


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.....	3
2. Safety Precautions.....	3
3. Technical characteristics.....	3
4. Detectors selecting.....	4
5. Control Panel appearance and functions of its terminals.....	5
6. Control Panel features.....	6
6.1. Operating mode selecting.....	6
6.1.1. Orlan CMS mode.....	6
6.1.2. Standalone Web mode.....	7
6.1.3. SIA DC-09 mode.....	7
6.1.4. Calling to owner.....	8
6.2. Message transmission and testing.....	8
6.3. Control panel zone types.....	9
6.4. Groups.....	9
6.5. Programmable outputs.....	11
6.6. External antenna.....	12
6.7. Control of fire detector false alarms.....	12
6.8. Schedule.....	13
7. LED indicators.....	14
8. Control Panel configuring.....	15
9. Firmware update.....	15
10. Control Panel remote control.....	15
11. Battery monitoring.....	16
12. Main power supply monitoring.....	16
13. Maintenance.....	16
14. Operating conditions.....	16
15. Storage.....	16
16. Transportation.....	16
17. Disposal.....	16
18. Appendix 1. Control Panel zones types.....	17
19. Appendix 2. Control Panel connection diagram.....	20

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, as well as to control strobes and/or sounders. It transmits all events to the central monitoring station (further called as "CMS") in proprietary Lun-I protocol or to any CMS in SIA DC-09 protocol, or works in stand-alone mode – events are sent to the user's monitoring center "Phoenix-Web" (registered user's Internet-based page).

CP uses 4G/3G/GSM cellular networks for transmitting events and receiving commands. Communication mode depends of the Control Panel modem type – see Table 2.

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

Control Panel has no open live parts posing the electrical shock hazard.

3. Technical characteristics

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

Table 1. Control Panel's basic technical parameters

Parameter name	Value
Number of wired zones	8
Maximum number of groups (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
Maximum number of users (freely appointed by groups)	512
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 of the armed Control Panel board, mA, max	160
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 18), kOhm	2±5%
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 cellular communication channel (ATS/D/M/T/S/I)	ATS5/D4/M4/T6/S2/I3

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

Table 2. Frequencies and emitted power

Control Panel's Version (Modem type)	Communication Mode	Band	Emitted power
3G (UC200)	GSM (GPRS)	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
4G (EC200)	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 18.

5. Control Panel appearance and functions of its terminals

The appearance of Control Panel circuit board and functions of some of its components are shown in Figure 1.

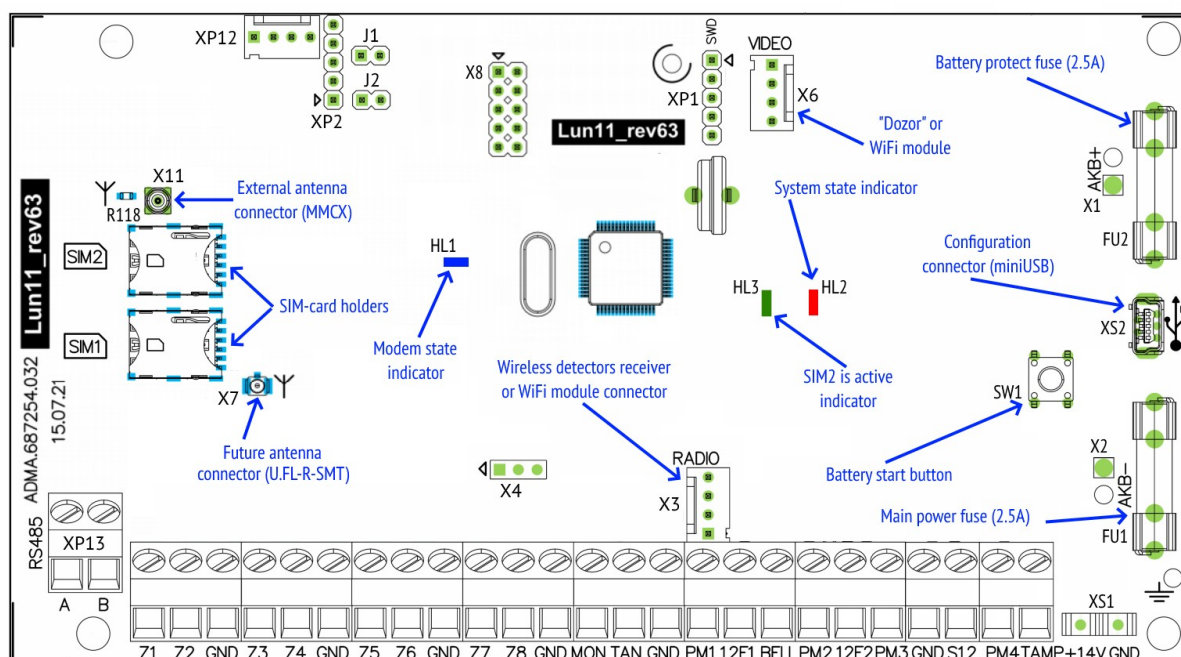


Figure 1. Control Panel circuit board appearance

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

Table 3. Control Panel terminals functions

Terminal marking	Function
RS485 A/B	RS-485 interface
Z1...Z8*	Connection of zones 1...8
GND	Common terminal (-) of Control Panel
MON	MON interface
TAN	TAN interface
GND	Common terminal (-) of Control Panel
PGM1**...PGM4**	Programmable outputs 1...4 (-) of "Open collector" type
12F1	Output for power-up (+) of "Lind" ICDs and siren (short-circuit current is limited)
BELL	Contact (-) of siren (short-circuit current is limited)
12F2	Output of power-up (+) of active detectors (short-circuit current is limited)
GND	Common terminal (-) of Control Panel
S12	Remote controlled (with CMS and keypad) power-up output (+) of active detectors (short-circuit current is limited)
TAMP	Input for wiring of housing opening tamper and housing shifting tamper
+14V	Power-up input (+) of Control Panel
GND	Common terminal (-) of Control Panel

* – Detectors connecting depends on the type of zone, which is selected in the "Configurator 11" software (see section 18).

** – 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 18.

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.

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.

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/GSM. 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).

Operating mode can be selected when the Control Panel is configuring with the “Configurator 11” software – “**CMS**” tab – “**Mode**” drop-down list (Figure 2). Depending on the configuration, the transmission of events to the CMS can be accompanied by calling to owners (to the preselected cell phone numbers as described in section 6.1.4).

6.1.1. Orlan CMS mode

If the value “**Phoenix – CMS**” selected in the “**Mode**” drop-down list (Figure 2), then the 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) you should set the time synchronization parameters on “**Extra**” tab in the Control Panel configuration. Then set the check-box “**Synchronize time on the control panels with the CMS**” in the Phoenix 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. Standalone Web mode

To work with the user's monitoring center "Phoenix-Web", you should select the "**Web**" value in the "**Mode**" drop-down list (Figure 2). 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 "**Data channel**" 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 2) for receive events from Control Panel setting on user's Internet-based page "Phoenix-Web" – click on "**Read IMEI**" button and write the number in the next field appears.

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

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

For correct logging (matching the date and time) you should set the time synchronization parameters on "**Extra**" tab in the Control Panel configuration.

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

6.1.3. SIA DC-09 mode

To work in SIA DC-09 mode, you need to select "**SIA DC-09**" value in the "**Mode**" drop-down list (Figure 2). Then all events and test messages will be sent to CMS as the SIA DC-09 protocol codes.

Faults/restoration SIA protocol codes for every connected module is supplemented by the "zone" number which corresponds to the type and number of the module as shown in the Table 4.

Table 4. SIA DC-09 codes for faults/restoration by device type

Fault type	Module type	SIA DC-09 code	"Zone" number
Loss/restoration of communication with the module	Keypad #1...#16	ER/EM	1...16
	Expansion module Lun-11(E,H) #1...#12		21...32
	Key reader Lind-11TM #1...#24		141...164
	Address module AM-11 #1...#31		41...71
	LanCom		81
	TK-17		91
	Radio receiver		101
	MPB-8M		111
	WiFi		131
Tamper violation/restoration	Keypad #1...#16	EJ/ES	1...16
	Expansion module Lun-11(E,H) #1...#12		21...32
	Key reader Lind-11TM #1...#24		141...164

For correct logging (matching the date and time) you should set the time synchronization parameters on **“Extra”** tab in the Control Panel configuration.

The mobile application “Phoenix-MK” can’t be used in “SIA DC-09” mode.

6.1.4. 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.

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 (Figure 2).

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.

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.

The screenshot displays the 'CMS' configuration window. On the left, a tree view shows the following structure: Groups, Schedule, Keys and passwords, Expanders MON, Zones, Wireless System, Wireless Zones, Wireless Sirens, Wireless Outputs, Keypads MON, Bus TAN, CMS (selected), SIM card #1, Data channel, SIM card #2, Data channel, WiFi/Lan MON, Automatic redial, Calling, Dozor, Sirens, Fire subsystem, Outputs, MPB-8 MON, Remote update, and Extra. The main configuration area includes: Mode (SIA DC-09), Read IMEI button, Encryption key field, Encrypt checkbox, The transmission number (1111), Keep connection (with Phoenix HD) checkbox (checked), SIM cards section with SIM1 and SIM2 settings (Period of sending a test by Data: 5 minutes for SIM1, 6 minutes for SIM2; Period of test for Lan/WiFi: 1 minute), Automatic redial section (Period for sending of test: 1439 minutes, The delay of the first test: 480 minutes), and Channels priority section (1. SIM card #1, 2. , 3. , 4.).

Figure 2. Communication channels and priorities setting

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 full.

6.3. Control panel zone types

Control Panel operates with the following types of zones (Table 5):

Table 5. Available zone types

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

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

Zones response time can be switched when Control Panel configuring.

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

6.4. Groups

In the process of configuration, the zones connected to the Control Panel can be logically combined into groups (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 uses 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:

- Remove the resistor marked **R118** (Figure 1), carefully biting it with sharp side cutters – this will turn off the communicator built-in antenna. Remember that rebuilding a resistor requires a special equipment and highly qualified personnel;
- Connect the external antenna to **X11** connector (MMCX connector type, see Figure 1). 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 7). 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. 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.

7. LED indicators

The Control Panel has a three indicators – red, blue and green (see Figure 1).

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 4G/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.

8. 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 1) 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.

“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 any data 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.

9. 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 8), or remotely (performed via any data channel; 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.

10. 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.

11. 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.

12. 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!

13. Maintenance

The Control Panel does not require any maintenance.

14. 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.

15. 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.

16. 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%.

17. Disposal

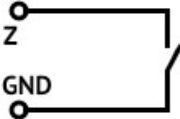
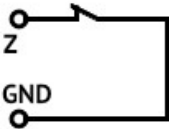
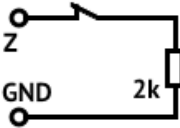
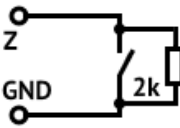
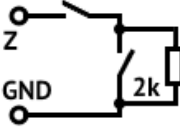
Product disposal shall be carried out according to electronic household appliance disposal rules established by the legislation of the State, where the product is operated.

18. 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”.

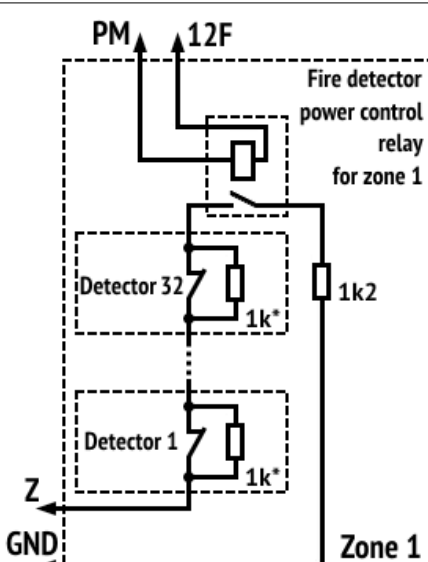
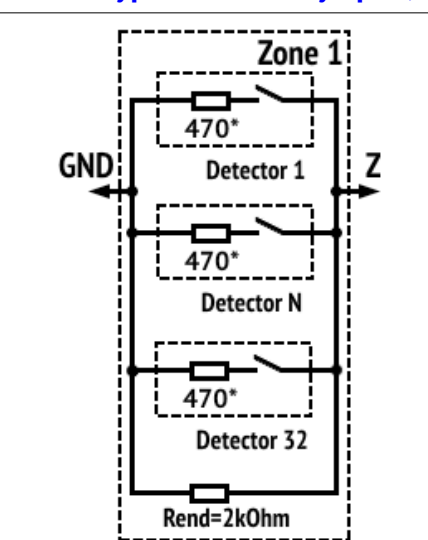
See the types of protective zones and events generated in case of their violation, in Table 6.

Table 6. Protective zones types

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

The types of fire zones and events generated in case of their violation see in Table 7.

Table 7. Fire zones types

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

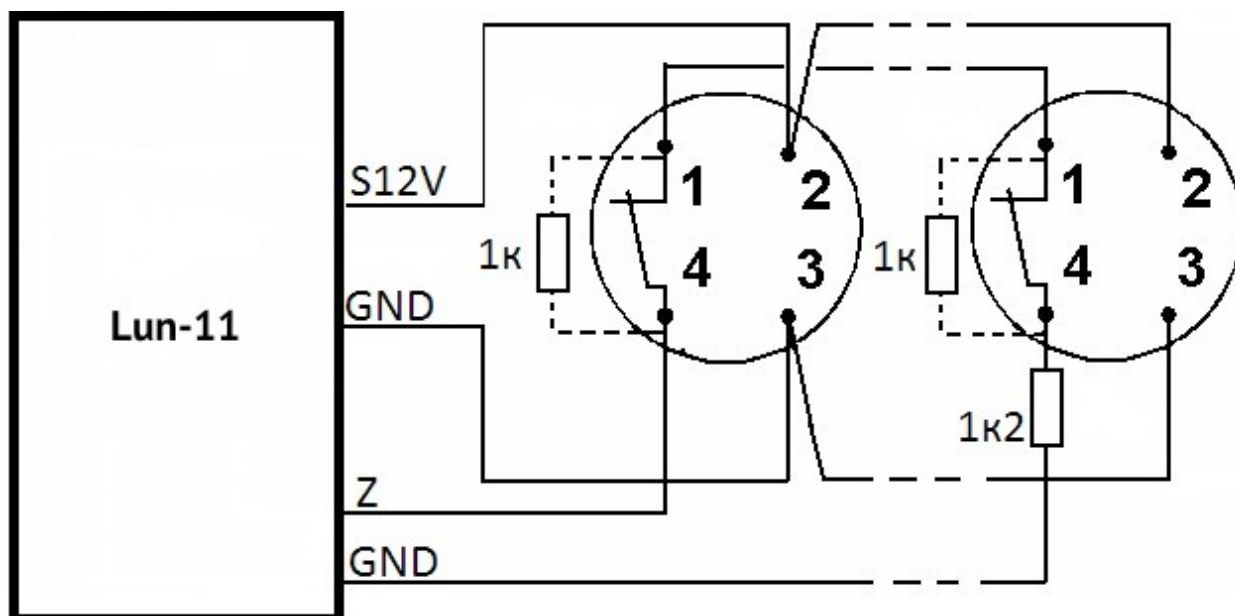


Figure 3. Fire detector connection diagram according to four-wire circuit

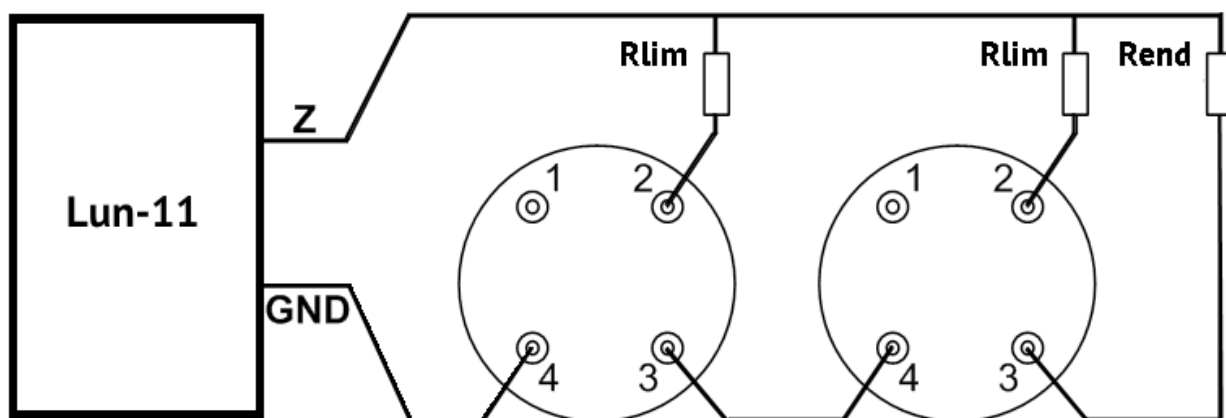


Figure 4. Diagram of connection of detectors to fire zone according to two-wire circuit

Table 8. An example of R_{lim} calculation

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

19. Appendix 2. Control Panel connection diagram

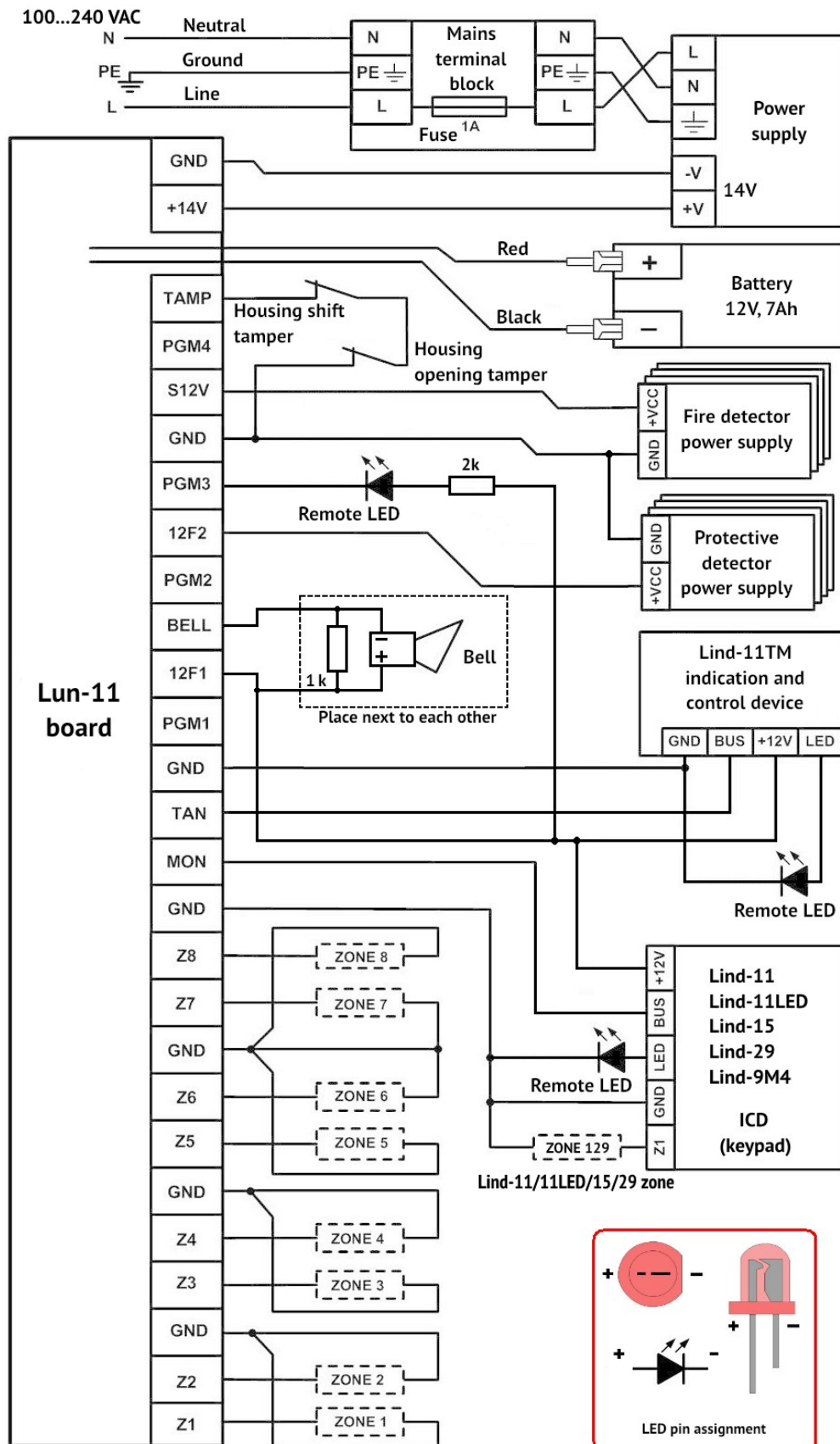


Figure 5. Control Panel connection diagram

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.



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