Warning! 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

GSM/3G/4G Wireless Security and Fire Alarm Control Panel “Lun-25” mod.2

Reference Manual

ORTUS Group	Product Compatibility Table		
	Control Panel	Lun-25	Version mod.2
	Control Panel Configuration Software	Configurator 11	Version
	Central Monitoring Station	Orlan	Version

Contents

1. Purpose

”Lun-25” mod.2 Control Panel (CP) are designed to monitor the status of alarm and fire system zones, as well as to control strobes and/or sounders and transmit announcements to the “Orlan” central monitoring station (CMS) or work in stand-alone mode – events are sent to the user's monitoring center “Phoenix-Web” (registered user's Internet-based page) or to the preselected mobile phones via SMS.

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

- “**Lind-7**”/“**Lind-11TM**” ICD (with TouchMemory DS1990A-F5 key reader);
- “**Lind-EM**” EM-Marine RFID-card reader;
- Any third party TouchMemory **Anti-vandal Key Reader** (general DS1990A-F5 keys or copy-protected DS1961S-F5 keys are supported);
- “**Lind-9M3**”, “**Lind-9M4**” ICD (keypad);
- **“Lind-15” / “Lind-29”** ICD (touch-sensitive keypad).

Depending on the model, on the front panel of the main unit can be installed TouchMemory key reader or contactless RFID-cards reader or keyboard. Variants are given in the table below:

Model	Built-in ICD
“Lun-25”	Not used
“Lun-25T”	TouchMemory key reader (DS1990A-F5, DS1961S-F5)
“Lun-25E”	EM-Marine RFID-card reader “Lind-23E”
“Lun-25TE”	“Lind-25” ICD (TouchMemory DS1990A-F5 key reader, extended indication)
“Lun-25TE+”	“Lind-25+” ICD (TouchMemory DS1990A-F5 key & EM-Marine RFID-card readers, extended indication)
“Lun-25K”	“Lind-27” ICD (touch-sensitive keypad)
“Lun-25 Light”	“AK-25” ICD (keypad)

CP supports up to **22 wired zones**, 5 of which (or 10 – when zone doubling is turned on) are located on the main unit PCB. Other zones can be connected to Address modules "**AM-11**" (up to 4 modules, everyone provides an additional 3 zones).

CP supports up to **16 wireless sirens** (Lun-R, Crow, Rielta) and up to **30 wireless zones/keyfobs** via an additional radio receiver. More about wireless subsystem you can see in Chapter 9.

All zones may be assigned into one of two groups. Every group can be controlled up to 256 keys/codes/mobile phone numbers.

GSM/3G/4G mobile communication channels (Table 2) and **Ethernet/WiFi** (via the Internet) can be used for remote control and to transmit events to the CMS.

Compatibility of the ICD is shown in the Table 4.

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

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

The Control Panel supports “binding” to a specific monitoring station, as well as “blocking” data transmission upon a command from the “Orlan” CMS.

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 voltage up to 1000V shall be allowed to install, routinely maintain and repair the Control Panel.

The Control Panel has open live parts posing the electrical shock hazard. The Control Panel has safety ground, termination point of which is indicated as "PE ⏚" and placed near the AC terminal block.

Control Panel is designed for permanent connection to a single-phase AC mains 220V. 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
Burglary zones connection scheme	By 2 wires
Fire zones connection scheme	By 2/4 wires
Number of wired zones / doubling	5/10
Maximum number of groups	2
Maximum number of NC detectors in the zone	32
Current in the fire zone for "normal" status, maximum, mA (for circuit with NC detectors)	8
Number of the controlled outputs (PGM)	2
Number of ICD ("Lind-7"/"Lind-11TM"/"Lind-EM"/"Lind-9M3"/"Lind-15"/"Lind-29"/ Anti-vandal TouchMemory Key Reader) connected	2
The total length of the TAN bus cable, without/with connected "Lind-7" and anti-vandal reader m, max	150/15
Number of "AM-11" address modules connected	4
Total number of binded wireless zones/sirens *	30/16
Availability of integrated Battery Charge Controller	+
Output current +12F, mA, max	350
Output current PM, mA, max	200
Output current Bell, mA, max	150
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
Failure detection time, seconds, max	300
Absorbed current of the Control Panel board in normal mode**, mA, max	140
Absorbed current of "Lind-25+" ICD, all indicators on/off, mA, max	90/60
Absorbed current of "Lind-25" ICD, all indicators on/off, mA, max	70/40
Absorbed current of "Lind-27" ICD, all indicators on/off, mA, max	105/35
Resistance of wired zone end-of-line resistor (see Section 21), kOhm	2±5%
AC mains power voltage, V	100...242
AC mains absorbed current, A, max	0,2
Battery power voltage, V	10.5...14.0

Parameter name	Value
Battery cut-off voltage, V, min	10.5
Battery voltage, when “Low battery” event is generated, V, min	11.5
Battery voltage, when “Normal charge” event is generated, V, min	12.5
Battery charge current, mA, up to	100
Bell output commutation voltage, V, max	18.0
Output ripple, mV, max	200
Battery and recharger fault location time, max, sec	300
Time of delay of mains supply failure message, sec	60
Recommended battery parameters (gel maintenance-free sealed lead battery, for example PowerSonic PS1223), voltage, V/capacity, Ah	12 / 2.3
Rated current of input wire fuse (FU1), A	0,3
Rated current of battery short circuit protection wire fuse (FU2), A	2,0
The size of non-volatile event queue	128
Housing dimensions, W*H*D, mm	190*140*43
Dimensions when packed, W*H*D, mm	200*150*45
Device weight, net/gross, kg, max	0.57 / 0.65

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

** – **Approximate** battery operating time for Control Panel (without ICD) under various conditions:

- Without detectors – 1 SIM, tests 15 minutes – up to 52 hours;
- With 5 wire detectors connected to the main board:
  - PIR detectors (total current 40mA), 1 SIM, tests 15 minutes – up to 16h;
  - PIR+Glass break detectors (total current 100mA), 1 SIM, tests 15 minutes – up to 12h;
- With 2 Crow wireless detectors connected:
  - 1 SIM, tests 15 minutes – up to 40h;
  - 1 SIM, tests 30 minutes – up to 44h.

Note: The battery operating time depends to battery state, GSM signal strength at the Control Panel location, the communication channel is using and others.

Table 2. Control Panel’s operating frequencies

Version	Mode	Frequency range	Emitted power
GSM	**GSM**	850/900 MHz	up to 2W
		1800/1900 MHz	up to 1W
3G	**UMTS/HSPA+**	900/2100 MHz	up to 0,25W
	GSM	850/900 MHz	up to 2W
		1800/1900 MHz	up to 1W
4G	**LTE-FDD**	B1/B3/B5/B7/B8/B20/B28	Class 3 (up to 0,2W)
	LTE-TDD	B38/B40/B41	
	GSM	850 MHz/900 MHz	Class 4 (up to 2W) – EGSM900/GSM850 Class E2 (up to 0,5W) – EGSM900/GSM850 8-PSK
		1800МГц/1900МГц	Class 1 (up to 1W) – DSC1800/PCS1900 Class E2 (up to 0,4W) – DSC1800/PCS1900 8-PSK

4. Detectors selecting

Control Panel allows the connection to both the burglar alarm and fire zones of any detectors with **normally open** or **normally closed** contacts by the **2-wire or 4-wire connection** circuit. Each zone type may be selected in the Control Panel's configuration.

The possible detector connection circuits are shown in Section 21.

5. Device appearance and functions of its terminals

Control Panel exterior, overall and mounting dimensions is shown in Figures 1, 2, 3. Degree of protection provided by enclosure – IP41 according to IEC 60529:2013.

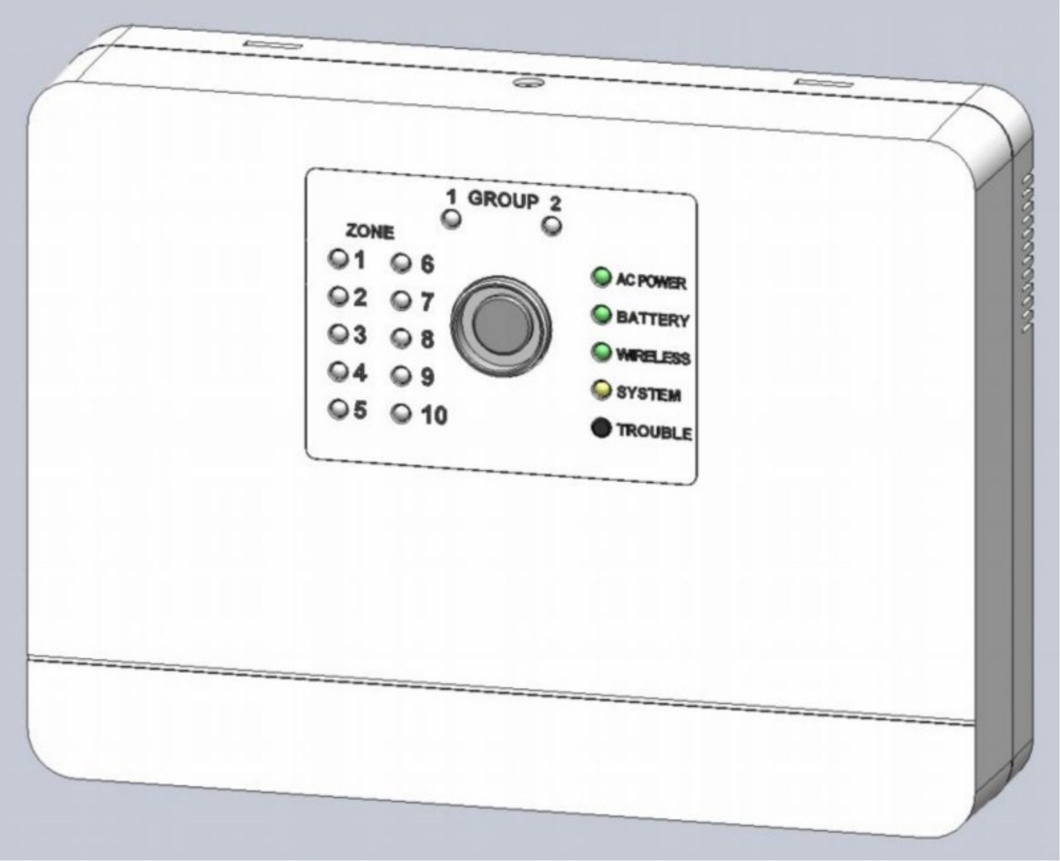


Figure 1. Control Panel exterior ("Lun-25TE" model)

Depending of the Control Panel's model the TouchMemory key reader or EM-Marine RFID card reader may be placed on the front surface of the housing.

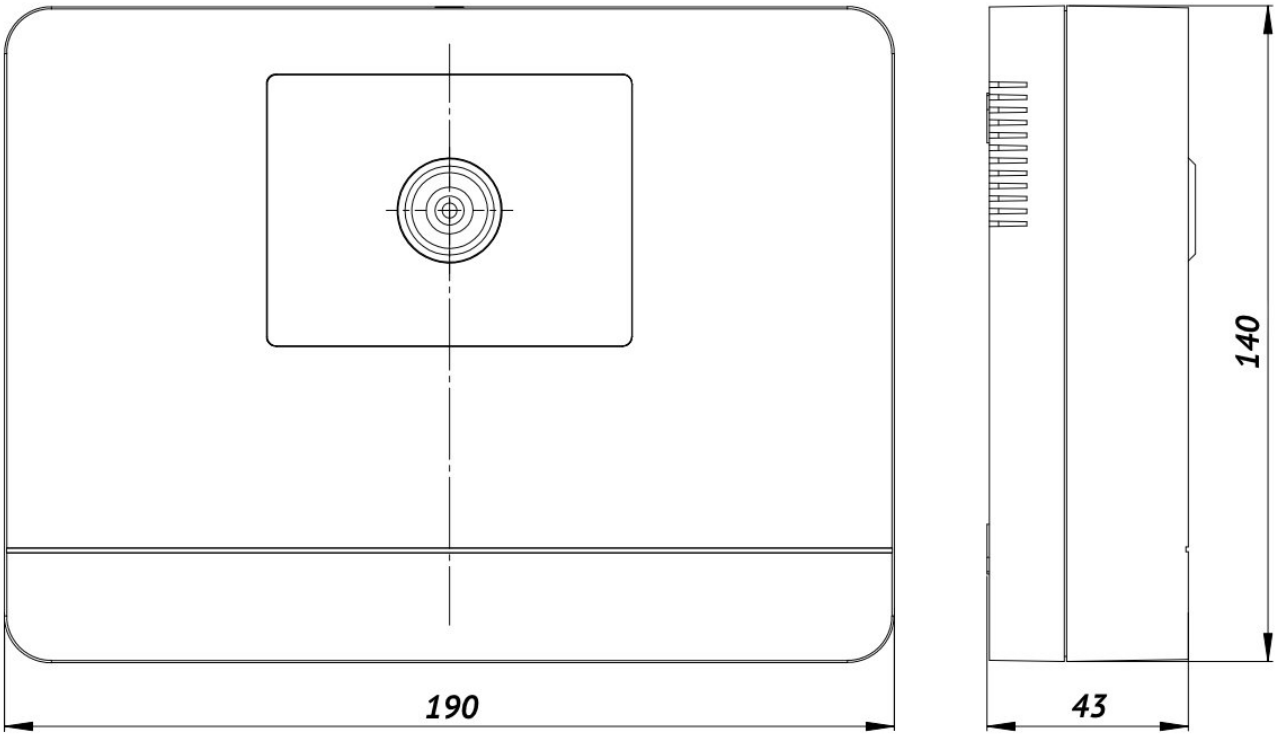


Figure 2. Control Panel's overall dimensions (“Lun-25T” model)

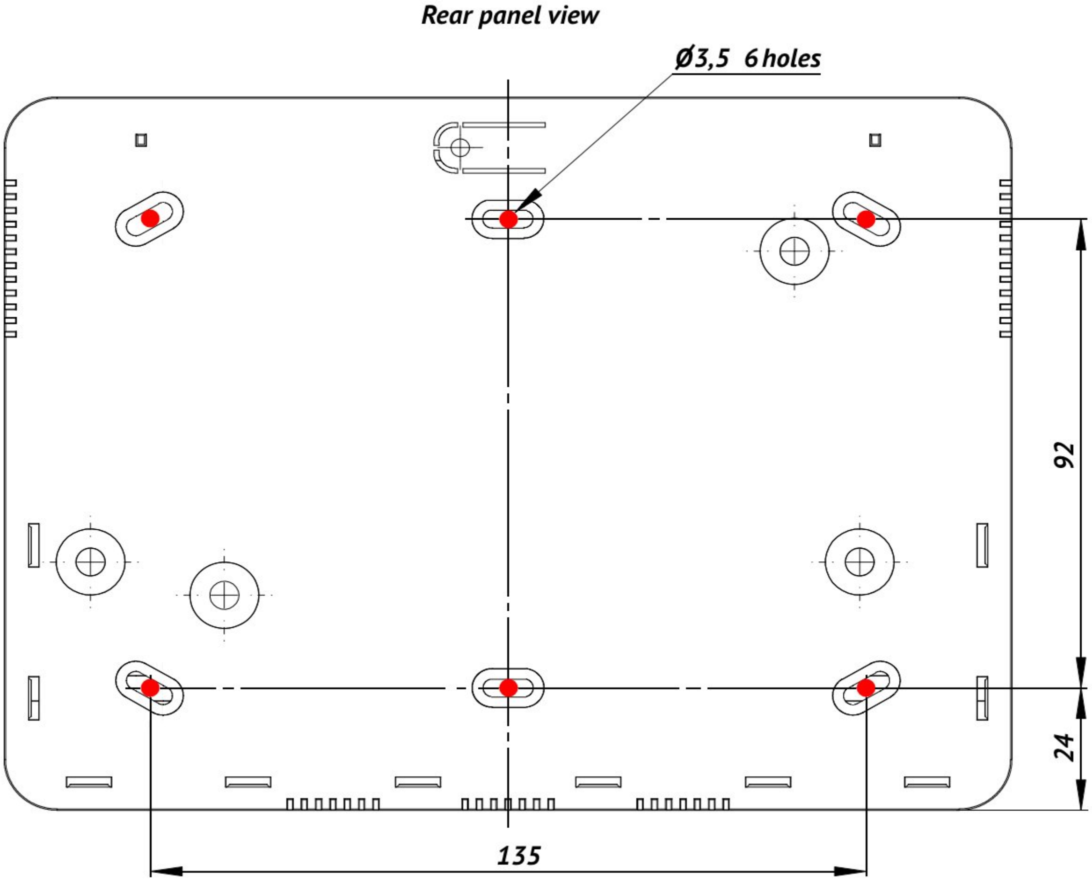


Figure 3. Control Panel mounting dimensions (rear panel view)

Arrangement and the appointment of the Control Panel PCB elements shown in Figure 4, the terminal assignment specified in Table 3.

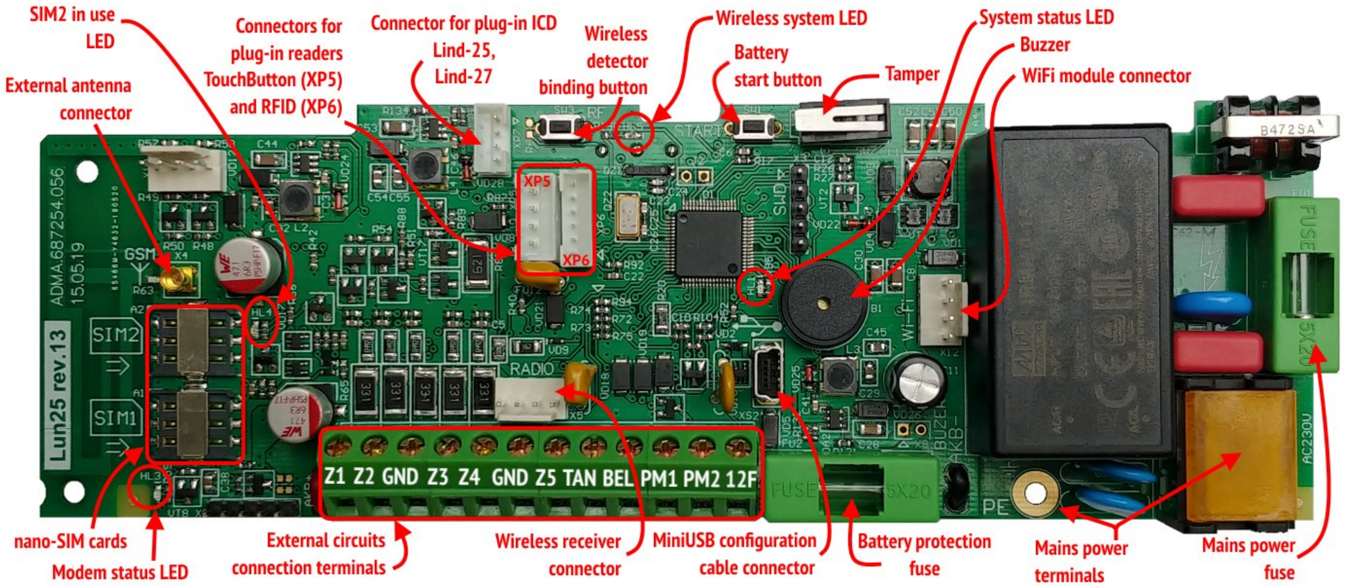

SIM2 in use LED
External antenna connector
Connectors for plug-in readers TouchButton (XP5) and RFID (XP6)
Connector for plug-in ICD Lind-25, Lind-27
Wireless detector binding button
Wireless system LED
Battery start button
Tamper
System status LED
Buzzer
WiFi module connector
XP5
XP6
Z1 Z2 GND Z3 Z4 GND Z5 TAN BEL PM1 PM2 12F
nano-SIM cards
Modem status LED
External circuits connection terminals
Wireless receiver connector
MiniUSB configuration cable connector
Battery protection fuse
Mains power terminals
Mains power fuse

Figure 4. Control Panel's PCB components location

Table 3. Control Panel terminals functions

Terminal marking	Function
Z1...Z5*	Connection of zones 1...5 (or 1...10 – when doubling is turned on)
GND	Common terminal (–) of Control Panel
TAN	Interface for the connection of “Lind-EM/7/11TM” readers, “Lind-15/9M3/29” keypads, “AM-11” modules or TouchMemory anti-vandal electronic key reader
BEL	Contact (–) with limited SC current for siren connection
PM1**	Programmable output 1 (–) of “Open collector” type
PM2**	Programmable output 2 (–) of “Open collector” type
12F	Output with limited SC current for power-up (+) of “Lind-EM/7/11TM”, “Lind-15/9M3/29”, “AM-11” and siren

** – “fire” or “burglar alarm” zones shall be set with the “Configurator 11” software, and they differ in detector connection.*

*** – function of PM1, PM2 controlled outputs shall be set with the “Configurator 11” software (see “Configurator 11” Guide). Sink current shall not exceed 0.2A (with voltage not exceeding 15V).*

The foiled twisted pair (as FTP CAT5/5e cable) should be used to wire any devices to TAN bus. The shield wire should be wired to GND contacts at both ends – the Control Panel and connecting device.

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

Note: The connection circuits of detectors depends of the of the Control Panel zones configuration (fire or burglar alarm – see Section 21).

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 common wire (GND) of the Panel 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

Due to differences in voltage levels on the TAN bus for different models of readers, there are some restrictions of the security system content. Possible compatibility of additional components in the security system based on "Lun-25" Control Panel are shown in Table 4. The built-in reader is compatible with any additional equipment specified in the this table.

Control Panel's firmware supports a few operating algorithms in cellular networks depending on the communication channel used. The device allow to select a number of cellular networks providers (1 or 2), transmission channels (only GPRS/3G/4G, only Voice channel, GPRS/3G+Voice). The Control Panel may be controlled via mobile phones of the responsible persons of the facility.

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

Control Panel supports the remote control via GPRS/3G/4G, Voice, and Ethernet/Wifi. "Phoenix" software automatically determines the list of available commands depending on the current communication channel.

Table 4. Compatibility chart for plug-in components

Additional device	Lind-7	Anti-vandal TouchMemory key reader	Lind-29	Lind-27	Lind-25	Lind-15	Lind-9M3	Lind-11TM	Lind-EM	AM-11
Lind-7	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Anti-vandal TouchMemory key reader	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Lind-29	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-27	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-25	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-15	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-9M3	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-11TM	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Lind-EM	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
AM-11	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Notes: ✓ – compatible equipment; ✗ – incompatible equipment.										

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 duplicated by sending an SMS, as well as accompanied by telephone calls to the owners (using pre-selected phone numbers, similar to that described in sections 6.1.3, 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).

To insert the correct date and time into the events to be sent, the “**Time synchronization via CMS**” and a **timezone offset relatively to CMS** should be set 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.

Note: 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. Stand alone 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!

Note: For "Phoenix-Web" mode use IP-address ***lun.ortus.io*** and port ***8089***, on the “**GPRS**” tab of each of the SIM cards with ***Internet*** network type.

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

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

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

To insert the correct date and time into the events to be sent, the “**Time synchronization via SNTP server**” and a **timezone offset** should be set in the Control Panel configuration.

Note: For “Phoenix-MK” application use address *lun.ortus.io* and port *8087.*

6.1.3. Stand alone 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 the parameters of “**Test period for SMS**” and “**SMS lower balance limit**”, and on the “**SMS**” tab you need to set the mobile phone numbers and the event types for each of them. On the “**CMS**” tab, you should select the desired SIM card; the channel type can be omitted.

The “**SMS balance lower limit**” is set for warning exhaustion of the SIM-card balance.

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.

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.

To insert the correct date and time into the events to be sent, the “**Time synchronization via SNTP server**” and a **timezone offset** should be set in the Control Panel configuration.

Note: The mobile application “Phoenix-MK” can’t be used in SMS mode.

6.1.4. TCP SUR-GARD mode

The Control Panel can send all events and tests to any CMS in SUR-GARD communication protocol. The remote control can’t be used in this mode.

Time synchronization by SNTP and the **time zone** value should be set in the configuration to the time stamp will be included to Control Panel’s events.

Note: The mobile application “Phoenix-MK” can’t be used in this mode.

6.1.5. Calling to owners

If "**Calling**" parameter on the “**SMS/Calling**” tab is set, then the **GSM** and **3G** versions of Control Panel performs phone call to the correspondent owner numbers, to attract their attention. Don’t answer the call. If the “**Only Alarm**” parameter is set, the call is performed only for alarm events. Calls to alarm events are accompanied by an audible "*Alarm*" message when the handset is picked up.

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

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

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

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

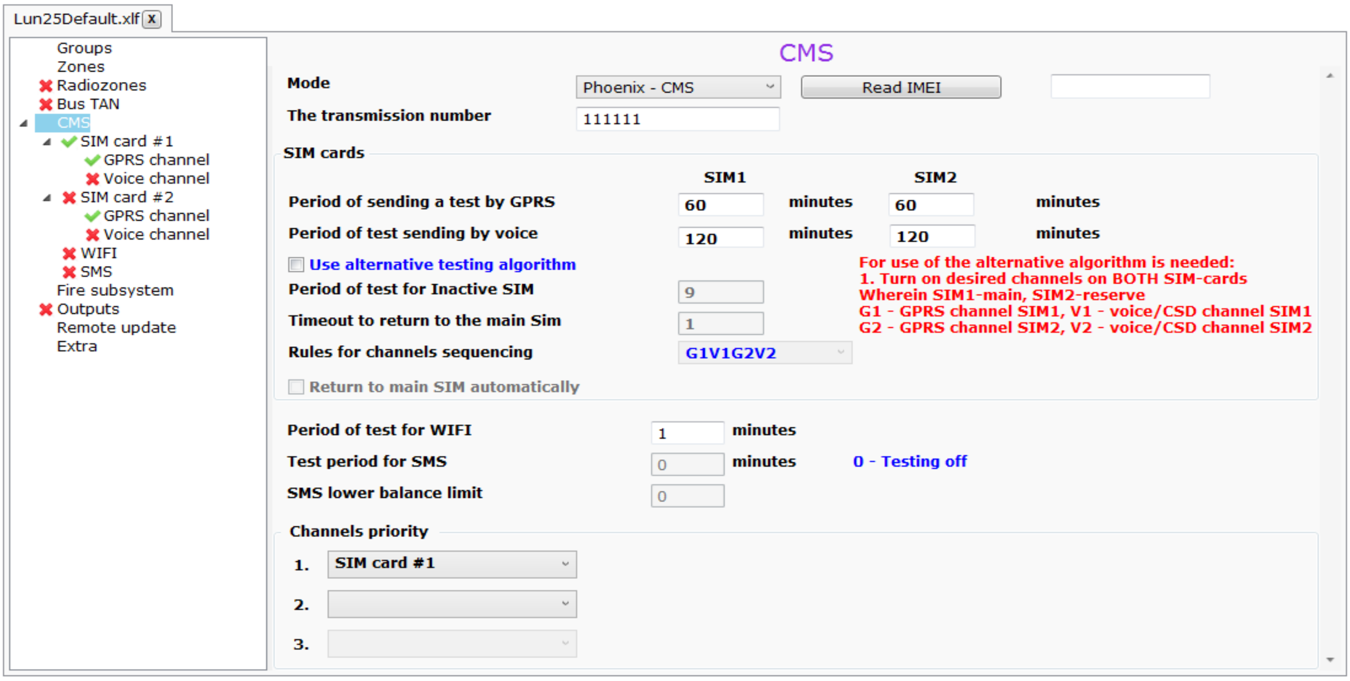
> Note: Call to the owner can be skipped when the mobile network problems occurred (for example, when the network is busy).

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).



Mode: Phoenix - CMS

The transmission number: 111111

SIM cards

	SIM1		SIM2	
Period of sending a test by GPRS	60	minutes	60	minutes
Period of test sending by voice	120	minutes	120	minutes

□ Use alternative testing algorithm

Period of test for Inactive SIM: 9

Timeout to return to the main Sim: 1

Rules for channels sequencing: G1V1G2V2

For use of the alternative algorithm is needed:
1. Turn on desired channels on BOTH SIM-cards
Wherein SIM1-main, SIM2-reserve
G1 - GPRS channel SIM1, V1 - voice/CSD channel SIM1
G2 - GPRS channel SIM2, V2 - voice/CSD channel SIM2

□ Return to main SIM automatically

Period of test for WIFI: 1 minutes

Test period for SMS: 0 minutes 0 - Testing off

SMS lower balance limit: 0

Channels priority
1. SIM card #1
2.
3.

Figure 5. Communication channels and priorities setting

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

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

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

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

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

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

Comment. The Control Panel **4G** version does not support **Voice** mode. Therefore, there are no **channels sequencing rule** and all the settings associated with **Voice** mode.

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 zones 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 in the entrance it is affected by the time delay only if the delayed zone has already been violated. For example, motion detector in walk-through corridors. Also, this type of zone is not analyzed in the Stay-Home Mode.
“Instant”	Standard type of zone that operates in the Armed Mode of Control Panel. This zone will only be activated when the Control Panel is armed. For example, window-mounted detectors.
“24hour”	Type of zone, which is always activated regardless of the Control Panel status (whether it is armed or not). For example, the alarm button.
“Arming”	Type of zone, violation of which disarms the group and recovery arms it.
“24h Fire”	Type of zone to operate with smoke detectors according to 2 or 4 connection circuit.
“Arm Stay”	Zones of this type are not analyzed, if the Control Panel is in the armed Stay-Home Mode. In this case, people can stay in the premise without causing an alarm, but violation of other zone types will cause a corresponding reaction of the Control Panel (e.g., glass brake will lead to the transmission of an alarm signal to CMS).
“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-25" 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.

6.4. Groups

Zones connected to the Control Panel can be logically combined into one or two groups (partitions), which allows to operate all the zones of each group as a one unit. Control Panel's groups are independent from each other.

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

"Configurator 11" assigns every key/code to some group (see Configurator 11 Guide). It is allowed to use any key for both groups. When using the key registered in both groups, arming/disarming will be done for both groups at the same time on their readiness (except for "Lind-11TM").

Any specific group can be remotely armed using CMS.

6.5. Programmable outputs

The Control Panel has two programmable outputs (of open collector type) – PM1, PM2. The function of each of them is set when configuring the Control Panel. One of the following functions for each output can be selected:

- **Not used**;
- **Siren*** – as an output for additional siren;
- **Remote LED*** – LED ***blinks*** (every second) when the corresponding group arming as long as the event is not received by the CMS. The LED ***lights***, if any group where the LED was assigned to, is armed, and the event was successfully sent to the CMS. When all groups where the LED is assigned to will be disarmed – LED will ***turns off;***
- **Alarm** – it is activated when an alarm occurs at **group** where the LED was assigned to, and remains this state while the siren works or up to disarm/cancel by a registered key/code;
- **Fire** – as a fire output signal;
- **Control from CMS or by user** – Output can be turning on/off by the user's or CMS operator's command.
- **Fire sensor's power*** – the output is used as a controllable power sink of fire detectors (power can be turned off/on in "**By second fire alarm**" mode);
- **Armed** – LED ***lights***, if any group where the LED was assigned to, is armed. When all groups where the LED was assigned to, disarmed – LED is ***turned off***;
- **Remote LED + alarm*** – LED ***blinks*** (every second) when the group where the LED was assigned to, armed and this event is not received by the CMS. The LED ***lights***, if any group where the LED was assigned to, is armed and the event was successfully sent to the CMS. LED ***quickly blinks*** (twice per second) when the alarm is registered in the group (if group is armed). When all groups where the LED is assigned to will be disarmed – LED will ***turns off***;
- **Zone repeater** – is activated if the selected zone is violated or faulty (except for the fire zone). When the zone is restored, the output is ***turned off***;
- **Remote LED with delay*** – LED ***blinks*** (every second) until the group arming event confirmation from CMS is not receiving **and** exit delay is not expired. The LED ***lights***, if any group where the LED was assigned to, is armed. When all groups where the LED is assigned to will be disarmed – LED will ***turns off;***
- **Remote LED with delay + alarm*** – LED ***blinks*** (every second) until the group arming event confirmation from CMS is not receiving **and** exit delay is not expired. The LED ***lights***, if any group where the LED was assigned to, is armed. LED ***blinks*** (twice per second) if the alarm event was registered while the group is armed. When all groups where the LED is assigned to will be disarmed – LED will ***turns off;***
- "**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** in seconds for each output (**except marked as ***). If the event ends before any of the parameters, the output will be turned off immediately (i.e. short events may switch off the output earlier than its time setting or don't switch it on at all). If the value is set to "0", the corresponding parameter is not used (that is, "there is no delay" or "the output works while the event is active").

If you tried to group arm while some zone 1…5 is violated the **remote LED** output will show this zone number by corresponding short flashes. If the number of flashes is 6, this means that the zone with number 6 or more is violated. If the several zones are violated, the flashes always indicate the zone with the lowest number.

If the **remote LED** output is assigned to several groups and one group will be disarmed – LED will ***turns off*** to 3 sec and then it will shows the next group's arming state.

6.6. Antenna connection

Control Panel has a built-in antenna, so prior to installation of the device in the facility it is necessary to evaluate the signal strength of the base station at the installation place. The communication shall be steady, the voice during a phone conversation shall not be echoed and distorted.

If the signal strength at the place of Control Panel installation is low, you can use an external antenna. To do this, **R63** resistor on Control Panel board (Figure 4) shall be cut with side cutters. Resistor **R63** for 3G Control Panel is placed on the PCB bottom side. Then you should connect the external antenna to **X4** connector (MMCX connector type). The external antenna with the 2.5m/5m/10m/15m cable length is available on request. The antenna cable shall be completely pulled out of the housing of Control Panel.

If you need to install several Control Panel with GSM/3G/4G modules, it is recommended to spread its remote antennas to distance of 0.5m or more from each other. The external antenna shall be located 1m from the detector with active electronic elements and at a minimum distance of 30cm from the Control Panel housing.

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

It is not recommended to install the antenna on a metal surface.

6.7. Control over false response of fire detectors

The Control Panel provides two different algorithms of fire alarm processing: after the first response or after the second response.

When "Fire after the first response" algorithm is used and alarm occurs in the fire zone, "Fire" message is immediately transmitted to CMS.

The Control Panel can recognize the fire zones false responses by set "By second fire alarm" option in the CP configuration and entering of the following parameters:

- "*Timeout for sensor reset*";
- *"Time of expectation readiness"*;
- "*Time of expectation for the repeat drawdown*".

Note: When "By second fire alarm" algorithm is used and alarm occurs in the fire zone, the Control Panel powered off the zone detectors for the period of "*Timeout for sensor reset*", while "Possible fire alarm" message is transmitted to CMS. Then the detectors are powered on, and the Control Panel is waiting for the fire sensors readiness ("*Time of expectation readiness*" option).

Then the Control Panel expects fire zone repeated alarm until *“Time of expectation for the repeat drawdown”*; and if it occurs, the “Fire” message will be sent to CMS.

All parameters described above are configured and applied to all fire zones.

The Control Panel allows to connect two detectors in one fire zone, and recognizes the response of one of the detectors or both of them (see Table 13). This option is available for “By second fire alarm” algorithm only. When it is happens, the CP sends “**Mass fire**” message to the CMS.

Note: “Recognize the second detector at the same fire loop” option applies to all fire zones.

6.8. Arming

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

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

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

2. When all zones are in a normal state, you shall touch Touch Memory key reader with the correct authorized electronic key or bring the RFID-card closer to “Lind-EM” reader – it depends of reader type used or enter the user’s regular code from the keyboard. If the key/card recognized, the reader emits a short beep. If the key/card/keyfob/code is not registered in the Control Panel's configuration, a specific sound will be played but arming will not starts.
   If only an anti-vandal TouchMemory key reader is installed to system, there are no zones status displayed, and the external LED should be used to armed mode display.

Note: 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...5. If the number of violated zone more than 5, the number of flashes will always be equal to 6.

If the “Lind-7/11TM”, “Lind-15/9M3/29”, “Lind-25/27” ICD installed then it displays zone violation by the corresponding ZONE LEDs. If the number of violated zone greater than 8/10/16 (it depends of ICD type) and you try to arming, then all ICD LEDs will flash three times and group will not arming.

If arming is carried out with “Lind-15/9M3/27/29” ICD, then instead of the key they use preliminary registered “ordinary” 4-valued digital user code. Codes of the users can be set at initial system configuration or added/changed at its subsequent operation. 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 (for “Lind-25/27/29” – group readiness LED lights up green), the arming process starts with countdown beeps (up to timeout ends). “**ARMED**” LED (“**GROUP**” for “Lind-25”, ·① or ·② for “Lind-27”, 🛡 for “Lind-29”) and remote LED begins to flash evenly (frequency ~1Hz) till arming event not sent to the CMS. At the same time, a repeated sound reminding of the need to leave the premises, will be enabled. Immediately after the “**ARMED**” LED and the remote LED start flashing, you should leave the house/object (until is not the end of the “**exit delay**” that is set in Control Panel's configuration).

Note: “**ARMED**” ICD LED displays the status of that group the ICD was assigned to.

Sensors violated for zones 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.

Note: 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. House/object has been armed.
    2. The related arming message was sent to CMS and the device received the confirmation from CMS.

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.

In this case, the following shall be checked:

1. Signal level and signal quality at the Control Panel's remote antenna installation place.
2. CMS connection configuration settings.

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 activated, when the "Delayed" or "Delayed/Instant" zones not violated while arming (timeout for exit) process **or** the "**Stay Home**" (or **A)** key was pressed before the user's password entered on "Lind-15/9M3/27/29" ICD.

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

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 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 the “entrance delay” time ends before the Control Panel disarmed then the siren will be turned on. Then touch/bring to the reader with the authorized key/card/keyfob or enter the user’s regular code from keyboard for the siren turn off.

If you use the illegal way to come into the room (for example, if the door lock failure) alarm and siren will instantly turn on. Then touch/bring to the reader with the authorized key/card/keyfob or enter the user’s regular code from keyboard for the siren turn off.

If the user “forced” password (“Lind-15/9M3/27/29”) is used to disarm, then the group disarming and the panic event will be sent 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. To ensure the correct operation of the schedule, the time synchronization must be enabled in the device – by the CMS or SNTP.

Notes:

1. Time synchronization by SNTP works only in an **open Internet** network via **GPRS/3G/4G/Ethernet/WiFi** communication channels.
2. When the Control Panel works with the “Orlan” CMS, an additional schedule in the “Phoenix” software can be used. Each schedule operates independently.

If the arming time according to the schedule coincides with the recording process during remote configuration, the arming will be delayed while the configuration is being recorded and restarting to apply the new settings.

6.12. Mobile phone control

The Control Panel **GSM** and **3G** versions supports the control maintained by calls from user mobile phones and further entering of commands using the mobile phone keypad. Each group allows for up to 8 phone numbers, which can be used to control the Control Panel. The numbers are set using “Configurator 11” software.

"Configurator 11" operation manual can be downloaded from the website: www.ortus.io.

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

To manage Control Panel from your mobile phone, you need to enable the voice channel in the device configuration.

To control the device from a mobile phone, the following shall be done:

1. Call the number of Control Panel. The device will take the incoming call only from the preprogrammed phone numbers;
2. Input ***<group number>*** on the mobile phone keypad;
3. Press ✶;
4. Input ***<command>***;
5. Press ***#***.

Next remote control commands are supported:

1 – **Arming**;

2 – **Disarming**;

3 – **Status poll** (armed – 1 tone beep, disarmed – 2 tone beeps);

5 – **Forced disarming**;

8 – **Stay Home arming**;

9 **1** **1** – **Panic**. This code can be entered while the Control Panel connection established. Don’t use the group number, no “✶” and “***#***” signs is required.

Command executing is accompanied with the beeps:

- One long beep – OK;
- Five short tone beeps (“trill”) – can't perform by any reason.

For example, group arming can't perform if any zones violated or the mobile phone number you are calling from is not assigned to this group.

Control Panel will break connection by:

- User hang up;
- 5 seconds idle timeout;
- 30 seconds global timeout (maximum communication session).

6.13. TAN bus devices operation features

TAN bus is used by the following peripheral equipment:

- “Lind-15”/“Lind-29” (touch-sensitive keypad);
- “Lind-9M3” ICD (keypad);
- “Lind-7”/“Lind-11TM” ICD (TM reader);
- “Lind-EM” RFID card/keyfob reader;
- “AM-11” address modules;
- Ethernet-Communicator LanCom23;
- Any third party TouchMemory anti-vandal key readers.

Every TAN bus device shall have its own unique address (assigned by the engineer when configuring the system). The only exceptions are the “Lind-7” ICD and anti-vandal reader, they have no address.

Note: You can connect any “Lind-7” and third-party anti-vandal TM key readers OR “Lind-EM/11TM”, “AM-11”, “Lind-15/9M3/29”, LanCom23, “Lind-25/27” ICD.

Don’t connect these devices simultaneously due to the TAN bus voltage is different for some devices (see Table 4 hardware compatibility)!

If the anti-vandal TM key reader is connected to the Control Panel while “Lind-EM/11TM” or “AM-11” or “Lind-15/9M3/29” or LanCom23 or “Lind-25/27” is configured, any touch to the reader by TouchMemory key will break down this key immediately!

Note: Built-in key reader is compatible with any external ICD, referred in section 1.

Note: Built-in EM-Marine RFID-card/keyfobs reader is compatible with any external ICD, referred in section 1.

The maximum TAN-bus (by shielded twisted pair) length is:

- “Lind-EM/11TM/15/9M3/29”, “AM-11”, LanCom23 devices are connected – up to **150m**.
- "Lind-7" / anti-vandal reader is connected and the DS1990A-F5 keys is used – up to **15m**.
- Anti-vandal reader is connected and the DS1961S-F5 keys is used – up to **5m**.

6.14. Zone expansion with “AM-11” address modules

Expansion in the number of the security system zones can be provided with “AM-11” compact address modules (Figure 6) with 3 additional zones. An example of use of the modules is shown in Figure 22.

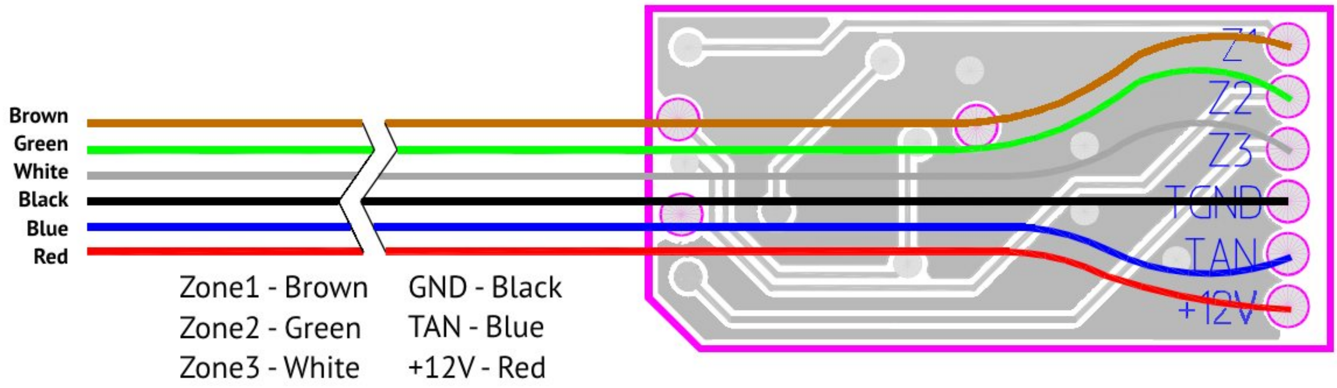


Figure 6. Appearance and functions of the hard-wired zone of “AM-11” address module

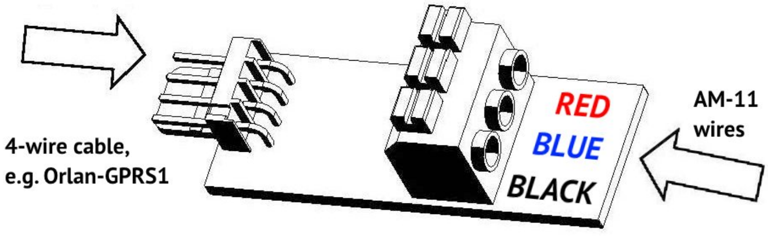
Note: “AM-11” has 3 “burglary alarm” zones of the “normally open” or “normally closed” line type. The “24-fire” zone type can’t be used.

The total wired zones count is always the same – **22**.

“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 configuring details you can see in “Configurator 11 Guide” at www.ortus.io.

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



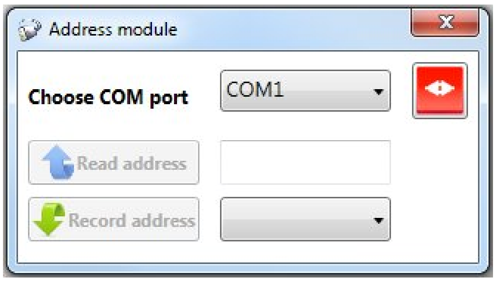


Figure 7. “Config-AM11” adapter appearance

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).

6.15. Detection of cellular signal jamming

The modem in the **GSM** and **3G** versions of the Control Panel detects cellular signal jamming automatically. Information about the signal lost is displayed on “Lind-11” ICD, and is also sent to the CMS over an available communication channel (if the check-box "**Detect GSM jamming**” set on the “**Extra**” tab in the “Configurator 11” software). In arming mode the Control Panel siren will turn on if jamming detect for more then 10s and the check-box “**Siren ON when GSM jamming**” set (on the “**Extra**” tab in the “Configurator 11” software).

7. Status LEDs

The Control Panel has some indicators as shown on Figure 4:

Blue (HL3) – modem status indicator;
Green (HL4) – indicator of operation with backup SIM (displayed with continuous light);
Red (HL1) – system status indicator;
Red (HL5) – radio system indicator.

Possible operation modes of the **modem status indicator (blue LED HL3)**:

GSM version of the Control Panel:

- **0.3s** period flashes – modem has been registered in GPRS network;
- **3s** period flashes – modem has been registered in GSM network;
- **0.8s** period flashes – modem is in the GSM network registration process;
- No light and no flashes – modem is not powered or out of service.

3G version of the Control Panel:

- Lights up – modem is in the network registration process;
- **0.4s** period flashes – data is transmitting;
- **1.6s** period flashes – modem has been registered in the network;
- No light and no flashes – modem is not powered or out of service.

4G version of the Control Panel:

- **0.25s** period flashes – data is transmitting;
- **2s** period flashes (short flashes) – modem is in the network search process;
- **2s** period flashes (long flashes) – modem is in the idle state;
- No light and no flashes – modem is not powered or out of service.

Possible operation modes of the **system status indicator (red LED HL1)**:

- Lights up – Control Panel is in configuration mode (both wired and remote), and at the start (for about 2 seconds after switching on) – works in bootloader mode;
- series of three flashes — the Control Panel is in firmware update mode (both wired and remote) —**do not turn off the power** until the update is completed;
- Long flash with a short pause – Control Panel operates in normal mode and has events that have not yet transmitted to the CMS. LED quick flashes while data is transmitting;
- Short flashes with a long pause – Control Panel operates in normal mode and all of the events have already been transferred to the CMS;
- Frequently flickers – Control Panel has no main firmware but the bootloader is working properly – you need to update the Control Panel’s main firmware (see section 12);
- No light and no flashes – Control Panel is not configured, not powered, or out of service.

Possible operation modes of **radio system indicator (red LED HL5)**:

- Blinking once per 3 seconds – all the wireless detectors in both groups have been registered, the radio system is functioning properly;
- Blinking three times with subsequent pause ~1 second – radio system is functioning properly, there are a few unregistered radio zones in any group;
- Blinking frequently – registering wireless detectors mode (see Section 9.7);
- Neither lighting nor blinking – radio system has been disabled in the Control Panel configuration;
- Lighting continuously – radio system is enabled in configuration, but the radio receiver/transmitter is not connected, so the wireless detectors registration mode is impossible.

8. Indication and Control Devices

Control Panel supports the built-in **TouchMemory key reader**, or **RFID-tags reader**, or combined TouchMemory and RFID-tags **"Lind-25"** ICD or touch-sensitive keypad **"Lind-27"** or keypad **"AK-25"** as well as the connection of additional devices:

- **"Lind-15"/"Lind-29"** ICD (touch-sensitive keypad);
- "**Lind-9M3**", "**Lind-9M4**" ICD (keypad);
- "**Lind-11TM**" or "**Lind-7**" ICD (TouchMemory key reader);
- "**Lind-EM**" RFID card reader;
- Any third party TouchMemory **anti-vandal key reader**.

Any additional ICD must be connected and used in strict accordance with its instruction manual (available at www.ortus.io).

Any additional ICD is connected to TAN expansion bus. Each device operating on the bus shall have its unique address (except the **anti-vandal key reader** and "**Lind-7**"). The address is set as described in its instruction manual. The selected address shall coincide with the address selected in "Configurator 11" software.

8.1. "AK-25"

ICD is a digital keyboard with indicators. ICD is designed as a part of the Control Panel housing (see Figure 9) and allows to display:

- The state of the **first 9 zones** of group #1;
- Group #1 **security status** and **readiness to arming**.

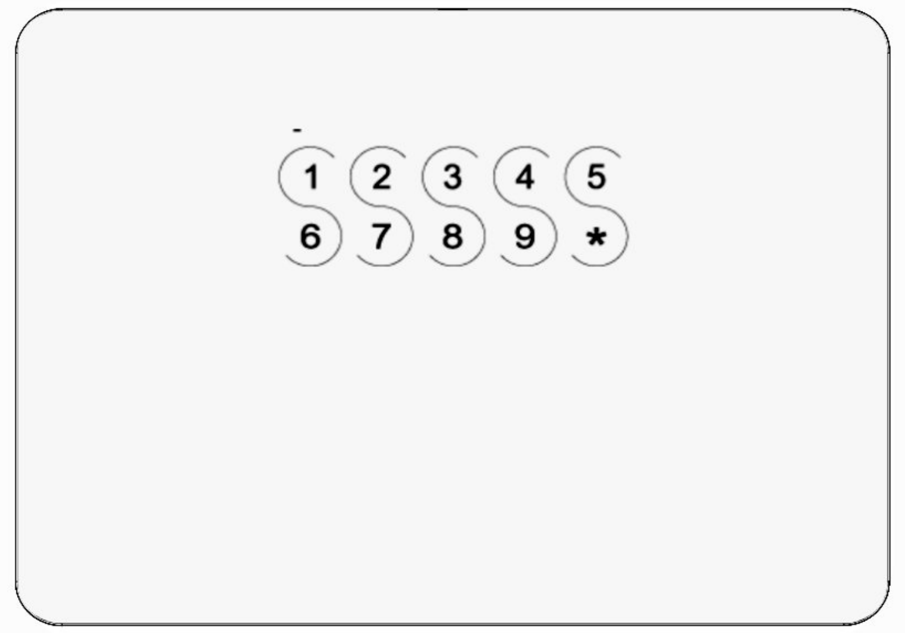


Figure 9. Control Panel appearance (model "Lun-25 Light")

ICD allows you to control the armed status of the group #1 by entering the corresponding 4-digit codes, pre-registered in the Control Panel configuration.

The ICD keyboard consists of 10 buttons and an additional indicator over the "1" button. The purpose of the buttons and their combinations is described in Table 6. Due to the lack of the "0" button on the keyboard, all user passwords should not contain a number 0. Entering the arming/disarming code is accompanied by a flashing button * .

Table 6. "AK-25" keys functions in the main mode

Key or combination	Function
1 … 9	Numeric buttons for **entering arming/disarming codes** and to display the status of the first 9 zones of the group #1. **Glows** – the zone is violated, **flashes** – the zone is faulty
*, *	Used as a "**Stay home**" button to arm the group #1 with the presence of people (press before entering the user code)
*, *, *	Change user password. Next, you need to enter an old user password, and then a new password. Each correct password is confirmed by the trill, otherwise the long monotonic signal will be sounded
*, *, *, *	Displaying the keyboard firmware version

Any keys combinations (including incomplete password input) are valid for 10 seconds and accompanied by a glowing button * *.*

The indicator displays the state of the group #1 and its readiness to arming as follows:

Indicator color and state	Group #1 arming state
Glowing in **red**	Armed
Glowing in **green**	Disarmed and ready to arm
Rare **flashes in red**	Disarmed and **not ready** to arm

8.2. "Lind-27"

ICD is a digital touch-sensitive keyboard with additional LED indicators. ICD is designed as a part of the Control Panel housing (see Figure 10) and allows to display:

- **Current group zones** state;
- **System faults**;
- Groups #1 and #2 **security status** and **readiness to arming**.

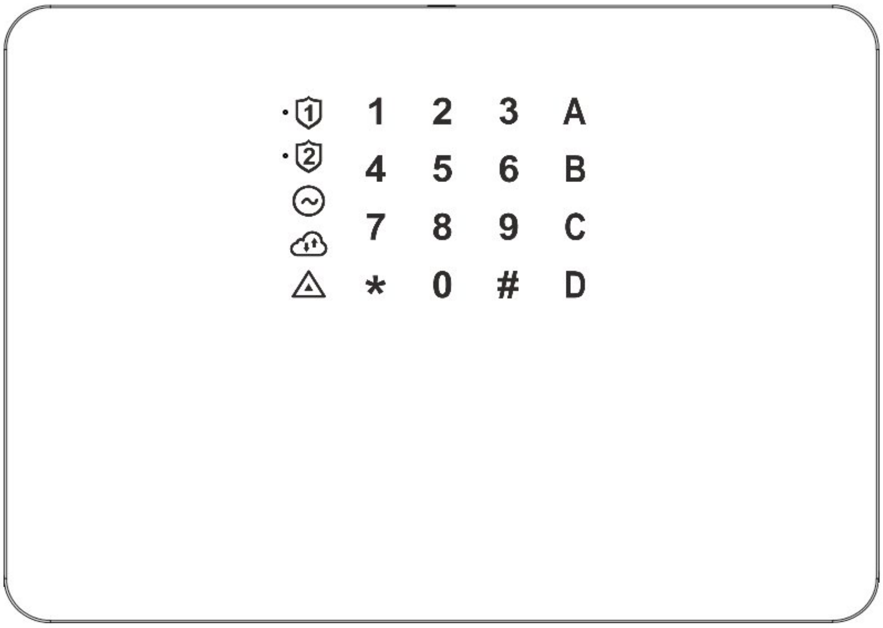


Figure 10. Control Panel appearance (model "Lun-25K")

The ICD allows to control the armed status of the both groups and reset the "fire" state by entering the corresponding 4-digit codes, pre-registered in the Control Panel configuration. Additional buttons A, B, C, D control the security status, keys and passwords management and display faults.

Built-in LED indicators (located under each key title) are used as follows (Table 7):

Table 7. "Lind-27" LEDs function

LED icon	Function
•🛡1	Security status of the correspondent group (red colour – armed, green – ready to arming, off – not ready to arming) and current group indication (by white dot)
•🛡2	
⊝ ~	Main power supply state
☁	Connection with CMS state
⚠	Presence of system faults (Table 10)
1 … 0	Violence/faults (red/yellow color) of the first 10 zones for current group

The purpose of the touch keys is as follows:

Table 8. "Lind-27" keys functions in the main mode

Key	Function
1 … 0	Numeric buttons for **entering arming/disarming codes**
*	Used as a **confirmation** button or to switch to group by command ✶, ***group_number***, ✶
#	Used as a **cancel** button or to select an additional function (section 8.2.1)
A	Used as a "**Stay home**" button to arm the current group with the presence of people (press <u>before</u> entering the user code)
B	Displays a full map of **system faults** (see Table 10). The faults is displayed by red digits 1…7
C	**Outputs control** (if output type is "*Control from CMS or by user*"). Enter the output number and confirm action (✶) to switch the output state
D	Zones state for current group is page by page, (10 zones each), page navigation: **A** (if lit then +10 to zone number), **B** (+20), **C** (+30), **D** (+40), press again to turn off (+0). **Red** digit – zone violated, **yellow** – zone fault

When the "Lind-27" ICD included to the alarm system the "Lind-7" ICD and anti-vandal key reader <u>shall not be used</u>.

8.2.1. Additional functions

ICD performs additional functions in accordance with Table 9.

Table 9. Access to advanced features

<table>
<tr><th>Keys*</th><th>Password**</th><th>Description</th></tr>
<tr><td rowspan="3">**#,3**</td><td colspan="2">**Managing "normal" user passwords and service passwords of the group**
Keys: **C** – the fire subsystem password edit.
D – the administrator password edit.</td></tr>
<tr><td>**Administrator**
(full access)</td><td>1. Enter the user's number **1...256** (while digits red flash) **or** service password select (**C** or **D**), then confirm the selection (✶).
2. The user's membership and the presence of passwords/key are displayed in red:
<table><tr><th>User is a member of</th><th>He has</th></tr><tr><td>**1** – the current group
2 – another group</td><td>**4** – an ordinary password
5 – under duress password
6 – key</td></tr></table>3. To manage a user's password, he should be a member of current group. You can:
A, (✶) – delete the user's password.
B, (✶) – edit the user's password.
D, (✶) – include/exclude user to current group. If he is already in another group, then enter his password or attach his key to the reader.
4. To edit password – enter a new user (or service) password while all digits blink green.
5. To exit the current password to step 1, press (**#**). Press (**#**) again to exit mode.</td></tr>
<tr><td>**User**
(user password editing only)</td><td>1. Enter a new user password while all digits flash green. Then the mode will exit.</td></tr>
<tr><td>**#,4**</td><td>**Administrator**
(full access)
or
User
(current user password editing only)</td><td>**Managing "under duress" user passwords and service passwords of the group**
Actions and indications are similar to the previous function (**#,3**).</td></tr>
<tr><td>**#,5**</td><td>**Fire subsystem**</td><td>**Management of the fire subsystem** Exit mode – automatic
A – turn on the fire alarm siren.
B – turn off the fire alarm siren.
C – fire reset.</td></tr>
<tr><td>**#,6**</td><td>**Administrator**</td><td>**User key management**
Actions and indications are similar to the function (**#, 3**).</td></tr>
</table>

Keys*	Password**	Description
#,7	**Installer**	**Radio devices enrolling** Press (**#**) to exit Indication: **Red** digits – cells already occupied with radio devices in the group. **Green** digits – cells that are free for enrolling radio devices. Keys: **A**, **B** – to switch pages (if lit, then **A**= +10, **B**= +20 to the radio devices number, press again to turn off = +0). **D** – to select the type of radio devices (**off** – sensors, **green** – sirens, **red** – outputs). 1. Select the radio devices type for enrolling (**D**). 2. Select the page (**A**, **B**) and the cell number on the page by digits (it will blink), then confirm the selection (✶). **Red numbers** – the signal level from the device enrolled in the current cell. 3. Select the action for the radio device and confirm it (✶): **A** – delete existing enrolled device. **B** – initiate enrolling into the current cell. 4. An enrolling signal is expected while the numeric keys are flashing. 5. To exit the current cell to step 2 – press (**#**).
#,8	**User**	**Zone bypass control** Press (**#**) to exit 1. **Red** number – this zone is bypassed. **A**, **B**, **C**, **D** – page switching (if lit, then **A**= +10, **B**= +20, **C**= +30, **D**= +40 to the zone number, press again to turn off = +0). 2. Select the page (**A**, **B**, **C**, **D**) and the zone number on the page with digits (flashes), then press (✶) to change the bypass state (on/off).
#,9	**---** (not required)	**Doorbell control** Press (**#**) to exit Indication by flashing digital keys: **red** – on; **green** – off. Buttons: **A** – **on** / **off** (the color of the button corresponds to the current state). 1. Switch the door bell (**A**) on or off.
#,0	**---** (not required)	**Additional Information** Press (**#**) to exit 1. Press key to information (version displays in binary code: 1 – LSB, 8 – HSB): **A** – "Lind-27" firmware version, switches: **Green** digits – the main firmware, **Red** digits – the boot loader. **B** – "Lun-25" firmware version, switches: **Green** digits – the main firmware. **Red** digits – the boot loader. **C** – GSM(3G) / WiFi signal strength, switches: **Green** digits – GSM/3G, **Red** digits – WiFi. **D** – test of indication (all LEDs and sound turn on for 10s).
** – the symbol “,” means the buttons should be pressed one by one, don't hold them* *** – Password should be entered immediately after pressing the mode keys – while all the numeric keys are flashing.*		

The firmware is updated via the **Lun-Config** cable (**XP2** connector) or remotely.

8.3. “Lind-25”

ICD has been designed to build-in to the Control Panel housing (see Figure 1) and allows displaying as follows:

- State of the **first 10 zones** of the **group #1 or/and group #2 (configurable)**;
- System **faults**;
- **Arming state** of groups #1 and #2.

ICD is made in two modifications:

1. Only the TouchMemory key reader is installed (for "**Lun-25TE**");
2. TouchMemory key reader and EM-Marine RFID-tag reader are installed (for “**Lun-25TE+**”).

ICD can to manage the arming status and reset the “fire” state by EM-Marine RFID-cards (125 kHz frequency, at distance of 3...8 cm), as well as TouchMemory keys.

If the “Lind-25” ICD is a part of the alarm system, the “Lind-7” ICD and anti-vandal key reader <u>shall not be used</u>.

Both readers are placed under the CP front panel.

On their left, there are two-color ZONE 1...10 LEDs. In the normal state, the indicators do not light. In case of violation of any of the first 10 zones (for the first or/and second group), the appropriate indicator of the zone **lights up red**, in case of the zone fault, it **lights up yellow**.

If the ICD connection to Control Panel faults, the ZONE LEDs displays of **“running fire” in yellow color**.

There are two arming state LEDs “GROUP” above the reader. This LEDs operates as follows:

- **Not lighting** – group has been disarmed or not used;
- **Lighting green** – group has been disarmed and ready for arming;
- **Blinking red** – group has been armed, the appropriate event is transmitted to CMS, but confirmation of arming has not been received yet;
- **Lighting red** – group armed.

System faults LEDs are rightwards of the reader:

AC POWER	<u>**Lighting,**</u> if the main power supply available; <u>Switched off,</u> if the main power supply fail
BATTERY	<u>**Lighting**</u>, if the battery is fault-free and charged <u>Switched off</u>, if the battery is not available, failed or discharged
WIRELESS	<u>**Lighting**</u>, if wireless system is operating properly or switched off; <u>Switched off</u>, if wireless system is failed or its communication is lost
SYSTEM	<u>***Blinking every 2 seconds***</u>, if **no system faults** have been found; <u>*Blinking twice per second*</u>, if **there are** any system faults (see below)

To display any available system faults with **zones LEDs in yellow color**, press and hold down the “**TROUBLE**” key (up to 10 seconds). The faults list shows in Table 10.

For arming groups, use a key/card/RFID tag pre-registered in the Control Panel configuration in one or both groups.

If the key/card/RFID-tag is registered in the one group only, then it controls the security status of the corresponding group.

If the key/card/RFID-tag is registered in both groups, it controls the security status of both groups as follows:

Groups 1/2 (or 2/1) status before the key/card/RFID-tag used	Arming status after the key/card/RFID-tag used	
🟢 🟢	🔴 🔴	
⚫ 🟢	⚫ 🔴	
🟢 🔴	🟢 🟢	The glow of green depends on the group's readiness to arming
🔴 🔴	🟢 🟢	

If it is not possible to arm a group due to a zone violation and this zone number greater then 10, all zone indicators flash three times.

ICD supports the local firmware updating by "Lun-Config" cable, being connected to **XP2** connector, located on the PCB back side. The "Configurator 11" software is used for firmware update. This software is available to download at www.ortus.io web site.

ICD also supports remote firmware updating as part of the security system.

When the "**TROUBLE**" button is held for a long time (more than 10 seconds), the zone LEDs display the current version of the ICD firmware in binary code:

- **ZONE1...5** – the main software version (**ZONE1** indicator is the least significant bit);
- **ZONE6...10** – bootloader version (**ZONE6** indicator is the least significant bit).

Table 10. System faults are displayed on the "Lind-25/27" ICD

Zone LED	System failure displays while the "TROUBLE" button hold
ZONE1	Main power lost
ZONE2	The battery absence/failure/discharge
ZONE3	CMS connection lost
ZONE4	"AM-11" connection lost (one or more)
ZONE5	Arming forbidden (set from the CMS)
ZONE6	Radio receiver connection lost
ZONE7	WiFi module connection lost
ZONE8	Tamper alarm in any device

8.4. Anti-vandal TouchMemory key reader

Control Panel supports the connection of any standard or third party anti-vandal TouchMemory key reader. With this reader you can arm/disarm any Control Panel's group and reset a fire alarm.

Note: Anti-vandal TouchMemory key reader arm/disarm the group to which be touching key assigned.

The reader connects to the TAN bus, for more details see Section 6.13.

If the anti-vandal TouchMemory key reader is a part of the alarm system, the "Lind-EM/11TM", "Lind-15/9M3", "Lind-25/27" ICD and "AM-11" address modules shall not be used.

8.5. Build-in readers

Depending on the model, on the front panel of the main unit can be installed TouchMemory key reader or contactless RFID-cards reader (“Lind-23E”, see Section 1).

Built-in readers are compatible with any plug-in to TAN bus equipment, they always turn on and do not require any configuration settings as an additional devices.

Any of built-in readers can arm and disarm of any Control Panel's group by the registered key.

Note: Build-in reader arms and disarms group to which key is assigned.

Note: The built-in reader's LED assigned to the first Control Panel's group only.

Built-in reader has a multicolored LED for Control Panel's first group status indication as follows:

- **Lit green** – group №1 disarmed, ready for arming;
- **Off** – group №1 disarmed, some zones violated. Rare red dim flashes indicate that Control Panel and reader are working;
- **Flashing yellow flashes every 3 seconds** – group №1 disarmed, **there are some system faults**;
- Evenly flashes red about every seconds – group №1 armed and this event is sent to the CMS now;
- **Lit red with yellow flashes every 3 seconds** – group №1 armed, **there are some system faults**;
- **Lit red** – group №1 armed, **there are no system faults**.

Each built-in reader responds to the following **system faults**:

- Main power lost;
- Battery absence/failure/discharge;
- GSM channel failure / CMS communication loss.

8.6. Encrypted keys

The antivandal key reader and the Lun-25T built-in reader supports the ordinary TouchMemory keys (DS1990A-F5) or encrypted keys (DS1961S-F5). If the encrypted keys is used then the “**Encrypted keys**” checkbox should be set in the Control Panel configuration (for the group where this keys are used), and the “**Encrypted keys secret**” parameter should be entered.

Encrypted keys should be pre-programmed with the appropriate “secret” and then registered in the Control Panel with the same “secret”.

Note: Arming/disarming with an encrypted key will be performed to groups where it is assigned (regardless of the group’s “**Encrypted keys**” box status).

If the ordinary key is assigned to some groups and at least one of them has the “**Encrypted keys**” checkbox is set, then none of the groups will be armed/disarmed (it includes groups where this check box is clear).

9. Wireless subsystem

9.1. General information

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

Table 11. 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 CP housing, 16
Rielta	■“Lun RKI v3” (with “Ajax RR108-Lun11 Adapter” cable)	433	ORTUS Group	Inside the CP housing, 14
	■or “L25_R433”			Inside the CP housing, 12
Crow	“L25−CROW rev.3” adapter	868		Inside the CP housing, 13
	“L25−CROW B” adapter			Outside the CP housing
ORTUS	“Lun-R”	433		Inside the CP housing, 11
	“Lun-R 868”	868		

First specify the type of the installed radio receiver in Control Panel configuration, number of wireless zones and their type with grouping by means of “Configurator 11” software.

Further, mount the radio receiver in the Control Panel housing in the way it is shown in the appropriate figures (see Table 11), then connect the radio receiver to **X5** (**RADIO**) connector on Control Panel PCB.

And finally, after the Control Panel turning on in the operating mode (i.e. on disconnecting from the computer), register wireless detectors in the zones 23…52, using the key **RF** on Control Panel PCB or with the “Lind-15/9M3/27/29” ICD.

Note: All the wireless detectors used in one Control Panel shall be of the same product range of the same manufacturer and operate in the same frequency band as the radio receiver.

Types of the supported wireless detectors for each used radio system, the main features of Control Panel operation with them and procedure of their registration are stated in Section 23.

9.2. “Lun-R”/“Lun-R 868” radio receiver

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

Module is installed in housing under Control Panel, as shown in Figure 11. Then it should be connected via its own cable to **X5 (RADIO)** connector on the Control Panel board.

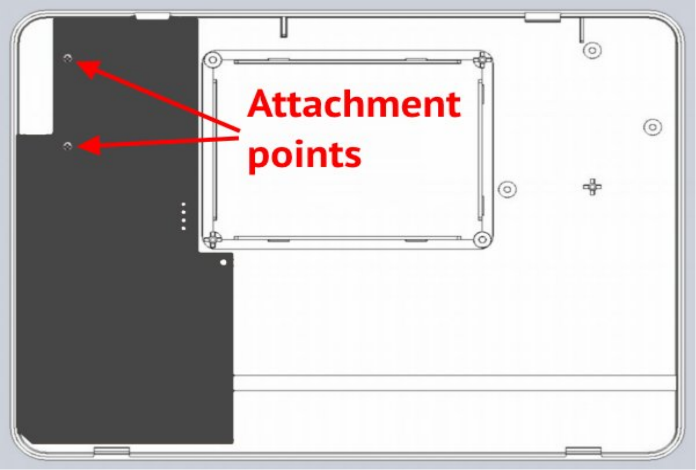


Figure 11."Lun-R" radio receiver in the CP housing

9.3. “L25_R433” radio receiver

L25_R433 radio receiver allows to connect of **Rielta** wireless sensors/keyfobs.

Module is installed in housing under Control Panel, as shown in Figure 12 (to do this, two destructive housing elements shall be broken out previously). Then it is connected via its own cable to **X5 (RADIO)** connector on the Control Panel board.

The module has two LEDs:

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

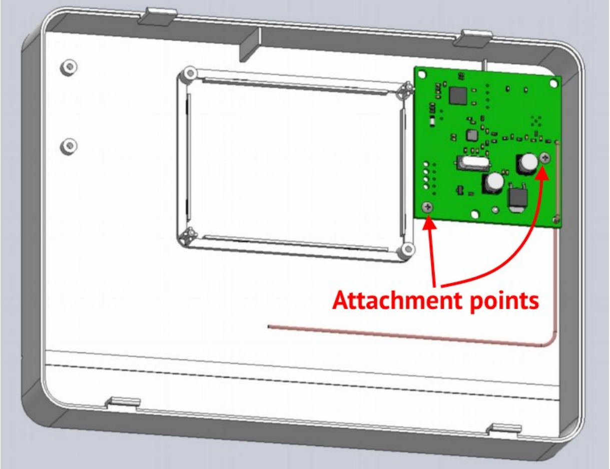


Figure 12. "L25-R433" series radio receivers in the CP housing

9.4. Crow radio receiver

To provide the operation of Control Panel with the wireless detectors and wireless sirens Crow, you should install one of the radio receivers and connect it to the **X5 (RADIO)** CP connector:

- "**Adapter L25-CROW rev.3**" – inside the Control Panel housing, as shown in Figure 13;
- "**Adapter L25-CROW B**" – 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 23. The cable free side can be cut for better installation.

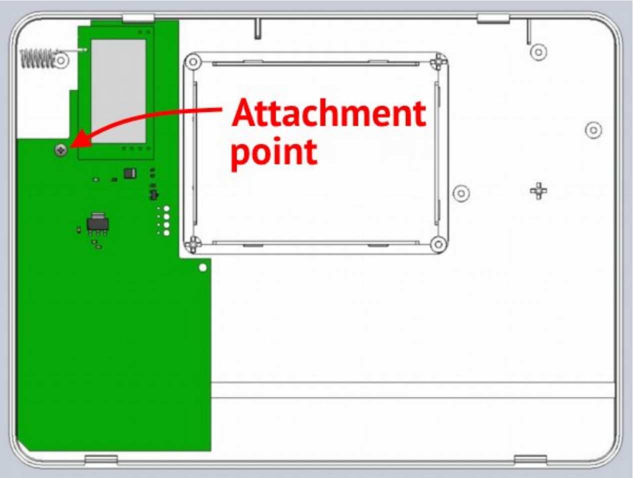


Figure 13. Radio module
"Adapter L25-Crow rev.3" inside the CP housing

9.5. Rielta radio receiver

To provide the operation of Control Panel with the wireless detectors and wireless sirens Rielta, you should install one of the radio receivers and connect it to the **X5 (RADIO)** CP connector:

- "**Lun RKI v3**" – inside the Control Panel housing, as shown in Figure 13. It connected by "Ajax RR108-Lun11 Adapter" cable. Only wireless devices are made on the red PCB can operate with this receiver;
- "**L25-433**" – is placed inside the Control Panel housing as described in Section 9.3.

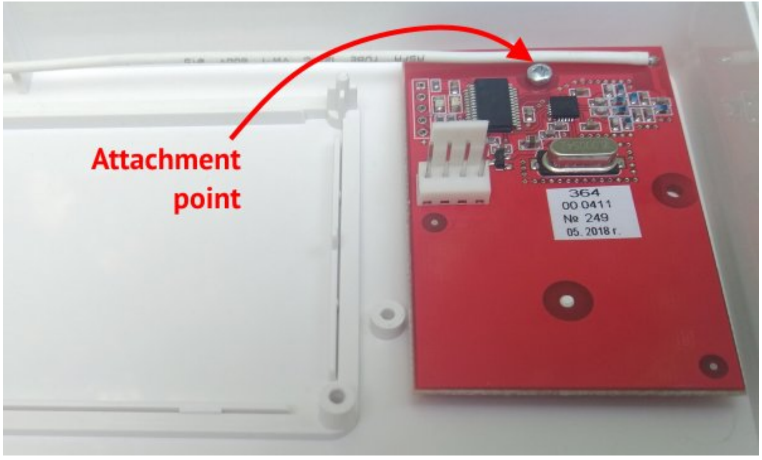


Figure 14."Lun RKI v3" radio receiver in the CP housing

9.6. Ajax radio receiver

To provide the operation of Control Panel with wireless detectors Ajax install the "Ajax uart-Bridge" radio receiver shall be installed (Figure 16). Then connect it to **X5 (RADIO)** connector on the Control Panel PCB with cable «Adapter Ajax RR108-Lun11» manufactured by ORTUS Group. Before installing the radio receiver, break off its parts marked in Figure 15 along the lines formed by the drilling holes. Discard broken parts of the radio receiver.

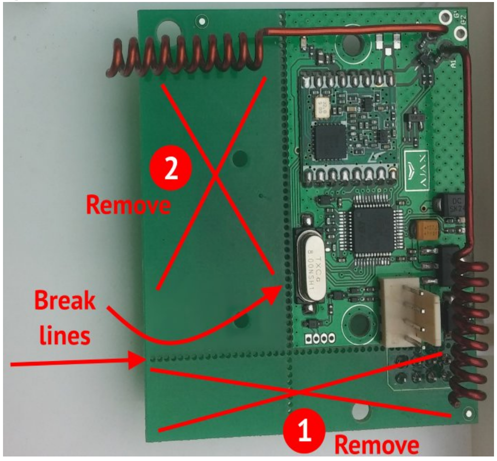


Figure 15. "Ajax uartBridge" preparation

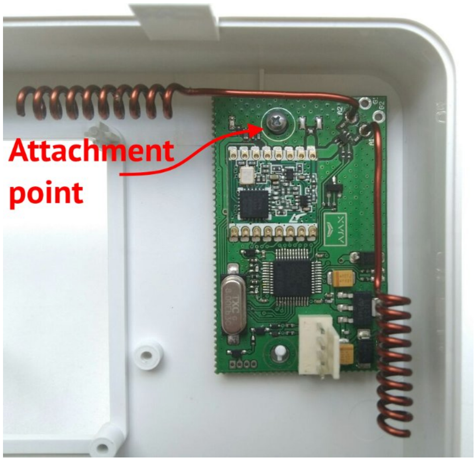


Figure 16. "Ajax uartBridge" radio receiver in the CP housing

9.7. Wireless detectors/sirens enrolling

Prior to enrolling be sure the type of radio system, number and type of wireless zones is specified in the Control Panel configuration by "Configurator 11" software.

Note: Prior to enrolling be sure the group (partition) is disarmed.

Note: Enrolling of wireless detectors is performed by ICD "Lind-15" / "Lind-9M3" / "Lind-27" or the **RF** (**SW3**) key (it placed on the Control Panel PCB, see Figure 4). To access to the key you need to open Control Panel housing with a special tool.

For enrolling of wireless detectors, the Control Panel should be in the operating mode with the radio receiver connected.

An indication of radio system status is carried out with LED **HL5** as follows:

In the Control Panel normal operating mode:

- **Neither lighting nor blinking** – radio system is switched off in Control Panel configuration, it is impossible to switch to the wireless detectors enrolling mode;
- **Lighting continuously** – radio system is switched on, but there is no connection with radio receiver or he is not connected, it is impossible to switch to the wireless detectors enrolling mode;
- **Blinking three times with subsequent pause ~1 second** – there are some non enrolled wireless zones in someone group;
- **Blinking once 3 seconds** – all the wireless detectors are enrolled in both groups, radio system works properly.

In the enrolling mode with **RF** key:

- **Blinking once with subsequent pause ~1 second** – Control Panel in enrolling mode for the first group, there are some free radio zones;
- **Blinking twice with subsequent pause ~1 second** – Control Panel in enrolling mode for the second group, there are some free radio zones;
- **Lighting ~3 seconds with pause ~0,5 seconds** – Control Panel in the enrolling mode, there are not any free radio zones in the current group (partition);
- **Blinking fast uniformly with frequency ~3 times per second** – enrolling signal waiting from wireless detector;

Switch to the enrolling mode with **RF** key is carried out with as follows:

- Fast **double** pressing the **RF** key – for the **group #1**;
- Fast **triple** pressing the **RF** key – for the **group #2**.

In this mode you can do as follows:

- *By single short pressing* the **RF** key – **start enrolling** to the next free wireless zone of the current group within ~30 seconds;
- *By long (~3 seconds) pressing* the **RF** key – **delete all enrolled** wireless detectors in this group –i.e. make free all the wireless zones of the group;
- *By fast double pressing* the **RF** key – **exit from the enrolling mode** and return to the operating mode.

Note: Enrolling the wireless detectors is performed subsequently, into the free wireless zone, by ascending numbers. Only one wireless detector must be turned on – the one that is currently being enrolled. After enrolling the current wireless detector, it should be turned off again until the enrolling of all wireless detectors in the Control Panel is completed.

The Control Panel waits for the next **RF** key pressing within ~3 minutes in the enrolling mode. The longer pause leads to the automatic exit to the operating mode with warning long sound.

If the enrolling is successful, it confirmed with “trill” sound.

Note: If some wireless detectors was enrolling/deletion, the Control Panel shall be automatically rebooted to apply it.

Wireless detectors/sirens enrolling sequence by the “Lind-9M3”/“Lind-15” ICD is described in its operating manual, available to download at site www.ortus.io. For “Lind-27” ICD this sequence is described in Section 8.2.

After enrolling is completed and Control Panel is rebooted, the wireless detectors should be checked by its violation/recovery events occurring.

When the wireless sensors is installed, be sure to evaluate the received signal level from each of them (it displayed by the “Lind-9M3/15/27/29” ICD). If the signal level is low (0…1), the radio communication with the wireless sensors may be interrupted, so the events and/or reports of malfunctions of wireless sensors may be lost. To increase the signal level, you can change the relative position of the wireless sensor and the radio receiver, or use the appropriate repeater.

10. Additional communication channels

Control Panel supports one of the additional communication channels – Ethernet or WiFi.

10.1. Ethernet communication channel

Ethernet communication can be used as an additional channel of communication to the CMS by the communicator **LanCom rev.14** or **LanCom23** or **LanCom25**.

Communicators **LanCom rev.14** and **LanCom23** are placed in a separate case, and can be mounted in a convenient place for installation – for example, near a router or behind a false ceiling of an office room – and then connected to the Control Panel via the TAN bus.

General connection requirements for **LanCom rev.14** and **LanCom23** are described in section 6.13. The connection diagram is shown on Figure 21.

Communicator **LanCom25** is placed as daughter board (figure 19) instead of WiFi module “W25M” (section 10.2).

Only one Ethernet communicator can be connected to the Control Panel.

The communicator sends all events, tests and control signals to/from the CMS via the “open Internet” communication channel.

10.2. WiFi communication channel

Wireless communication can be used as an additional channel of communication with the CMS. Communication through this channel provides an additional module “W25M”.

Module “W25M” (see Figure 17) 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 2.4GHz 802.11b/g/n with protection according to the WPA2 PSK.

Control Panel with “W25M” module will communicate with 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.

The **X12 (Wi-Fi)** connector is used to connect this module – see Figures 4, 18).

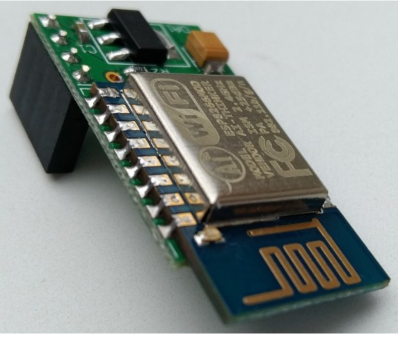


Figure 17. Module "W25M"

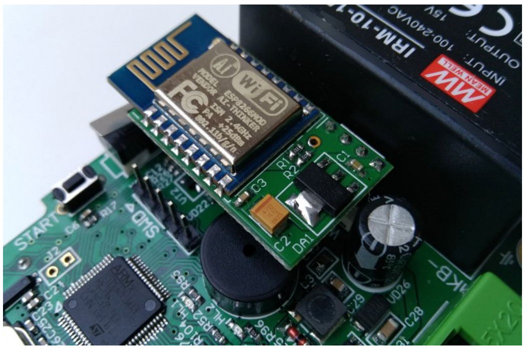


Figure 18. Installation of WiFi module

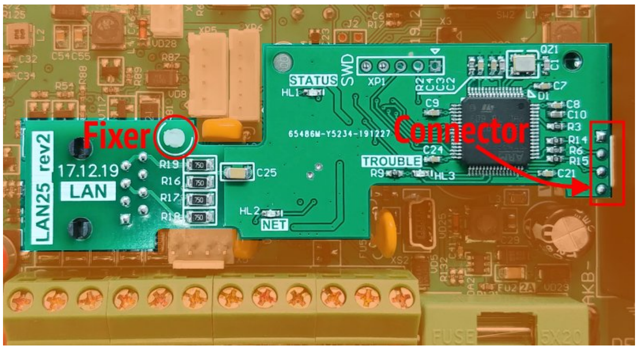


Figure 19. Installation of "LanCom25" module

11. 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 miniUSB cable.

You should use **XS2** connector (see Figure 4) on the Control Panel PCB for configuring. The details of connection and configuring process can be found in "Configurator 11" Guide" available at www.ortus.io.

Note: "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 "Lun USB" cable, the further configuring of the device installed at the facility shall be carried out remotely using GPRS/3G/4G/Ethernet/WiFi channel (this channel shall be activated and configured previously).

For the remote Control Panel configuration, the same program "Configurator 11" is used.

12. Firmware update

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

Control Panel supports firmware update locally (performed by "Lun USB" cable, plug-in as described in Section 11), or remotely (performed via GPRS/3G/4G/Ethernet/WiFi connection).

"Configurator 11" software commands are used for local updating.

Remote firmware update is performed by "Phoenix" software (by command of CMS operator). The main power and battery are required and all Control Panel's groups should be disarmed to remote firmware update.

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 – by the CMS operator command or locally – by 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.

13. Remote control

The remote control is available from CMS using "Phoenix" software, as well as from a mobile phone (from the preconfigured numbers).

Control Panel supports remote control via mobile application "Phoenix-MK" (GPRS or WiFi channel should be turn on). "Phoenix-MK" is available for devices on Android OS and iOS.

14. Battery monitoring

The battery monitoring function in Control Panel is enabled by default and runs automatically.

15. Main power supply monitoring

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

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

16. Maintenance

The Control Panel does not require any maintenance.

17. Operating conditions

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

18. Storage

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

19. Transportation

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

20. Disposal

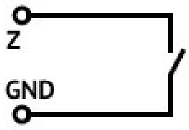
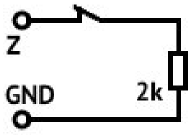
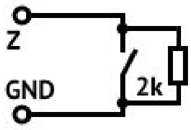
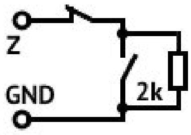
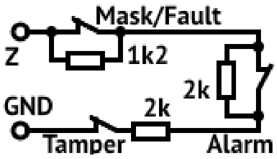
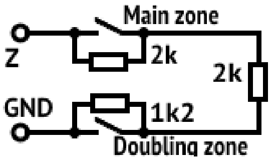
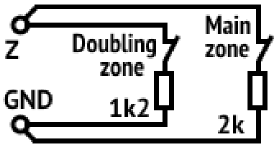
Product disposal shall be carried out according to electronic household appliance disposal rules established by the legislation of the State, where the product is operated.

21. 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”.

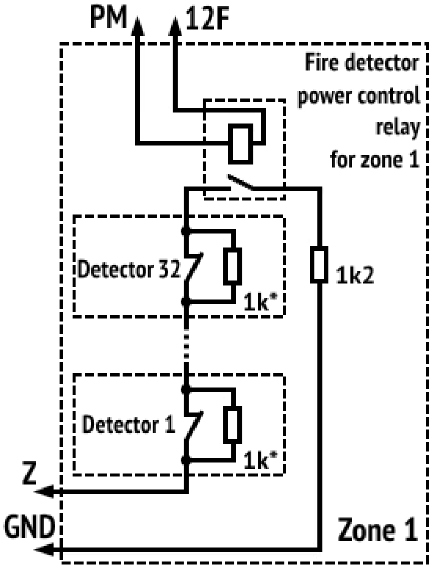
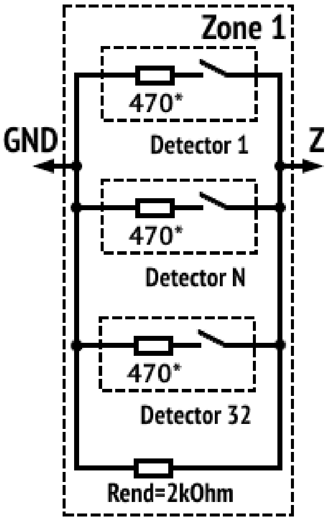
See the types of protective zones and events generated in case of their violation, in Table 12.

Table 12. Burglary zones types

Connection circuit	Short circuit-generated event	Disconnection-generated event
1. Zone type – “Normally open”		
	**alarm**	norm
2. Zone type – “Termination resistor, alarm upon disconnection”		
	*zone fault*	**alarm**
3. Zone type – “Termination resistor, alarm upon short circuit”		
	**alarm**	*zone fault*
4. Zone type – “Termination resistor, alarm upon disconnection and short circuit”		
	**alarm**	**alarm**
5. Zone type – “Triple termination resistor”		
 Mask/Fault Z 1k2 2k GND 2k Tamper Alarm	norm	**Burglary alarm** (**Alarm** contacts) **Tamper alarm** (**Tamper** contacts) **Fault** (**Fault** contacts)
6. Zone type – “Normally open line (with doubling)”		
	**alarm**	norm
7. Zone type – “Normally closed line (with doubling)”		
	*both zones fault*	**alarm**

Fire zones types and events generated in case of their violation, shown in Table 13.

Table 13. Fire zones types

Connection circuit	Short circuit-generated event	Disconnection-generated event
5. Zone type – "Normally closed, 2 resistors" (example of 4-wires connection scheme; the PM output should be set as "Fire sensor supply")		
 PM 12F Fire detector power control relay for zone 1 Detector 32 1k* 1k2 Detector 1 1k* Z GND Zone 1 * – *To recognize second detector in the zone, the resistance of the additional resistor for each detector should be* ***1 kOhm***	*zone fault*	*zone fault*
	detector circuit break – alarm	
6. Zone type – "Normally open, 2 resistors" (example of 2-wires connection scheme)		
 Zone 1 470* Detector 1 GND Z 470* Detector N 470* Detector 32 Rend=2kOhm * – *To recognize second detector in the zone, the resistance of the additional resistor for each detector should be* ***820 Ohm***	*zone fault*	*zone fault*
	closing of detector circuit – alarm	

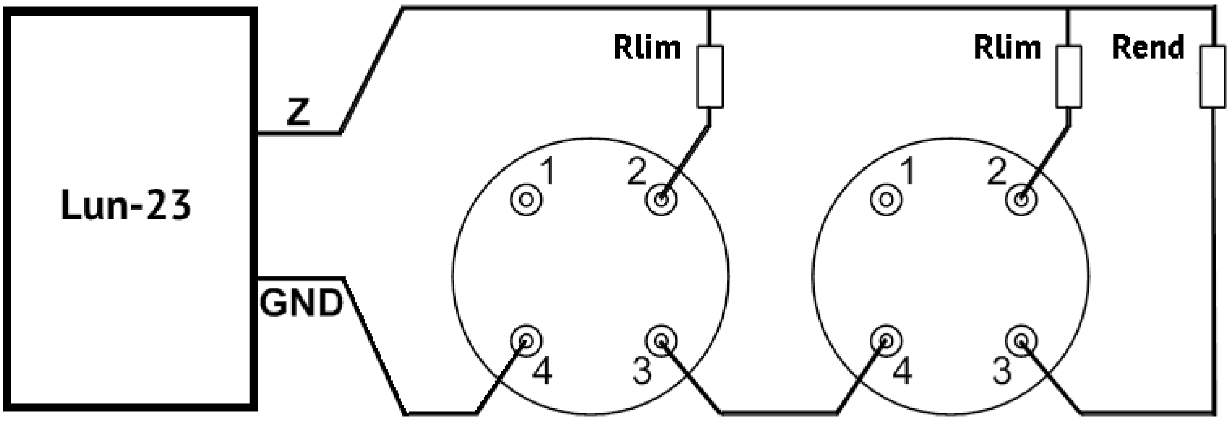


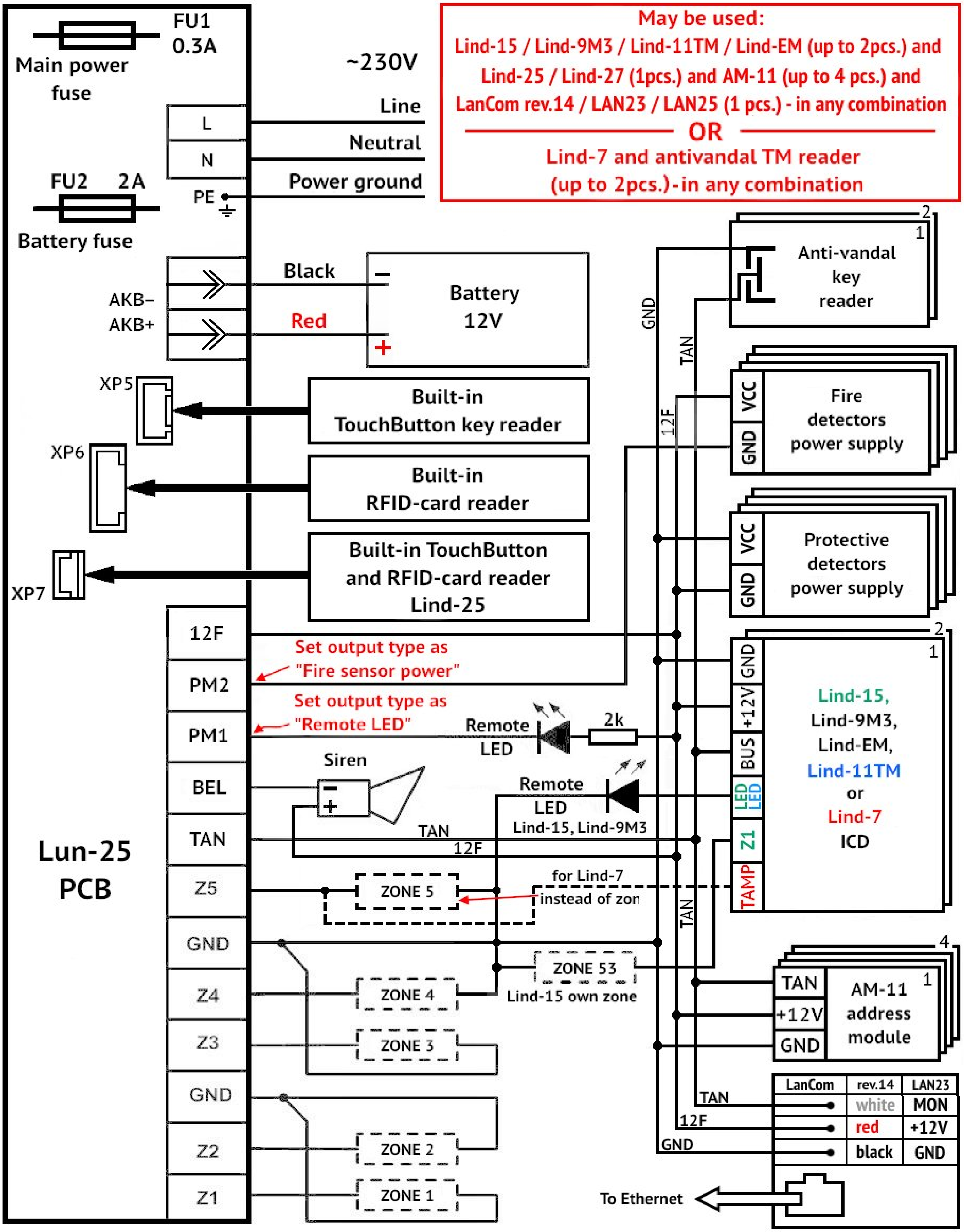
Figure 20. Fire zone two-wire circuit detectors connection diagram

Table 14. An example of Rlim calculation

Detector type	Rlim nominal value
IPK-8	200 Ohm
SPD-3	470 Ohm
Any other fire detector	**Rlim** is calculated by the formula: **Rlim=800 Ohm – Rfire** (for **one** detector fire alarm recognizing), or **Rlim=1150 Ohm – Rfire** (for **two** detectors fire alarms recognizing), where **Rfire** is the detector resistance in the “Fire” state, Ohm

22. Appendix 2. 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.



May be used:
Lind-15 / Lind-9M3 / Lind-11TM / Lind-EM (up to 2pcs.) and
Lind-25 / Lind-27 (1pcs.) and AM-11 (up to 4 pcs.) and
LanCom rev.14 / LAN23 / LAN25 (1 pcs.) - in any combination
OR
Lind-7 and antivandal TM reader
(up to 2pcs.)-in any combination

LanCom	rev.14	LAN23
	white	MON
	red	+12V
	black	GND

Figure 21. Control Panel connection diagram

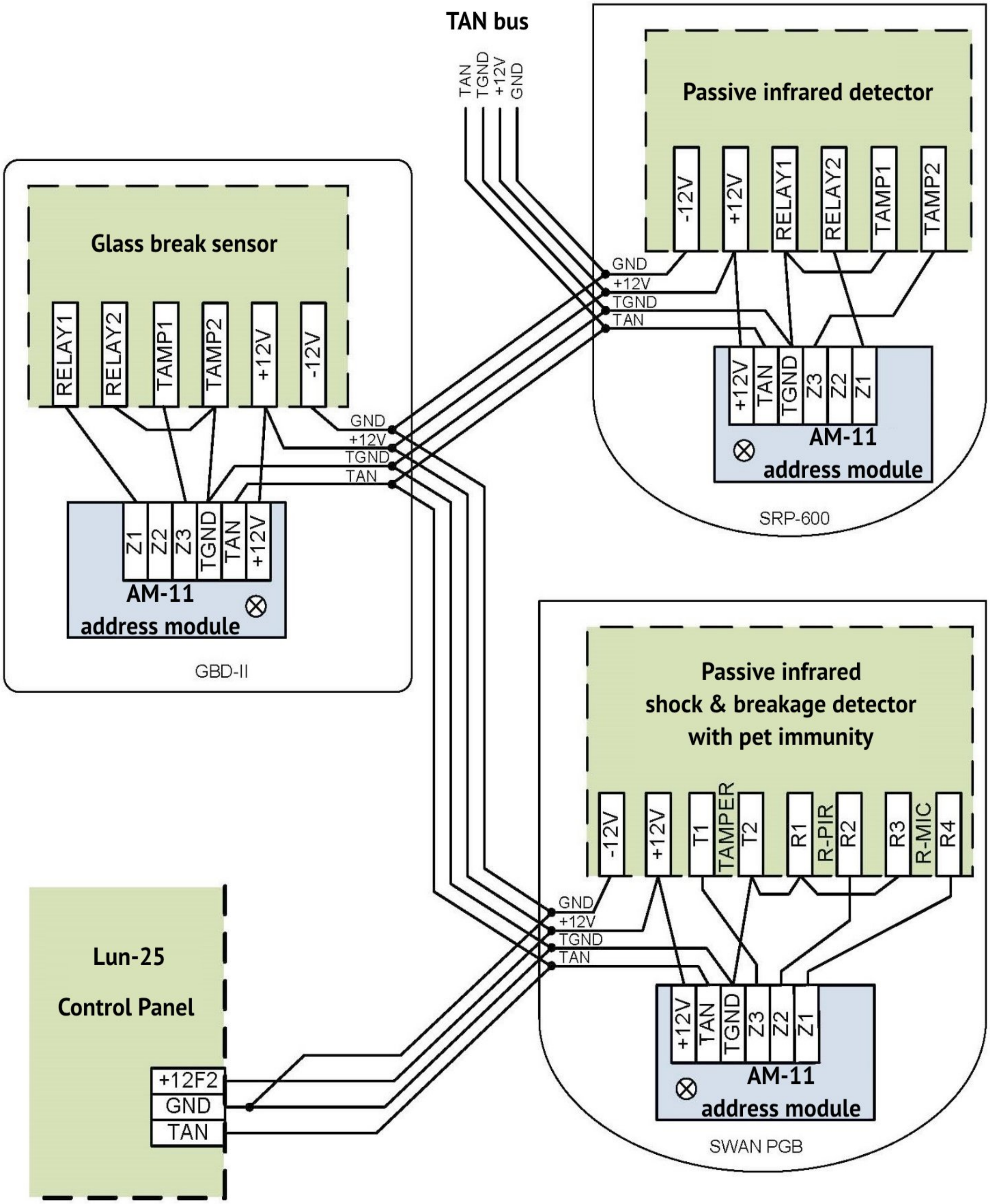


Figure 22. An example of "AM-11" address modules using

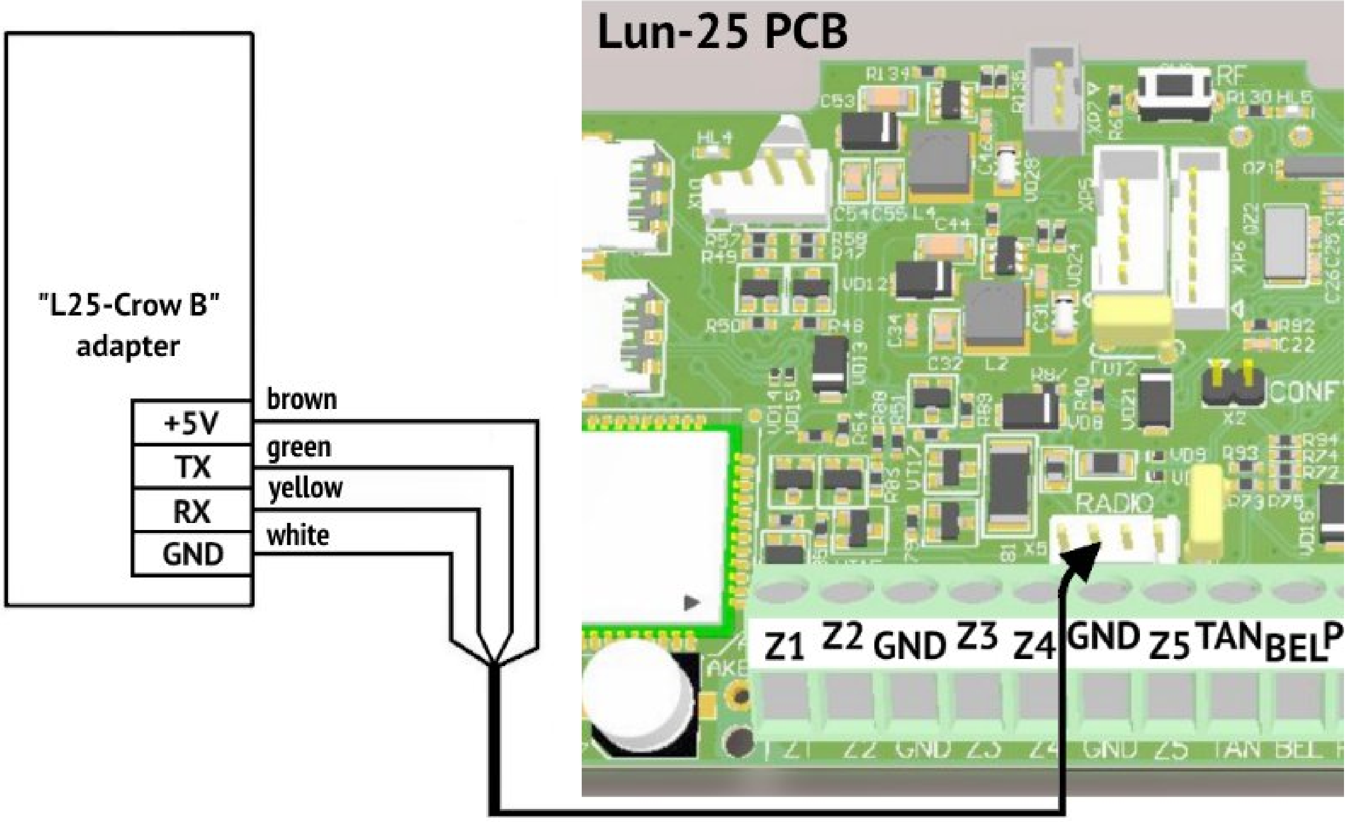


Figure 23. Adapter "L25-Crow B" connection diagram

23. Appendix 3. Wireless devices handling

23.1. “Lun-R”

The Control Panel can operate with the following ORTUS wireless devices:

- “**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;
- “**Relay-R**” – Controlled relay;
- “**Siren-R**” – Indoor siren.

You should set the receiver type as “**Lun-R**” in the Control Panel configuration.

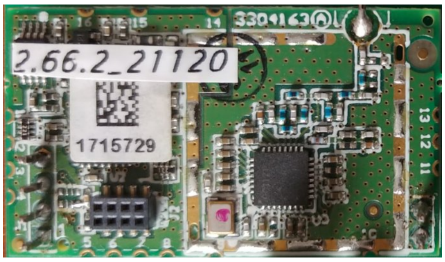
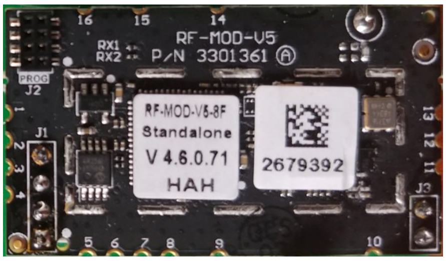
To register (bind) one ORTUS wireless device the following shall be done:

- Remove battery from the wireless device;
- Enter the registration mode of wireless devices of the desired group (see Section 9.7). If LED **HL5** is <u>blinking non-uniformly</u> (fast once/twice then pause ~1 second), it means the current group has free wireless zone and you can start wireless device registration by the **RF (SW3)** button short press. The **HL5** LED starts blinking fast while waiting for registration signal from wireless device.
- If there are no free radio zones in the group you choose, then **HL5** LED will be <u>lighting through short intervals</u> in the registration mode – so you should delete <u>all</u> the wireless devices in this group with long pressing the button **RF (SW3)** <u>or</u> by clear “**Sensor ID**” field for the <u>desired</u> wireless zone in the “Configurator 11” software. Be sure a successful delete by built-in buzzer sound “trill”;
- 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.
- Visually monitor the wireless device binding by sound signal “trill” of the built-in buzzer. If Control Panel has not received binding signal from device within 40 seconds, then it exits from the binding signal waiting mode with the long sound signal.

23.2. Crow

Depending on the installed Crow module, the Control Panel supports of the following Crow wireless devices (see Table 15):

Table 15. Crow wireless devices

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

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

To register (bind) one Crow wireless detector by RF (SW3) key:

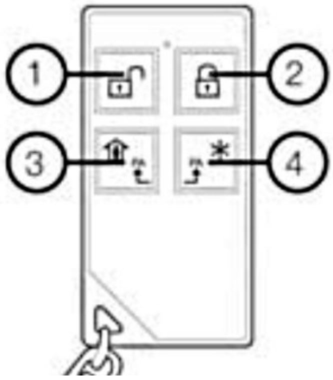


Figure 24. Keyfob Crow FW2-RMT-8F

- Remove the power supply unit from the wireless detector;
- Enter the registration mode of wireless detectors of the desired group (see Section 9.7). If LED **HL5** is <u>blinking non-uniformly</u> (fast once/twice then pause ~1 second), it means the current group has free wireless zone and you can start wireless detector registration by the **RF (SW3)** button short press. The **HL5** LED starts blinking fast while waiting for registration signal from wireless detector.
- If there are no free radio zones in the group you choose, then **HL5** LED will be <u>lighting through short intervals</u> in the registration mode – so you should delete <u>all</u> the wireless detectors in this group with long pressing the button **RF (SW3)** <u>or</u> by clear "**Sensor ID**" field for the <u>desired</u> wireless zone in the "Configurator 11" software. Be sure a successful delete by built-in buzzer sound "trill";
- To register:
  1. Wireless detector – install the battery to the wireless detector, wait for the two-color LED indicator to stop flashing, change its tamper status – recover then violate it. For **EDS3000** – don't use its tamper – detector will be automatically registered;
  2. Keyfob – delete the previous registration by pressing the ② and ③ buttons at the same time. Registration – press ③ and ④ buttons at the same time (see Figure 24);
- Control successful registration (automatic operation) by sound signal "trill" of the built-in buzzer. If Control Panel has not received registration signal from detector within 40 seconds, then it exits from the registration signal waiting mode with the long sound signal.

To register (bind) Crow wireless siren you should use "Lind-9M3"/"Lind-15" ICDs.

Wireless detectors/sirens can be enrolling by the "Lind-9M3"/"Lind-15" ICDs.

Enrolling sequence for "Lind-9M3"/"Lind-15" ICDs is described in their operating manuals available to download from www.ortus.io.

To register (bind) one Crow wireless repeater by RF (SW3) key:

- The wireless zone type for the repeater in the Control Panel configuration should be set to "Radio keyfob";
- Open the cover of the repeater housing and disconnect the backup battery cable;
- After 30 seconds, turn on the repeater's battery cable, close the cover of its housing;
- Enter the registration mode of wireless detectors of the desired group (see Section 9.7). If LED **HL5** is <u>blinking non-uniformly</u> (fast once/twice then pause ~1 second), it means the current group has free wireless zone and you can start wireless detector registration by the **RF (SW3)** button short press. The **HL5** LED starts blinking fast while waiting for registration signal from wireless detector.
- If there are no free radio zones in the group you choose, then **HL5** LED will be <u>lighting through short intervals</u> in the registration mode – so you should delete <u>all</u> the wireless detectors in this group with long pressing the button **RF (SW3)** <u>or</u> by clear "**Sensor ID**" field for the <u>desired</u> wireless zone in the "Configurator 11" software. Be sure a successful delete by built-in buzzer sound "trill";
- Insert the repeater plug into the mains socket for automatic binding. It occurs when the repeater indicator stops flashing.

23.2.1. 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.

23.3. Rielta

The Control Panel can operate with the following Rielta wireless detectors:

- Ladoga IPR-RK – wireless channel manual fire detector;
- Ladoga KTS-RK – wireless channel manual burglar alarm detector;
- Ladoga MK-RK – wireless channel magnet contact burglar alarm detector;
- Ladoga PD-RK – electrooptical smoke detector;
- Steklo-3RK – wireless channel sound surface burglar alarm detector;
- Foton-12-RK – wireless channel electrooptical burglar alarm detector;
- Foton-SH – electrooptical surface burglar alarm detector;
- Foton SH2-RK – electrooptical surface burglar alarm detector.

Make sure that the red PCB is used in every wireless detector.

To register (bind) one Rielta wireless detector the following shall be done:

- Remove battery from the wireless detector;
- Enter the registration mode of wireless detectors of the desired group (see Section 9.7). If LED **HL5** is blinking non-uniformly (fast once/twice then pause ~1 second), it means the current group has free wireless zone and you can start wireless detector registration by the **RF (SW3)** button short press. The **HL5** LED starts blinking fast while waiting for registration signal from wireless detector.
- If there are no free radio zones in the group you choose, then **HL5** LED will be lighting through short intervals in the registration mode – so you should delete all the wireless detectors in this group with long pressing the button **RF (SW3)** or by clear "**Sensor ID**" field for the desired wireless zone in the "Configurator 11" software. Be sure a successful delete by built-in buzzer sound "trill";
- Install battery to wireless detector (for repeater – don't use the mains power), set the binding mode by short closing of "RESET" jumper (accompanied by green LED flashing);
- To register:
  1. Repeater – close the "START" jumper shortly up to LED lights up green. Press and hold tamper then close the "START" jumper to LED flashing green;
  2. Wireless detector – close the "START" jumper shortly;
  3. Keyfob – press any key shortly. If LED don't flashing green then press all 3 keys up to LED light up red, then press any key.
- Visually monitor the wireless detector binding by sound signal "trill" of the built-in buzzer. If Control Panel has not received binding signal from detector within 40 seconds, then it exits from the binding signal waiting mode with the long sound signal.

Potential problems and solutions ():

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. Board failure. Both LEDs are lit at the same time.

   Solution: The board shall be changed and wireless detectors shall be re-registered.
3. Radio receiver firmware error. The LEDs flash alternately.

   Solution: Update the radio receiver firmware or replace the radio receiver.

4. 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.

23.4. Ajax

The Control Panel can operate with the following Ajax wireless detectors:

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

To register (bind) one Ajax wireless detector by RF (SW3) key:

- Turn the radio detector power switch **OFF** (located on the back of the radio detector housing);
- Enter the registration mode of wireless detectors of the desired group (see Section 9.7). If LED **HL5** is blinking non-uniformly (fast once/twice then pause ~1 second), it means the current group has free wireless zone and you can start wireless detector registration by the **RF (SW3)** button short press. The **HL5** LED starts blinking fast while waiting for registration signal from wireless detector.
- If there are no free radio zones in the group you choose, then **HL5** LED will be lighting through short intervals in the registration mode – so you should delete all the wireless detectors in this group with long pressing the button **RF (SW3)** or by clear "**Sensor ID**" field for the desired wireless zone in the "Configurator 11" software. Be sure a successful delete by built-in buzzer sound "trill";
- To register the detector, turn the detector power switch **ON**; registration process takes 3...5 sec. For remote control, press the buttons ○ and ⏼ at the same time;
- Control successful registration (automatic operation) by sound signal "trill" of the built-in buzzer. If Control Panel has not received registration signal from detector within 40 seconds, then it exits from the registration signal waiting mode with the long sound signal.

When replacing radio receiver Ajax "uartBridge" (for example, because of its failure) is required to re-register all the radio detectors in the new receiver (you should remove them from the Control Panel configuration previously).

If you want to change the zone number for the already registered radio 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 radio detector sticker/label with its zone number (you should apply this sticker/label on every new registration of each radio detector).

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.

When registering of wireless detectors some optional radio zones **are considered occupied** and **it is impossible to register any detector in them** – this comes automatically when registering of radio detector in the primary radio zone.

Note: 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.

If the wireless detectors enrolling is carried out by the “Lind-15” ICD, additional functions are possible for:

- check the signal level of each wireless detector – allows to optimally place the wireless detector in the room;
- sensitivity adjustment of the wireless detector (detection zone), depending on the size of the room and the presence of pets and other factors.

For more details about wireless detectors enrolling by the “Lind-15” ICD, see its operating manual, which is available for download from www.ortus.io.

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