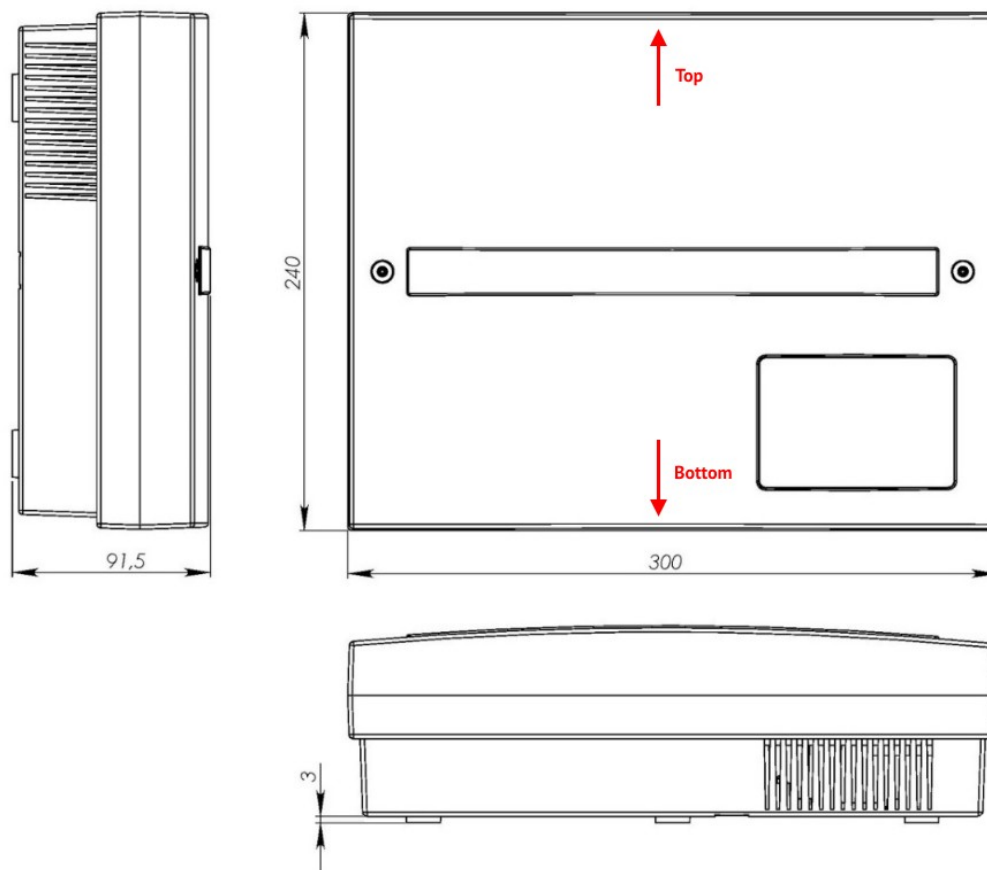


Figure 2. Control Panel housing overall dimensions

*Back side; dimensions - mm*

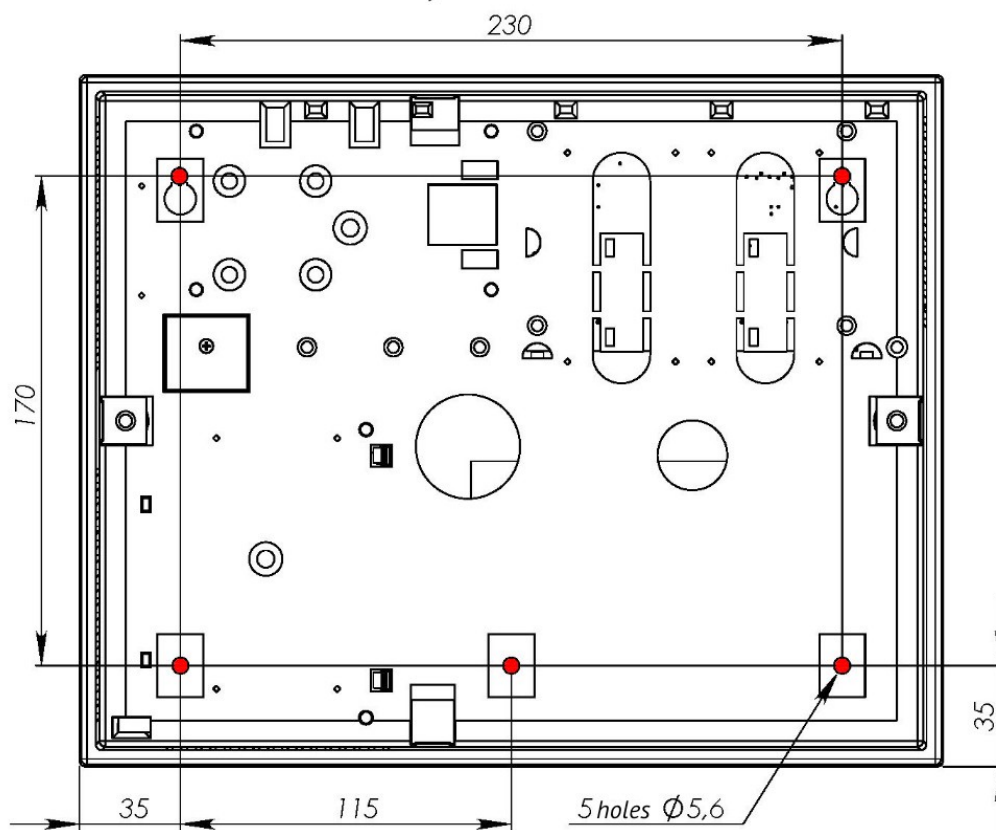


Figure 3. Control Panel housing mounting dimensions

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



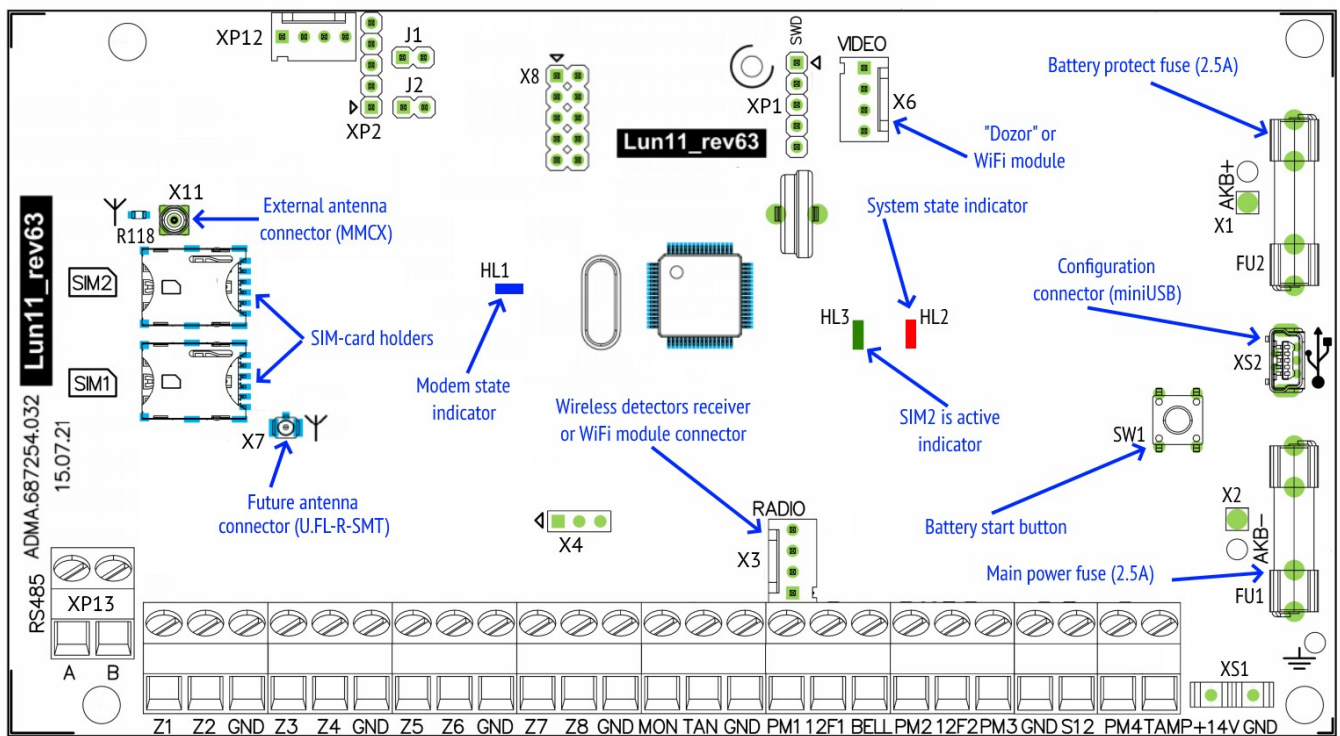


Figure 4. Control Panel circuit board appearance

Control Panel circuit board contains the following terminals (Table 3):

Table 3. Control Panel terminals functions

Terminal marking	Function
<b>RS485 A/B</b>	Non-inverting line <b>A</b> and inverting line <b>B</b> of the RS-485 interface for connecting "Lun-11E/11H", "Lind-9M4", "MON-485"
<b>Z1...Z8*</b>	Connection of zones 1...8
<b>GND</b>	Common terminal (-) of Control Panel
<b>MON</b>	Interface for the connection of "Lind-11/11LED/9M4/15/29", "Lun-11E/11H", "MPB-8M", "TK-17"
<b>TAN</b>	Interface for the connection of "Lind-11TM", "Lind-EM", "AM-11" or TouchMemory anti-vandal electronic key reader
<b>GND</b>	Common terminal (-) of Control Panel
<b>PGM1**...PGM4**</b>	Programmable outputs 1...4 (-) of "Open collector" type
<b>12F1</b>	Output for power-up (+) of "Lind" ICDs and siren (short-circuit current is limited)
<b>BELL</b>	Contact (-) of siren (short-circuit current is limited)
<b>12F2</b>	Output of power-up (+) of active detectors (short-circuit current is limited)
<b>GND</b>	Common terminal (-) of Control Panel
<b>S12</b>	Remote controlled (with CMS and keypad) power-up output (+) of active detectors (short-circuit current is limited)
<b>TAMP</b>	Input for wiring of housing opening tamper and housing shifting tamper
<b>+14V</b>	Power-up input (+) of Control Panel
<b>GND</b>	Common terminal (-) of Control Panel

\* – Detectors connecting depends on the type of zone, which is selected in the "Configurator 11" software (see section 24.).

\*\* – PGM1...PGM4 function shall be set with "Configurator 11" software. Maximum sink current is 0.5A (maximum voltage is 15V).

To connect alarm zones, a straight-through cable, e.g. ALARM 6x0.22, can be used.  
Fire or burglar alarm zones wiring is described in section 24..

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.

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

Built-in software supports multiple data algorithms, depending on the communication channels used. You can choose: the number of mobile operators (1 or 2), transmission channels (4G/GPRS, Ethernet/WiFi, switched telephone communication).

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

Control Panel support the remote control via 4G/GPRS and Ethernet/Wifi. CMS software automatically determines the list of available commands depending on the communication channel used.

### 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.

**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](http://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](http://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](http://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):

**“Low SIM balance = 19.75”**

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.

### 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.

**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.

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).

The screenshot displays the 'Communication channels and priorities setting' window. On the left, a sidebar lists various system components, with 'CMS' currently selected. The main configuration area is divided into several sections:

- Mode:** Set to 'Phoenix - CMS'. A 'Read IMEI' button is present.
- The transmission number:** Set to '111111'.
- Checkboxes:**
  - ☒ Keep connection (with Phoenix HD)
  - ☒ Don't use Voice channel for control panel tied to CMS (Note: It is used only at the moment of binding to the CMS)
- SIM cards configuration:**
  - SIM1:**
    - Period of sending a test by GPRS: 5 minutes
    - Period of test sending by voice: 120 minutes
    - ☐ Use alternative testing algorithm
    - Period of test for Inactive SIM: 1439
    - Timeout to return to the main Sim: 1
    - Rules for channels sequencing: G1V1G2V2
    - ☐ Return to main SIM automatically
  - SIM2:**
    - Period of sending a test by GPRS: 6 minutes
    - Period of test sending by voice: 120 minutes
- Alternative testing algorithm notes:**
  - For use of the alternative algorithm is needed:
  - 1. Turn on desired channels on BOTH SIM-cards
  - 2. Turn off ALL OTHER channels
  - Wherein SIM1-main, SIM2-reserve
  - G1 - GPRS channel SIM1, V1 - voice/CSD channel SIM1
  - G2 - GPRS channel SIM2, V2 - voice/CSD channel SIM2
- Other parameters:**
  - Period of test for Lan/WiFi: 1 minutes
  - SMS mode testing period: 0 minutes (0 - Testing off)
  - SMS lower balance limit: 1
  - Automatic redial:**
    - Period for sending of test: 1439 minutes
    - The delay of the first test: 480 minutes
  - Channels priority:**
    - 1. SIM card #1
    - 2. (Empty dropdown)
    - 3. (Empty dropdown)
    - 4. (Empty dropdown)

Figure 5. Communication channels and priorities setting

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).

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 4):

Table 4. Available zone types

Zone type	Description
<b>“Delayed”</b>	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.
<b>“Interior delayed”</b>	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.
<b>“Instant”</b>	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.
<b>“24hour”</b>	Type of zone, which is always activated regardless of the Control Panel status (whether it is armed or not). For example, the alarm button.
<b>“Arming”</b>	Type of zone, violation of which disarms the group and recovery arms it.
<b>“24h Fire”</b>	Type of zone to operate with smoke detectors according to 2 or 4 connection circuit.
<b>“Arm Stay”</b>	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 an alarm of the Control Panel (e.g., glass brake will lead to the transmission of an alarm signal to CMS) – more see Chapter 6.9. The Stay-Home Mode can be activate if the following zones types presence in the CP configuration: 1. “Arm Stay”; 2. “Delayed” or “Delayed/Instant”.
<b>“General Alarm”</b>	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.
<b>“Delayed/Instant”</b>	Type of zone identical to “Delayed” zone in the Armed Mode and to “Instant” zone in the Stay-Home Mode.
<b>“Interior delayed/Instant”</b>	Type of zone identical to “Interior delayed” zone in the Armed Mode and to “Instant” zone in the Stay-Home Mode
<b>“Arming by pulse”</b>	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 (partitions). It 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 “Grif” 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. External antenna

Control Panel has a built-in antenna, so prior to installation it is necessary to check the 4G/GSM 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 4G/GSM signal strength is pure, you can use an external antenna. To do this:

- Cut the **R118** resistor 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.

**Note:** Connector X7 is currently unused and intended for future expansion.

If you need to install several Control Panels with 4G/GSM 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**

**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 start.

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-29/15/11LED/11/9M4" ICD is used then it displays zone violation by its ZONE LEDs. If the number of violated zone is 9 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-29/15/11LED/11/9M4" 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. "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-15/9M4"** 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.

## 6.10. 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-29/15/11LED/11/9M4") is used to disarm, then the group disarming and the panic event is transmitted to CMS simultaneously.**

## 6.11. 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 communication channels.

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

## 6.12. Arming confirmation by Siren

The Control Panel can confirm of the arming by a short siren beep (about 0.5 seconds long). This is valid for the arming from the wireless keyfobs and for the "Arming" zone types and can be enabled in the CP configuration.

## 7. Connect to interface buses

The peripheral equipment of the security system is connected to the CP board using TAN, MON, RS-485 interface buses. TAN bus can be used independently of the other buses. The remaining buses are mutually exclusive – only one of them can be used – MON or RS-485. The type of bus used is indicated in the CP configuration.

To connect any devices to MON, RS-485 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 connected 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).

Connection diagram to wired the network devices to the MON bus is shown in Figure 36.

The RS-485 bus must be built according to the "Common Bus" scheme with a sequential bypass of all devices. In the terminals of the physically the most remote devices on the bus, terminal resistors 100 Ohm resistance must be installed.

The maximum total RS-485 bus length between all system modules should not exceed 1000m.

An example of connecting network devices to the RS-485 bus is shown in Figure 37.

## 7.1. Operation features for MON/RS-485 devices

Depending on the buses used in the CP (the bus type is selected in the CP configuration), it is possible to connect the following peripheral equipment:

Table 5. Hardware Compatibility for MON and RS-485 buses

Connecting to MON bus		Connecting to RS-485 bus	
By "MON-485" module	Directly	Directly	By "MON-485" module
Lun-11E rev.8	Lun-11E rev.1...7	Lun-11E rev.8	Lun-11E rev.1...7
Lun-11H rev.8	Lun-11H rev.1...7	Lun-11H rev.8	Lun-11H rev.1...7
×	Lind-9M4		×
×	Lind-9M4		×
×	Lind-11	×	Lind-11
×	Lind-11LED	×	Lind-11LED
×	Lind-15	×	Lind-15
×	Lind-29	×	Lind-29
×	MPB-8M	×	MPB-8M
×	TK-17	×	TK-17
×	LanCom rev.15	×	LanCom rev.15
×	LanCom23	×	LanCom23

Thus, the compatibility of any peripheral devices of the system is provided by the MON-485 module. The number and location of MON-485 modules are selected based on the physical location and distances between the network devices of the security system. Power supplies (see Figure 37) must ensure uninterrupted operation of peripheral network devices, while the CP remains operational. Using MON-485 modules as a chain like MON-RS485-MON-RS485... or RS485-MON-RS485-MON... – **not allowed**.

Each device on the bus (regardless of the type of bus) must have a unique address (selected by the engineer when setting up the system). Exception – devices indicated in red, which already have predefined addresses.

## 7.2. TAN bus devices operation features

TAN bus is used 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.

Each device on the TAN bus must have a unique address (selected by the engineer when setting up the system). The only exception is the anti-vandal reader, which has no address.

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!

**Wiring of TM anti-vandal key reader with the configured "Lind-11TM"/"Lind-EM"/"AM-11" shall result in the immediate breakdown of any TouchMemory key when it touches the reader!**

### 7.3. Zone expansion with “AM-11” address modules

You can expand the number of the security system zones with either “Lun-11E”/“Lun-11H” expansion modules (with 10 zones each), or by “AM-11” compact address modules (Figure 6) with 3 additional zones. Line type for every zone is “normal-open” or “normal-closed”, zone type is any other than “24-fire”. An example of use of the modules is shown in Figure 35.

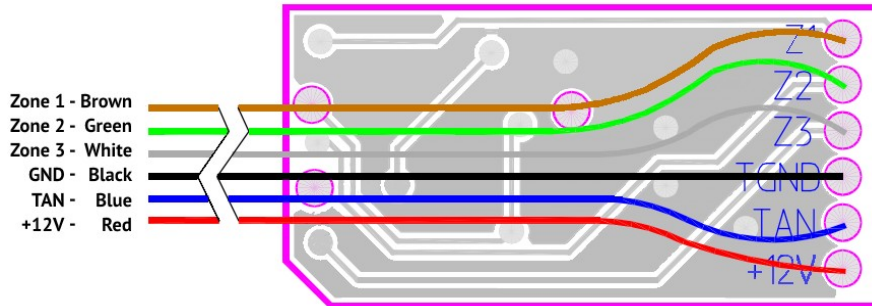


Figure 6. Appearance and functions of the hard-wired zone of “AM-11” address module

The total wired zones count in the security system 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 8) 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](http://www.ortus.io).

To connect “AM-11” modules to a computer in the configuration process, “Config-AM11” adapter is required (Figure 7).

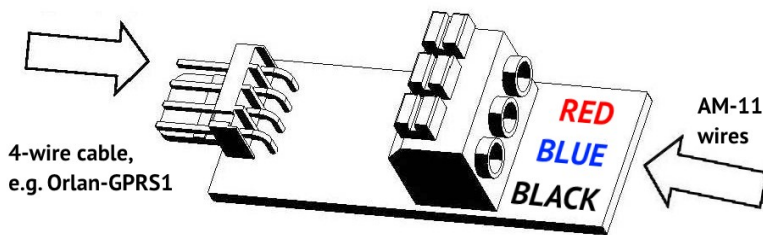


Figure 7. “Config-AM11” adapter appearance

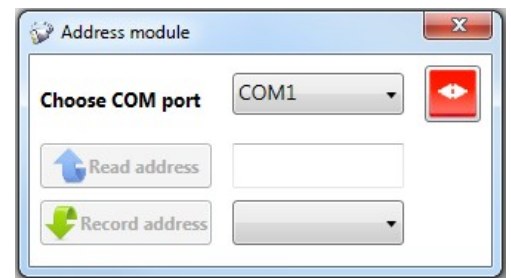


Figure 8. Configuring of “AM-11”

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).

## 8. LED indicators

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

**Red** – **system state indicator**;

**Blue** – **modem state indicator**;

**Green** – **SIM #2 is active** (displayed with continuous light).

**System state indicator (red LED)** operation modes:

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

**Modem state indicator (blue LED)** operation modes:

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



## 9. Indication and control devices

Control Panel allows for connection of the following indication and control devices:

- keypads “Lind-29”; “Lind-15”; “Lind-11LED”; “Lind-11”; “Lind-9M4”;
- TouchMemory key reader “Lind-11TM”;
- RFID card reader “Lind-EM”;
- Any third party TouchMemory anti-vandal key reader.

### 9.1. “Lind-15”



Figure 9. Appearance of the “Lind-15” ICD

“Lind-15” ICD is used to control and indicate the Control Panel’s status (Figure 9).

The ICD must be connected and used in strict accordance with its instruction manual. An example of connecting ICD is shown in Figure 24.

**“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](http://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-9M4”

ICD (16 zones red LEDs, Figure 10) is used to control the main functions of Control Panel and indication of its status.

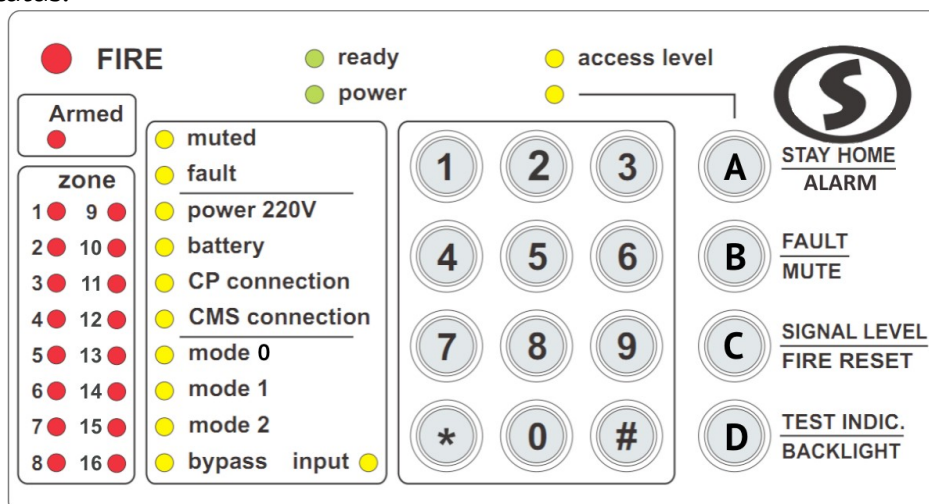


Figure 10. Appearance of “Lind-9M4” ICD

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. This should be considered when configuring the security system in the "Configurator 11" software.

### 9.3. “Lind-29”



Figure 11. Appearance of the "Lind-29" ICD

“Lind-29” ICD is used to control and indicate the Control Panel’s status (Figure 11).

ICD must be connected and used in strict accordance with its instruction manual. An example of connecting ICD is shown in Figure 38.

**“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](http://www.ortus.io). The selected address shall coincide with the address selected in “Configurator 11” software.**

Arming/disarming process and arming state indication is [relate](#) just for group, where the specific ICD is assigned to.

## 9.4. “Lind-11”, “Lind-11LED”

“Lind-11” ICD (Figure 12) and “Lind-11LED” ICD (Figure 13) are designed to manage of Control Panel and indicate its status.



Figure 12. “Lind-11” ICD with open cover



Figure 13. “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  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](http://www.ortus.io)).

## 9.5. “Lind-11TM”

“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 14, 15. 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](http://www.ortus.io)). An example of ICD connection is shown in Figure 34.



Figure 14. “Lind-11TM” ICD front view

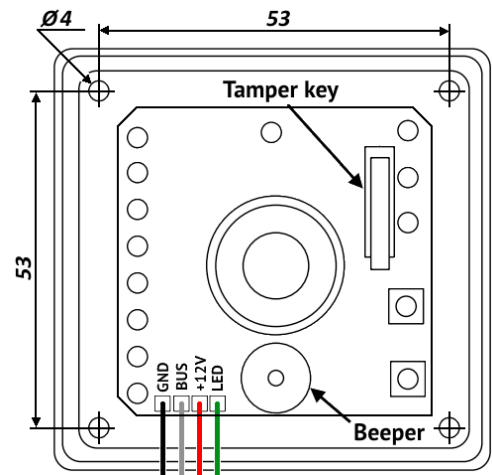


Figure 15. “Lind-11TM” ICD without cover

**“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.

## 9.6. “Lind-EM”

“Lind-EM” reader (Figure 16) 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.

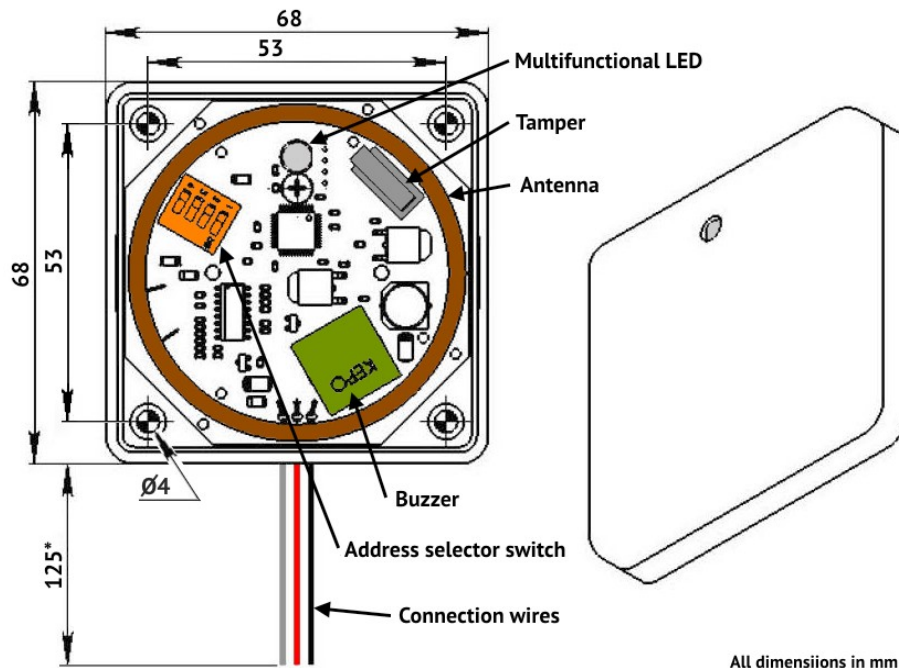


Figure 16. Appearance and arrangement of “Lind-EM” ICD

**“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](http://www.ortus.io)).

## 9.7. 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 7.1.. 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.

**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.**



## 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 17.

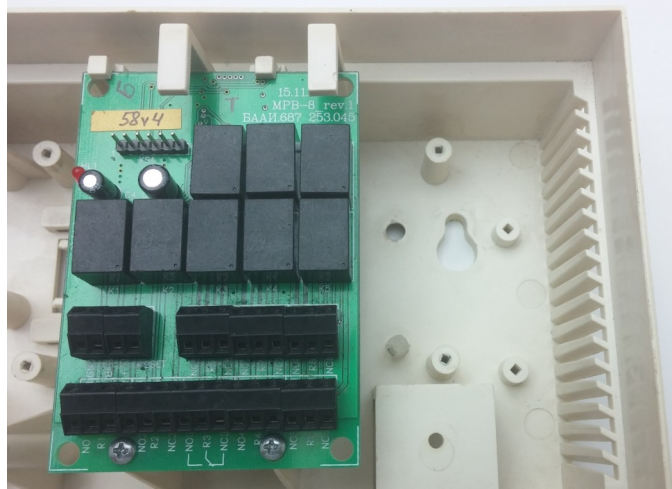


Figure 17. “MPB-8M” module in the housing

Only one “MPB-8M” module can be connected to the 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 relay output is set independently when configuring Control Panel using “Configurator 11” software. Supported functions are similar to the CP PGM outputs (see section 6.5.).

**Note.** The mechanical relays is used in the module and they have a limited triggering counts, so it is not recommended to assign functions with a large number of switches (for example, functions with “flashing”) at the module outputs.

# 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	Radio receiver required	Frequency range, MHz	Radio receiver manufacturer	Mounting method, Figure #
Ajax	“Ajax uartBridge” (with “Ajax RR108-Lun11 Adapter” cable)	868	“Ajax Systems Inc.”	Inside the housing, 24
Rielta	◆ “R433” / “L25_R433”	433	ORTUS Group	Inside the housing, 19
	◆ or “Lun RKI” rev.3.3			Inside the housing, 18
Crow	◆ “CROW-Lun-11” Adapter	868		Inside the housing, 20
	◆ or “L25_CROW” (rev3 or rev4) Adapter			Inside the housing, 21, 23
	◆ or “L25-CROW B” Adapter			Outside the housing
ORTUS	Lun-R	433		Inside the housing, 18
	Lun-R 868	868		

Radio receiver shall be installed in the device housing as shown in correspondent figures (Table 6) 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 shall be specified in the Control Panel configuration.

Finally, turning the Control Panel into operation mode (disconnect it from the computer) should to bind the wireless detectors/sirens/outputs by "Lind-11/9M4/15/29" ICD using the "engineer" access level.

All wireless devices used in the Control Panel shall be of the same product range of the same manufacturer and works in the same frequency range.

Supported wireless devices types for each radio system and their binding sequence written in section 26..



## 11.2. Lun-R, Lun-R 868 radio receivers

“**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 18, and connected with its own wire loop to the **X3 (RADIO)** connector on the control panel board.

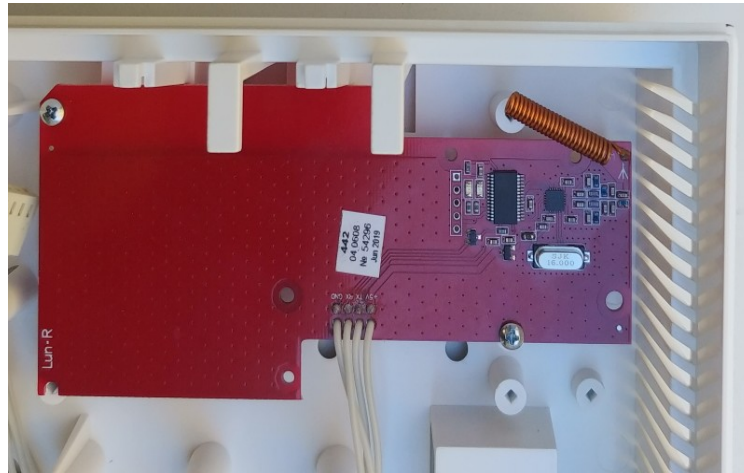


Figure 18. “Lun-R” radio receiver in the device housing

## 11.3. R433 radio receiver

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

Module is installed in housing under Control Panel, as shown in Figure 19 (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 module have two LEDs:

- “**Radio**” (**HL2**) - flashes in the process of radio exchanging with detectors;
- “**Alarm**” (**HL1**) - flashes in the case of any detector alarm.

Module has **XP2** connector is used to change the network of Rielta wireless system.

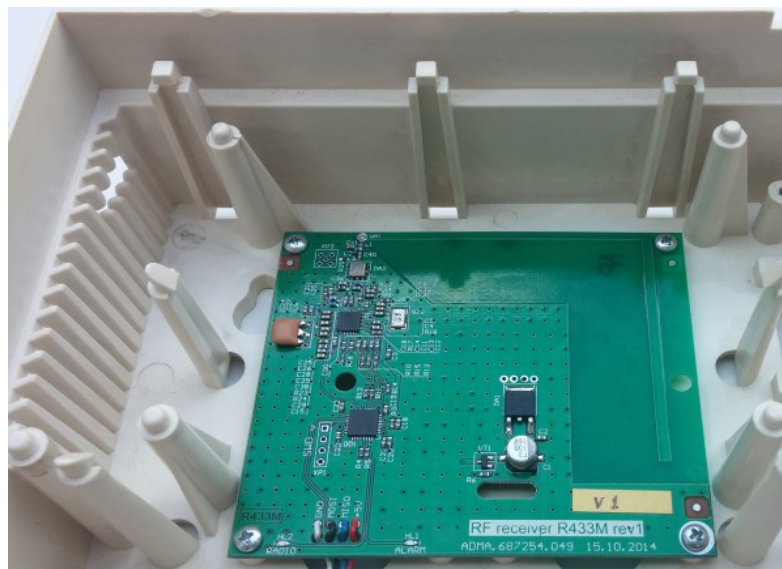


Figure 19. “R433” radio receiver in the device housing

## 11.4. “L25\_R433” radio receiver

This radio receiver may be used instead of R433 radio receiver (see section 11.3.).

This receiver should be installed in the free space of the device housing on a piece of 3M double-sided adhesive tape then it should be connected in the same way as described in section 11.3.

## 11.5. “Lun RKI” rev.3.3 radio receiver

Radio receiver is used to operate with wireless devices manufactured by Rielta. It should be installed in the Control Panel housing like as shown in Figure 18. This receiver should be connected by built-in cable to Control Panel **X3** connector.

## 11.6. Crow radio receiver

To provide the operation 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 20);
- “**L25\_CROW\_rev3**” Adapter – prepare a place for adapter (Figure 22) then install the adapter with double-sided tape (Figure 23);
- “**L25\_CROW\_rev4**” Adapter – should be installed into the device housing (Figure 21);
- “**L25-CROW B**” Adapter – should be installed outside the Control Panel 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 39. The cable free side can be cut off for best fitting.

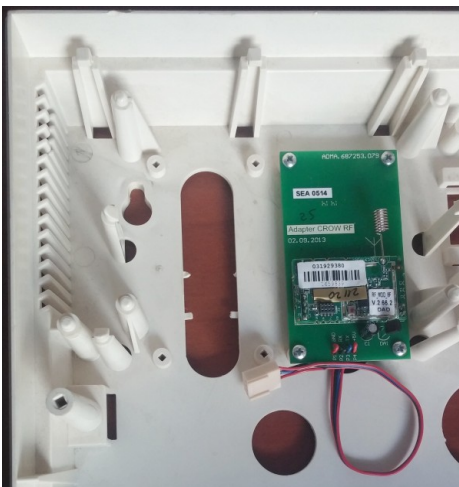


Figure 20. “Crow-Lun-11” adapter in the device housing

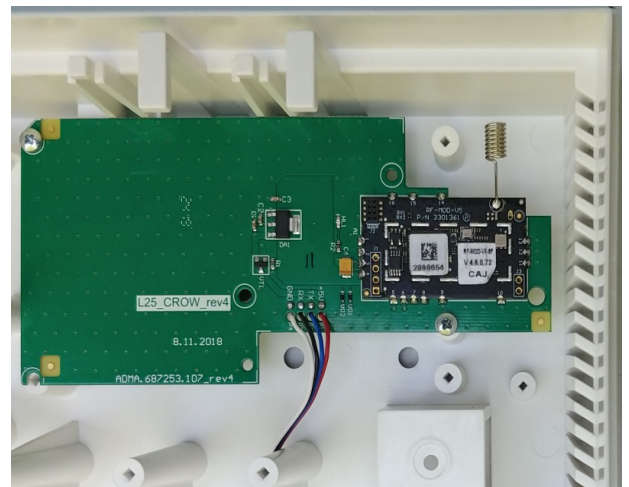


Figure 21. Adapter “L25\_Crow\_rev4” in the device housing

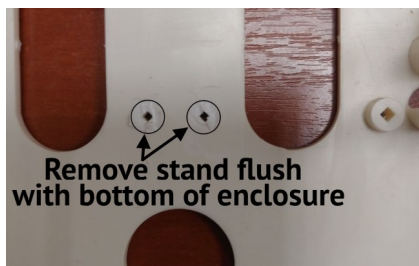


Figure 22. Preparing the device housing for the adapter "L25\_Crow\_rev3"

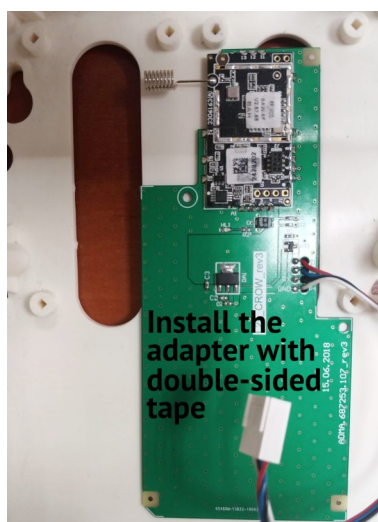


Figure 23. Adapter "L25\_Crow\_rev3" in the device housing



Figure 24. Ajax "uartBridge" radio receiver in the device housing

## 11.7. Ajax radio receiver

To provide the operation of Control Panel with Ajax wireless detectors, "Ajax uartBridge" radio receiver shall be installed in the housing as shown in Figure 24. Then, it shall be connected to **X3** Control Panel connector by "Ajax RR108-Lun11 Adapter" cable (manufactured by ORTUS Group).

## 11.8. Wireless devices binding

Prior to bind of wireless devices, you should select and save to the Control Panel configuration: the type of radio system, number and type of wireless zones.

To bind of wireless devices, the Control Panel must be turned on to working mode. The radio receiver that was configured previously should be installed and connected.

Prior to bind of wireless devices, the group (partition) to be changed shall be disarmed.

Binding of wireless **detectors** can be performed via "Lind-29/15/11/9M4" ICDs.

Binding of wireless **sirens** can be performed via "Lind-29/15/11/9M4" ICDs.

Binding of wireless **outputs** can be performed via "Lind-29/15/9M4" ICDs.

The process of registration of wireless devices depends on the type of ICD used and is described in the appropriate ICD operation manual. Operation manuals of each ICD are available at [www.p-sec.eu](http://www.p-sec.eu).

When installing wireless devices, be sure to evaluate the signal level from each of them (displayed by the Lind-29/15/11/9M4 ICD). If the signal level is too low (0...1), then radio communications with wireless devices can be interrupted, which will lead to loss of events and/or malfunctioning of wireless devices. To improve the signal level, try changing the mutual location of wireless devices and a radio receiver or use the appropriate repeater.

After binding or deletion of wireless devices, the Control Panel shall be automatically rebooted to apply the changes you made.

After binding wireless devices, they must be checked by the monitoring station commands or events that occur in violation/restore zones and displaying in ICD or by event codes that are sent to the monitoring station.

## 12. Additional communication channels

Control Panel allows for transmission of events to “Orlan” CMS via Ethernet using “**LanCom rev.15**” or “**LanCom23**” Ethernet communicators, or via WiFi by “**W11M**” module or via wired phone line using “**TK-17**” phone communicator.



Figure 25. “LanCom rev.15” communicator in the device housing



Figure 26. “LanCom23” communicator

### 12.1. “LanCom rev.15” Ethernet-communicator

To use the communicator with the Control Panel the following shall be done:

1. Switch the communicator to the “**Lun-11**” mode (using built-in Web-configurator on page “**Control Panel type**”);
2. Place the communicator into the housing (Figure 25) and connect it with the Control Panel board according to the schematic diagram in Figure 36;
3. Enable and configure the communication parameters and channels priority in the Control Panel configuration.

More see in “LanCom rev.15 Operating Manual” available at [www.ortus.io](http://www.ortus.io).

### 12.2. “LanCom23” Ethernet-communicator

To use the communicator with the Control Panel the following shall be done:

1. Switch the communicator to the “**Lun-11**” mode (using “Configurator” software, “**Connected to Lun-11**” option shall be selected);
2. Place the communicator into the housing (Figure 26) and connect with the Control Panel board according to the diagram in Figure 36;
3. Enable and configure the communication parameters and channels priority in the Control Panel configuration.

The detailed description of the communicator can be found in “LanCom23 Operating Manual” available at [www.ortus.io](http://www.ortus.io).



### 12.3. “W11M” WiFi module

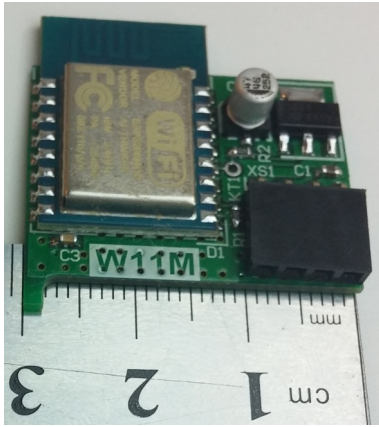


Figure 27. “W11M” module

Communication through WiFi channel provides an additional module “W11M”.

Module “W11M” (see. Figure 27) 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.

**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 28) or **X6** (“Dozor” module connector – see Figure 29) is used to install the WiFi “W11M” module.

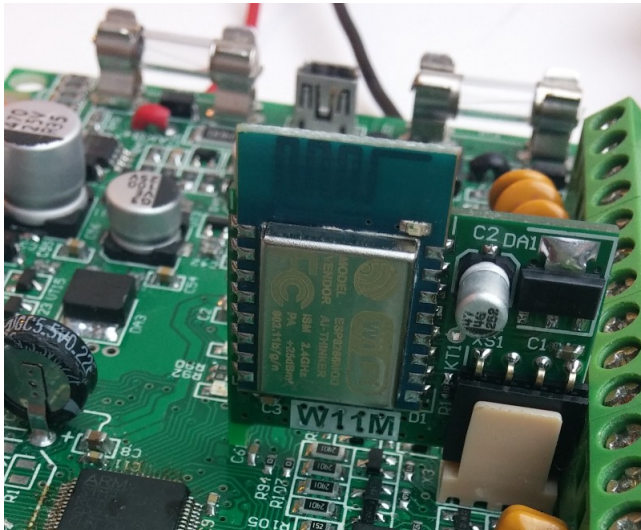


Figure 28. Installing “W11M” to X3 connector

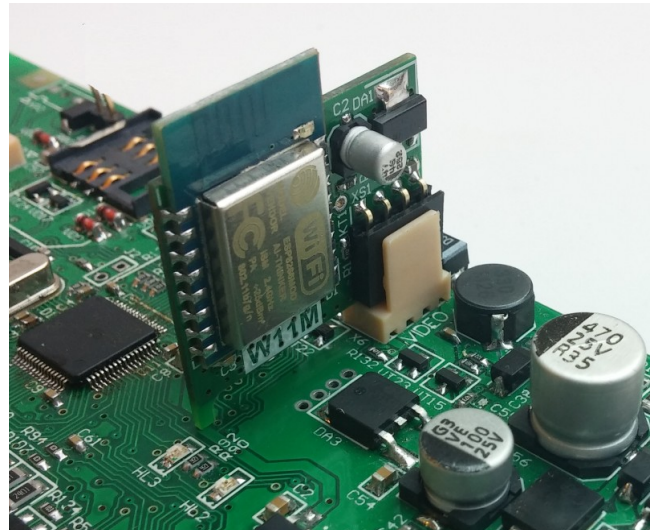


Figure 29. Installing “W11M” to X6 connector

So can not be used or any 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](http://www.ortus.io) website).

**“W11M” module installs to X3 connector (instead of radio receiver) or to the X6 connector (instead of “Dozor” module). You should select a correct install location in advance and then save the configuration to the Control Panel!**

## 12.4. “TK-17” phone communicator

To use the communicator with the Control Panel the following shall be done:

1. Switch the communicator to the “**Lun-11**” mode (using “Configurator” software, “**Connected to Lun-11**” option shall be selected);
2. Place the communicator into the housing (Figure 30) and connect with the Control Panel board according to the diagram in “TK-17 phone communicator. Installation Guide” available at [www.ortus.io](http://www.ortus.io);
3. Connect the wires to the telephone line and telephone (if required);
4. 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 “TK-17” phone communicator can be found in “TK-17 phone communicator. Installation Guide” available at [www.ortus.io](http://www.ortus.io).

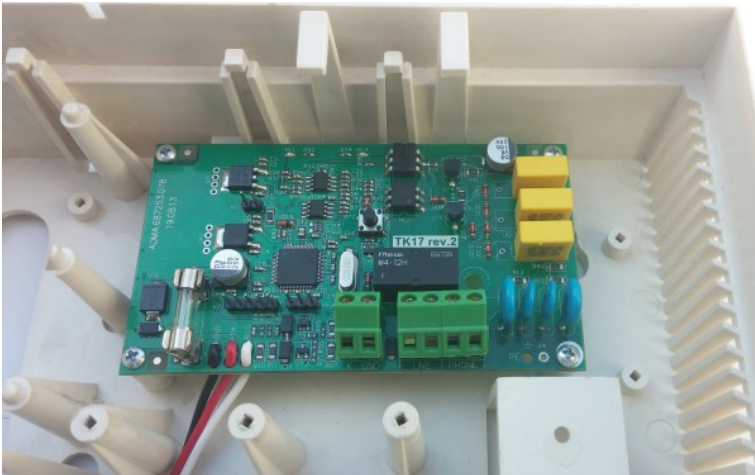


Figure 30. “TK-17” communicator installation

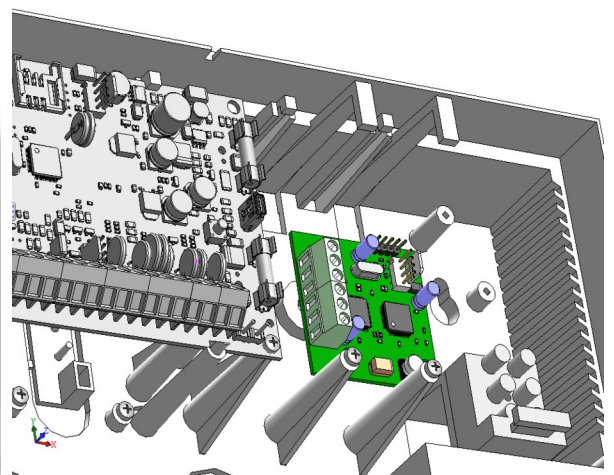


Figure 31. Installation of “Dozor” module

## 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 are transmitted via 4G/GPRS/WiFi channels to “Orlan” CMS.

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 31. To connect it to the Control Panel board (to **X6** connector), the supplied cable shall be used. The connection diagram is given in section 25..

## 14. Control Panel configuring

**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](http://www.ortus.io).

"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 4G/GPRS/WiFi 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.

## 15. 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 14.), or remotely (performed via 4G/GPRS/Ethernet/WiFi connection; main power and battery power are required).

"Configurator 11" software commands are used for local updating. Remote update is performed by "Phoenix" 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.**

## 16. Control Panel remote control

The remote control is available from CMS using “Phoenix” software.

Control Panel supports remote control via mobile applications “Phoenix-MK”. It is available for devices on Android OS and iOS.

## 17. 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.

The battery can be replaced as described in section 5..

## 18. 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 wait for 10s before turns it on!

## 19. Maintenance

The Control Panel does not require any maintenance.

## 20. Operating conditions

The Control Panel shall be used in the environmental class I (Indoor) (EN 50131-1:2014) at the temperature of +5°C to +40°C with average relative humidity of 75% non-condensing.

## 21. Storage

1. Storage temperature shall be of -50°C to +40°C at the relative humidity of 5% 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.

## 22. 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% to 98%.

## 23. 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.

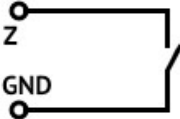
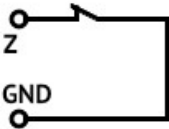
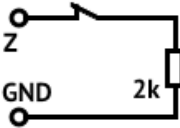
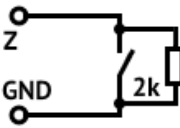
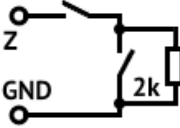


## 24. Appendix 1. Control Panel zones types

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”.

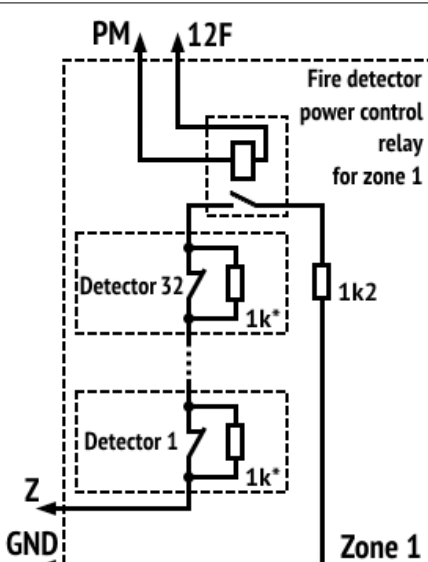
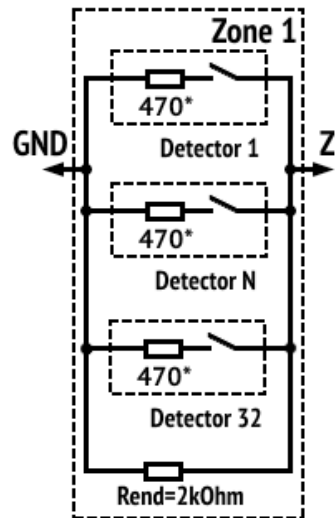
See the types of protective zones and events generated in case of their violation, in Table 9.

Table 9. Protective zones types

Connection circuit	Short circuit-generated event	Disconnection-generated event
<b>1. Zone type – “Normally open”</b>		
	alarm	norm
<b>2. Zone type – “Normally closed”</b>		
	norm	alarm
<b>3. Zone type – “Termination resistor, alarm upon disconnection”</b>		
	zone fault	alarm
<b>4. Zone type – “Termination resistor, alarm upon short circuit”</b>		
	alarm	zone fault
<b>5. Zone type – “Termination resistor, alarm upon disconnection and short circuit”</b>		
	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”		
<div><p>* – To recognize second detector in the zone, the resistance of the additional resistor for each detector should be <b>1 kOhm</b></p></div>	zone fault	zone fault
detector circuit break – alarm		
7. Zone type – “Normally open, 2 resistors”		
<div><p>* – To recognize second detector in the zone, the resistance of the additional resistor for each detector should be <b>820 Ohm</b></p></div>	zone fault	zone fault
closing of detector circuit – alarm		

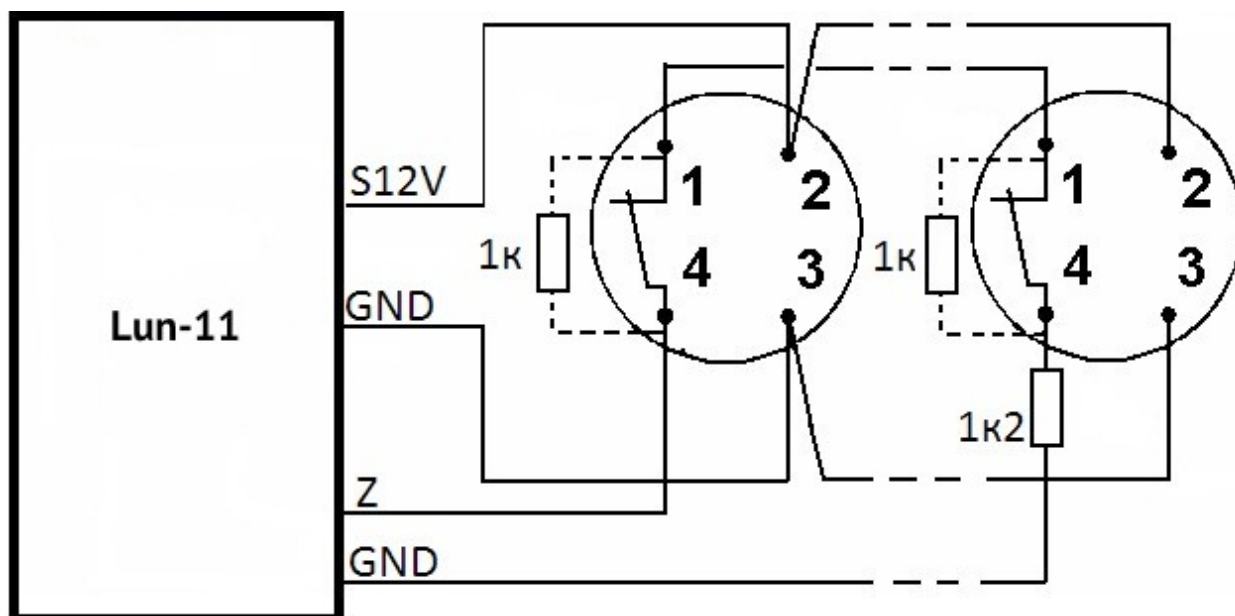


Figure 32. Fire detector connection diagram according to four-wire circuit

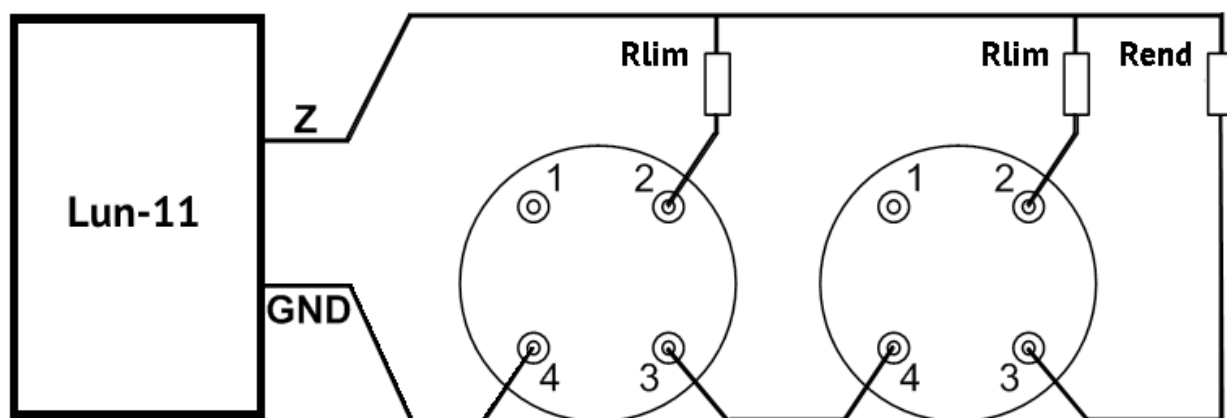


Figure 33. Diagram of connection of detectors to fire zone according to two-wire circuit

Table 11. An example of Rlim calculation

Detector type	Rlim nominal value
IPK-8	200 Ohm
SPD-3	470 Ohm
Any other detector	<p>Rlim is calculated by the formula:</p> <p><b><math>R_{lim}=800 \text{ Ohm} - R_{det}</math></b>, (to recognize the response of <b>one</b> detector in the loop)</p> <p>or</p> <p><b><math>R_{lim}=1150 \text{ Ohm} - R_{det}</math></b>, (to recognize the response of <b>two</b> detectors in the loop)</p> <p><b>Rdet</b> is the detector resistance in the "Fire" state, Ohm</p>

## 25. Appendix 2. Control Panel connection diagram

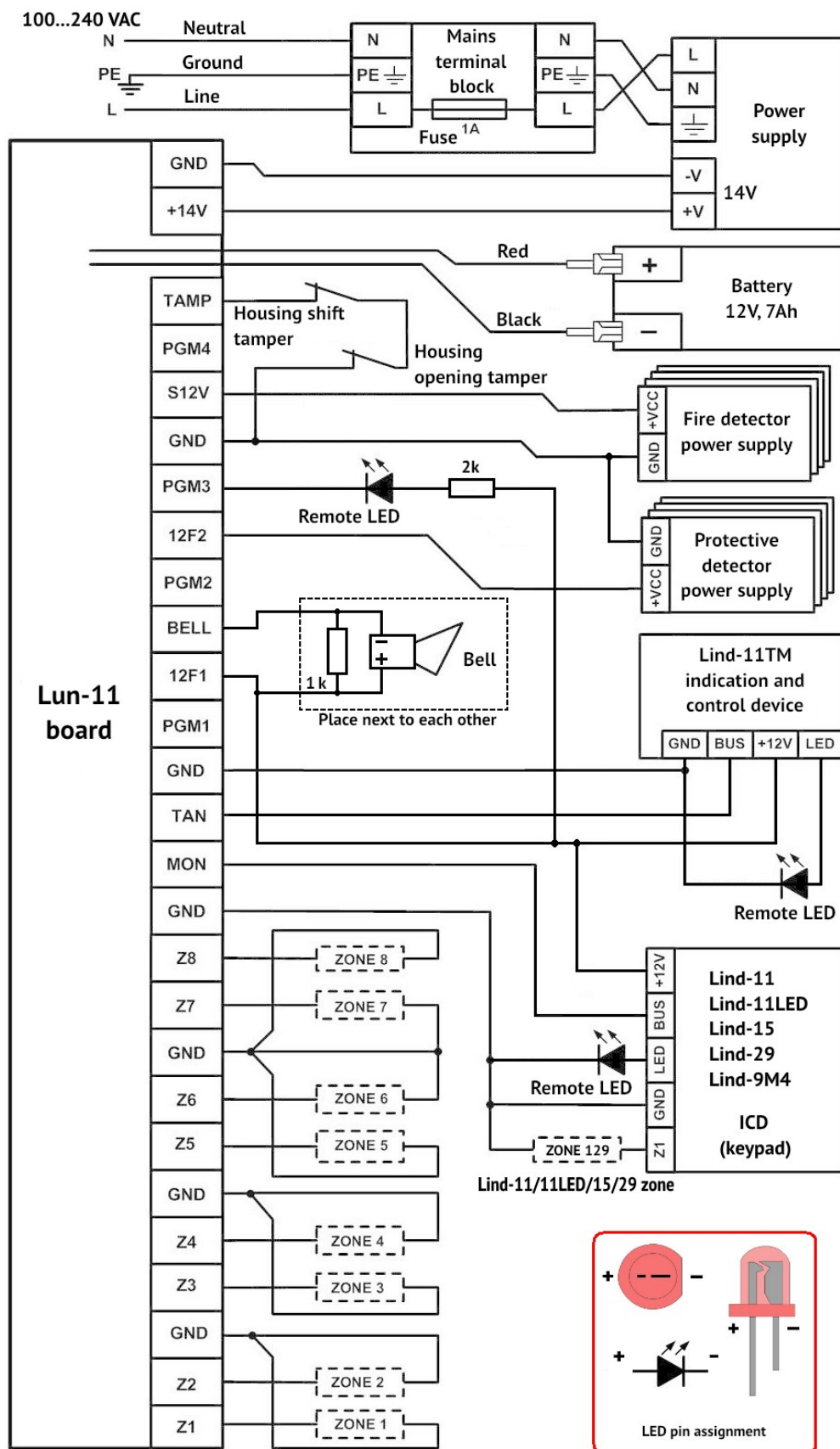


Figure 34. Control Panel connection diagram

**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.

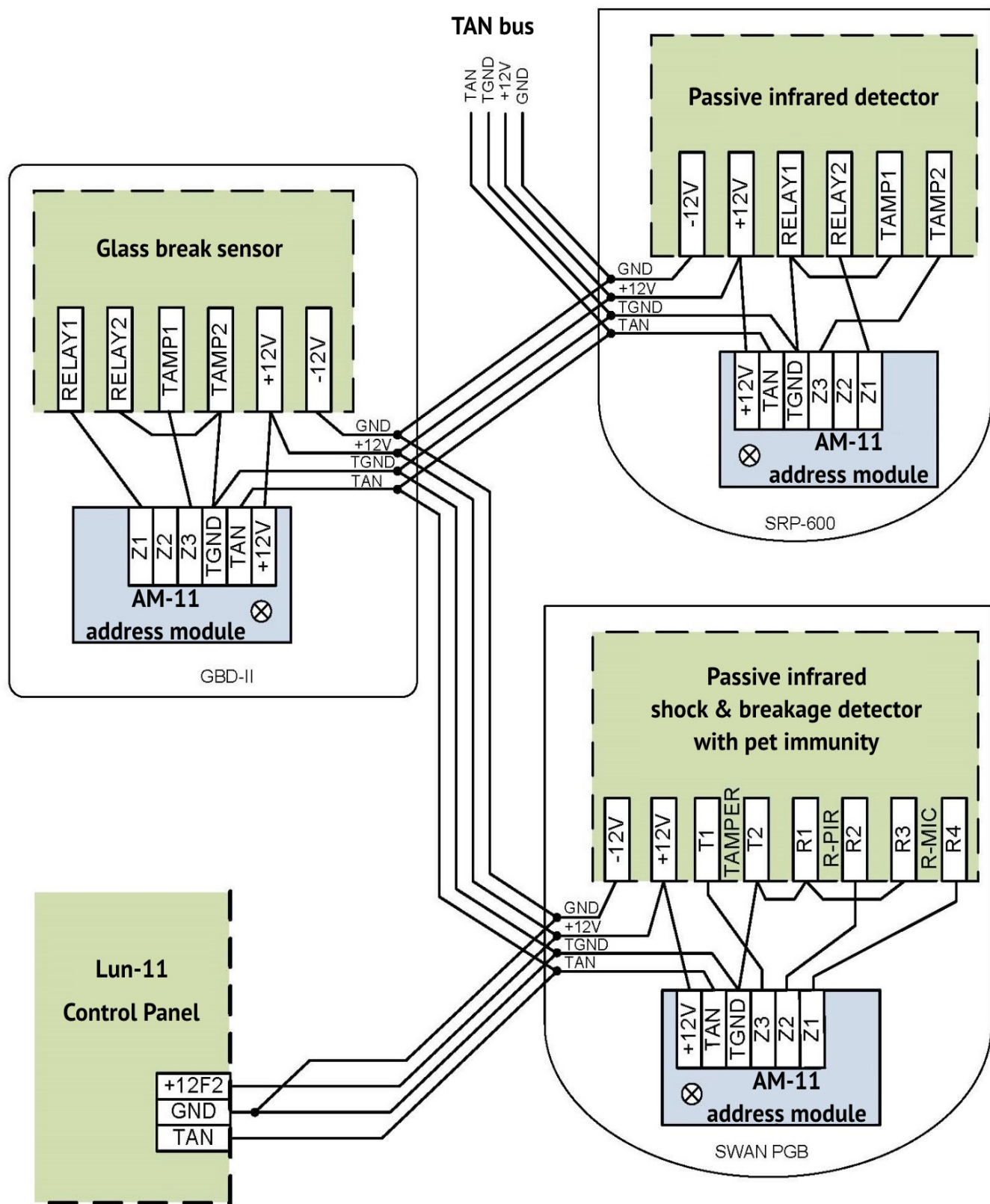


Figure 35. An example of use of “AM-11” address modules

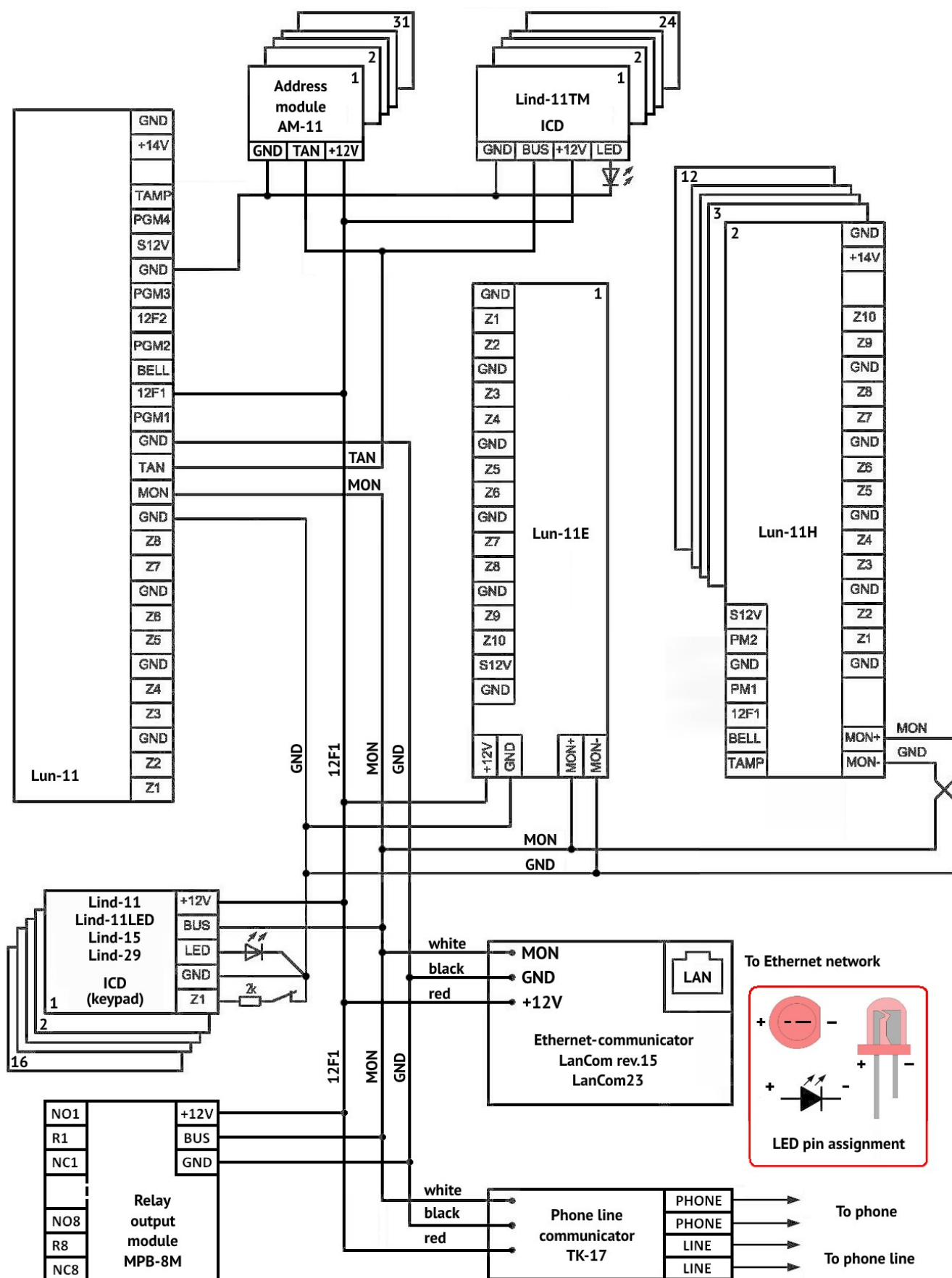


Figure 36. Network device connection to MON/TAN interface buses

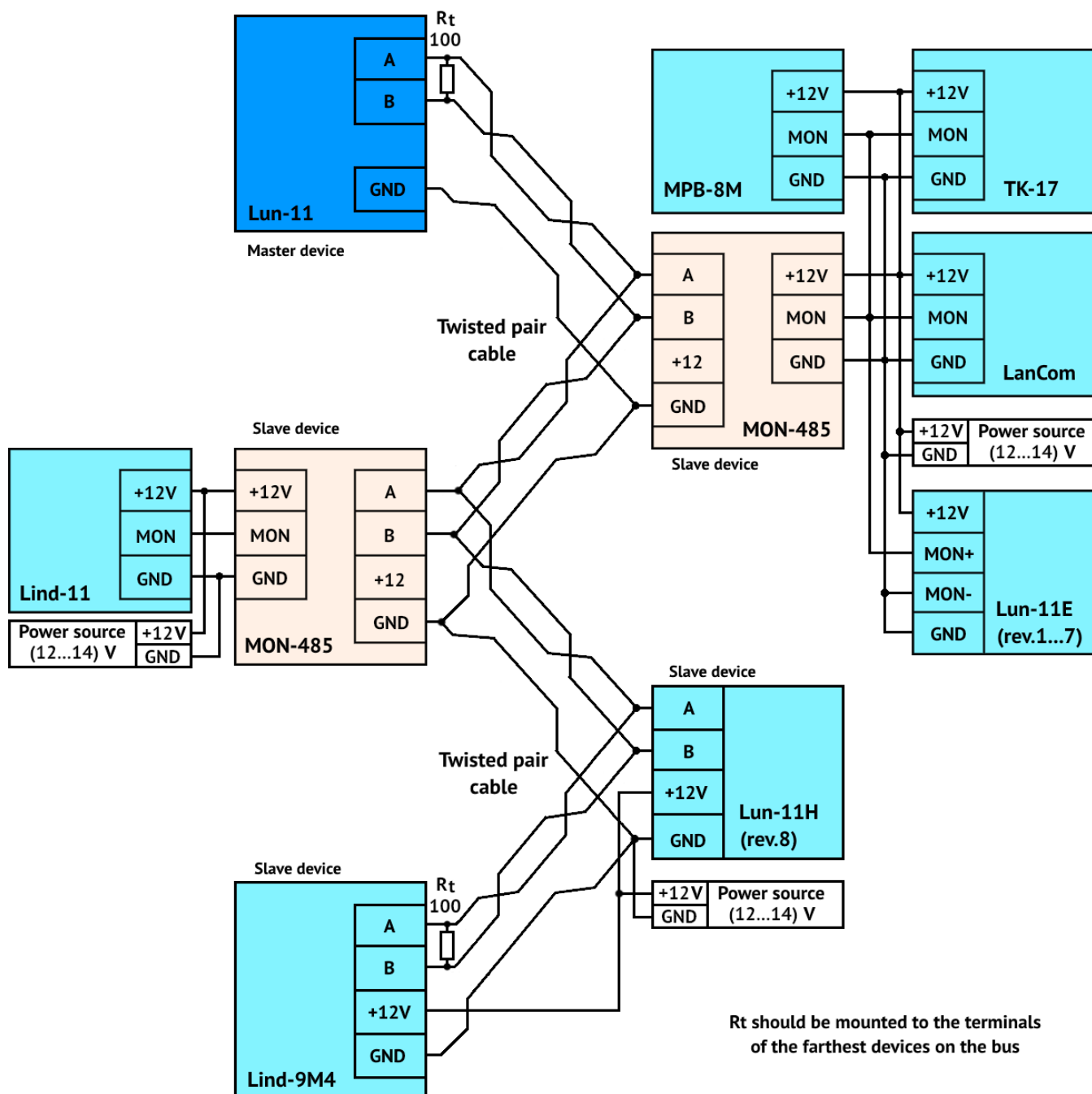


Figure 37. Network devices connection to the RS-485 interface bus (Example)

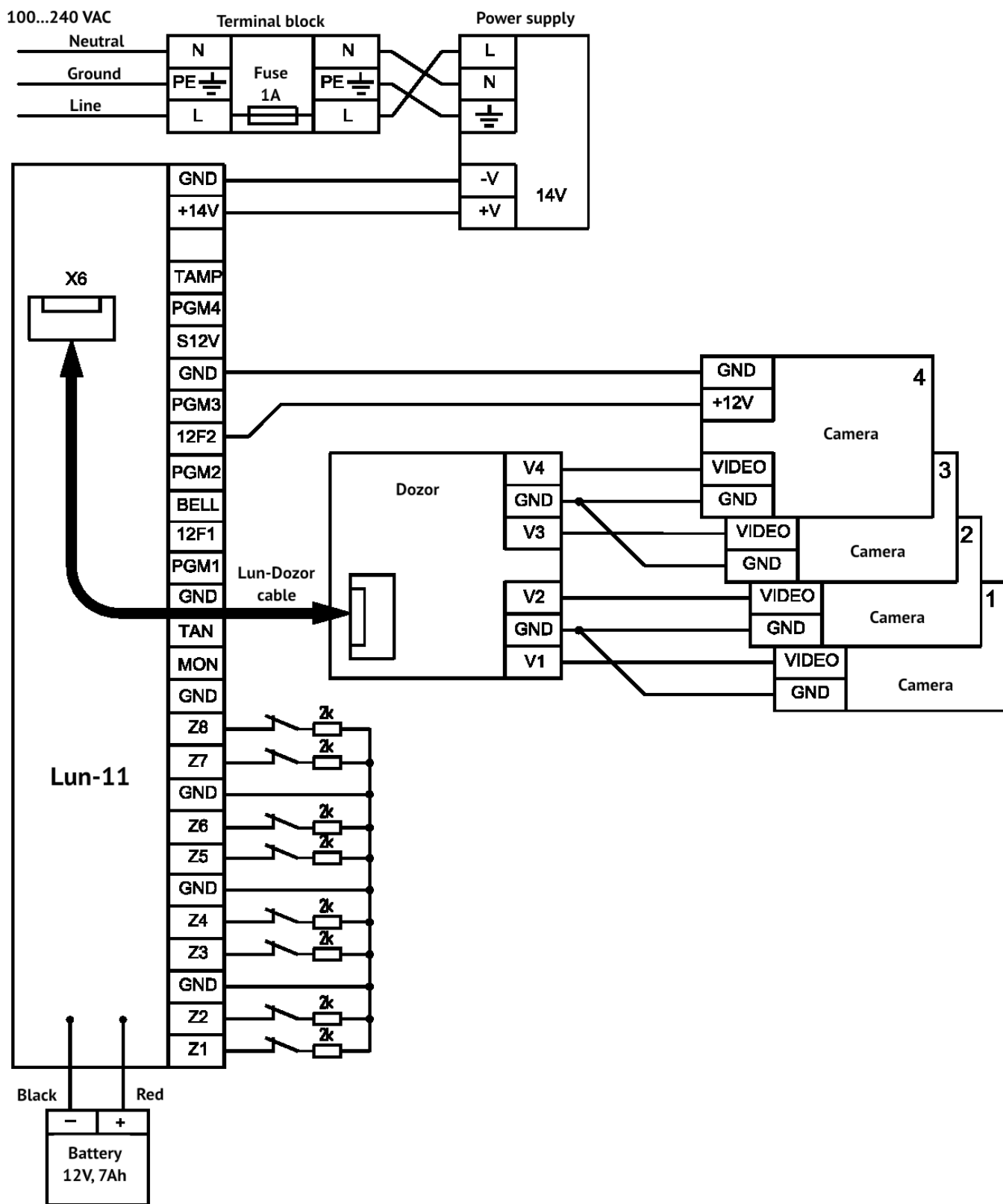


Figure 38. Connection diagram for "Dozor" alarm photo-proof module



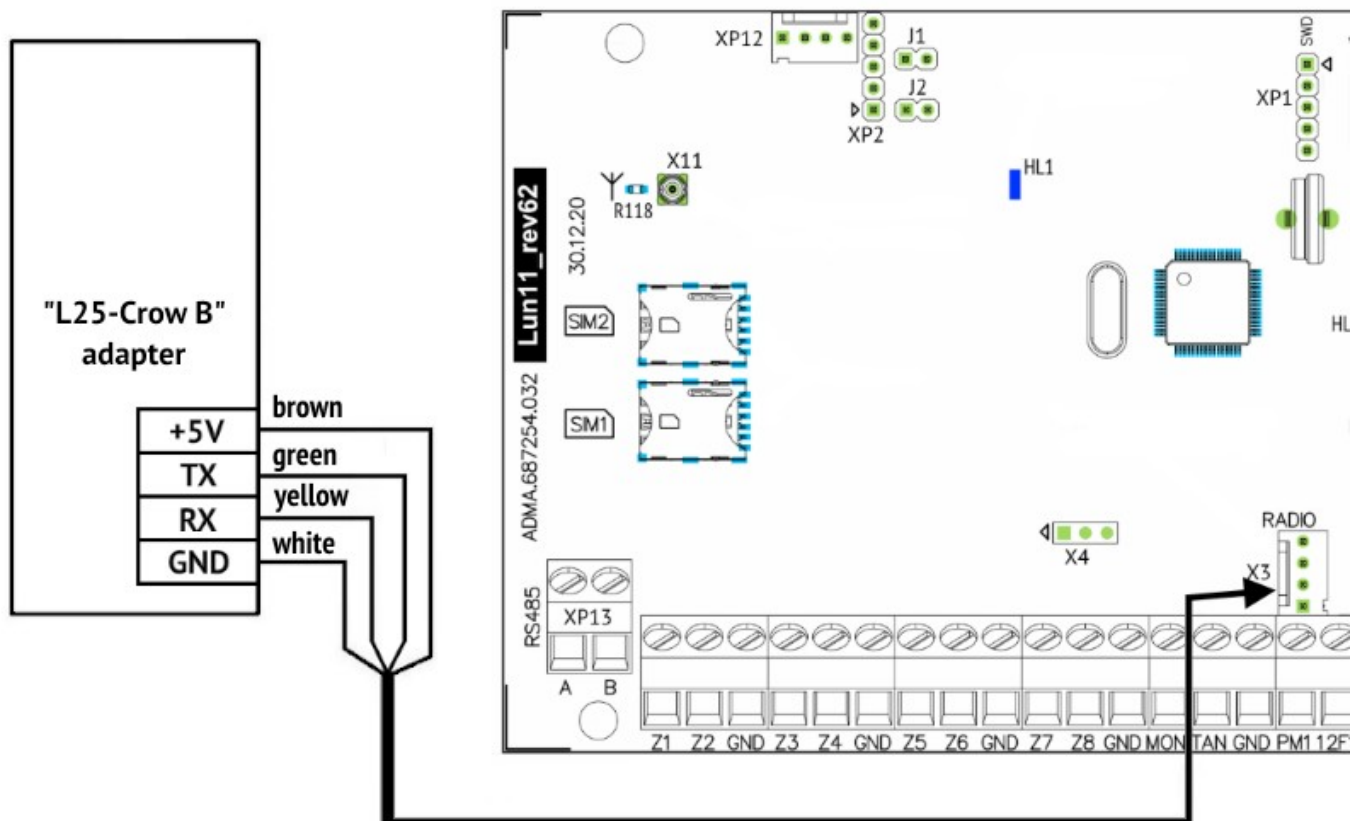


Figure 39. Adapter "L25-Crow B" connection diagram

## 26. Appendix 3. Wireless devices handling

### 26.1. 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 device by keypad the following shall be done:**

- Remove battery from the wireless detector;
- Enter the desired group (partition) and check that it is disarmed;
- Switch the Control Panel to the binding mode, select the wireless device kind (detector/siren/output). If there are free cells for binding (check by the ICD indication), then select the free cell number and initiate the binding process. Control panel waits a binding signal up to 40 seconds, if a binding fails the process ends with a long beep;
- If there are no free cells for binding, you must first remove one or more wireless devices by ICD keyboard **or** clear the **“DeviceID”** field of the cell you choose by the “Configurator 11” software;
- 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 device is registered by the ICD sound trill.

## 26.2. Crow


Depending on the installed Crow module, the Control Panel supports of the following Crow wireless devices (see Table 12).

Table 12. Crow wireless devices

Receiver based...	...on RF UART 0034638 module	...on RF EFM 32 V5 module
<b>Wireless device</b>	<b>Model No.</b>	
FW2-MAG-8F – magnet contact	0034590 0034895	0034895
FW2-RMT-8F – keyfob	0022012 (release date <u>earlier 5016</u> with the receiver version <b>2.66 only</b> ; release date <u>0916 and higher</u> with receiver version <b>2.67 and higher</b> )	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 <b>2.67 and higher</b> )	---
FW2-VESTA-8F – indoor siren	0020580 (release date <b>1018 and higher</b> with the receiver <b>version 2.67 and higher</b> )	---
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, then each registered wireless device in the system should be re-powered 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 device by keypad the following shall be done:**

- Remove battery from the wireless detector;
- Enter the desired group (partition) and check that it is disarmed;
- Switch the Control Panel to the binding mode, select the wireless device kind (detector/siren/output). If there are free cells for binding (check by the ICD indication), then select the free cell number and initiate the binding process. Control panel waits a binding signal up to 40 seconds, if a binding fails the process ends with a long beep;
- If there are no free cells for binding, you must first remove one or more wireless devices by ICD keyboard **or** clear the “**DeviceID**” field of the cell you choose by the “Configurator 11” software;
- 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 40);
  3. **Keypad ICON** – delete previous registration – **C, 0000, SOS+SOS** to  off; then press any key to new binding;
  4. **Siren** – remove the previous binding from wireless siren – press and hold **LEARN** key then turn on wireless siren battery. Wait until the LED flashing starts then release the key. Then send the binding signal by short press **LEARN** key;
  5. **Repeater** – 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. Insert the repeater plug into the mains socket for automatic binding. It occurs when the repeater indicator stops flashing;
- Make sure the wireless device is registered by the ICD sound trill.

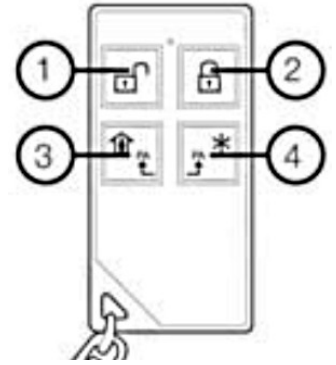




Figure 40. Keyfob Crow FW2-RMT-8F

**Alternative way to bind any CROW wireless device:** enter the serial number of the device (last 7 digits) in the “**DeviceID**” field manually. In this case, after entering all serial numbers and restarting the Control Panel, it is necessary to repower each registered wireless device in the system after the Control Panel began to work in normal mode (i.e. **not** in update or configuration mode).


### 26.2.1. 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:

2145     


– 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:

2145 

– 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:

032964 

– 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 return 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.

## 26.3. Rielta

The device can operate with the following Rielta wireless detectors:

- Ladoga BRSHS-RK-RTR modification 2 – repeater;
- 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;
- Piron-8-RK – electrooptical burglar space detector;
- Steklo-3RK – wireless channel sound surface burglar alarm detector;
- Trubach-RK – fire siren;
- Foton-12-RK – wireless channel electrooptical burglar alarm detector;
- Foton-SH – electrooptical surface burglar alarm detector;
- Foton SH2-RK – electrooptical surface burglar alarm detector.

The “**Rielta–RKI New**” radio receiver should be set in the Control Panel configuration.

**To register (bind) one Rielta wireless device by keypad the following shall be done:**

- Remove battery from the wireless device;
- Enter the desired group (partition) and check that it is disarmed;
- Switch the Control Panel to the binding mode, select the wireless device kind (detector/siren/output). If there are free cells for binding (check by the ICD indication), then select the free cell number and initiate the binding process. Control panel waits a binding signal up to 40 seconds, if a binding fails the process ends with a long beep;
- If there are no free cells for binding, you must first remove one or more wireless devices by ICD keyboard **or** clear the “**DeviceID**” field of the cell you choose by the “Configurator 11” software;
- 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 device is registered by the ICD sound trill.

### 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.

## 26.4. Ajax “uartBridge”

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.

The “**Ajax uartBridge**” radio receiver should be set in the Control Panel configuration.

**To register (bind) one Ajax wireless detector by keypad the following shall be done:**

- Turn the wireless detector power switch **OFF** (located on the back of the wireless detector housing);
- Enter the desired group (partition) and check that it is disarmed;
- Switch the Control Panel to the binding mode, select the wireless device kind (detector/siren/output). If there are free cells for binding (check by the ICD indication), then select the free cell number and initiate the binding process. Control panel waits a binding signal up to 40 seconds, if a binding fails the process ends with a long beep;
- If there are no free cells for binding, you must first remove one or more wireless devices by ICD keyboard **or** clear the “**DeviceID**” field of the cell you choose by the “Configurator 11” software;
- To register the detector, turn the detector power switch **ON**; registration process takes 3...5 sec. For keyfob, press the buttons **○** and **①** simultaneously;
- Make sure the wireless device is registered by the ICD sound trill.

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.

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 – for example, at “Lind-11” ICD select “**Wireless Zone**” menu item, 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” keypad.

You can check the detection area and change the sensitivity for **MotionProtect/Plus**, **GlassProtect** and **CombiProtect** wireless detectors – for example, at “Lind-11” ICD select “**Wireless Zone**” menu item, 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 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 wire-based 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.



Manufacturer:  
ORTUS Group  
1 East Liberty, 6th Floor  
Reno, NV 89501, USA  
Tel.: +1 650 240 27 62  
mail: [info@ortus.io](mailto:info@ortus.io)  
<http://www.ortus.io>