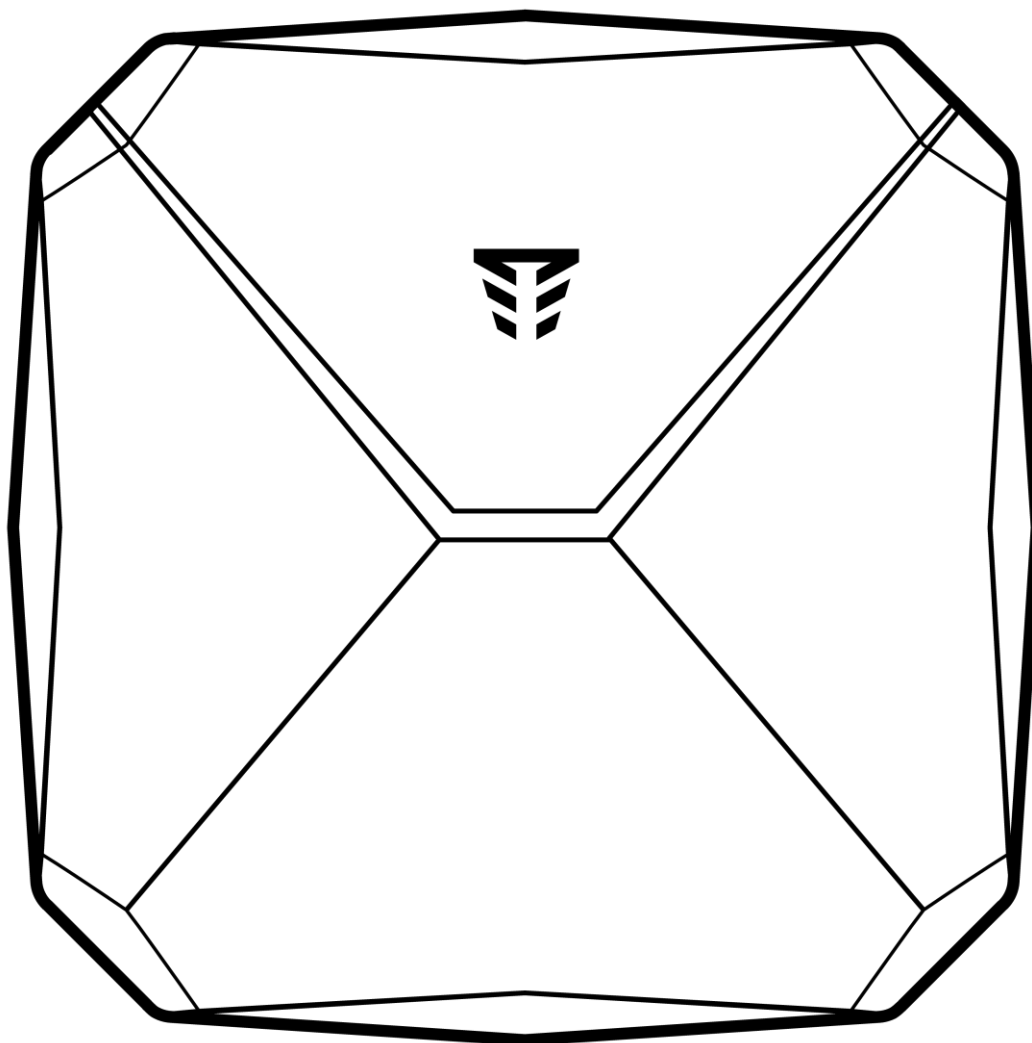




Orion NOVA X (LTE)
Wireless security control panel

User manual

SCP version 1.1.X



 Before getting started with Orion NOVA X (LTE) wireless security control panel (further – SCP), we strongly recommend reading this user manual.

Installation of the SCP must be carried out in accordance with the electrotechnical regulations and fire safety regulations.



Maintenance of the SCP must be carried out by qualified personnel with disconnected power supplies: main (230V) and alternative (battery).

Installation, disassembly, and maintenance of the SCP **should be carried out only when the device is powered off.**

The following notations are used in this document:



- Additional information;



- Important information that needs special attention.

Use the following QR codes to download documents and software for mobile devices or PCs:

KNOWLEDGE BASE:



SCP "Orion NOVA X (LTE)"

SOFTWARE FOR MOBILE DEVICES AND PCS:



Control NOVA II
(iOS)



Control NOVA II
(Android)



oLoader II
(Windows/MacOS)



oLoader II
(Android)



oLoader II
(iOS)

Manufacturer's website: **tiras.technology**

CONTENT

TERMS AND DEFINITIONS.....	5
1. GENERAL INFORMATION AND SCP SPECIFICATIONS	7
1.1 Purpose of SCP	7
1.2 System composition.....	7
1.2.1 SCP	7
1.2.2 Compatible devices.....	7
1.2.3 Communication modules.....	8
1.3 Specifications.....	8
2. SYSTEM INSTALLATION.....	10
2.1 System installation plan	10
2.2 Location of devices.....	10
2.3 Main power connection (230V)	10
2.4 Devices installation	11
2.5 "Start" button functions and SCP indication.....	11
2.6 Working with GSM/LTE module.....	14
2.7 Working with Wi-Fi module.....	14
2.8 Working with wireless devices.....	15
2.9 Complex inspection after installation	15
2.10 System operability	15
3. SYSTEM CONFIGURATION.....	17
3.1 Configuring SCP using oLoader II software	17
3.2 Description of SCP settings	18
3.2.1 Communication settings	18
3.2.2 System and security settings	20
3.3 Description of devices settings.....	21
3.3.1 Detectors.....	21
3.3.2 Key fobs.....	24
3.3.3 Keypads.....	25
3.3.4 Sirens	26
3.3.5 Repeaters	27
3.4 Settings of groups.....	28
3.4.1 "Use group mode" option is disabled	28
3.4.2 "Use group mode" option is enabled.....	28
3.5 User settings.....	29
4. INSTALLER OPERATIONS WITH DEVICES	31
4.1 Wireless device adding	31
4.2 Wireless device deleting	32
4.2.1 Deleting using oLoader II or Control NOVA II software	32
4.2.2 Deleting using the "Start" button 	32
4.3 Switching on wireless device	33
4.4 Switching off wireless device	33
4.5 Features of wireless devices	33
4.5.1 X-Key.....	33
4.5.2 X-Motion.....	34
4.5.3 X-Motion+.....	34
4.5.4 X-Motion Alarm	34

4.5.5	X-Shift	35
4.5.6	X-Shift+	35
4.5.7	X-Pad.....	35
4.5.8	X-Siren	35
4.5.9	X-Water.....	36
4.5.10	X-Cover S	36
5.	FUNCTIONS AVAILABLE TO THE INSTALLER.....	38
5.1	Arming/Disarming	38
5.2	Testing detectors.....	38
5.3	Restart of the SCP.....	38
5.4	SCP firmware update	38
5.5	Reset to factory settings.....	38
5.6	Communication status.....	39
5.6.1	View the Wi-Fi network signal strength.....	39
5.6.2	View the GSM/LTE signal strength.....	39
6.	SCP CONTROL	40
6.1	System control by means of keypads	40
6.1.1	Sound indication of keypads.....	42
6.2	Arming/Disarming	42
6.2.1	Arming.....	42
6.2.2	Disarming.....	43
6.2.3	Arming in "I'm at home" mode.....	43
6.2.4	Arming/Disarming by means of the keypad.....	43
6.2.5	Arming/disarming several groups with one code by X-Pad keypad	44
6.2.6	Arming/disarming by means of X-Key.....	44
6.3	Preventing from arming.....	45
6.4	Alarms and faults handling with keypads	45
6.4.1	Alarm handling.....	46
6.4.2	Fault handling.....	46
6.5	Remote control and monitoring.....	47
6.5.1	Control NOVA II software.....	47
6.5.2	SMS notification.....	51
6.5.3	Check call.....	51
6.6	Changing access and attack codes.....	51
6.6.1	Changing access codes using X-Pad	51
6.6.2	Changing access codes with Control NOVA II	52
7.	ADMINISTRATOR OPERATIONS WITH KEYPADS	53
7.1	SCP registration mode.....	53
7.2	Deleting SCP data on the Tiras CLOUD II server	53
APPENDIX A		54
APPENDIX B		55
APPENDIX C		56
APPENDIX D		59

TERMS AND DEFINITIONS

Access code – a digital combination used by a user for authorization via keypad or the Control NOVA II software.

Access ID – a digital combination used by a user for authorization via keypad or the Control NOVA II software. Each user can have two access IDs – access code and attack code.

Activation – a process of joining the wireless devices to the SCP. For activation, it is necessary to enable the Adding mode in the SCP and press the  "Start" button on the wireless device.

Adding – a process of configuring wireless devices, which includes entering the serial number in the configuration of the SCP (assignment) and joining wireless devices to the SCP (activation).

Alarm mode – the state of the SCP, the response to any danger (intrusion or penetration).

Armed mode (security mode) – the system state in which an alarm notification can be generated and transmitted to the centralized monitoring station (further – CMS), the Control NOVA II software, by SMS messages, and a control call to the user phone numbers.

Attack code – a digital combination used by a user for the attack notification transmission to the CMS and the Control NOVA II software, with a corresponding entry in the SCP event log.

Autonomous mode – the SCP mode when messages are not transmitted to the CMS. In this mode, the SCP can transmit messages to the Control NOVA II software, generate SMS messages and a control call to defined user phone numbers.

CMS – a centralized monitoring station representing a set of software and hardware tools that allows a security company to monitor the status of the object and respond to the events sent by the intrusion and hold-up alarm system.

Control NOVA II – a mobile application for remote monitoring and control of the security systems available for Android (version 8.0 or later) and iOS (version 15.0 or later) devices.

Detector (sensor) – a device intended to generate an alarm signal at penetration or attempt to penetrate the protected object.

Disarmed – the system state in which the intrusion alarm notification cannot be generated and transmitted. The system can have "24h" detectors which cannot be disarmed.

Entry delay – time for disarming after the intrusion of the entrance door after which the SCP will generate an alarm if the system is armed.

Exit delay – time for "Entrance Door" and "Corridor" detectors arming after its initiation.

Group – a logical system element that can combine "Entrance Door", "Corridor" and "Security" detectors and provides the user with an opportunity to control their state.

Intrusion – an unauthorized intrusion into the protected premises by an unauthorized person(s).

Intrusion and hold-up alarm system (further – system) – an automated complex (consists of the SCP, keypads, detectors, sirens, etc.) intended for the protection of various premises (buildings, including adjoining territory, separate premises, safe deposits, etc.). The main purpose is to prevent or facilitate the prevention of situations in which people will be harmed, or material and nonmaterial assets will be damaged due to the actions of intruders.

Keypad (X-Pad) – a keypad equipped with LED indicators for user interaction and the possibility to control and monitor system state.

oLoader II – software intended for local and remote control of the SCP, available for Windows OS (Windows 7 or later), MacOS (MacOS X 10.7 Lion or later), iOS (version 15.0 or later) and Android OS (version 8.0 or later) devices.

Penetration – opening (or removing from the wall) of the enclosure of any system device equipped with a tamper.

Protection of common premises – when enabled, this option allows the detector arming after all detectors of all groups in which it is included have been armed. The detector will be disarmed when any group in which it is included is disarmed.

Siren – a device intended to generate sound and light signals when the system goes into alarm mode. The siren can also be used to confirm group arming/disarming.

Tamper – a button intended to detect unauthorized tampering in the enclosure or removal of the device from the mounting.

Tiras CLOUD II – the cloud service used to manage the SCP with the Control NOVA II software.

1. GENERAL INFORMATION AND SCP SPECIFICATIONS

This document describes the structure and operating principles of the SCP with 1.1.X version (hardware version (HW)/firmware version/firmware revision).

Due to the improvements in the system functionality, the version and (or) revision of the built-in firmware of the SCP can be changed. The SCP version is displayed in the oLoader II and Control NOVA II software. We strongly recommend updating the firmware to the latest version before installing the SCP.

1.1 Purpose of SCP

The SCP is intended for autonomous or central monitoring protection of premises.

The system can be controlled by local access devices (X-Pad and X-Key) and remotely via the Internet using the Control NOVA II software.

The SCP can transmit information about the state of the system to the CMS, the Control NOVA II software, by SMS messages, and a control call to the specified user phone numbers.

The SCP is intended for continuous operation in the premises with controlled climatic conditions with no direct influence of climatic factors of the environment.

1.2 System composition

1.2.1 SCP

Depending on the requirements of the protected object, wireless detectors, keypads and sirens are connected to the SCP.

Main power source – general network (230 V, ~50 Hz).

In case of no main power supply, the SCP case has a built-in battery with a capacity of 2600 mA·h. The SCP can work from a fully charged battery for ~24 hours. The battery is fully charged in 3 hours.

Alternative power supply – USB Type-C input (5V/1.5A). It can be used instead of the main power supply or simultaneously with it.

The main power fault occurs only when there is no main and alternate power supply. The SCP can be powered via the USB Type-C input both from a USB-adaptor and from a Power Bank.

1.2.2 Compatible devices

Up to 64 wireless devices can be connected to the SCP.

Detectors (up to 64):

- **X-Shift** – wireless opening detector (for windows and doors);
- **X-Shift+** – wireless opening, shock, and tilt detector (for windows and doors);
- **X-Motion** – wireless motion detector;
- **X-Motion+** – wireless motion and glass break detector;
- **X-Motion Alarm** – wireless motion detector with sounder;
- **X-Water** – wireless water leak detector;

Key fobs (up to 32):

- **X-Key** – wireless key fob;

Keypads (up to 4):

- **X-Pad** – wireless keypad;

Sirens (up to 4):

- **X-Siren** – wireless outdoor siren;

Repeaters (up to 4):

- **X-Cover S¹** – wireless radio signal repeater.

1.2.3 Communication modules

The SCP is equipped with following built-in modules for communication with the CMS and Tiras CLOUD II service:

Wi-Fi provides communication via a wireless 2.4 GHz Wi-Fi network (IEEE 802.11 b/g/n). The protection of information transmitted over the Wi-Fi channel is provided by WPA PSK and WPA2 PSK technologies. The SCP connects to the Internet via the Wi-Fi access point specified in the settings.

GSM/LTE ensures communication via the cellular network using 2G and 4G technologies. The module provides the possibility to send SMS messages and make a control call to the user's mobile phone.

When M-WiFi and GSM/LTE communication modules operate simultaneously, Wi-Fi communication is prioritized.

1.3 Specifications

The SCP specifications are given in Table 1.1.

Table 1.1 – Specifications of the SCP

No	Parameter	Value	
1.	Maximum number of wireless detectors	64	Maximum number of connected wireless devices – 64
2.	Maximum number of wireless key fobs	32	
3.	Maximum numbers of wireless keypads	4	
4.	Maximum number of wireless sirens	4	
5.	Maximum number of repeaters	4	
6.	Radio signal frequency range (SRD), MHz	868.0-868.6	
7.	Maximum SRD transmitter power, mW	25	
8.	Maximum bandwidth, kHz	100	
9.	Maximum deviation of the channel frequency, kHz	6	
10.	Maximum number of groups in the system	16	
11.	Maximum number of users in the system	32	
12.	Communication protocol with CMS	“NOVA”, “Sur-Gard” (Contact ID)	
13.	Communication channels with CMS	2G (EGSM900/DCS1800), Wi-Fi (802.11 b/g/n)	

¹ One repeater supports up to 8 wireless devices for amplification, so maximum number of wireless devices that can be amplified by all four repeaters equals 32.

14.	Radio technology, max RF output power	EGSM900 (max RF output power 33 dBm $\pm$ 2 dB): (TX:880.1–915.0) / (RX:925.1–960.0) MHz, DCS1800 (max RF output power 30 dBm $\pm$ 2 dB): (TX:1710.0–1785.0) / (RX:1805.0–1880.0) MHz, LTE-FDD: B20 (TX:832–862) / (RX:791–821) MHz, B8 (TX:880–915) / (RX:925–960) MHz, B7 (TX:2500–2570) / (RX:2620–2690) MHz, B3 (TX:1710–1785) / (RX:1805–1880) MHz, B1 (TX:1920–1980) / (RX:2110–2170) MHz, Wi-Fi (max RF output power 20 dBm): 2412.0 – 2484.0 MHz, SRD (max RF output power 13.98 dBm): 868.0 – 868.6 MHz
15.	Maximum Wi-Fi transmitter power, mW	100
17.	Maximum GSM transmitter power, mW: - EGSM-900 - DCS-1800	2000 1000
18.	Main power source: - supply voltage (AC), V - frequency, Hz	187-253 50 $\pm$ 1
19.	Alternative power source (via USB Type-C cable): - voltage, V - current, A	5 1.5
20.	Maximum current consumption from main power source, mA	100
21.	Alternative (backup) power supply (battery) - voltage, V - capacity, mA·h	3.7 2600
22.	Maximum full charge recovery of the battery, hours	3
23.	The operation time from a fully charged battery, hours, not less than	24
24.	The operating temperature range with relative humidity up to 75% without condensation, °C	from -10 to +40
25.	Dimensions (W×H×D), mm, ($\pm$ 5 mm)	170×170×34
26.	Net weight (without battery), kg, not less than	0.4
27.	Average service life, years, not less than	10

2. SYSTEM INSTALLATION



All electrical connections should be made only when the power supply is switched off.

2.1 System installation plan

Before installation, we strongly recommend designing the system: the SCP, keypads, detectors, sirens, and other devices. Thick walls, metal partitions, mirrors, etc. reduce the range of GSM/LTE, Wi-Fi signal and wireless devices. It should be considered when choosing the place for the SCP mounting. The location of the SCP and other system devices should be within the detector-covered area.

2.2 Location of devices

The SCP and devices (except X-Key and X-Water) are intended for wall mounting. The SCP and devices are installed on the bracket fixed to the flat surface by screws. The location of the holes on the SCP allows it to be fixed to the socket box. The detachable element on the bracket of the SCP enclosure (see Figure B.1, Appendix B) and other devices is used to detect detachment from the wall. It should be fixed to the wall with a screw. When the SCP bracket is detached from the wall, the detachable element remains on the surface, which leads to tampering.

The installation dimensions of the SCP are shown in Figure B.1, Appendix B.

2.3 Main power connection (230V)

All installation and connection works should be completed before the power supply is switched on. A separate 230V power supply line protected by a circuit breaker with the parameters in accordance with the specifications of the SCP should be available at the SCP installation place. The SCP is supplied with the main power cable with an EU standard Type C plug that is already connected to it. To supply the main power of the SCP, it is necessary to insert the plug into power outlet (EU type C or F) of the 230 V network.

If necessary, another cable for the SCP main power supply may be used. We strongly recommend using the cable with a conductor cross-section of at least 0.5 mm².



Before connecting the main power cable to the SCP connector, make sure that there is no voltage on the cable conductors.

The main power is connected via the connector on the SCP board. The cable conductors are connected to the removable part of the connector (Figure 2.1). The insulated area of the cable conductors should not protrude beyond the joint (recommended insulation stripping length is 8 mm).

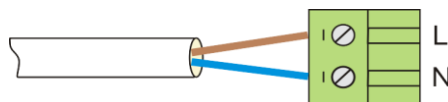


Figure 2.1 - Connecting the cable to the connector

The detachable part of the cable connector is connected to the AC 230V connector on the SCP board (Figure 2.2). After connecting, the plug and the power cable should be attached to the case using the screws and protective cap provided with the SCP.

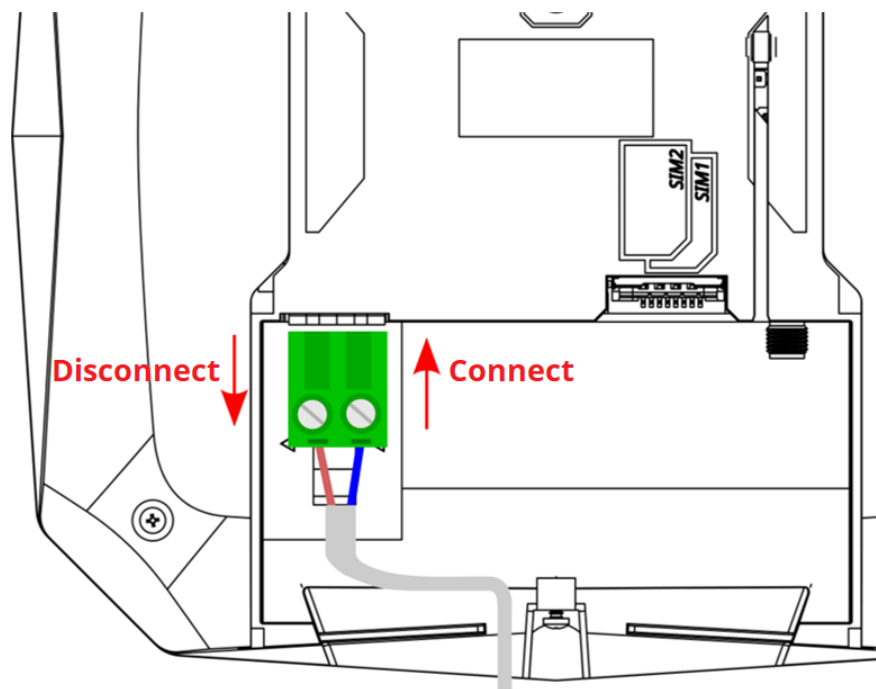


Figure 2.2 - Connecting the 230 V connector



Do not disconnect the connector by pulling on the power cord.

2.4 Devices installation

Before installing wireless devices (detectors, keypads, and sirens), they should be added according to section 4.1.

After adding devices, it is necessary to check the possibility of transmitting signals to the SCP from the place of the planned installation.

To check the signal strength, it is necessary to perform a signal test for each wireless device in the oLoader II or Control NOVA II software. If the signal strength is unsatisfactory or the SCP does not receive signals from the wireless device, it is necessary to change the location of the device. Once a good or satisfactory signal strength is achieved between the SCP and the wireless device, it can be installed in the location.



When tampering with the SCP, the keypad or detector, the siren is activated only if there are armed detectors with the set "Security", "Entrance door" or "Corridor" mode in the system.

2.5 "Start" button functions and SCP indication

The SCP is turned on after pressing and holding the  "Start" button for 3 seconds.

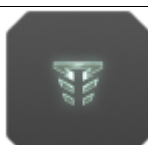
Depending on the time the  "Start" button is pressed, one of the service functions described in Table 2.1 is performed. To select a specific function, release the button while the TIRAS logo flashes in the corresponding color. The execution of the command is confirmed by the double flashing of the logo in the same color.

In autonomous mode, the TIRAS logo displays the current state of the SCP (see Table 2.2).

Table 2.1 –  “Start” button functions

Pressing type (in standby mode)	Indication	Reaction
Pressing and holding for up to 3 s	 Indicator does not light	Button press is ignored (no reaction)
Holding from 3 s to 10 s	 Blinking green	Switching off the SCP (the TIRAS logo gradually goes out – the SCP switches off)
Holding from 10 s to 15 s	 Blinking yellow	Resetting user codes
Holding from 15 s to 20 s	 Blinking blue	Resetting the SCP communication channel settings
Holding from 20 s to 25 s	 Blinking violet	Resetting to factory settings
Holding longer than 25 s	 Turning off the status indication	Exit function selection mode

Table 2.2 – Indication of the SCP status by the TIRAS logo

SCP mode/status	TIRAS logo indication	
	230V on	230V off
No communication with the Tiras CLOUD II server (trying to establish)	 Alternately blinks white and green	Flashes white and green alternately every 10 seconds
The SCP is in registration mode (connection established)	 Alternately lights up white and slowly goes out (available connection via one communication channel)	Does not depend on the availability of 230 V
	 Alternately lights up green and slowly goes out (available connection via two communication channels)	
Connected to Tiras CLOUD II server (regular communication)	 Constantly lighting white (available connection via one communication channel)	Blinks white once every 10 seconds (connection available on one communication channel)
	 Constantly lighting green (available connection via two communication channels)	Blinks green once every 10 seconds (two-channel connection available)
Firmware update	 Blinks blue	Does not depend on the availability of 230 V

2.6 Working with GSM/LTE module

The SCP is equipped with a built-in GSM/LTE-module. For the SCP to work via the cellular network, install SIM cards in the holders (Figure A.1, Appendix A). After the SIM cards installation, it is necessary to check the cellular network signal strength for each SIM card. After installing the SIM cards, it is necessary to check the signal strength of the cellular network for each SIM card. The gradation of the signal strength is given in Table 2.3. The cellular network signal strength can be viewed on the keypad or in the Control NOVA II and oLoader II software.

Table 2.3 – Gradation of the signal strength of the cellular network

Relative cellular network signal strength in the graphic displaying (divisions)	Compliance with GSM/LTE signal strength, dBm	Signal quality
1	-111...-101	Insufficient (possible loss of connection)
2	-100...-93	Minimally permissible (possible transmission delay of messages)
3	-92...-85	Sufficient
4	-84...-53	High

If the test does not show a sufficient cellular network signal strength (3 flashes of the SIM indicator) with the built-in antenna, or the unstable operation of the GSM/LTE channel is observed during the SCP operation, we strongly recommend using an additional Wi-Fi channel or connecting an external GSM antenna to the SMA connector (Figure A.1, Appendix A).

 **For the SCP to start working with the external antenna, it is necessary to enable the option "Use external GSM antenna" in the SCP settings using oLoader II software:**

"SCP Settings → Connection → GSM antenna → External"

This option can be enabled only after the connection of the external antenna to the connector.

 **It is not recommended to install the antenna near sources of powerful electromagnetic radiation (electric motors, X-ray machines, etc.).**

 **Installation/removal of the SIM card should be carried out only when the SCP is switched off.**

2.7 Working with Wi-Fi module

The SCP is equipped with a built-in Wi-Fi module (2.4 GHz). For the SCP to work via the Wi-Fi channel, set the network settings using oLoader II software. The Wi-Fi signal strength can be viewed on the keypad or in the Control NOVA II and oLoader II software. The gradation of Wi-Fi signal strength is given in Table 2.4.

Table 2.4 – Gradation of the Wi-Fi signal strength

Relative Wi-Fi signal strength in the graphic displaying (divisions)	Signal quality
1	Insufficient (possible loss of connection)
2	Minimally permissible (possible transmission delay of messages)
3	Sufficient
4	High

2.8 Working with wireless devices

The SCP operates with wireless devices. The gradation of the signal strength of the wireless devices is given in Table 2.5.

Table 2.5 – Gradation of the signal strength of the wireless devices

Relative signal strength in the graphic displaying (divisions)	Compliance with the signal strength of the wireless devices, dBm	Signal quality
1	<-91	Insufficient (possible loss of connection)
2	-90...-80	Minimally permissible (possible transmission delay of messages)
3	-79...-70	Sufficient
4	-69...-10	High

If the test does not show a sufficient signal strength of the wireless devices or the unstable operation is observed during the SCP operation, we strongly recommend bringing the wireless device into the range of the SCP and choose a permanent place of operation with the best signal strength.

2.9 Complex inspection after installation



After setting the SCP at the premises and after each subsequent change in its configuration, we strongly recommend checking the SCP operation via all communication channels to eliminate the possibility of improper downloading of the settings and equipment malfunctions.

To verify the system's proper operation after installation, it is necessary to perform the following tests:

- 1) Make sure that the SCP transmits the messages listed below to the CMS and/or Tiras CLOUD II, alternately in each configured communication channel (each SIM card, Wi-Fi):
 - change of the security mode (armed/disarmed) using each registered user access ID;
 - transition to armed mode of each detector of the system;
 - generation of alarm message in case of triggering each detector and interference with the tamper of each device in the system.
- 2) Make sure that the enclosures of all detectors, keypads, sirens, and the SCP during system operation are closed.



For tamper detection, the "Tamper control" option should be enabled.

2.10 System operability

As a result of the failure of any of the system devices, the level of protection decreases. Devices installed outdoors (for example, outdoor sirens) are exposed to adverse environmental effects. Atmospheric phenomena, such as thunderstorms or atmospheric lightnings, may damage devices connected to electrical systems.

The SCP is equipped with a range of protective solutions and automatic diagnostic functions that check the system's operability. Fault detection is indicated by the 🔧 LED on the keypad and is transmitted to the CMS. It is necessary to respond to such a situation in time

and, if necessary, consult the system installer.

For the device to meet the Grade 2 safety grade, you need to configure:

- indication of the system status and zones status is available only after entering the access code, therefore, the permanent indication of the keypads must be disabled;
- generation time of "CMS connection malfunction" message should be less or equal to 2 minutes;
- it is not allowed to disable tamper protection of the devices;
- user access IDs must consist of at least 4 digits;
- if there is any fault in the system, group arming is allowed only for the users having the "Ignore faults" authority;
- alarm sounding time must be at least 90 seconds;
- entry delay should not exceed 45 seconds;
- auto-arming delay of the hold-up button must be at least 180 seconds.

3. SYSTEM CONFIGURATION

The SCP can be configured with Windows PC/MacOS or iOS/Android device with installed oLoader II software.

3.1 Configuring SCP using oLoader II software

oLoader II is a special software that is intended to configure the SCP. The Windows PC/MacOS versions are available for download on the manufacturer's website: **tiras.technology** in the Software section. The Android version is available on Google Play, while the iOS version you can find in App Store. A detailed description of the SCP settings in the oLoader II software is given in section 3.2.

The SCP may be configured only in remote mode using the oLoader II software via the Tiras CLOUD II service. The local SCP setting is not available.

The remote SCP configuring is possible when it works with the Tiras CLOUD II service and requires the connection of the Windows PC/MacOS or iOS/Android device to the Internet.

For remote configuration of the SCP, you need to do the following:

- 1) launch the pre-installed oLoader II software – the registration window opens to create an account or log in;
- 2) configure one of the communication channels for the SCP:
 - set a Wi-Fi access point in the mobile phone or other device with available Internet traffic according to Table C.1 (Appendix C). Access point name – TIRAS, password – 12345678;
 - install a SIM card with available Internet traffic in the SIM1 slot (while doing this, the SCP should be disconnected from the power supply);
- 3) power on the SCP and wait for the SCP connection to the Wi-Fi or GSM network and establishment of a communication with the Tiras CLOUD II server (see Table 2.2);
- 4) add the SCP to the Tiras CLOUD II account within 10 minutes after its start. To add the SCP, do the following in the oLoader II software:
 - in the "Objects" window, click the "+" button (add);
 - in the "Device serial number" field, enter the 9-digit serial number of the SCP;
 - in the "Access code" field, enter the default installer access code (9-digit serial number of the SCP);
 - in the field "Object name", enter the name of the object (from 1 to 50 characters);
 - click the "Add" button;
- 5) select the required SCP from the list of objects and enter the current installer code (after entering the installer code, the settings from the SCP will be downloaded to the oLoader II software);
- 6) change the SCP settings.



Changing the SCP settings is possible if the groups or detectors are disarmed; the state of the 24-hour detectors does not affect this.

3.2 Description of SCP settings

3.2.1 Communication settings

The communication settings include the settings of the Wi-Fi, SIM cards, CMS, and service Tiras CLOUD II.

Table 3.1 – Settings of Wi-Fi and SIM cards

Parameter	Description
Wi-Fi settings	
Wi-Fi	This option allows to enable or disable the Wi-Fi communication module.
Wi-Fi access point	The name of the Wi-Fi access point. The field accepts values from 1 to 31 characters (available characters: 0-9, A-z).
Wi-Fi password	Wi-Fi access point password. The field accepts values from 8 to 31 characters (available ASCII characters).
SIM-cards settings	
Using SIM	If this option is enabled , the SCP checks the SIM card availability in the corresponding slot.
Roaming	Forbidden - the use of roaming is prohibited. National and international - allows the use of roaming. Only national - allows the use of only national roaming.
Access point name	For each SIM card to be used, an Internet access point (determined by the mobile operator) should be specified.
PIN-code	SIM card security code. If PIN code is disabled for the SIM card when setting, this field should be empty.
Balance check code	The following combination will be used to check the SIM card account, default – *111#.
Number check code	The combination will be used to define the SIM card number, default – *161#.
User name	User name will be used for registration in the GSM network. The field is optional.
Password	Password will be used for registration in the GSM network. The field is optional.
Additional settings	
Automatic network selection	Disabling the option allows to set the MCCMNC binding code for each SIM card to a specific mobile operator network (5 or 6 digits). When enabling this option, the MCCMNC field must be filled in for each SIM-card enabled.
SMS send permission	Global option that allows or prohibits sending SMS messages to all users of the system.
GSM antenna	This option allows to select the antenna to be used by the SCP for the operation of the GSM/LTE module: internal or external.
GSM Jamming analysis	Enabled – the SCP will analyze GSM/LTE channel jamming.

	Disabled – the SCP will not generate a message about the GSM/LTE channel jamming (the option is used for the premises where messages about the GSM/LTE channel jamming are falsely generated due to the interference using third-party equipment).
--	---

Table 3.2 – CMS settings

Parameter	Description
Device operating mode	Autonomous mode In this operation mode of the SCP, no messages are transmitted to the CMS. In autonomous mode, the SCP transmits messages about the system status to the Control NOVA II software, SMS-messages and makes check calls to specified user phone numbers. Central monitoring station mode ("NOVA" protocol) In this operation mode, the SCP transmits messages to MISTO or MOST CMSs using the NOVA protocol. Console mode – "Sur-Gard" protocol (Contact ID) In this operation mode, the SCP transmits messages to the CMS using the Sur-Gard (Contact ID) protocol. The list of messages transmitted to the CMS in the Sur-Gard (Contact ID) protocol is given in Table B.3 of Appendix B.
CMS	This option allows to select the CMS for the SCP communication. The following options are available: MOST and MISTO Security Platform. The option is configured only for the NOVA protocol.
Encryption algorithm	This option allows to select the encryption algorithm for exchange between the SCP and the CMS. DES and AES are the options available for selection. This option is configured only for the MISTO Security Platform. The selected encryption algorithm must match the encryption algorithm in the object card in the CMS.
Hidden number	This value provides additional crypto protection when the SCP operates with MISTO or MOST using the NOVA protocol. The entered value must match the hidden number in the object card in the CMS.
Object number in Sur-Gard (Contact ID) protocol	A 4-digit number is used to identify the object when the SCP communicates with the CMS using Sur-Gard protocol (Contact ID). The entered value must match the object number in the object card in the CMS.
CMS addresses settings	Up to three addresses for communication with the CMS can be configured. The address setting specifies the IP address (or domain name) and the CMS port. The transition between the addresses of the CMS occurs automatically when required by priority.
Test message interval (main connection channel)	Test message sending interval to control the main communication channel with the CMS. It is set from 30 to 990 seconds.
Test message interval (alternate connection channel)	Test message sending interval to control an alternative communication channel with the CMS. It is set from 60 to 3600 seconds. This option is available only in the NOVA protocol.
Generation time of "CMS connection malfunction" message	Time (after fault detection), after which the SCP generates a message of data exchange violation with the CMS. We recommend setting this option value equal to the test message control interval in the object card in the CMS.

Table 3.3 – Tiras CLOUD II service

Parameter	Description
Informing users	Complete – messages are sent to all users of the system. Partial – messages are sent to the users with the Administrator and Installer rights only.
Delay time for notification of loss of connection with the control panel	Time (after detection of the loss of communication between the SCP and Tiras CLOUD II), after which a communication fault message will be generated. It is set from 1 to 10 minutes.

3.2.2 System and security settings

The system and security settings are described in the tables below.

Table 3.4 – Security settings

Parameter	Description
Exit delay (option is available when the "Use group mode" option is disabled)	For each group, if it includes an "Entrance door" detector, the exit delay is set from 10 to 90 seconds.
Quick arming (option is available when the "Use group mode" option is disabled)	If the option is enabled, the group will be immediately armed after the transition of the detector of the "Entrance door" type to the "normal" state during the exit delay.
Number of messages of the same type	Limitation of the maximum number of repeated events to be sent to the CMS and recorded in the event log is set from 5 to 100.
Alarm formation	Up to three alarm formation options for the following events can be configured: When security zones are violated during entry delay: Enabled - if the detectors of the "Security" type are violated during the entry delay, the SCP immediately sends an alarm (to the CMS and Tiras CLOUD II). Disabled - if the detectors of the "Security" type are violated during the entry delay, the alarm will be transmitted (to the CMS and Tiras CLOUD II) after the entry delay expiring (if disarming has not occurred). When connection to an armed wireless device is lost. When arming failed.
Form a fault if power is missing	The option allows to enable or disable fault formation if power (230V, USB) is missing. At least one option should be selected.
Tamper control	The option allows to enable or disable the software analysis of the SCP tamper.

Table 3.5 – System settings

Parameter	Description
Device language	The language of SMS and event log. Ukrainian, English, and Russian are available.
Time zone of SCP	Time zone selection for setting the SCP time depending on its territorial location.
Auto-update software	The SCP can independently check the availability of the firmware update, download, and install it. The following values are available: Turned off – the SCP will not automatically download and install the firmware update.

	Wi-Fi only - if the update is available, the SCP will automatically download and install it in case there is communication with Tiras CLOUD II via the Wi-Fi module. Enabled (through all present communicators) - if the update is available, the SCP will automatically download and install it in case there is communication with Tiras CLOUD II regardless of the type of communication module.
Upgrade to beta versions	The option allows to access early versions of the firmware.
LOGO LED lighting	The option allows to enable or disable the logo backlight.
Brightness	The option allows to set the brightness of the LOGO LED backlight from 10% to 100%.

3.3 Description of devices settings

3.3.1 Detectors

Up to 64 detectors can be configured to work with the SCP.

Table 3.6 – General settings of detectors

Parameter	Description
Common settings	
Detector name	Name of the detector in the system.
Serial number	A 10-digit identifier of the wireless detector for its identification in the system.
Communication with SCP	
Communication test interval	Interval for sending tests by the detectors to monitor communication. This option can be set from 30 to 3590 seconds. This option affects the detector battery life.
Number of missed tests	The number of missed test messages to generate a detector communication loss event. This option can be set from 3 to 20 tests.
Detectors operation modes	
Operation mode	For each detector, it is necessary to select one of the following types: Guard type – the detector (Security type) that can be armed or disarmed. When violating the armed detector of this type, the SCP generates an alarm and activates the siren. Front door – the detector (Entrance door type) with a time delay, which at the entrance to the premises should always be violated first. From the moment of this detector violation, the entry countdown begins. After the entry time expires, if the group has not been disarmed, the SCP generates an alarm. Hall – the detector (Corridor type), which at the entrance to the premises should always be violated after the Entrance door zone. In this case, the alarm is not generated by the SCP during the entry time delay. In case of its violation before the Entrance door zone, the SCP immediately generates an alarm. 24-hour type – the detector (24h type) that is always armed. When violating this detector, the SCP generates an alarm and activates the siren. The zone is automatically re-armed by the time set in the "Auto arming delay" option after triggering, if the detector is in the normal state.
Entry delay	The option allows to set the entry delay time from 0 to 90 seconds. This option is only available for "Entrance door" type detectors.

	If during the entry delay the communication with the detector is lost or the tamper is activated, the entry delay is canceled, and alarms are generated on previously activated wireless devices.
Auto arming delay	The option allows to set the time (from 1 to 300 seconds), after which the detector will be re-armed after the alarm, if the corresponding detector is in the normal state.
I'm at home	When arming the group in the "I'm at home" mode, the detectors with this option enabled (as well as the detector of the "Corridor" type) will not be armed. The option is available only for the detectors of the "Security" type.
Security of common areas	This option is available only for the detectors configured as "Entrance door" and "Corridor". It is not allowed to create groups comprising the detectors only with enabled "Security of common areas" option.
Notifications to CMS	If the option is disabled, messages from this detector will not be transmitted to the CMS.
Disarming with CMS	The detectors with enabled option will be disarmed upon receipt of the corresponding command from the CMS. This option is available only for the detectors configured as "Security", "Entrance door", and "Corridor" types.
Light indication of alarms	If the option is enabled, the LED indicator on the detectors will light up briefly when the detector is alarmed. If the option is disabled, the LED indicator on the detector will not light up when the detector is triggered.
Other	
Tamper control	This option allows to enable or disable the software analysis of the detector's tamper protection.
Turn off	This option allows to disable the device. In the disabled state, the device remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.
X-Motion /X-Motion+/X-Motion Alarm settings	
Motion sensor	
Sensitivity	This option allows to select the motion sensor sensitivity settings: high, medium, low.
Number of alarms in one security session	This option allows to configure the number of alarms in one security session. It is possible to configure 3, 5, 10 alarms and an unlimited number. A large number of alarms reduces the battery life of the detector.
Constantly active motion sensor	Enabled – the motion sensor will detect a violation immediately after receiving the arming command from the SCP. Disabled – after receiving the arming command from the SCP, the motion sensor will detect violations after its activation (~ in 30 seconds). Constantly active motion sensor reduces the battery life of the detector.
Glass brake sensor (option is available only for X-Motion+ detector)	
Sensitivity	This option allows to select the glass break sensor sensitivity settings: high, medium, low.

Always guarding	Enabled – the glass break sensor will detect a violation regardless of whether the detector is armed or not. Disabled – the glass break sensor will detect a violation if the detector is armed.
Activate Siren	When motion is detected – this option allows to enable or disable the sounding of the siren for this alarm. When glass brakes – this option allows to enable or disable the sounding of the siren for this alarm.
Built-in siren (option is available only for X-Motion+)	
State information	Whole system – the siren will be activated when any armed group in the system is violated; Groups (detectors) – the siren will be activated when a previously selected armed group or groups are violated.
Event indication	This option allows to enable events (Security alarms, Device tamper alarms, Loss of communication with the detector during guarding, Successful arming, Disarming) that will activate the built-in siren.
Autonomous notification	If the detector is armed and its communication with the SCP is lost, the built-in siren will be activated depending on the option selected: ▪ "When motion is detected" – loss of communication with the SCP and motion detection; ▪ "When the enclosure is opened" – interference with the detector tamper and loss of communication with the SCP; ▪ "When communication with the SCP is lost" – only the loss of communication between the detector and the SCP activates the siren. By selecting this option, you can specify the delay time for activating the built-in siren of the detector. If you do not select any option, the built-in siren will not be activated in case the detector loses communication with the SCP during arming.
X-Shift/X-Shift+ setting	
Opening sensor	This option allows to enable or disable the opening detection.
Wired connection	If option is enabled, the device connected to the additional X-Shift contact should be specified: Confirmation LED – the LED will display an indication of the detector arming status (lit for 5 seconds when arming is confirmed) to which it is connected and an indication of a failed group arming it is part of (if "Groups Mode" is enabled). Alarms and entry/exit delays are not displayed. External detector – the SCP will analyze the status of the additional (wired) detector with NC contacts connected to it.
Turn off	This option allows to disable the device. In the disabled state, the device remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.
Shock sensor and Tilt sensor (option is available only for X-Shift+)	
Impact sensor	This option allows to enable or disable shock detection.

Sensitivity (of the shock sensor)	This option allows to set the sensor sensitivity (high, medium, low) when the sensor is enabled.
Tilt sensor	This option allows to enable or disable tilt detection.
Ignore single strokes	This option allows to enable or disable single shock ignoring.
Activate Siren	
When opening a door (window)	This option allows to enable or disable the sounding of the siren for this alarm.
When opening is detected by wired detector	
When tilt is detected (available only for X-Shift+)	
When an impact is detected (available only for X-Shift+)	
X-Water settings	
Sound alarm indication	This option allows to enable or disable the sound indication of alarms.
Confirmation of water leak	This option allows to enable or disable water leakage verification (an alarm is generated when two pairs of contacts are triggered simultaneously).
Displacement control	This option allows to enable or disable the flip and displacement control.
Turn off	This option allows to disable the device. In the disabled state, the device remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.
Activate Siren	When a leak is detected – this option allows to enable or disable the siren for this alarm.

3.3.2 Key fobs

Up to 32 key fobs can be configured to work with the SCP.

Table 3.7 – Key fobs settings

Parameter	Description
Serial number	A 10-digit identifier of the wireless key fob for its identification in the system.
Name	Key fob name in the system.
Operation mode	This option allows to select a key fob type: – User – Hold-up button
User (for "User" type only)	This option allows to assign the key fob to the user.
Group (for "User" type only)	This option allows to assign the key fob to the group.

Alarm button (for "Hold-up button" type only)	This option allows to enable or disable hold-up button.
Press method	This option allows to select press method: any press/long press only.
Auto arming delay (for "Hold-up button" type only)	This option allows to set auto arming delay time from 1 to 300 seconds.
Light indication of alarms (for "Hold-up button" type only)	This option allows to enable or disable indication on key fob when hold-up button is pressed.
Other	
Turn off	This option allows to disable the key fob. In the disabled state, the key fob remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.

3.3.3 Keypads

The SCP supports up to 4 X-Pad keypads.

Table 3.8 – Keypad settings

Parameter	Description
Keypad name	Specify the name of the keypad in the system.
Serial number	Specify the serial number of the keypad for identification in the system.
Communication settings	
Communication test interval	Interval for sending tests by wireless keypads to monitor communication. This option can be set from 10 to 3590 seconds. This option affects the keypad battery life.
Number of missed tests	The number of missed test messages to generate a keypad communication loss event. This option can be set from 3 to 20 tests.
Operation mode	
"Armed" indicator	This option allows to select the group from previously created ones to display the status at the 1 st access level.
Switching to standby mode	This option allows to set the time to enter pending mode after the last key press on the keypad. The time is set from 5 to 20 seconds. In standby mode, the keypad is not backlit, and the status of the system and zones are not displayed on the indicators.
Adaptive brightness	This option allows to enable automatic brightness adjustment.
Sound when buttons are pressed	When this option is enabled, pressing the keys on the keypad will be accompanied by a buzzer.
Exit buzzer	When this option is enabled, the keypad will emit an intermittent sound signal on any detector of the "Entrance door" type during an exit delay.

Indication	
Permanent indication (indication without entering the access code)	Indication will be displayed without entering the access code.
Display status (if the "Use group mode" option is enabled)	This option allows to set status display of detectors or groups.
Detectors for display (if the "Use group mode" option is enabled)	This option allows to select detectors to display their status.
Groups for display (if the "Use group mode" option is enabled)	This option allows to select groups to display their status.
Other	
Tamper control	This option allows to enable or disable the program analysis of the keypad tamper protection of the keypad.
Turn off	This option allows to disable the keypad. In the disabled state, the keypad remains in the system, the settings are saved, but it does not notify about alarms and faults, does not execute system commands, and does not transmit user command to SCP.

3.3.4 Sirens

The SCP supports connection up to 4 X-Siren sirens.

Table 3.9 – Siren settings

Parameter	Description
Siren name	Specify the name of the siren in the system.
Serial number	Specify the serial number of the siren for identification in the system.
Operation with SCP	
State information	This option allows to select the siren operation mode: whole system or groups (detectors) .
Whole system	The siren will be activated when group or 24h detectors are triggered.
Groups (detectors)	The siren will be activated when groups (detectors) are triggered.
Groups (if "Groups (detectors)" option is enabled)	This option allows to select the groups for siren activation.
24 hour detectors (if "Groups (detectors)" option is enabled)	This option allows to select the 24h detectors. When triggered, the siren will be activated.
External supply	This option allows to enable or disable external power supply control.
Event indication	
Security alarms (On/Off)	This option allows to set the indication for the corresponding events.
Device tamper alarms (On/Off)	
Loss of communication with the detector during guarding (On/Off)	
Successful arming (On/Off)	

Armed (On/Off) (available when "External supply" option is enabled)	
Unsuccessful arming (On/Off) (option is available when the detector is set as "Entrance door")	
Disarming (On/Off)	
Unviewed alarms (On/Off) (available when "External supply" option is enabled)	
Entry delay (On/Off) (option is available when the detector is set as "Entrance door")	
Communication settings	
Communication test interval	Interval for sending tests by wireless sirens to monitor communication. This option can be set from 10 to 3590 seconds. This option affects the siren battery life.
Number of missed tests	The number of missed test messages to generate a siren communication loss event. This option can be set from 3 to 20 tests.
Other	
Tamper control	The option allows to enable or disable the software analysis of the siren tamper protection.
Turn off the sound	The option allows to enable or disable siren sound.
Turn off	The option allows to disable the siren. In the disabled state, the siren remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.

3.3.5 Repeaters

The SCP supports operation with up to 4 X-Cover S repeaters.

Table 3.10 – X-Cover S settings

Parameter	Description
Name	Specify the name of the repeater in the system.
Serial number	Specify the serial number of the repeater for identification in the system.
Communication settings	
Communication test interval	Interval for sending tests by a repeater to monitor communication. This option can be set from 30 to 3590 seconds.
Number of missed tests	The number of missed test messages to generate a repeater communication loss event. This option can be set from 3 to 20 tests.
Other	
Amplification devices	This option allows to select the wireless devices for amplification: X-Shift, X-Shift+, X-Motion, X-Motion+, X-Motion Alarm, X-Water, X-Siren and X-Key.
Power indicator light	The option allows to enable or disable the repeater's power indicator light.
Tamper control	The option allows to enable or disable the software analysis of the repeater tamper protection.
Turn off	The option allows to disable the repeater. In the disabled state, the repeater remains in the system, the settings are saved, but it does not notify about alarms and faults and does not execute system commands.

3.4 Settings of groups

The groups are set with the help of "Use group mode" option (disabled by default) located in the "About object" tab.

3.4.1 "Use group mode" option is disabled

Disabling the option leads to the following changes:

- "Groups" settings tab – unavailable;
- all security detectors are armed and disarmed together;
- all users are authorized to access the whole system (to all detectors);
- user can arm/disarm/review the whole system at the same time;
- when added to the system, 24h detectors are automatically assigned to all previously created users;
- when a new user is created, he is automatically granted authority to manage existing system detectors.

For premises that require more complex configuration, you can enable "Use group mode" in the "About object" tab.

3.4.2 "Use group mode" option is enabled

When the option is enabled, the "Groups" settings tab appears, after that the Installer can distribute detectors and authorities. Group settings and new user settings become available in the oLoader II software.

Enabling the option leads to the following changes:

- all security detectors remain in Group 1;
- all users have access and authority to Group 1;
- all users have access to 24h detectors;
- sirens assigned to all groups and 24h detectors.

Up to 16 groups can be created in the system. Additional parameters can be specified for each of the groups.

Table 3.11 – Description of group configuration with enabled "Use group mode" option

Parameter	Description
Group name	The group name in the system.
Detectors	Detectors can be selected for each group that will be a part of it. Detectors of "Security", "Entrance door", and "Corridor" type are available for selection. The group cannot include detectors of the "Corridor" type if it does not include "Entrance door" detector.
Exit delay	For each group, if it includes a detector of the "Entrance door" type, an exit delay in the range of 10...90 seconds is set.
Quick arming	If the option is enabled, then, at exit delay, the group will be immediately armed after the transition of the zone of the "Entrance door" type to the Normal state.



If the "Use group mode" option is disabled, system will return to operation according to p. 3.4.1.

3.5 User settings

Up to 32 users can be created in the system. The "Installer", "Installer with administrator rights" and "Administrator" users have special authorities.

Table 3.12 – Description of user settings

Parameter	Description
Personal information	
Phone	User phone number
E-mail	User E-mail
Name	User name in the system
Access rights	
User role	You can choose one of the following types for each user of the system: ▪ Administrator – the main user of the system, which has the authority to control groups. The administrator can change the settings of users and deny the installer access to the SCP. Typically, this type of user is assigned to the owner of the premises. ▪ Installer – a user who can change system settings (if allowed by the administrator). The installer can also control groups. Typically, this type of user is assigned to an employee of the organization that installs and maintains the SCP. There is also an opportunity to select the Installer with administrator rights for the installer to obtain the administrator privileges. Typically, this option is used by the owner of the object in case of the autonomous operation of the system. ▪ User – a user who can control groups.
User rights	
Authority	Arming alarm – this authority allows to arm groups but does not allow to disarm them. Disarming – this authority allows to disarm groups added to the user. Bypass of unassembled zone – this authority allows to arm the group when there is one unassembled detector in this group (only using the Control NOVA II software). Ignore faults – this authority allows to arm the group when there are faults in the system and allows to arm the group with bypassing these faults.
Groups	This option allows to select the groups to which user can apply his authorities.
24 hour detectors	This option allows to select the 24h detectors to which user can apply his authorities.
Access type	Local – allows the user to control the system using keypads and key fobs but does not allow to control the system using the Control NOVA II software. Remote – allows the user to control the system using the Control NOVA II software but forbids the control with keypads and key fobs. Full – this value combines local and remote access permissions.
Access period	Never - access is disabled. Infinitely - permanent access.

	During (DD.MM.YYYY - DD.MM.YYYY) – access is limited to the specified period.
User main action	This option allows to select one of the user groups that will be available immediately after entering user access code from the keypad.
Fast action	This option allows to use the X-Pad to arm/disarm a group, skipping the stage of viewing its status, i.e. the action is performed after entering the access code and one press # . The option is not available for "Installer" and "Administrator" users.
View video cameras	This option allows the user to view previously added video cameras (CCTV).
Access	
Access code	A combination of 1 to 12 digits used for user authorization in the system. When reading the settings from the SCP, the valid user codes are displayed as "*".
Attack code	A combination of 1 to 12 digits providing the user with all the authorities available when entering access code, but at the same time an attack message is transmitted to the CMS and Control NOVA II software, with the corresponding entry in the event log of the SCP.
Key fob	This option allows to configure the user's X-Key wireless key fob. One key fob can be assigned to only one user.
Additional information	
Additional information	Enable/disable additional user notification.
Phone number	The user phone number which will receive SMS messages from the SCP.
Sending SMS	To set SMS notifications, the following options should be enabled: Alarms – permission to send SMS about alarms in the user groups and detectors. Arm/disarm – permission to send messages about the status of groups that can be managed by this user. Service – permission to send SMS about faults and tamper alarms (may be sent only to Administrator). The list of possible SMS messages is shown in Table B.2 of Appendix B.
Check call	The option is available only in autonomous mode. When the option is enabled , the SCP will make a call to the specified user phone number in case of an alarm. During the check call, the operation with the Control NOVA II software (monitoring and control) is disrupted. We do not recommend enabling the "Check call" option for more than 5 users.

4. INSTALLER OPERATIONS WITH DEVICES

4.1 Wireless device adding

Wireless device should be added and activated to work with the SCP. To add the wireless device, the following steps should be carried out:

- select the "Devices" tab in the oLoader II software;
- press the "+" button;
- enter the serial number of the device or scan the QR code;
- select the operation mode (only for the detectors and key fobs);
- enter the device name;
- press the "Start" button  on the device (or any button on the X-Key) when the activation timer starts.

After pressing the "Start" button  (or any button on the X-Key), the device will enter the activation mode and start searching for the SCP that is in the adding mode. The indication on the device during the SCP search is shown in Table 4.1.

Table 4.1 – Indication of searching for the SCP in the activation mode

Device	Indication
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Cover S	Blinking green LED up to 6 times
X-Pad	Red flashing of the zone indicators up to 6 times accompanied by a buzzer sound
X-Key, X-Siren	Red LED flashing up to 6 times
X-Motion Alarm, X-Water	Up to 6 buzzer sounds



If after pressing the "Start" button the device does not display the indication according to Table 4.1, but only one short flashing of the LED, this indicates that this device has already been added to another SCP. In this case, you need to perform the procedure of deleting the device (see section 4.2.2), after which try to activate it again.

As a result of the search for the SCP, the indication will be generated on the device according to Table 4.2.

Table 4.2 – Activation result

Device	Successful activation of the device and addition to the SCP	Activation failed	
		The device is out of range of the wireless network, or the SCP is turned off or not in the adding mode	The serial number of the device does not match the serial number entered in the SCP settings
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Cover S	Three short flashes	One long flash	Two long flashes
X-Pad	Three short flashes accompanied by a beep	One long flash followed by a buzzer sound	Two long flashes accompanied by a beep
X-Key	Three short flashes of green	One long red flash	Two short flashes of red

X-Siren	Three short flashes	One long flash accompanied by a beep	Two long flashes accompanied by a beep
X-Motion Alarm, X-Water	Three buzzer sounds	One buzzer sound	Two buzzer sounds

4.2 Wireless device deleting

There are two ways to delete the wireless device: deleting using the "Start" button  or the oLoader II or Control NOVA II software.

4.2.1 Deleting using oLoader II or Control NOVA II software

The system installer can delete the device by means of the **oLoader II** software. To delete it, it is necessary to go to the "Devices" tab, select the required device from the list and click  "Delete".

The wireless device can be deleted by the administrator or installer by means of the **Control NOVA II** software. To delete the device using the **Control NOVA II** software, you should log in, go to the "Wireless devices" menu, select the required device from the list and select the  "Delete" item.

The device is deleted from the settings, and the SCP sends it a delete command. After receiving command, the device resets to the factory settings and turns off (if it is in the SCP range). For X-Key to receive the delete command, press any button on it while it is in the range of the SCP signal.



In case of communication fault with the SCP during deletion, the device will not receive the delete command and will remain added. For further use of the device, it must be deleted using the "Start" button (see section 4.2.2).

After deletion, the device will confirm the received command (see Table 4.3).

4.2.2 Deleting using the "Start" button

To delete the device (except X-Key), press and hold the "Start" button  until it flashes twice (6 seconds), then immediately release the "Start" button .

To delete the X-Key, press and hold the  and  buttons simultaneously (5 seconds) until the red indicator lights up for a long time, then release the  and  buttons. During next two seconds (while the red indicator lights up), briefly press the  button.

If there is communication with the SCP when using the "Start" button  for deletion, the SCP will receive the corresponding command and deactivate it.

The indication on the device when deleting using the "Start" button  is given in Table 4.3.

Table 4.3 – Indication on the device when deleting using the "Start" button

Device	Successful deleting	The device was deleted only on the device side (if there is no communication between the SCP and the device)
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Cover S	Two long flashes of the indicator	One long flash of the indicator
X-Pad, X-Siren	Two long flashes accompanied by a beep	One long flash accompanied by a beep
X-Key (at the button)	Two long flashes of the green indicator	One long flash of the green indicator

press)		
X-Motion Alarm, X-Water	Two long buzzer sounds	One long buzzer sound

4.3 Switching on wireless device

To turn on the activated device, remove it from the bracket and press the  "Start" button. The indication of activation is given in Table 4.4.

Table 4.4 – Indication of the activated device switching on

Device	Indication
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Siren, X-Cover S	Three short flashes
X-Pad	The keypad buzzer sounds three times, pause, one more time
X-Motion Alarm, X-Water	Three short buzzer sounds

If the device is not activated, when it is switched on, it will display the indication according to Table 4.1.

4.4 Switching off wireless device

To switch off the activated device, press and hold the "Start" button  until the second short flashing of the indicator (the first flashing occurs when the "Start" button  is pressed). The indication of the successful switching off is given in Table 4.5.

Table 4.5 – Indication of the activated device switching off

Device	Indication
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Cover S	One long flash
X-Motion Alarm, X-Pad, X-Siren, X-Water	One long buzzer sound

If the device is not activated, it switches off automatically immediately after failed activation.

4.5 Features of wireless devices

4.5.1 X-Key

When the "Hold-up button" is pressed, the alarm message about an attack is transmitted to the Control NOVA II software to all users except the initiator of the action.

The key fob has protection against false presses. To execute the command, it is necessary to press the button from 0.3 to 2 seconds and release it, then the LED indicator on the added key fob will flash one of the following colors:

- green – the command has been transmitted;
- red – the command has not been transmitted (try again);
- two short green flashes – incorrect pressing (the button was held for more than 2 seconds), the command will not be executed.

After the command has been successfully transmitted, the indicator flashes at intervals of 1 second, confirming the command execution:

- short triple flashing of the green indicator – the command has been executed;
- short triple flashing of the red indicator – the command is forbidden to execute.

There is no command execution indication for the "Hold-up button" and when the previous command is repeated.

The key fob set as the "Hold-up button" transmits an attack message when any of its buttons is pressed.

4.5.2 X-Motion

To ensure long battery life, X-Motion generates 5 alarms per security session by default. The detector will respond to motion after repeated or automatic arming. The number of the detector alarms is set using the oLoader II software. If the "Constantly active motion sensor" option (see Table 3.6) is disabled, after receiving the arming command, X-Motion requires ~30 seconds for the PIR sensor to start detecting motion.

4.5.3 X-Motion+¹

The oLoader II software allows to set glass break sensor with three levels of sensitivity, as well as to enable the "Activate siren" option with two values for selection: "When motion is detected" and "When glass brake is detected".

Be careful with the microphone connection cable because it can be easily damaged when replacing the battery (CR123A).

4.5.4 X-Motion Alarm¹

X-Motion Alarm has a built-in siren, which can be switched off to preserve the detector battery life. The "Autonomous notification" option activates the siren if X-Motion Alarm is armed and the connection with the SCP is lost.

The following events can be selected to activate the built-in siren²:

- The "Security alarms" option – the siren will be activated when the armed detector is violated.
- The "Device tamper alarms" option – the siren will be activated when the tampers of the devices included in the security system are violated.
- The "Loss of communication with the detector during guarding" option – the siren will be activated when communication with the predefined detectors is lost. The "State information" option should be configured as "Groups (detectors)".
- The "Successful arming" option – confirmation of arming from the CMS will be accompanied by the siren activation (one short sound signal).
- The "Disarming" option – the siren will be disabled following two short sound signals before it turns off.

In the detector settings, you can select one of two siren state information options:

- The "Whole system" option – the siren will be activated when any armed group in the system is violated.
- The "Groups (detectors)" option – the siren will be activated when a previously selected armed group or groups are violated.

¹ Except advanced features, it has all the features of X-Motion.

² In the oLoader II software, the given option is set in "Another indication" item located in the "Built-in siren" tab.

4.5.5 X-Shift

The magnet can be placed both on the right and on the left side of the detector, parallel to its axis. The detector with a magnet can be placed in a vertical and horizontal position. The maximum distance between the magnet and the detector on a non-metallic surface is 15 mm. The maximum distance between the magnet and the detector on the metal surface is 4 mm.

After installing the X-Shift in the place of permanent use, it is necessary to calibrate its magnetic field sensor. X-Shift calibration increases the accuracy of door/window opening detection and detection of tampering with a powerful magnet. The calibration process can be launched in the oLoader II or Control NOVA II software. Calibration is performed with closed windows/door on which the detector is installed.

It is possible to connect a remote LED or an external detector to the X-Shift. To do this, open the X-Shift case and connect the remote LED or the external detector to the terminal connector in the middle of the case. Then, in oLoader II software, when configuring the detector, enable the "Wired connection" option and select the connection type:

- The "External detector" option – when connecting the external detector.
- The "Confirmation LED" option – when connecting the LED. When connecting the LED, it is necessary to consider the wire polarity.

4.5.6 X-Shift+¹

It is also possible to select the break sensor sensitivity level if it is enabled. The available sensitivity levels are as follows: high, medium (by default), and low. When the "Ignore single shocks" option is enabled, the alarm is generated only if the sensor detects more than one shock.

4.5.7 X-Pad

For the correct operation of the touch keys of the keypad, there must be no foreign objects on the touch field.

Before entering the access code on the activated keypad, press any button to "wake up the keypad", a multi-tone signal will sound.

4.5.8 X-Siren

The siren can operate in two notification modes:

- The "Whole system" option – the siren will be activated when any armed group in the system is violated.
- The "Groups (detectors)" option – the siren will be activated when a previously selected armed group or groups are violated.

In the siren settings, there is a list of event indications that can be enabled:

- The "Device tamper alarms" option – the siren will be activated when the tampers of the devices included in the security system are violated. Additional settings are available: Logo LED lightning and LED indication by contour, Signal volume, and Signal duration.
- The "Loss of communication with the detector during guarding" option – the siren will be activated when communication with the predefined detectors is lost. The "State information" option should be configured as "Groups (detectors)".
- The "Armed" option – the siren will be activated according to the settings when the group is armed.

¹ Except advanced features, it has all the features of X-Shift.

- The "Successful arming" option – the siren will be activated according to the settings when arming is successful with confirmation from the CMS.
- The "Unsuccessful arming" option – the siren will notify about the failed group arming, which may be caused by the failure to arm one or more zones.
- The "Disarming" option – the siren signals when the group is disarmed.
- The "Entry delay" option – the siren will be activated when the entry delay starts.
- The "Unviewed alarms" option – the siren will notify about the presence of unreviewed faults in the system.

In addition, it is possible to customize the logo LED lightning and LED indication by contour, signal volume, and signal duration.

The siren can be also activated when its own tamper is triggered, if there are armed groups in the system. It is impossible to turn off or delete the siren with the button if there are armed groups in the system.

When using an external 12V power supply, the "External supply" option should be enabled in the siren settings.

4.5.9 X-Water

We strongly recommend testing the X-Water at least once a quarter by wetting the sensors (terminal pairs) with water. After the "Water leak" alarm is generated, wipe the detector's enclosure, sensors, and installation place with a dry cloth.

If the "Confirmation of water leak" option is enabled, the "Water leak" alarm will be generated, when any two sensors (terminal pairs) are triggered.

The "Flip control" option monitors the vertical position of the detector. If the detector is turned over, it will produce sound signals.

The "Displacement control" option monitors the horizontal position of the detector. If the detector is displaced, it will produce sound signals.



When changing the testing intervals of communication with the wireless device from longer to shorter, the communication loss message can be generated before the device accepts the new setting.

4.5.10 X-Cover S

The wireless devices that can be configured for amplification by means of the repeater are as follows: X-Shift, X-Shift+, X-Motion, X-Motion+, X-Motion Alarm, X-Water, X-Siren, and X-Key.

When configuring the wireless devices for amplification, you should first add the repeater and then add the wireless devices, or vice versa. The wireless devices with poor signal strength that have been previously added to the system can also be configured for amplification.

The general configuring algorithm is as follows.

Step 1: Add a repeater and new wireless devices.

Step 2: Select the wireless devices for amplification.

Step 3: For a wireless device to receive settings and start working with the repeater, this device should be brought into the range of the SCP or you should tamper with the device or wait for several communication test intervals.

Step 4: Place the repeater in a possible place of installation and conduct a signal test to determine the permanent place of operation of the repeater.

Step 5: After successful configuration and location of the repeater, move the wireless device to a possible installation location and conduct a signal test to determine the location with the best signal strength for permanent operation of the wireless device.

Specifics of configuring:

1. Adding new wireless devices for amplification and a new repeater.

To add new wireless devices for amplification and a new repeater, you should follow steps 1-5.

2. Adding new wireless devices for amplification to the previously activated repeater.

It is necessary to add new devices and follow steps 2-5 of the general configuring algorithm described above. After successful activation in the range of the SCP, you should install the wireless device in a permanent place of operation by selecting it with the help of a signal test.

3. Adding existing wireless devices with poor signal strength to a new repeater for connection stability.

After configuring the wireless device for amplification, it should be brought into the range of the SCP or you should tamper with the device or wait for several communication test intervals for the wireless device to receive the settings and start working with the repeater.

4. Removing the wireless devices from amplification.

After changing the settings, removing the necessary wireless device from the list of devices for amplification, you should tamper with the device, wait for several communication test intervals within the range of the repeater. After that, you should bring the wireless device into the range of the SCP and choose a permanent place of operation using the signal test.



For the X-Key to start working with the repeater, after the configuration of the SCP and the repeater, as well as setting the X-Key for amplification, it is necessary to press any button of the key fob within the range of the SCP. The X-Key works only with the repeater it is assigned to.

5. FUNCTIONS AVAILABLE TO THE INSTALLER

For the installer to access the device functions via keypad, the "Access type" option should be set as "Full".

Using the keypad, the installer can:

- view system status;
- control security (arming/disarming);
- change one's own access IDs;
- restart the SCP;
- restore factory settings;
- view the signal strength of the GSM or Wi-Fi network.

5.1 Arming/Disarming

The installer, like other system users, can manage the groups added to him/her, as well as view their status, if this is allowed in his/her authorities. The system management is described in section 6.

5.2 Testing detectors

It is possible to perform a signal test of the detectors and check their status in the oLoader II and Control NOVA II software, in the "Wireless devices" menu.

Testing the activation of the detectors is performed in the Control NOVA II software, in the "Arm" menu. In this case, the detectors or groups of the detectors that need to be checked must be assigned to the installer.

5.3 Restart of the SCP

When the SCP is restarted, the current settings and event log will be saved.



If the SCP restart is performed during the firmware update download process, the firmware update download has to be initiated again.

To restart the SCP by means of X-Pad, enter the combination:

installer access code # 13 # installer access code #

To restart the SCP using the oLoader II software, click the "Reboot" button in the "SCP" settings tab.

5.4 SCP firmware update

The "Auto update software" option (see section 3.2.5) allows the SCP to independently check for firmware update (once a day in normal mode or 10 minutes after switching on), download and install it (if there are no armed groups in the system, as well as power faults).

5.5 Reset to factory settings



When restoring the factory settings, all SCP settings different from the factory ones will be lost. All data about the SCP in the Tiras CLOUD II service will be cleared, and the SCP will be deleted from all Control NOVA II software accounts.

The SCP can be reset to factory settings in one of the following ways:

- press and hold the "Start" button , releasing it when the logo flashes purple (see section 2.5);
- enter the combination on the keypad: **installer access code # 5 # installer access code #**.

After using one of the above methods, the device reboots and turns on.

5.6 Communication status

Using the keypad, the installer can check the signal strength of the Wi-Fi network and the GSM/LTE signal strength.

5.6.1 View the Wi-Fi network signal strength

To check the Wi-Fi network signal strength, enter the following combination:

installer access code # 11 #

After entering the combination, indicators 1-4 of the keypad will display the signal strength of the Wi-Fi network as described in Table 5.1.

Table 5.1 – Indication of the signal strength of the Wi-Fi network

Indicators 1-4 status	Wi-Fi signal strength, dBm	Signal quality
Indicator 1 lights	< -81	Insufficient (connection losses are possible)
Indicators 1, 2 light	-80...-71	Minimum allowable (message transmission delays are possible)
Indicators 1, 2, 3 light	-70...-61	Enough
Indicators 1, 2, 3, 4 light	-60...-10	High
Indicators 1, 2, 3, 4 blink	-	Unable to determine (no connection, invalid password, etc.)

5.6.2 View the GSM/LTE signal strength

To view the current GSM/LTE signal strength of the network, enter the following combination on the keypad:

installer access code # 12 #

After entering the combination, the indicators 1-4 of the keypad will display the GSM/LTE signal strength of the active SIM-card as described in Table 5.2.

Table 5.2 – Indication of the GSM/LTE network signal strength

Indicators 1-4 status (green – active SIM1, red – active SIM2)	GSM/LTE signal strength, dBm	Signal quality
Indicator 1 lights	-111...-101	Insufficient (connection losses are possible)
Indicators 1, 2 light	-100...-93	Minimum allowable (message transmission delays are possible)
Indicators 1, 2, 3 light	-92...-85	Enough
Indicators 1, 2, 3, 4 light	-84...-53	High
Indicators 1, 2, 3, 4 blink	-	Unable to determine (when SIM-card is changed or the registration is lost)

6. SCP CONTROL

The system can be controlled from local access identification devices (keypads, key fobs) and remotely, via the Internet, using the Control NOVA II software.

Access to the SCP functions is provided at four levels:

- **1st access level (unauthorized user)** – access for any person. It is not necessary to enter the access ID; to enter the first access level, it is necessary to wake up the keypad by pressing any key. At the first level, alarm notifications and a warning indication on the keypad ("i" indicator) are available, if the permanent indication mode is not configured.
- **2nd access level (authorized user)** – access for system users, which is limited by an access ID. The second level displays the system status indication on the keypad indicators (Table 6.1). Users from the second access level can manage the elements added to their settings.
- **3rd access level (authorized user)** – access for users of the "Installer" type. This level provides access to change all system settings.



Users of Administrator type can grant/block access to the 3rd access level.

- **4th access level** – access level for the manufacturer; the manufacturer can make changes to the devices, equipment design, and built-in firmware of the SCP.

6.1 System control by means of keypads

The SCP supports wireless LED keypads – X-Pad (Figure 6.1).



Figure 6.1 – X-Pad

To work with the keypad, you need to press any button (for 1 s) to "wake up", after that a multi-tone signal will sound. Controlling the system using keypads takes place after user authorization – entering a valid access code and pressing #. User authorization is confirmed

by three short beeps of the keypad buzzer, after that the indicators on the keypad display the current system status according to Table 6.1.

If an invalid access ID is entered, one long sound signal is generated. If the invalid access ID is entered four times in a row, the keypad is blocked for 90 seconds, and the notification about selecting the code is sent to the CMS and the Control NOVA II software.

Table 6.1 – Operating modes of system status indicators on the keypads

Indicator	Access level	No lights	Blinks	Lights
 “Attention”	I	No faults and alarms in the system	There are unviewed alarms and/or faults	All available faults and alarms are viewed
	II, III	No user-related faults and alarms in the system	There are user-related unviewed alarms and/or faults	All user-related available faults and alarms are viewed
 “Ready”	I	–	–	–
	II, III	Group arming is forbidden	Indication of the steps of access IDs changing	All detectors in the controlled group are in normal mode (detectors with delay can be violated), no faults
 “Security”	I	All groups are disarmed	One or more (but not all) groups are armed – partial protection	All groups are armed
	II, III	The controlled group is disarmed	Entry/exit delay	The control group is armed
 “Alarm” ¹	I	No alarms	Unreviewed group alarm and/or penetration into the device housing	There are viewed alarms (group alarm, 24h detector, penetration into the device housing)
	II, III	No user-related alarms in the system	Blinking once – unviewed group alarm and (or) penetration into the device housing Blinking twice – unviewed alarm memory (group alarm and/or penetration in the device housing)	There are viewed alarms (group alarm and/or penetration into the device housing)
 “Fault”	I	No faults	There are unviewed faults in the system	There are viewed faults
	II, III	No user-related faults in the system	There are user-related unviewed faults in the system	There are user-related viewed faults
 “Power”	I	Power of all devices is normal	There is a power fault in the system	The power of all devices is normal
	II, III			
Groups or detectors status indication on LED keypads				
Indicator state		Detector state		Group state
No lights		Detector is disarmed		All detectors of the group are disarmed
Blinking red (once)		Entry delay in detector		Unviewed alarms in any detector of the group
		A detector is violated and is in alarm		
Blinking red (double)		Unviewed memory of alarms in detectors		–
Lights red		Viewed alarm in the detector		Viewed group alarm
		The detector is violated and cannot be		

¹ The "Alarm" indicator does not display the operation of the detectors of the "Panic button" type at the 1st access level.

	armed	
Blinking green	Exit delay for "Entrance door" or "Corridor"	Group exit delay is counted
Lights green	The detector is armed	Group or its part is armed

6.1.1 Sound indication of keypads

Each keypad is equipped with a buzzer that emits a sound signal at certain events in the system or actions from the keypad. The operating modes of the keypad buzzer are described in Table 6.2.

Table 6.2 – Keypad buzzer sounds and their meaning

Sound	Description
One multi-tone beep	Keypad wakeup
One short beep	Button press on the keypad
Three short beeps	Action confirmation
One long beep	Denial
Repeated sounding of four short sound signals	Exit delay countdown
One long repeating beep	The keypad is locked

6.2 Arming/Disarming

6.2.1 Arming

To arm, it is necessary to do the following:

- 1) close all doors, windows and rooms in the armed premises. Using available SCP control tools, make sure that the group or detectors are ready for arming;
- 2) if the detectors with a delay ("Entrance door", "Corridor") are not available, it is necessary to leave the premises that are being armed and close the entrance door. If the X-Pad is located inside the armed premises, the detectors with delay ("Entrance door", "Corridor") must be configured to ensure the correct setting. The detectors with delay may remain triggered during the exit delay countdown;
- 3) initiate arming:
 - if there are no detectors with delay, arming will occur immediately;
 - if the group contains the detectors with delay, then during the exit delay, you should leave the room and close the entrance door. When the exit delay expires or when all detectors return to the normal state, the system will be armed.

After arming the group, the notification is sent to the CMS about arming the corresponding detectors, if the SCP has been previously configured to work with the CMS.



Depending on the load of the CMS and the communication channel between the SCP and the CMS, the interval between the execution of arming and the receipt of the confirmation is from 1 to 20 seconds.



If, at the moment of the exit delay, at least one detector of the "Entrance door" type is triggered, this detector and all detectors of the "Corridor" type will not be armed. The corresponding detector/group indicators and the "Security" indicator (Table 6.1) will not light green. In this case, it is necessary to eliminate the cause of the failed arming and try again.



If one group has common detectors or is part of another group, then when arming the first group, the second one will be set as "Partial armed". To switch a group from the "Partial armed" to the "Armed" mode, it is necessary to unarm this

group and then arm it again.

The confirmation LED will light if all detectors of the group or all entrance doors of the group are armed.

Confirmation by siren will be provided when all detectors of the group are armed.

6.2.2 Disarming

If the X-Pad is inside the armed premises, to disarm the group, it is necessary:

- 1) to open the entrance door – the entry delay will start;
- 2) to disarm the system during the entry delay using the X-Pad.

If the X-Pad is outside the premises, the group should be disarmed using the SCP control tools.

6.2.3 Arming in "I'm at home" mode

The "I'm at home" mode allows to protect the perimeter of the premises (entrance doors, windows, etc.), while ignoring the violation of the marked detectors by the user inside the premises.

Setting in "I'm at home" mode can be done using the keypad or the Control NOVA II software, if there is at least one detector with the "I'm at home" option enabled.

Arming by means of the keypad

For arming in the "I'm at home" mode, it is necessary to initiate arming and do not trigger the detectors of the "Entrance door" type during the exit delay. After the exit delay expires, all detectors will be armed, except for the detectors of the "Corridor" and "Security" types configured in the "I'm at home" mode.

Arming by means of Control NOVA II software

To arm in the "I'm at home" mode, click on the "I'm at home" icon after authorization in the object. All detectors will be armed, except for the detectors of the "Corridor" and "Security" types configured in the "I'm at home" mode.

If the group (object) is armed in the "I'm at home" mode, when the "Entrance door" detectors are triggered, the siren (X-Siren) is activated without delay; the alarm is generated immediately.



The group (object) including the detectors with the "I'm at home" option should contain the detectors with delay ("Entrance door"). If they are absent, the "I'm at home" mode will be ignored.

6.2.4 Arming/Disarming by means of the keypad

At the 1st access level, the indicators of the keypad detectors/groups display the current state of the detectors/groups specified in the keypad settings, only if "Permanent indication" option is enabled for the keypad. If the "Permanent indication" option is disabled for the keypad, then at the 1st access level, the indicators of the system status and detectors/groups on the keypad are permanently turned off.

To control the group (object) from LED keypads, enter the combination:

access code ##



With the keypads, the user can manage the whole object or groups added to its settings. If the user has several groups, the group selected in the "Main action" option will be managed by the first group in the list of groups added to the user. If one user needs to manage several groups separately, it is necessary to create users in the system for each group.

After entering the valid access code and pressing once, three short beeps will sound

(entering the 2nd access level). If the X-Pad works in "Permanent indication" mode, after entering the access 2nd level, the indication mode of the detectors/groups will not change, the indicators will display the status of the detectors/groups specified in the keypad settings (see Table 6.1). If the "Permanent indication" mode is disabled in the keypad settings, after entering the 2nd access level, the indicators of the detectors/groups on the keypad will display the current state of the detectors of the group (the number of the indicator corresponds to the detector number in the group). If the detectors in the "24h" or "Panic button" mode are added to the user, their status will be also displayed on the keypad alarm indicators (after the group alarms).

The  indicator at the 2nd access level displays the state of the group being managed:

- **lights up green** (ARMED) – all detectors of the group (object) are armed. When the  button is pressed again, the group (object) will be disarmed;
- **does not light up** (DISARMED) – if the  indicator lights up green, then the group (object) is ready for arming. When the  button is pressed again, the group (object) will be armed.

Exiting the 2nd access level occurs after arming or disarming or automatically after 10 seconds of user inactivity. Four short beeps sound. All indicators, except the  indicator, (if there is an unviewed fault or alarm in the system) on the keypad turn off, if the "Permanent indication" option is disabled for the keypad.



If the "Quick action" option is enabled for the user, then the stage of viewing the status of the group is skipped; group arming/disarming occurs after one press of the  button.

6.2.5 Arming/disarming several groups with one code by X-Pad keypad

Control of several groups with one code may be carried out using the keypads with the "Quick action" option disabled. The users can control groups added to their settings. Groups are managed by their numbers in the system.

To arm/disarm a group, enter the combination on the X-Pad:

user access code  0 group number  

After the user is authorized, the status of the first user-configured group is displayed on the status indicators of the detectors/groups (the "Permanent indication" option is enabled). After entering **0** and group number, the status of the selected group is displayed on the status indicators of the detectors/groups (the "Permanent indication" option is disabled).

When pressed again, the state of the group changes.



After user authorization and input of "user access code  0 group number  ", the indication of the keypad detector/group corresponds to the control of one group by the keypad.



With permanent indication, the display of detectors/groups does not change after entering "user access code  0 group number  .

6.2.6 Arming/disarming by means of X-Key

The control of the groups using X-Key key fobs is carried out by pressing the following buttons:

-  - arming;
-  - disarming;

□ - arming in "I'm at home" mode;

△ - hold-up button.

The key fob has protection against false presses. To execute the command, it is necessary to press the button from 0.3 to 2 seconds and then release it, after that the LED indicator on the assigned key fob will flash one of the following colors:

- **green** – the command has been sent;
- **red** – the command has not been sent (try again).

After the command has been successfully sent, the LED indicator will briefly flash three times with a green indicator at an interval of 1 s, confirming the execution of the command, and briefly flash three times with a red indicator if the command is prohibited from being executed.

The command execution indication is not available for the "Hold-up button" and when the previous command is repeated.

6.3 Preventing from arming

The SCP can prevent the group from arming if the user has not the appropriate rights. Prevention from arming can be performed in the cases described in Table 6.3.

Table 6.3 – Possible cases of arming prevention

No	Reason for prevention	Amendment
1.	A user does not have the rights to arm the group	It is necessary to grant the appropriate rights to the user.
2.	In case of penetration into the system device housing	To arm the group, it is necessary to eliminate the existing penetration.
3.	One triggered detector of the "Security" type in the group	To arm the group, the user must be granted the "Bypass of unassembled zone" authority. Bypassing the unassembled zone can be performed only when arming the group by the Control NOVA II software.
4.	Several triggered detectors of the "Security" type in the group	In this case, the group arming is impossible. Restore triggered detectors and repeat arming.

6.4 Alarms and faults handling with keypads

Alarms and faults can be viewed with the keypad. When an alarm or fault is detected in the system, the  indicator starts blinking.

After the user is authorized, one of the indicators starts blinking:

 – when a fault is detected in the system;

 – when there is a user-related alarm.

If the  indicator blinks at the 1st access level, but after the user's authorization, the  and  indicators do not blink or light, this means that the user does not have the rights to view the fault or alarm (for example, there is alarm of the detector absent in the groups or there is alarm of 24h detectors of the user).

After reviewing all the alarms that are available to the user, the indicator  lights up if the alarms are not handled (for example, penetration in the case or alarm of the armed detectors). After eliminating all the alarms, the  indicator goes out.

After viewing all of the system faults, the  indicator lights up. When all faults are handled, the  indicator goes out.



When controlling a group status (arming, disarming, partial arming) with the Control NOVA II software, the alarms of the zones included in this group and the 24h zones added to the user are viewed. System faults also become viewed.

6.4.1 Alarm handling

To handle alarms with the keypad, the user must be authorized: enter the access code and press the **#** button. If the user active alarms are available in the system, the  indicator blinks red once. If an **alarm memory** is available in the system, the  indicator blinks red twice.

If there is the detector alarm, the  indicator will blink simultaneously with the appropriate keypad indicator of the triggered detector. In the case of a tamper alarm, only the  indicator blinks. To handle this alarm, press the ***** button at the 2nd access level.

After viewing the list of all alarms, the  indicator goes out if there are no active alarms or lights up if active alarms still remain (after active alarms are handled, the  indicator automatically goes out).

All alarms are automatically cleared after disarming the group.

6.4.2 Fault handling

If there is a fault in the system, the  indicator blinks once after the user authorization. To enter the handling mode, enter the combination on the keypad (the  indicator starts blinking 4 times per second):

access code **# 3 #**

In the faults viewing mode, the system shows the next fault when pressing the **#** button. The detector indicators on the keypad display one of the current faults described in Table 6.4.

Table 6.4 – Faults that can be analyzed in the system

№	Fault	Reasons for formation	The keypad zone indicator state (● – lights, ○ – no lights)			
			1	2	3	4
1.	No 230 V	Formed by the SCP in case of main power supply of 230 V lost (within 10 minutes).	●	○	○	○
2.	Battery discharged	Formed by the SCP when the battery voltage decreases below 3.45±0.2 V.	○	●	○	○
3.	No battery	Formed by the SCP in case of no voltage on the battery terminals.	●	●	○	○
4.	No communication with CMS	Formed by the SCP when it is impossible to transmit the message to the CMS via any of the configured communication channels.	●	○	●	○

After viewing the last faults, the system returns to the first fault. When all faults are viewed, the  indicator starts lighting continuously if the faults are not handled, or goes out if the faults are handled. Exit troubleshooting mode by pressing the ***** button.

If you try to enter the faults handling mode when there are no faults in the system, there you will hear a long sound signal; the system does not enter handling mode.

6.5 Remote control and monitoring

The users can monitor the system status in the following ways:

- using the Control NOVA II software;
- SMS messages to users' phone numbers;
- a check call in case of alarm (only in the autonomous mode of the SCP).

6.5.1 Control NOVA II software

Control NOVA II software is designed for remote control and monitoring of the system status. It is available for mobile devices running on Android or iOS. The software communicates with the SCP via the Tiras CLOUD II cloud service.

To operate the Control NOVA II software, your mobile device must be connected to the Internet.



The use of the Tiras CLOUD II services (remote control, firmware update, etc.), increases the amount of Internet (GPRS) traffic used by the SCP. We strongly recommend using a mobile phone service plan with an average of 50 MB per month (the amount of Internet traffic used by the SCP depends on the intensity of the use of the Tiras CLOUD II services).

The Control NOVA II software allows to do the following:

- arming/disarming;
- receive alarm, fault and other notifications;
- monitor the system status in real-time mode;
- view the event log;
- administrators and installers can invite other users to manage the system and perform some settings;
- view videos from the added CCTV cameras;
- change user access code.

Installation, first launch, and update of the Control NOVA II software

To install the Control NOVA II software, go to the store (Google Play for Android, App Store for iOS), find the Control NOVA II software, and install it. For the correct operation of this software, it is required to provide all permissions it asks when installing, or during the operation. To start the Control NOVA II software, select the appropriate icon in the main menu of the mobile device. To launch the Control NOVA II software, select the corresponding icon in the main menu of your mobile device. The language of the software (Ukrainian, Russian, or English) is set automatically according to the language settings of the mobile device. If the Google Play or App Store settings do not have permission to auto-update, then you will get the notification about the available updates after the release of a new software version.

Account registration

To register the account, follow these steps:

- open the software and click the "Register" button;
- add user photo from camera or gallery (optional);
- enter username in the "Name" field (at least 1 character);
- enter the correct user email in the "E-mail" field;
- enter a valid user phone number, in the following format "+380XXXXXXXXXX" in the "Phone" field;

- enter the password in the "Password" field (minimum 6 characters);
- enter the same password as in the previous step in the "Repeat password" field;
- agree to the terms of use;
- click the "Registration" button.

After clicking the "Registration" button, a confirmation code entry box with an SMS message appears (sometimes the code window is not displayed, the activation is executed immediately). The Control NOVA II software automatically reads the code from an SMS message and goes to the next step. In some cases, when the SMS-message code does not automatically appear in the field, you should enter it manually.



The SMS message may not come if your phone number is registered with Google, in this case the authorization will be executed automatically.

After successful SMS verification of the phone number, you will get the message stating that the email has been sent to your mailbox confirming the account registration in the Control NOVA II software. To confirm the account registration, open the email with the help of the mobile device used for registration. In the email, click the hyperlink that will confirm the registration and open the Control NOVA II software.



If you have not got the registration confirmation letter, it is necessary to check the correctness of the entered email, the messages in the "Spam" category, and also whether the mailbox is full.



If the actions described above do not help, do not reinstall the Control NOVA II software; it is better to immediately contact the technical support.

Authorization

After completing the registration procedure, log in to your account:

- enter the email used at the registration stage;
- enter the password used during registration;
- click the "Login" button.

Adding the SCP to the administrator or installer account

The first person who adds the SCP to one's own account must be the administrator or the installer. After adding the SCP, the administrator or the installer may invite other users.

Before adding the SCP to the account, it is necessary to enable the registration mode (see section 7.1), which is valid for 10 minutes. After enabling the registration mode, perform the following actions:

- in the "Objects" window, click the "+" button (add);
- in the "Serial number of device" field, enter the 9-digit serial number of the SCP;
- in the "Object name" field, enter the name of the object (from 3 to 50 characters);
- add a photo of the object from a camera or a gallery (optional);
- select the user role (administrator or installer) that adds the object to the account (user access code must match the chosen type);
- in the "Access code" field, enter the administrator or installer access code. If the mobile device is equipped with a fingerprint scanner, you may optionally enable the "Use of fingerprint scanner" option to enter the object. Note that when you first enter the "Object", you should enter the access code for the Control NOVA II software to remember and associate it with your fingerprint;

- click the "Add" button.



An object with only one user of a specific device can be added to one account.

If the data is filled correctly, after clicking the "Add" button, the SCP will appear in the "Objects" window.

Adding the SCP to user accounts

After adding the SCP to the account, the administrator can view the list of system users and their data by going to the "Settings/Users" item. User data is obtained from the SCP settings and is displayed only for the installer to view, the administrator or the installer with administrator rights can change some user settings. In this section, the Control NOVA II user account with the SCP user can be associated. To do this, it is necessary to perform the following actions:

- select the required system user (user must have full or remote access);
- click the button in the form of the envelope;
- enter user email and click "OK".

If you have entered an email that is not registered with the Control NOVA II software, an invitation letter will be sent to this email with the offer to register with Control NOVA II. After the account registration and user authorization, the SCP will automatically appear in the list of its objects.

If you have entered the email that is registered in the Control NOVA II software, the SCP will automatically appear in the list of objects of the given user.



The Control NOVA II software provides the user with the ability to control and monitor the protected premises remotely. The software does not replace local access devices – keypads or key fobs. When designing the security system, we strongly recommend using at least one keypad.

Push messages in the Control NOVA II software

Users can receive information about the security system status with push messages that are sent to the Control NOVA II software. If any event occurs in the security system, the software receives push messages with the specific content (depending on the settings in the "Notifications" section). There are 4 event types for which the notifications can be sent:

Alarms – sent when alarms (intrusion, tamper etc.) are detected in the system, which the user has the right to view;

Faults – sent when a fault is detected in the system (no 230 V power supply, battery discharged, etc.);

Arming/Disarming – sent when controlling the status of groups that are added to the user;

System – sent when system events occur, such as changing system settings, starting the SCP, changing the access code, etc.

Push messages with alarms have a specific sound signal. All push messages received by the software are stored in the notification center. Clicking the message opens the Control NOVA II software.



Push messages are no longer received if the number of unviewed messages exceeds 50.

Some problems with receiving push messages may appear if:

- 1) energy-saving mode is switched on (for example, Stamina on Sony devices);
- 2) user does not have any activated Google Account on the device;
- 3) device does not have the latest version of Google Play, or Google Play is not defined as a system application;
- 4) notifications for the Control NOVA II software are disabled (in the "Notifications" window in the device settings);
- 5) there are restrictions on the operation of the Control NOVA II software in the background;
- 6) device is not connected to the Internet;
- 7) authorization is not performed in the object at the first start of the Control NOVA II software;
- 8) when closing the Control NOVA II software, the account was logged out.



Notification sounds (including alarms) from the Control NOVA II software may be interrupted by notifications from other applications on the smartphone (calls, SMS, etc.).

Adding IP cameras to the Control NOVA II software

The Control NOVA II software enables the connection of IP cameras (regardless of the manufacturer) supporting the RTSP protocol.



RTSP (real-time streaming protocol) is the protocol used to view a stream from IP-cameras remotely.

Before adding a camera to the Control NOVA II software, do the following:

- make sure that the camera supports the RTSP protocol (this information should be specified in the technical specification of camera);
- find out from Internet provider if provided an external static IP address;
- configure the network equipment (port forwarding, IP address for the camera);
- configure the camera (using the manufacturer's instructions);
- create an RTSP link to the video stream (usually the RTSP link format is specified in the manufacturer's documents or in the camera's web interface);
- add a camera to the Control NOVA II software.

Adding the camera to the Control NOVA II software is completed by entering an RTSP link to the video stream in the object settings. The administrator or installer with administrator rights can do that.

To add the camera, do the following:

- enter the object;
- click the  icon in the upper left corner;
- go to the "Settings" section and select "CCTV";
- press "+" in the lower right corner;
- specify the camera name (from 3 to 20 characters);
- insert RTSP-links to the stream;
- click "Add";
- go to the "System" section and select "Users";

- select the user to grant access to the camera and select "CCTV" in its settings;
- select cameras the user can view (after selecting the camera, the user will see the "CCTV" tab in the "Control" window).

6.5.2 SMS notification

The SCP can send SMS to the user phone numbers specified in their settings (see section 3.5). The following categories of SMS notifications can be configured for each user:

- **Alarms** – SMS about alarms available in user groups and detectors.
- **Arm/Disarm** – SMS about the status of groups that can be managed by this user.
- **Service** – SMS about system alarms (tamper of the SCP or devices) and faults.

The list of SMS messages that can be sent to the user phone numbers is given in Table C.2 (Appendix C).

6.5.3 Check call

When using the SCP in autonomous mode, it is possible to set a "Check call" option in case of an alarm.

If the "Check call" option is enabled in the user settings, then when an alarm message is received for the user, the SCP calls to the specified user phone number. Check call is made without voice message. For the check call and sending SMS messages, one phone number specified in the user settings is used.

Check calls are made one by one to users' phone numbers in ascending order.

The SCP considers the check call **successful** when the user **rejects the call**; in other cases, it is considered that the user has not received the call and the SCP repeats the attempts. The maximum number of attempts to dial a single user per alarm is three attempts.

If the SCP fails to dial the user, it will try again after calling the remaining users, but not earlier than in 5 minutes (the interval between attempts to connect to one user).

If other events which are transmitted to Tiras CLOUD II or sent to SMS occur when ringing round the users, they are sent in regular mode. If at the moment of occurrence of such an event, someone calls the user, the call is not interrupted (the attempt is executed in full).



The call caused by tamper of the system devices is made only for the users of the Installer and Administrator types (if the "Check call" option is set).

6.6 Changing access and attack codes

The users can change their own access and attack codes using keypads or the Control NOVA II software.



The users with enabled "Quick action" option cannot change their own access IDs with keypads.

6.6.1 Changing access codes using X-Pad

To change the **access code**, enter the following on the keypad:

- 1) current access code **# 1 #** (the ✓ indicator starts blinking once per second);
- 2) new access code **#** (the ✓ indicator starts blinking twice per second);
- 3) re-enter the new access code.

To change the **attack code**, enter the following on the keypad:

- 1) current access code **# 2 #** (the ✓ indicator starts blinking once per second);

- 2) new attack code # (the ✓ indicator starts blinking twice per second);
- 3) re-enter a new attack code.

Successful change of access codes is confirmed by four short sound signals of the keypad buzzer. If the code change failed (the entered and re-entered combinations do not match, or the entered code is already used), you will hear one long sound signal.

6.6.2 Changing access codes with Control NOVA II

To change your own access code, do the following:

- enter the object;
- click the ☰ icon in the upper left corner;
- go to the "System/Object/Security" section;
- click the "Change access code" (the keypad will appear);
- enter a valid access code and press ✓ (confirm);
- enter a new access code and press ✓ (confirm);
- repeat the new access code and press ✓ (confirm).

After confirmation, you will get the message that the access code has been changed successfully. If an error occurs (if a new code cannot be set), repeat the operation using a different value.

7. ADMINISTRATOR OPERATIONS WITH KEYPADS

The administrator is the main system user having the rights available when working with keypads. There may be several administrators in the system.

Using the keypad, the administrator can perform the following actions:

- arm/disarm groups;
- view the system state;
- change one's own access IDs;
- enable the SCP registration mode in Control NOVA II;
- delete the SCP data in the Tiras CLOUD II service.

7.1 SCP registration mode

Enabling registration mode is required to add the SCP to the Control NOVA II account.

After enabling the registration mode from the keypad (or after the SCP start), within 10 minutes users of the "Administrator" and "Installer" types will be able to add the SCP to their accounts (if the data is correctly specified in the Control NOVA II software).

To increase the system security, users will be prohibited from adding the SCP to Control NOVA II accounts if the SCP registration mode has not been enabled by the system administrator, or if more than 10 minutes have passed since enabling the registration mode (or the SCP start).



Any error when adding an object (access code entered incorrectly, user type incorrectly specified, remote control rights missing, etc.) resets the 10-minute permission, after that it is necessary to re-enable the SCP registration mode.

Note that if the registration mode is enabled by restarting the SCP, you should wait at least a minute after turning on the SCP before adding the object to the account. This is necessary for the SCP to establish a communication with the Tiras CLOUD II service.

The SCP registration mode can be enabled in one of the following ways:

- 1) enter the combination on the keypad:

administrator access code # 7 #

- 2) restart the SCP (turn it off and on using the  "Start" button)

7.2 Deleting SCP data on the Tiras CLOUD II server

The administrator can delete the SCP data stored on the Tiras CLOUD II server (the SCP serial number, event log, etc.). If the SCP is available in Control NOVA II user accounts, it will also be removed.

To delete the data, enter the combination on the keypad:

administrator access code # 6 # administrator access code #

After entering the combination, the SCP data will be deleted.

APPENDIX A

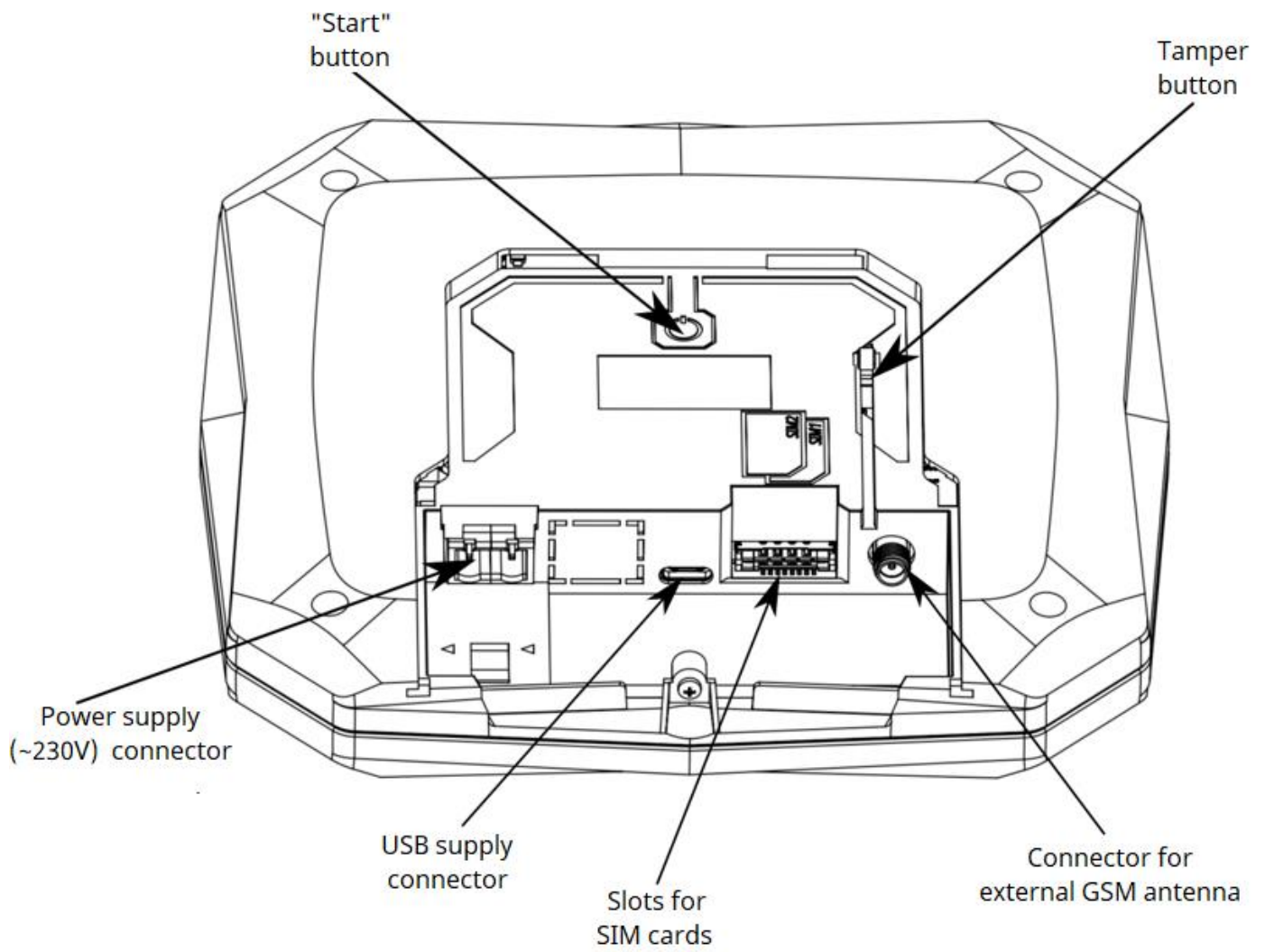


Figure A.1 – Connectors, slots and buttons of the SCP

APPENDIX B

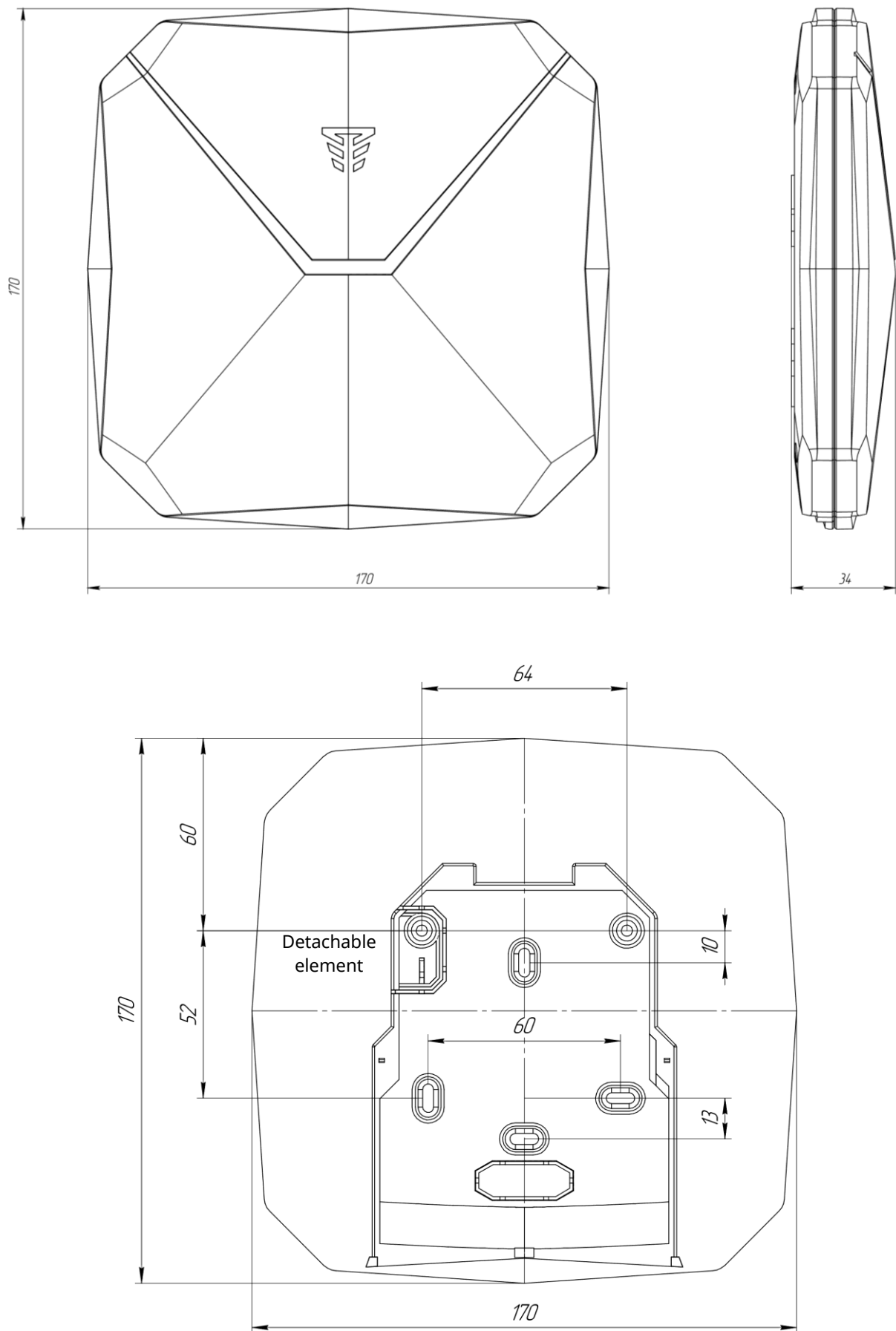


Figure B.1 –Installation dimensions of the SCP

APPENDIX C

Table C.1 – Default settings

Section	Setting
SCP settings	Connection: ▪ Wi-Fi access point – TIRAS, password – 12345678; ▪ SIM-cards: SIM1 – enabled, access point – Internet, without PIN; ▪ Automatic network selection – enabled; ▪ SMS send permission – enabled; ▪ GSM antenna – internal; ▪ GSM jamming analysis – enabled. Working with CMS: ▪ Device operating mode – autonomous mode. Tiras CLOUD II: ▪ Informing users – complete; ▪ Delay time for notification of loss of communication with the control panel – 7 min. Security settings: ▪ Number of messages of the same type – 50; ▪ Alarm formation when security zones are violated during entry delay – enabled; ▪ Alarm formation when connection to an armed wireless device is lost – enabled; ▪ Alarm formation when arming failed – disabled; ▪ Form a fault if power is missing – 230V enabled, USB – disabled; ▪ Tamper control – enabled. System settings: ▪ Device language – Ukrainian; ▪ Time zone of SCP – Europe/Kyiv (+2:00); ▪ Auto-update software – enabled (through all present communicators); ▪ Upgrade to beta versions – disabled; ▪ Logo LED lighting – enabled. ▪ Brightness – 50%.
Devices	No devices
Groups	"Use group mode" option: disabled
Users	User No.1 – name from account ▪ user role – installer, with administrator rights; ▪ access type – full; ▪ authority – arming alarm, ignore faults, bypass of unassembled zone, disarming; ▪ access period – infinitely; ▪ groups – absent; ▪ access IDs – access code – 9 digits of the serial number of the SCP; ▪ attack code – absent; ▪ additional information – disabled.

Table C.2 – List of SMS-messages, which can be sent to the user phone number

Event	SMS-message type
Detector alarm	DD.MM HH:MM ALARM, MOTION, "Detector name"
	DD.MM HH:MM ALARM, SHOCK, "Detector name"
	DD.MM HH:MM ALARM, TILT, "Detector name"
	DD.MM HH:MM ALARM, OPENING, "Detector name"
	DD.MM HH:MM ALARM, OPENING WIRED OPENING DETECTOR, "Detector name"
	DD.MM HH:MM ALARM, SABOTAGE, "Detector name"
	DD.MM HH:MM ALARM, GLASS BREAK, "Detector name"
	DD.MM HH:MM ALARM, TAMPER TRIGGERING, "Detector name"
SCP tamper	DD.MM HH:MM ALARM, INTRUSION IN SCP
X-Pad / X-Siren tamper	DD.MM HH:MM ALARM, INTRUSION IN "Detector name"
Arming by user	DD.MM HH:MM "Group Name" ARMED, "User name"
Arming by CMS command	DD.MM HH:MM "Group name" ARMED FROM CMS
Automatic arming	DD.MM HH:MM "Group name" ARMED
Disarming	DD.MM HH:MM "Group name" DISARMED, "User name"
	DD.MM HH:MM "Group Name" DISARMED FROM CMS
SCP 230 V power supply fault	DD.MM HH:MM SCP 230V POWER FAULT
SCP 230 V power supply restored	DD.MM HH:MM SCP 230V POWER OK
USB power supply fault	DD.MM HH:MM SCP USB POWER FAULT
USB power supply restored	DD.MM HH:MM SCP USB POWER OK
Battery discharge	DD.MM HH:MM SCP BATTERY DISCHARGED
No SCP battery	DD.MM HH:MM NO SCP BATTERY
SCP battery is normal	DD.MM HH:MM SCP BATTERY OK

Note.

* - DD.MM – day, month, HH:MM – hours, minutes.

Table C.3 – Messages transmitted to CMS in «Sur-Gard» protocol (Contact ID)

No	Event	Event type	Sur-Gard code	Notes
1.	Group arming	Arming	R401_(group number)_ (user number)	
2.	Group arming with detector overriding	Arming	E570_00_(overridden detector number)	
3.	Group disarming	Disarming	E401_(group number)_ (user number)	
4.	Detector alarm: security, entrance door, corridor, 24h	Alarm	E130_00_(detector number)	
5.	Hold-up button alarm	Alarm	E120_00_(detector number)	
6.	Detector tamper	Alarm	E137_00_(detector number)	
7.	SCP tamper	Alarm	E140_00_000	
8.	Keypad tamper	Alarm	E341_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
9.	Entering the user attack code	Alarm	E423_00_000	
10.	Keypad blocking	Alarm	E461_00_000	
11.	System error	Fault	E303_00_000	
12.	SCP battery is missing	Fault	E311_00_000	
13.	SCP battery is discharged	Fault	E302_00_000	
14.	SCP battery is exhausted	Fault	E309_00_000	
15.	No 230 V power supply in SCP	Fault	E301_00_000	
16.	GSM/LTE module power supply failure	Fault	E353_00_000	
17.	SCP jamming	Fault	E353_00_000	
18.	Low keypad power supply	Fault	E300_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
19.	No connection with keypad	Fault	E330_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
20.	Unsuccessful arming	Fault	R457_(group number)_ (user number)	
21.	The wireless detector power supply is low	Fault	E384_00_(detector number)	
22.	No connection with wireless detector	Fault	E380_00_(detector number)	
23.	Normal status of detectors: Security, Entrance doors, Corridor, 24h is restored	Restoring	R130_00_(detector number)	
24.	Detector tamper restored	Restoring	R137_00_(detector number)	
25.	Normal status of hold-up button restored	Restoring	R120_00_(detector number)	
26.	SCP battery is restored	Restoring	R311_00_000	
27.	230V power supply is restored	Restoring	R301_00_000	
28.	SCP tamper restored	Restoring	R140_00_000	
29.	GSM/LTE module power supply restored	Restoring	R353_00_000	
30.	Jamming is eliminated	Restoring	R353_00_000	
31.	Keypad power supply restored	Restoring	R300_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
32.	Keypad tamper restored	Restoring	R341_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
33.	Connection with keypad restored	Restoring	R330_00_(501-504)	501-504: the number of the keypad in the system from 1 to 4, respectively
34.	Wireless detector power supply restored	Restoring	R384_00_(detector number)	
35.	Connection with the wireless detector restored	Restoring	R380_00_(detector number)	
36.	Switching on SCP	Informative	R308_00_000	
37.	Switching off SCP	Informative	E308_00_000	
38.	Change of the SCP configuration	Informative	E429_00_000	
39.	SCP firmware update	Informative	E306_00_000	
40.	Change of user access ID	Informative	E462_00_(user number whose code was changed)	
41.	User access ID changed by the administrator	Informative	E462_00_(user number whose code was changed)	
42.	Periodic test messages	Test	E602_00_000	

APPENDIX D

Table D.1 – Subsection numbers for X-Pad

Number of key* (subsection)	Function	Administrator	Installer	User
1	Change of one's own access code	+	+	+
2	Change of attack code	+	+	+
3	Fault viewing	+	+	+
5	Resetting to factory settings [# installer code]	-	+	-
6	Clearing data on Tiras CLOUD II [# administrator code]	+	-	-
7	Enabling registration mode on Tiras CLOUD II	+	-	-
11	Wi-Fi signal strength displaying	-	+	-
12	GSM/LTE signal strength displaying	-	+	-
13	SCP restarting [# installer code]	-	+	-

Note.

*Entering format – [access code # number of key #]. For subsection 6 – [access code # number of key # access code]



tiras.technology

CONTACTS OF THE MANUFACTURER:

Tiras-12 LTD

Khmelnytskoho Shose lane 2, building 8, Vinnytsia, 21021, Ukraine

In case you have any questions, please contact us:

Sales department: market@tiras.ua

Technical support: support@tiras.ua

Warranty and post-warranty service: otk@tiras.ua