


Security control panels
Orion NOVA L (LTE)
Orion NOVA M (LTE)
Orion NOVA S (LTE)

 Before getting started with Orion NOVA L (LTE), Orion NOVA M (LTE), Orion NOVA S (LTE) security control panels (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: both 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 S \(LTE\)](#)



[SCP Orion NOVA M \(LTE\)](#)



[SCP Orion NOVA L \(LTE\)](#)

SOFTWARE FOR MOBILE DEVICES AND PCS:



[Control NOVA II \(iOS\)](#)



[Control NOVA II \(Android\)](#)



[oLoader II \(Windows/MacOS\)](#)



[oLoader II \(Android\)](#)

Manufacturer's website: tiras.technology

CONTENT

TERMS AND DEFINITIONS.....	7
1. GENERAL INFORMATION AND SCP SPECIFICATIONS	10
1.1 Purpose of SCP	10
1.2 System composition	10
1.2.1 SCP.....	10
1.2.2 Expansion and indication modules	10
1.2.3 Keypads.....	12
1.2.4 Communication modules	12
1.3 Specifications.....	13
2. SYSTEM INSTALLATION.....	16
2.1 System installation plan	16
2.2 Calculation of electricity consumption in the system	16
2.3 Location of devices	16
2.4 Cable connections.....	16
2.5 Connection of the SCP board.....	18
2.6 Keypads connection.....	18
2.6.1 Wired keypads connection	18
2.6.2 Wireless keypads connection	19
2.7 Expansion and indication modules connection.....	20
2.8 Detectors connection	22
2.8.1 Connection of the wired detectors	22
2.8.2 Connection of the detectors requiring a power reset.....	22
2.8.3 Connection of the wireless detectors.....	23
2.9 Siren connection	23
2.10 Confirmation indicator connection	23
2.11 TM key readers connection.....	24
2.12 Working with GSM/LTE module	24
2.13 Working with M-NET+ and M-WiFi modules	25
2.14 Working with the wireless devices	26
2.15 Complex inspection after installation.....	26
2.16 System operability	26
3. SYSTEM CONFIGURATION.....	28
3.1 Configuring the SCP by means of oLoader II software	28
3.1.1 Local SCP configuring using oLoader II software	28
3.1.2 SCP default settings configuring in oLoader II software	29
3.1.3 Reset of user access IDs.....	29
3.1.4 Remote SCP configuring using oLoader II software	30
3.2 Description of the SCP settings	30
3.2.1 Devices.....	30
3.2.2 Keypads.....	32
3.2.3 Zones.....	34
3.2.4 Outputs.....	36
3.2.5 Groups	37
3.2.6 Scripts	38
3.2.7 Security guard monitoring (SGM).....	40
3.2.8 Users	42
3.2.9 Communication settings.....	44
3.2.10 Setting of system parameters.....	46

3.3	Check call	47
4.	INSTALLER OPERATION WITH KEYPADS	49
4.1	Change of the installer access IDs	50
4.1.1	Change of access IDs using display keypads	50
4.1.2	Change of access IDs using LED keypads.....	50
4.1.3	Change of access IDs using oLoader II software	51
4.2	SETTINGS section of the main menu	51
4.3	Group settings.....	52
4.4	Tiras wireless devices	54
4.4.1	Wireless devices setting.....	54
4.4.2	Steps for adding wireless devices.....	58
4.4.3	Description of the device addition algorithm.....	59
4.4.4	Wireless device unassigning	63
4.4.5	Switching on the wireless device	64
4.4.6	Switching off the wireless device.....	64
4.4.7	Features of the wireless devices	64
4.5	Language menu	67
4.6	Keypad options.....	67
4.6.1	Doorbell.....	68
4.6.2	Presence	68
4.6.3	Night light.....	68
4.7	Zone testing.....	69
4.7.1	Testing using the display keypads.....	69
4.7.2	Zone testing using the LED keypads	70
4.8	Device control (RS-485)	70
4.9	SCP restart	70
4.10	Firmware update.....	70
4.10.1	Automatic update	71
4.10.2	Update to beta version	71
4.10.3	Devices.....	72
4.11	Default settings	72
4.11.1	Restoring default settings using display keypads	72
4.11.2	Restoring default settings using LED keypads.....	73
4.12	Formatting the SCP flash-memory drive.....	73
4.12.1	Formatting the SCP flash drive using display keypads	73
4.12.2	Formatting the SCP flash drive using LED keypads.....	73
4.12.3	Formatting the SCP flash drive using the "Reset" button on the SCP board	73
4.13	Calibration of EOL resistors	73
4.13.1	Calibration of EOL resistors via LED keypads.....	74
4.13.2	Calibration of EOL resistors via display keypads	74
4.14	Communication status	74
4.14.1	Checking the communication status on the display keypads	74
4.14.2	Checking the communication status using the LED keypads.....	76
4.15	USSD-request	77
5.	SCP CONTROL	78
5.1	System control via keypads	78
5.1.1	Sound indication of keypads	80
5.2	Groups arming and disarming	80
5.2.1	Group arming.....	80
5.2.2	Group disarming.....	81


5.2.3	Group arming in "I'm at home" mode	81
5.2.4	Groups arming/disarming using display keypads.....	81
5.2.5	Group arming/disarming using LED keypads.....	83
5.2.6	Group arming/disarming with single code using LED keypads.....	83
5.2.7	Group arming/disarming using Touch Memory (TM) / Card readers.....	84
5.2.8	Group arming/disarming using radio key fobs	84
5.2.9	Group arming/disarming using X-KEY	84
5.3	Prevention of the group arming	85
5.4	Alarm and fault handling using keypads	85
5.4.1	Alarm handling using display keypads	85
5.4.2	Fault handling using display keypads	86
5.4.3	Alarm handling using LED keypads.....	86
5.4.4	Fault handling using LED keypads.....	87
5.5	Control of automatics.....	88
5.5.1	Output control and script running using functional buttons of display keypads.....	88
5.5.2	Output control and script running using display keypads	88
5.5.3	Output control and script running using functional buttons of LED keypads	89
5.5.4	Output control using LED keypads.....	89
5.5.5	Script running using LED keypads.....	89
5.5.6	Output control using readers.....	90
5.5.7	Script running using readers	90
5.6	Remote control and monitoring.....	90
5.6.1	Control NOVA II installation, first run, and update.....	90
5.6.2	Account registration.....	91
5.6.3	Authorization.....	91
5.6.4	Adding the SCP to the administrator or installer account	91
5.6.5	Adding SCP to user accounts	92
5.6.6	Push notifications	92
5.6.7	Adding IP cameras to the Control NOVA II software.....	93
5.7	Assign/Change of access IDs.....	94
5.7.1	Change of access ID using display keypads	94
5.7.2	Change of the access IDs using LED keypads	94
5.7.3	Change of the access code with the Control NOVA II software	95
6.	ADMINISTRATOR OPERATIONS WITH KEYPADS	96
6.1	Administrator operation with display keypads.....	96
6.2	"Settings" section	97
6.2.1	User settings	97
6.2.2	Menu language.....	101
6.2.3	Installer access.....	102
6.2.4	Keypad options	102
6.3	Event Log.....	103
6.4	Event log export	103
6.4.1	Event log export by display keypads	103
6.4.2	Log export with LED keypads	104
6.5	Balance checking.....	104
6.6	SCP registration mode.....	104
6.6.1	Enabling the registration mode from display keypads	104
6.6.2	Enabling the registration mode from LED keypads	105
6.7	Deleting the SCP data from the Tiras CLOUD II server.....	105
6.7.1	Deleting the SCP data from display keypads.....	105
6.7.2	Deleting the SCP data from LED keypads	105

6.8 About device	105
APPENDIX A	106
APPENDIX B	108
APPENDIX C	110
APPENDIX D	111
APPENDIX E.....	119

TERMS AND DEFINITIONS

Access code – a digital combination containing up to 12 digits used by a user for authorization via a keypad or the Control NOVA II software.

Access ID – a digital combination used by a user for authorization. Each user can have three access IDs – access code, key/card, and attack code.

Activation – a process of joining wireless devices and modules. For activation, it is necessary to enable the Adding mode in the SCP (possibly without pre-assignment if you have a display keypad) 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, penetration, or masking).

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 check call to the user phone numbers.

Assigning – a pre-setting of the wireless device in the SCP using the oLoader II software: enter the serial number, name of the wireless device, set test intervals and the number of missed tests, etc.

Attack code – a code 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 check call to the defined user phone numbers.

Confirmation of fulfillment of security guard duties – is when the guard, during activation of the patrol mode, briefly breaks the zone, and then restores it or logs in from the keypad, or both, to confirm his presence at the post or bypass the guarded object (see [3.2.7](#)).

Control NOVA II – the mobile software 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.

Dependent zone – a zone that is armed after all zones from all the groups it is included in are armed. The dependent zone is disarmed when disarming any group in which it is included.

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

Disarmed – the system state in which intrusion alarm notification cannot be generated and transmitted. The following zone types in the system cannot be disarmed: "24h", "Panic button", "Universal input", "Tamper", and "Anti-masking".

Display keypads – the keypads equipped with a display for user interaction and the possibility to control and monitor the system status. This type includes the following keypads: K-GLCD+, K-PAD OLED and K-PAD OLED+.

Entry delay – time for disarming after the entrance door intrusion.

Exit delay – time for arming of the "Entrance door" and "Corridor" detectors after initiating.

Expansion module – a device intended to increase the number of zones and (or) outputs.

Group – a logical system element that integrates zones of the "Entrance door", "Corridor" and "Security" types and provides a user with the ability to control their state.

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

Intrusion and hold-up alarm system (further – the 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 as far as possible 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.

Key/card – a symbolic combination of Touch Memory (further – TM) key, NFC card, etc., used by a user when logging in with readers.

LED keypads – the keypads equipped with LED indicators for user interaction and the possibility to control and monitor system status. This type includes the following keypads: K-PAD4, K-PAD4+, K-PAD8, K-PAD8+, K-PAD16, K-PAD16+, and X-Pad.

Masking – the lens view blocking on the motion detector (coloring or gluing with opaque material, covering).

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

Output – the system element that allows to control the devices connected to it by switching on and off the power.

Patrol mode (patrolling) – a defined period of time during which the security guard must perform actions to confirm the fulfillment of his duties set in the SGM script (see [3.2.7](#)).

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

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

Reader – a device intended to read and transmit user access ID to the SCP, thus controlling system elements (according to the user's rights). The SCP works with connected readers having the TM output protocol, the list of TM key families suitable for this SCP is given in section [2.11](#). The following keypads: K-GLCD+, K-PAD4+, K-PAD8+, K-PAD16+, and K-PAD OLED+ have a built-in contactless reader allowing to use static NFC tags (cards and key fobs) as a user access ID.

Script – a programmed sequence of actions that can be performed by the SCP on controlling outputs. Script settings are described in detail in [3.2.6](#).

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 (see [3.2.5](#)).

Tamper – 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 SCPs with the Control NOVA II software.

USB flash drive of the SCP – memory storage (integrated into the SCP board) used to

store and modify the configuration file of the SCP, download the firmware update file, and save the log file when exported from the keypad. When the SCP is connected to the Windows/Mac OS or Android/iOS device (see [3.1.1](#)), it is defined as a USB flash drive.

Zone – premises, its part or territory controlled by the detectors.

1. GENERAL INFORMATION AND SCP SPECIFICATIONS

This document describes the structure and operating principles of the SCP with 1.2.X (HW1) 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 with automation control functions.

Depending on the requirements of the protected object, wired and/or wireless detectors, sirens, expansion modules and access identification devices are connected to the SCP.

The system can be controlled with local access devices (keypads, TM key readers, key fobs) and remotely via the Internet using the Control NOVA II software or the CMS.

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

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

1.2 System composition

1.2.1 SCP

The SCP board has terminals for connecting zones (Orion NOVA S (LTE) – 4, Orion NOVA L/M (LTE) – 8), RS-485 interface modules (Orion NOVA L(LTE) only), keypads, TM key readers, and sirens. To control external devices there are relay outputs and transistor outputs to connect remote confirmation LEDs.

- Orion NOVA L (LTE) – two transistor outputs, two multifunctional alert outputs, two relay outputs;
- Orion NOVA M (LTE) – one transistor output, one multifunctional alert output;
- Orion NOVA S (LTE) – one transistor output, one multifunctional alert output.

The SCP case has the place for the installation of a battery with a capacity of 7 or 9 A·h (Orion NOVA L/M(LTE)) or 2.2 A·h (Orion NOVA S(LTE)) intended for standby power supply if there is no main power supply (230V).

1.2.2 Expansion and indication modules

Up to 15 modules can be connected to the SCP Orion NOVA L(LTE) using the RS-485 interface: M-Z box, M-ZP mBox, M-OUT2R box, M-OUT8R and P-IND32. The data exchange between the SCPs and modules is encrypted. Protection against device substitution is provided by a unique serial number.

M-Z box – a zone expansion module (further – module) intended for adding 8 zones to the system. It has a plastic enclosure and is powered from the SCP or an external power supply unit (further – PSU).

M-ZP mBox – a zone expansion module (further – module) intended for adding 8 zones to the system (16 zones when the M-Z module is installed) and 4 outputs (6 outputs when the

M-OUT2R module is installed). Transistor outputs Q1 and Q2 can operate in two modes: Remote LED (for direct connection of remote LED) or Open Collector (for external devices control). Universal outputs OUT1 and OUT2 can be used to connect an additional siren or to control external devices. The module has an input for connecting TM key readers. The module is powered by 230V AC. The module has a slot for 7 or 9 A-h battery and can be used as an additional uninterruptible power supply for external devices. The outputs + 12V, OUT1 and OUT2 with a maximum total load current of 1A are intended for this case.

M-OUT2R box – an outputs expansion module (further – module) intended for adding 2 relay outputs ("dry contacts") to the system which can switch the 230V voltage at an alternating current of 5A. The module is powered by the SCP or external PSU.

M-OUT8R – an outputs expansion module (further – module) intended for adding 8 relay outputs ("dry contacts") to the system which can switch 230V (AC) voltage at an alternating current of 5A. The module is powered by the SCP or external PSU.

P-IND32 – an indication panel (further – panel) intended for displaying the status of 32 zones or groups (depending on the selected operating mode) with its LED indicators, as well as for generating a sound signal during an alarm.

M-OUT2R and M-X expansion modules are intended for connecting to the special slots on the SCP mainboard.

M-OUT2R – an outputs expansion module (further – module) intended for adding 2 relay outputs (dry contacts) to the system. The switching parameters of the relay outputs are described in Table 1.3.

M-X – a wireless expansion module (further – module) for connection with wireless devices. This module allows to connect:

- up to 64 wireless detectors;
- up to 32 key fobs;
- up to 4 wireless keypads;
- up to 4 wireless sirens.

However, the number of all wireless devices cannot exceed 64. The SCP supports only one M-X module. M-X module supports the following wireless devices:

- **X-Shift** – wireless opening detector (for window and doors) (further – detector);
- **X-Shift+** – wireless opening, shock, and tilt detector (for window and doors) (further – detector);
- **X-Motion** – wireless motion detector (further – detector);
- **X-Motion+** – wireless motion and glass break detector (further – detector);
- **X-Motion Alarm** – wireless motion detector with sounder (further – detector);
- **X-Pad** – wireless keypad (further – keypad);
- **X-Key** – wireless key fob (further – key fob);
- **X-Siren** – wireless siren (further – siren);
- **X-Water** – wireless water leak detector (further – detector);
- **X-Cover S** – wireless radio signal repeater (further – repeater).

M-Z+ – a zone expansion module (further – module) intended for adding 8 zones. The SCP supports operation with two modules installed simultaneously.

1.2.3 Keypads

The keypads are intended to monitor and control the system status and connected automation. The SCP supports operation with the following keypads: K-GLCD+, K-PAD4, K-PAD4+, K-PAD8, K-PAD8+, K-PAD16, K-PAD16+, K-PAD OLED, K-PAD OLED+, and X-PAD.

Maximum number of keypads supported by the SCP is as follows:

- Orion NOVA L (LTE) – 12;
- Orion NOVA M (LTE) – 8;
- Orion NOVA S (LTE) – 4;

All the wired keypads are connected via the RS-485 interface (to the A1, B1 terminals of the SCP). For X-PAD wireless keypad connection M-X module should be used. Data exchange between the SCP and the keypads is encrypted. Protection against keypad substitution is provided by a unique serial number. The following keypads: K-PAD4+, K-PAD8+, K-PAD16+, K-PAD OLED+, and K-GLCD+ have a built-in contactless reader allowing to use static NFC tags (cards and key fobs) operating at 13.56 MHz as a user access ID. Identifiers must meet the following standards: ISO14443A, ISO14443B – MIFARE Classic, MIFARE Ultralight, etc.

A short description of the features of the keypads is given in Table 1.1.

Table 1.1 – Short description of the keypad features

Name	Display	Zone state indicators	Two zones can be connected to the keypad	Transistor output	Connection of TM readers	NFC reader
K-PAD4	✗	4	✗	✗	✗	✗
K-PAD4+	✗	4	✗	✗	✗	✓
K-PAD8	✗	8	✓	✓	✓	✗
K-PAD8+	✗	8	✓	✓	✗	✓
K-PAD16	✗	16	✓	✓	✓	✗
K-PAD16+	✗	16	✓	✓	✗	✓
K-PAD OLED	✓	✗	✓	✓	✓	✗
K-PAD OLED+	✓	✗	✓	✓	✗	✓
K-GLCD+	✓	✗	✓	✓	✗	✓
X-Pad	✗	8	✗	✗	✗	✗



When designing a project of the system, we strongly recommend selecting the keypad taking into account the maximum number of zones that can be displayed on it (see Table 1.2).

Table 1.2 – Selecting the keypad depending on the maximum number of zones in the group

Maximum number of zones in groups	K-PAD4, K-PAD4+	K-PAD8, K-PAD8+, X-PAD	K-PAD16, K-PAD16+	K-PAD OLED, K-PAD OLED+, K-GLCD+
1 - 4	✓	✓	✓	✓
1 - 8	✗	✓	✓	✓
1 - 16	✗	✗	✓	✓
1 - 250	✗	✗	✗	✓

1.2.4 Communication modules

The following communication modules are provided for the duplex communication between the SCP and the Tiras CLOUD II service:

M-NET+ is an Ethernet communication module that provides communication via the Ethernet network, requires LAN connection through the RJ-45 physical interface. Orion NOVA L (LTE) is equipped with a built-in Ethernet interface.

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

GSM/LTE ensures communication over the GSM network using 2G and 4G technologies. The module provides the possibility to send SMS messages and make a check call to the user phone number. The module is built-in in the SCP board (Figures A.1 – A.3, [Appendix A](#)) and has a built-in antenna.

1.3 Specifications

The SCPs specifications are given in Table 1.3.

Table 1.3 – SCPs specifications

No	Parameter	Orion NOVA S (LTE)	Orion NOVA M (LTE)	Orion NOVA L (LTE)
1	Number of zones of the SCP / in the system (wired and wireless total), pcs:	4/64 ¹	8/64 ¹	8/250 ¹
2	Number of controlled outputs of the SCP / in the system, pcs:	2/16 ¹	2/32 ¹	6/128 ¹
3	Maximal number of groups in the system	16	32	128
4	Maximal number of users in the system	64		128
5	Maximal number of keypads (interface RS-485)	4	8	12
6	Maximal number of expansion modules (RS-485 interface)	-		15
7	Communication protocol with CMS	"NOVA", "Sur-Gard" (Contact ID)		
8	Radio technology: 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 EGSM900: (TX:880–915) / (RX:925–960) MHz DCS1800: (TX:1710–1785) / (RX:1805–1880) MHz	max RF output power: LTE-FDD: 23 dBm ± 2 dB EGSM900: 33 dBm ± 2 dB DCS1800: 30 dBm ± 2 dB	max RF output power: LTE-FDD: 23 dBm ± 2 dB EGSM900: 33 dBm ± 2 dB DCS1800: 30 dBm ± 2 dB	max RF output power: LTE-FDD: 23 dBm ± 2 dB EGSM900: 33 dBm ± 2 dB DCS1800: 30 dBm ± 2 dB

¹ Expansion of the number of zones and outputs is provided using expansion modules and keypads.

	Wi-Fi ² : 2400.0 – 2483.5 MHz SRD ² : 868.0 – 868.6 MHz	Wi-Fi: 20 dBm SRD: 13.98 dBm	Wi-Fi: 20 dBm SRD: 13.98 dBm	Wi-Fi: 20 dBm SRD: 13.98 dBm
9	Main power source, voltage/frequency/current	187-253 V, 50 Hz ± 1		
		0.09A	0.12A	
10	Backup power supply (battery), voltage/capacity	12 V, 2.2 A·h	12 V, 7 or 9 A·h	
11	Operation time from a fully charged battery of (without considering the consumption of detectors, sirens, additional modules, and keypads), hours, not less than:	30		
12	Protection class	IP 30		
13	Current consumption from the battery, mA, not more than:			
13.1	SCP (without the consumption of external detectors and sirens, without additional devices and keypads)	90	100	140
13.2	M-OUT2R outputs expansion module	40		
13.3	M-X wireless expansion module	25		
13.4	P-IND32 indication panel	-	80	
13.5	M-OUT2R box outputs expansion module <ul style="list-style-type: none"> ▪ all module relays are deactivated ▪ all module relays are activated 	-	30	100
			100	
13.6	M-OUT8R module <ul style="list-style-type: none"> ▪ in normal mode ▪ in activation mode, all relays 	-	25	360
			360	
13.7	K-PAD4, K-PAD4+ keypads	30		
13.8	K-GLCD+ keypad	220		
13.9	K-PAD8, K-PAD8+, K-PAD16, K-PAD16+ keypads	55		
13.10	K-PAD OLED, K-PAD OLED+ keypads	120		
13.11	M-NET+ communication module	80	-	
13.12	M-WiFi communication module	50		
14	M-Z+ module	30		
15	Maximum message transmission time to CMS via Ethernet/Wi-Fi/GPRS/LTE channels, s, not more than	20		
15.1	Zones loop parameters:			
15.2	Maximum resistance of loop wires, Ohm, not more than	470		
15.3	Minimum duration of zone intrusion for the alarm generating, ms, and more	400		
15.4	Resistance of terminal resistor (0.5 W), kOhm	3±1%		
15.5	Zone voltage in the armed mode, V	8-12		
16	Zone current in the armed mode, mA	2.2-5		
17	Switching voltage/current parameters of SCP relay outputs, not more than: <ul style="list-style-type: none"> ▪ DC, V/A 	No relay outputs		24/3 36/3

	<ul style="list-style-type: none"> ▪ AC, V/A 		
18	Switching voltage/current parameters of M-OUT2R relay outputs, not more than: <ul style="list-style-type: none"> ▪ DC, V/A ▪ AC, V/A 	30/5 42/10	
19	Maximum total length of communication lines (distance between end-of-line resistors) with modules and keypads for copper twisted-pair cable with impedance of 100–200 Ohm, and the cross-section diameter 0.51 mm, capacity 40–100 pF/m, m, not more than	1000	
20	Wire cross-section for connecting to SCP terminals, mm ²	0.2-1.5	
21	Maximum technical readiness time, s, not more than	10	
22	Maximum total current load for outputs SIR and +12V and modules in MODULE1 and MODULE2 slots, mA	1000	
23	Maximum current for outputs, mA, not more than: <ul style="list-style-type: none"> ▪ SIR ▪ +12V (for each) 	500 500	
24	Maximum power supply current for each of remote LED outputs (Q1, Q2), mA, not more than	5	
25	Operating temperature range with relative humidity up to 75% without condensation	-10...+40°C	
26	Dimensions (L×W×H), mm, (± 5 mm)	200×200×57	280×280×85
27	Net weight (without battery), kg, not more than	0.8	1.6
28	Maximum 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, expansion modules, detectors, sirens, and other devices. Thick walls, metal partitions, mirrors, etc. reduce the signal range of GSM/LTE, Wi-Fi, and wireless devices. It should be considered when choosing the place for mounting the SCP. The location of the SCP and other system devices should be within the detector-covered area.

2.2 Calculation of electricity consumption in the system

At the designing stage, the currents consumed by all the system devices should be calculated: the SCP, keypads, expansion modules, detectors, sirens, etc. If the total current exceeds the maximum output current of the power outputs on the SCP, expansion modules with their own power supply units (for example, M-ZP mBox – total load current is 1A) or an external PSU should be used.

The total current consumed by all the devices connected to separate power outputs (the SCP, expansion modules with their own power supply units, etc.) should not exceed the maximum output current of these outputs.

If there are no sirens and expansion modules connected to MODULE1/MODULE2 slots in the system, the power outputs of the SCP can be maximally loaded with a consumption current of up to 1000 mA.

2.3 Location of devices

The design of the SCP, expansion modules and keypads allow wall mounting. The basis of the SCP enclosure contains openings for attaching it on screws and holes for fixing with a screw on the wall. The G3 element on the SCP enclosure (see Figures B.1, B.2, [Appendix B](#)) is intended to detect detachment from the wall. It should be wall-mounted using a screw. When enclosure is removed from the wall, G3 remains on it, causing the separation tamper activation. The mounting dimensions of the SCP are shown in Figures B.1 and B.2, [Appendix B](#). The installation dimensions of the keypads and expansion modules are given in the corresponding documentation.

2.4 Cable connections

Electrical connections should be connected according to the electrical connection diagram (see Figures A.1 – A.3, [Appendix A](#)).

To connect the line with the keypads or expansion modules (RS-485 interface), twisted pair cable should be used. In case of a high level of electromagnetic interference at the controlled premises, we recommend using a shielded twisted pair cable (for example, FTP CAT 5e). The cable shield is connected to the GND terminal of the SCP only on one side of the cable, the screen on the second end of the cable must be isolated. If it is necessary to use an already laid line of a long length (especially if the line is laid between buildings), we recommend using additional lightning protection modules for the RS-485 interface.

When designing cable connections in the premises, pay attention to the requirements for the RS-485 bus topology (see Figure 2.1).

Figure 2.1 exemplifies the connection of keypads and expansion modules.

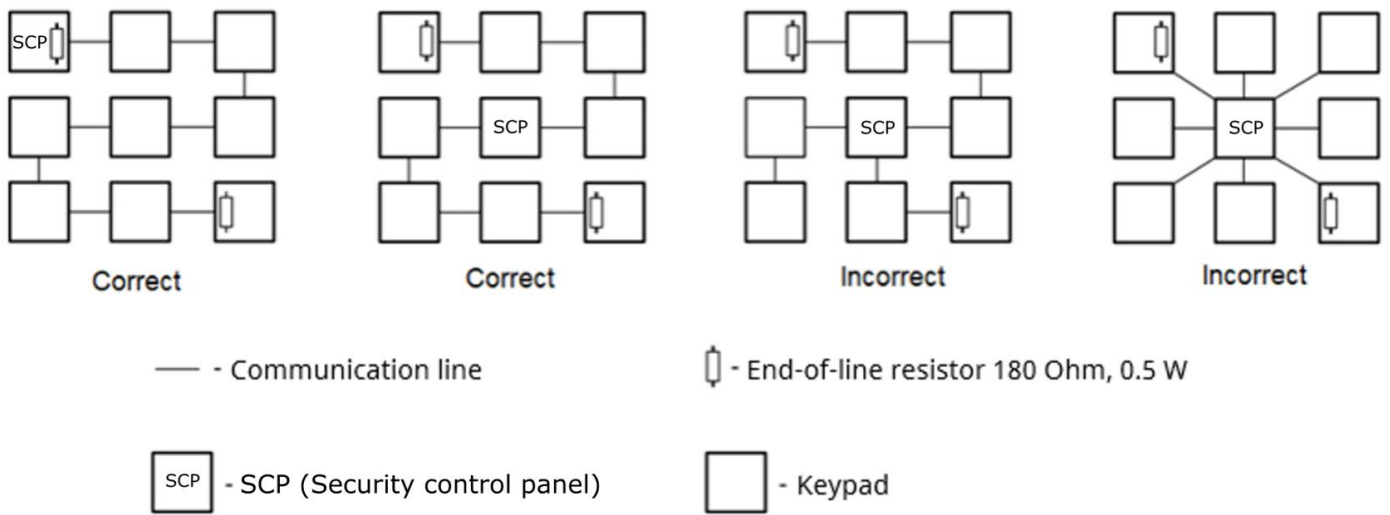


Figure 2.1 – RS-485 bus topology options

For RS-485 interface bus connection (the A, B terminals), the wires of a single twisted pair must be used (see Figure 2.2 – a). The use of different twisted pairs (see Figure 2.2 – b) or the cable wires of different twisted pairs (see Figure 2.2 – c) is not allowed.

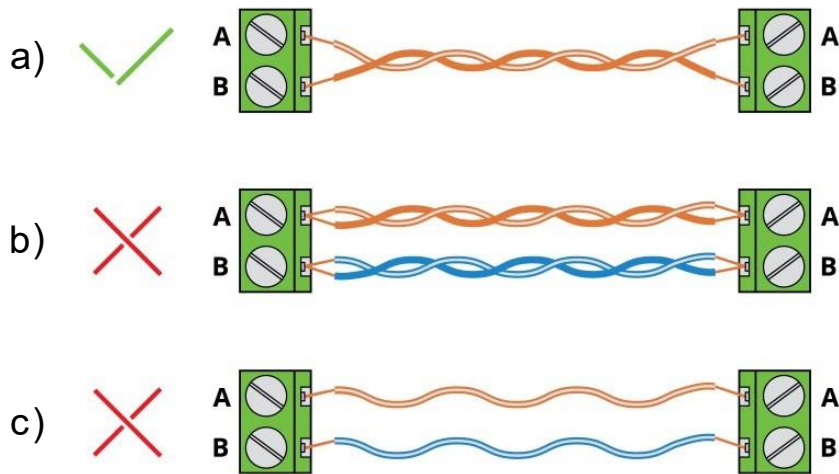


Figure 2.2 – Example of RS-485 interface bus connection

If the length of the communication line exceeds 10 meters, end-of-line resistors 180 Ohm (supplied with the SCP) should be installed at the ends of the communication line (in parallel between the A and B terminals). The circuit ground of the SCP and the elements of the communication line must be interconnected.



If the communication line cable is not of a twisted pair type, the end-of-line resistors are not installed.

When choosing a cross-section of the power wires, the voltage drop between the power output and the connected device must not exceed 1V. If an additional external power supply unit is used, the circuit ground of the additional power supply and the SCP must be interconnected.

2.5 Connection of the SCP board

The SCP board is shown in Figures A.1 – A.3, [Appendix A](#). The description of the terminal block connectors of the SCP is given in Table 2.1.

Table 2.1 – Description of the terminal connectors of the SCPs

Name	Description
Orion NOVA L (LTE)	
Z1...Z8	zones (end-of-line resistors 3 kΩ)
GND	circuit ground
+12V	power outputs
A1, B1	RS-485 keypads bus
A2, B2	RS-485 expansion module bus
Q1, Q2	transistor outputs
SIR1, SIR2	siren
REL1, REL2, NO, NC	relay outputs
TAMPER	connection of intrusion tamper to the SCP
TM	connection of TM key readers
XP1	power input to connect the SCP with a power supply unit
Orion NOVA M (LTE)	
Z1...Z8	zones (end-of-line resistors 3 kΩ)
GND	circuit ground
+12V	power outputs
A1, B1	RS-485 keypads bus
Q1	transistor output
SIR1	siren
TAMPER	connection of intrusion tamper to the SCP
TM	connection of TM key readers
XP1	power input to connect the SCP with a power supply unit
Orion NOVA S (LTE)	
Z1...Z4	zones (end-of-line resistors 3 kΩ)
GND	circuit ground
+12V	power outputs
A1, B1	RS-485 keypads bus
Q1	transistor output
SIR1	siren
TAMPER	connection of intrusion tamper to the SCP
XP1	power input to connect the SCP with a power supply unit

The terminal connector TAMPER on the SCP board is intended for connecting the tamper of intrusion detection to the SCP enclosure. The TAMP2 button on the other side of the SCP board is used to detect the separation of the SCP enclosure from the wall.

2.6 Keypads connection

2.6.1 Wired keypads connection

The RS-485 keypad interface (the A and B terminals) is connected to the terminals A1 and B1 of the SCP. The example of the keypad connection is shown in Figure 2.3 (the SCP at the beginning of the communication line) and Figure 2.4 (the SCP in the middle of the communication line). To connect the communication line and power supply line of the

keypads, use the wires of a single cable, if the cable length does not exceed 30 m. If the quality of the communication line is low (the number of lost packages with the keypad exceeds 10 in the Installer "Devices control" menu), check the quality of installation and its compliance with the requirements of this section.

In case of equipment replacement, when the signal cable for the communication line with the keypad is already mounted on the object, the "Enable lower speed of transition between SCPs and keypads" option can be enabled to improve the exchange (see [3.2.10](#)).

2.6.2 Wireless keypads connection

The system supports up to 4 wireless keypads. Before installing the X-Pad wireless keypad, it should be added to the M-X module. The procedure of wireless keypads adding is described in section 4.4.

After adding the keypad, it is necessary to check its ability to transmit signals to the SCP from the place of the planned installation. To check the quality of the communication, it is necessary to check the status of the keypad (section 4.4). If the communication quality is low or the SCP does not receive signals from the keypad, the location of the keypad should be changed. After achieving the high or medium communication quality between the SCP and the keypad, it can be fixed in place.



In case of M-X module replacement, the activation of X-Pad should be repeated.

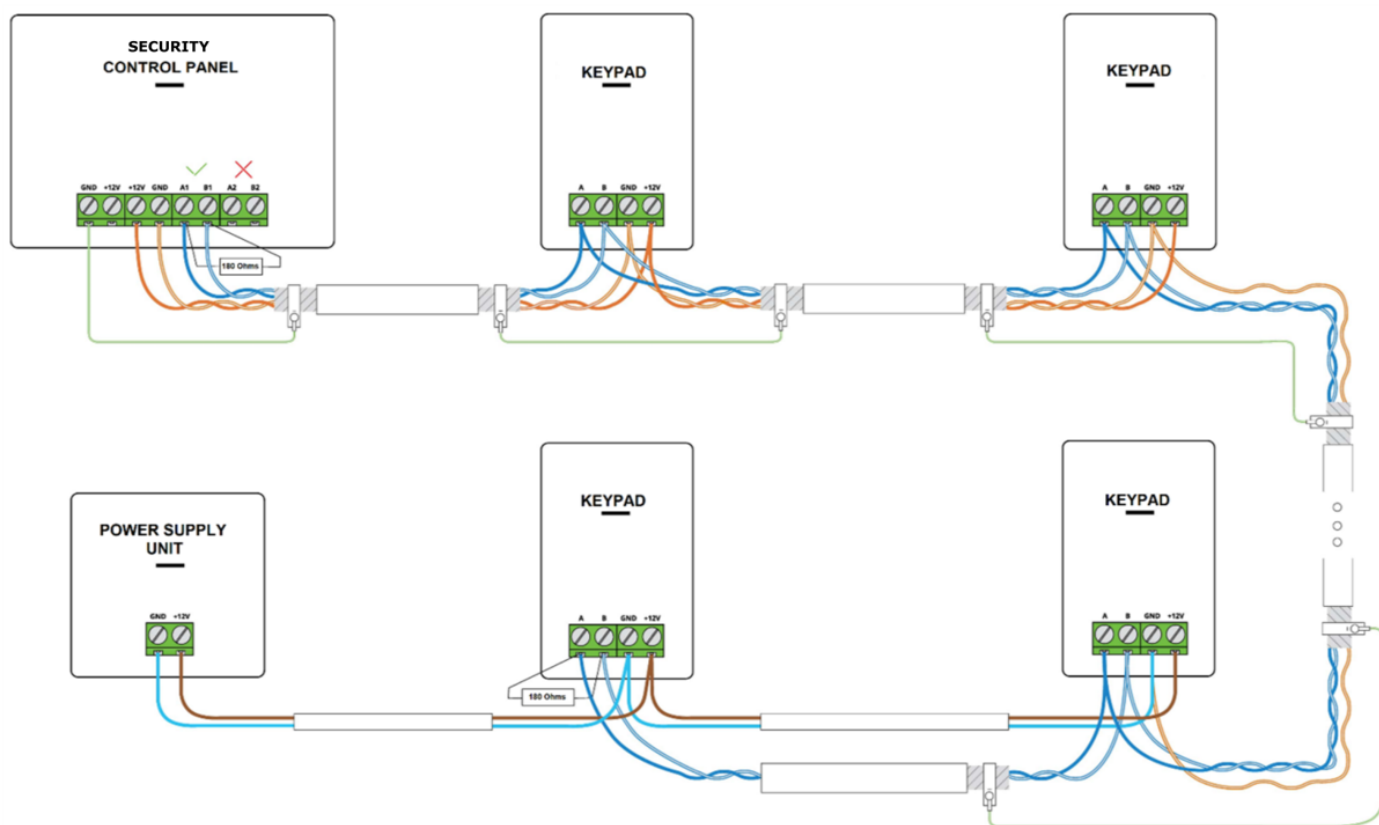


Figure 2.3 – Example of keypads connection (the SCP is at the beginning of the communication line)

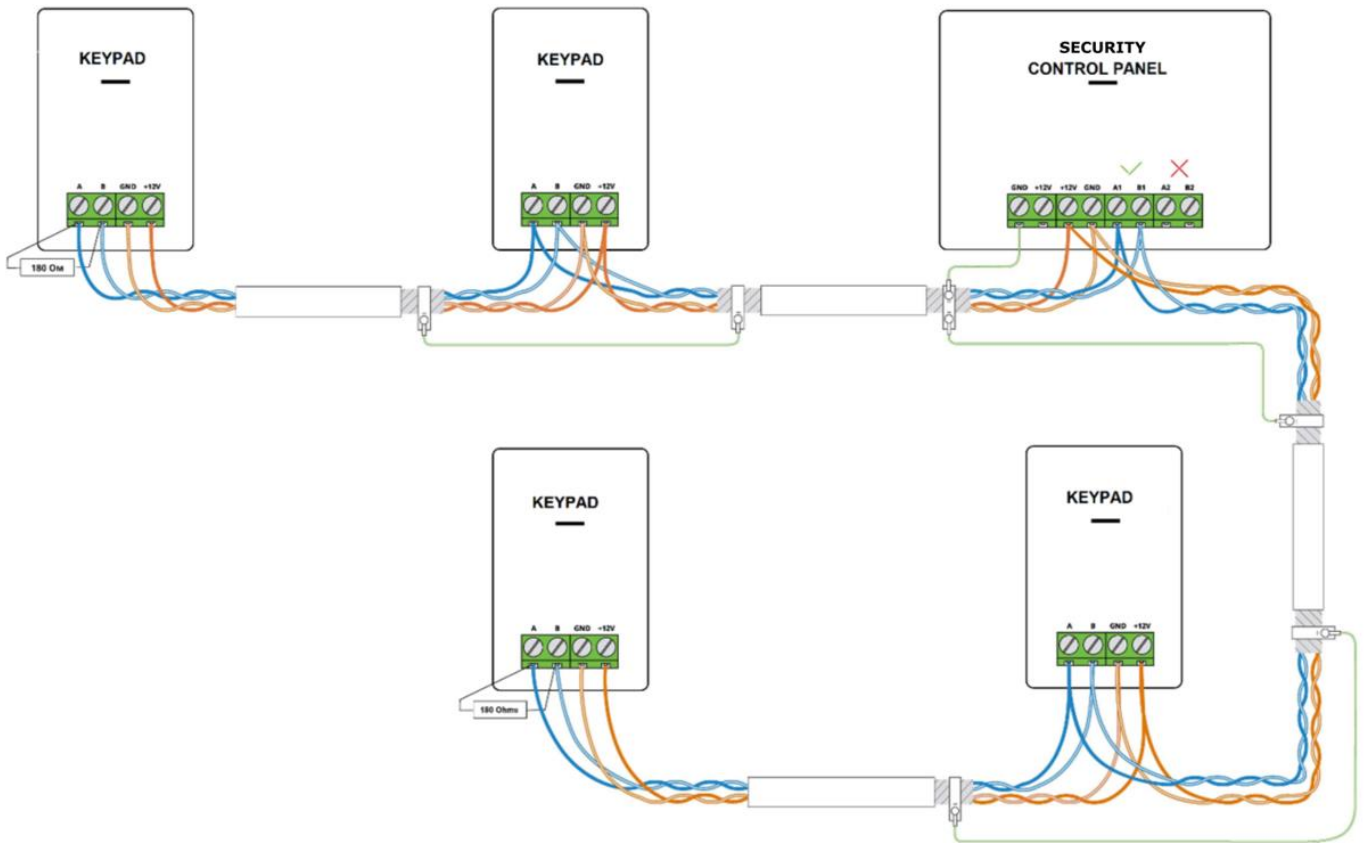


Figure 2.4 – Example of keypads connection (the SCP is in the middle of the communication line)

2.7 Expansion and indication modules connection

The RS-485 interface of expansion and indication modules is connected to the A2 and B2 terminals of the SCP. The example of such a connection is shown in Figure 2.5 (the SCP is at the beginning of the communication line) and Figure 2.6 (the SCP is in the middle of the communication line). For the modules requiring an external power supply, use the wires of a single cable to connect the communication line and +12V power supply line, if the distance does not exceed 30 m. If the quality of the communication line is low (the number of lost packages with the keypad exceeds 10 in the Installer "Devices control" menu), check the quality of installation and its compliance with the requirements of this section.

The SCP supports operation with the following modules: M-OUT2R module, M-Z+ module and the M-X module for wireless devices connection. These modules are installed on the SCP board in the MODULE1 or MODULE2 connector (see Figures A.1 - A.3, [Appendix A](#)). The LED indicators on the SCP are intended to show the operating status of the M-X module: HL1 – for the MODULE2 connector, HL2 – for the MODULE1 connector (see Figure A.1 – A.3, [Appendix A](#)). These indicators operate in pulse mode according to Table 2.2.

Table 2.2 – Operation modes of HL1 and HL2 indicators with M-X¹ module

Indicator operation mode	Value
No lights	Module is not configured in the system
Blinks	Data exchange with wireless device (test or event)

¹ The description of the indicators' operation is given for the operating mode of the SCP.

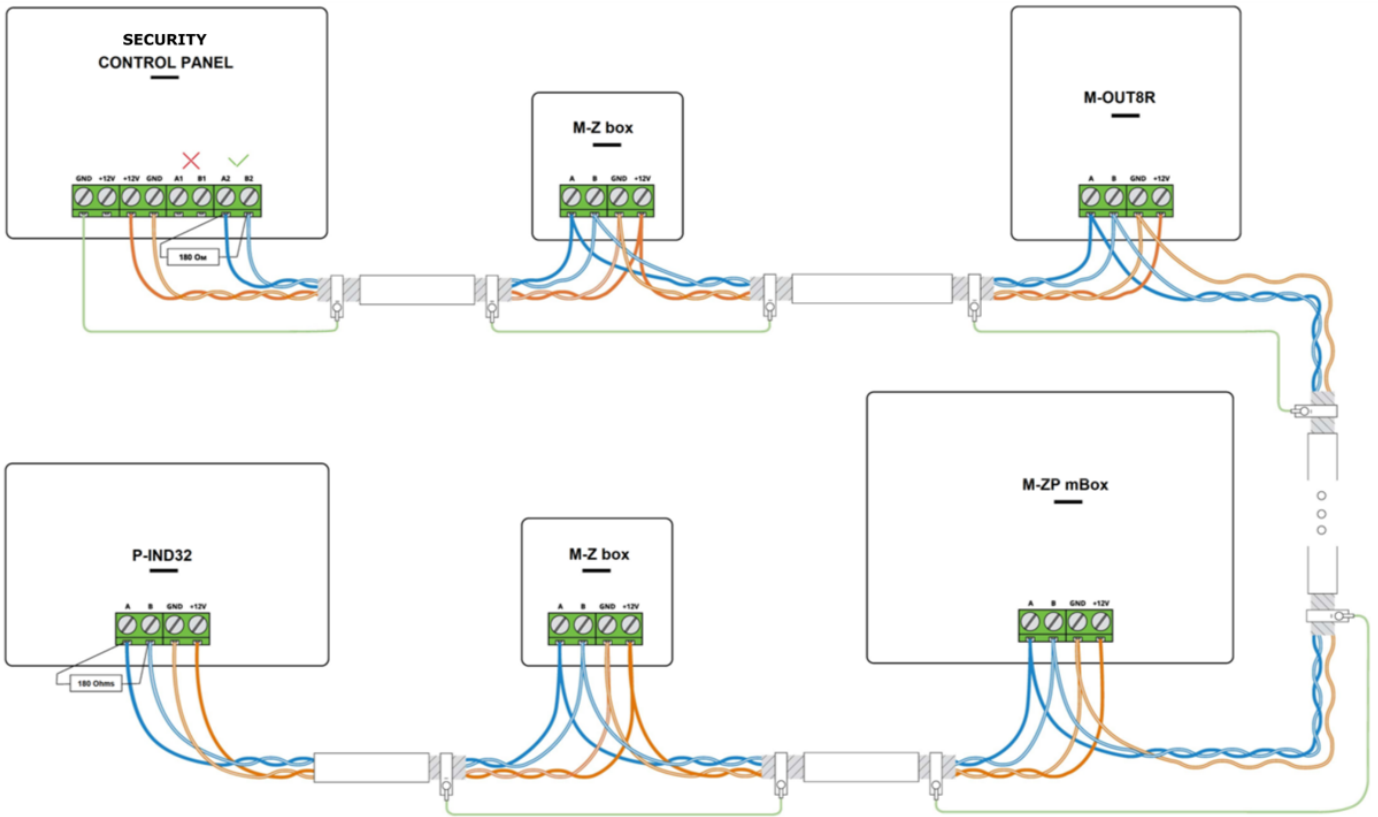


Figure 2.5 – Example of remote modules connection (the SCP is at the beginning of the communication line)

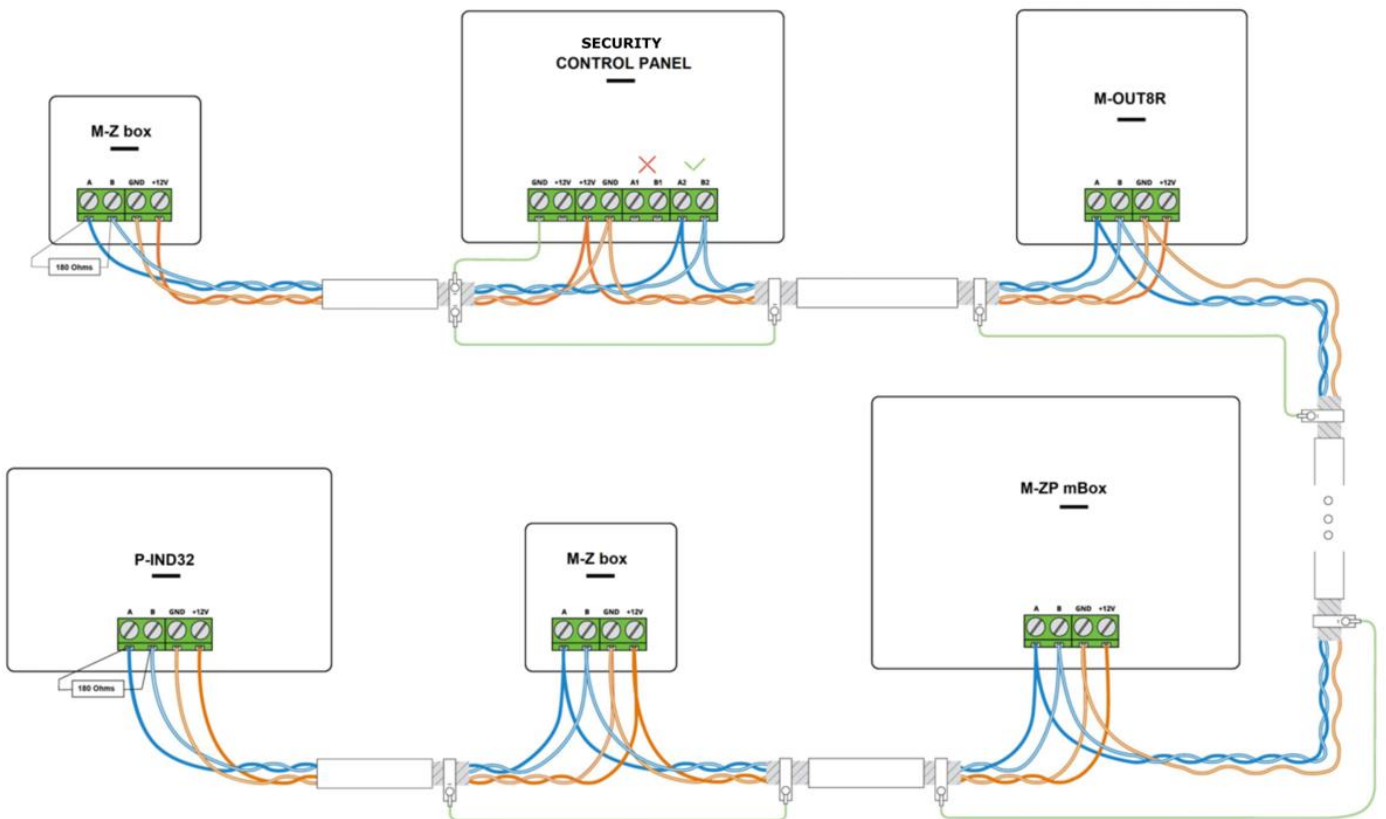


Figure 2.6 – Example of remote modules connection (the SCP is in the middle of the communication line)

2.8 Detectors connection

The keypads have "Zones testing" option to test the performance of the connected detectors (see 4.8).

2.8.1 Connection of the wired detectors

Wired detectors are connected according to Figure 2.7. The technical documents for the expansion modules and keypads contain information about the connection of wired detectors to zones terminals.

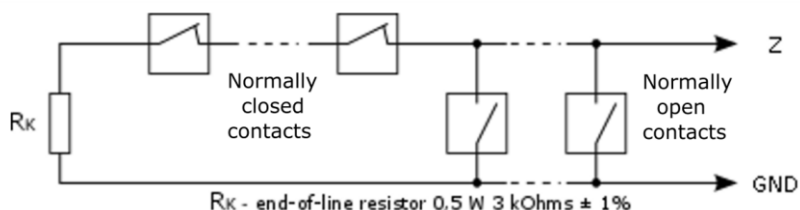


Figure 2.7 – Connection diagram for intrusion detectors with normally closed and normally open contacts

Zones of 2EOL type can be connected to the SCP zones and zones of the M-ZP mBox module. The "2EOL" option in the zones' settings should be enabled. The connection of the 2EOL type zones allows simultaneous control of the detector and its tamper state due to the change of resistance in the zone (see Table 2.3).

Table 2.3 – Change of zone status depending on the loop resistance

Zone state	Penetration alarm	Norm	Intrusion alarm	Penetration alarm
Resistance, kOhms	0 - 2.2	2.3 - 4.2	4.3 - 10	10 - ∞

Examples of 2EOL type detectors' connection are shown in Figure 2.8, a) – connection using three cable wires, b) – connection using four wires.

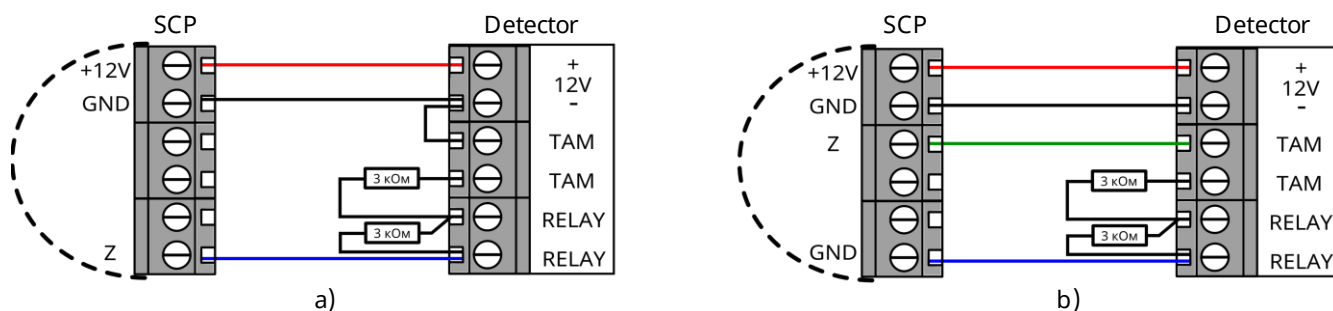


Figure 2.8 – Examples for connecting the 2EOL type detectors

The detectors requiring +12V for operation are connected to +12V terminal connectors on the board of the SCP or expansion modules with their own PSU (for example, M-ZP mBox). The detectors and/or devices requiring a controlled power supply of +12V are connected to the SIR terminal on the SCP board. The output must be respectively set.

2.8.2 Connection of the detectors requiring a power reset

Two-wire detectors requiring a power reset must be connected according to the diagram shown in Figure 2.9. The number of two-wire detectors that can be connected in parallel is limited by their total current consumption in the armed mode $I_{max} = 1 \text{ mA}$.

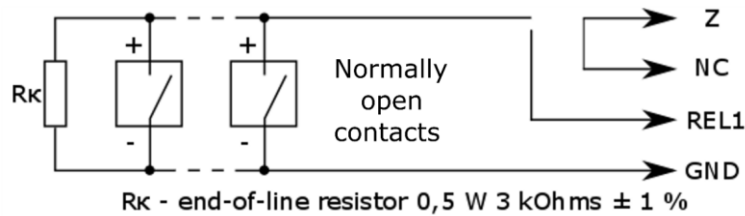


Figure 2.9 – Connection diagram for two-wire detectors with normally open contacts

To enable the alarm reset of two-wire detectors after their triggering, it is required to configure a script that opens the contacts of the relay output of the SCP for 5 seconds.

2.8.3 Connection of the wireless detectors

Before installing the wireless detectors, they should be added to the zone of the M-X module. The wireless detectors adding process is described in section 4.4.



The process of the wireless detector adding to the zones can be carried out with any keypad type (except X-Pad) or when the SCP is running.

After adding the detectors to the zones, check the possibility of transmitting signals to the SCP from the place of the planned installation. To check the connection quality, the detector state polling or detector tamper activation should be initiated. If the SCP does not receive signals from the detector, change the detector location. Once a stable connection between the SCP and the detectors is achieved, they can be installed in the planned location.

X-Shift and X-Shift+ detectors allow to connect an additional detector (with NC contacts) to an external contact. Triggering the main and additional detectors are informatively different.



In case of M-X module replacement, the adding of detectors should be repeated.

2.9 Siren connection

The sirens are connected to the SIR terminal on the SCP board or to the appropriate outputs of expansion modules. To monitor the communication line with the detector, connect the EOL resistor of 3 kΩ to the terminal connectors of the detector as it is shown in Figures A.1 – A.3, [Appendix A](#). It is also possible to calibrate the EOL resistors from 1 kΩ to 7.5 kΩ. The description of the "EOL CALIBRATION" setting is described in 4.14.



When tampering the SCP, keypads, expansion modules, 2EOL zones and zones of the Tamper type, the siren is activated only if the armed groups are available.

2.10 Confirmation indicator connection

LED confirmation indicators can be connected to the outputs of the SCP, expansion modules and keypads according to the diagrams shown in Figure 2.10: a) connection according to the Remote LED scheme, b) connection according to the Open collector scheme.

The operating modes of the "Confirmation" indicator are described in Table C.1, [Appendix C](#).

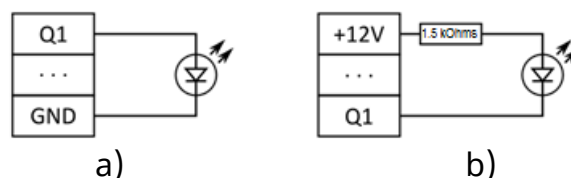


Figure 2.10 – Connection diagrams for "Confirmation" indicators

2.11 TM key readers connection

TM key readers are connected to the appropriate terminals of the SCP (see Figures A.1 – A.3, [Appendix A](#)), expansion modules and keypads (connection diagrams are provided in the appropriate documents). The SCP works with the keys of the following series: 1961S, 1963L, 1971, 1972, 1973, 1977, 1982, 1982U, 1985, 1990A, 1992, 1993, 1995, 1996, together with key readers, as well as key fobs, along with the readers emulating operation in TM readers. The attachment of the key fobs is equivalent to applying TM keys. The LEDs built into the reader can be connected to the SCP as remote confirmation LEDs. The connection diagram for the TM reader is shown in Figure 2.11.

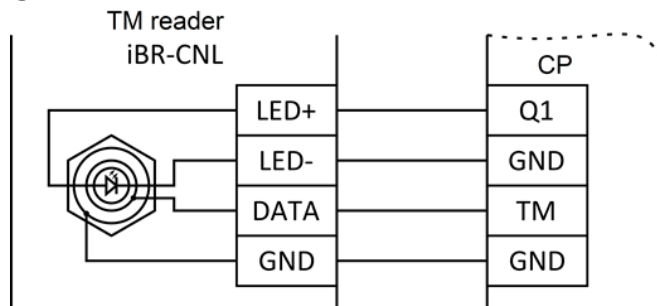


Figure 2.11 – Connection diagram for the TM key reader

The maximum length of the communication line of the SCP with the TM key readers is limited by its capacity (4 nF) and is ~30 m for a wire of 2×0.4 mm² type. The maximum line resistance is 100 Ohm. The required number of readers is connected in parallel. When connecting readers, comply with the requirements described in the documents on the reader.



Some readers switch to external indication control only after the first change of output state to which the reader's LED is connected.

2.12 Working with GSM/LTE module

To work via the GSM/LTE channel, install SIM cards in the corresponding holders. Check the GSM signal strength for each SIM card. To display the signal strength, SIM1/SIM2 indicators on the SCP are used, the signal strength gradation is given in Table 2.4. The GSM/LTE signal strength can be viewed from the keypads or the Control NOVA II software.

Table 2.4 – Gradation of the signal strength of the GSM network on the SIM1 and SIM2 indicators of the SCP

GSM signal strength (number of dials on the indicator SIM1/SIM2)	Compliance with GSM 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 GSM signal strength (three flashes of the SIM indicator) with the supplied antenna, or the unstable operation of the GSM/LTE channel is observed during the operation of the SCP, we strongly recommend using an additional Ethernet/Wi-Fi channel (M-NET+/M-WiFi is required) or connecting an external GSM antenna

to the SMA connector (see Figures A.1 – A.3, [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 (see 3.2.9). This option can be enabled only after the connection of the external antenna to the connector.

To determine the state of the GSM/LTE connection, the GSM-NET LED indicator on the board of the SCP is in pulse mode according to Table 2.5.

Table 2.5 – Operating modes of GSM NET, SIM1, and SIM2 indicators on the SCP board

GSM NET indicator state (2G)	GSM NET indicator state (4G)	Registration status
Lights	Lights	Network searching
Blinks once per second	Blinks three times per second	Registered in the network
Blinks three times per second		Data transmission
No lights	No lights	No connection or turned off



We do not recommend installing the antenna near sources of powerful electromagnetic radiation (electric motors, X-ray machines, etc.). Insert/remove SIM card only when the SCP is powered off.

2.13 Working with M-NET+ and M-WiFi modules

Depending on the model of the SCP, the configuration of the Ethernet communication channel differs.

Orion NOVA L (LTE) is equipped with a built-in Ethernet interface (marked as ETHERNET in Figure A.1, [Appendix A](#)) to which the Ethernet network cable (RJ-45 interface) is connected ensuring the communication via Ethernet.

Orion NOVA S (LTE) and Orion NOVA M (LTE) do not have a built-in Ethernet interface, therefore, to work via the Ethernet channel, install the M-NET+ module (supplied separately) in MODULE1 or MODULE2 of the SCP (see Figures A.2 and A.3, [Appendix A](#)). The Ethernet network cable (RJ-45 interface) should be connected to the RJ 45 socket marked as the X1 connector on the M-NET+ board.

To work via the Wi-Fi channel, install the M-WiFi module (supplied separately) in MODULE1 or MODULE2 of the SCP (see Figures A.1 – A.3, [Appendix A](#)). Wi-Fi signal strength can be viewed on the keypad (section 4.15) or in the Control NOVA II or oLoader II software. The gradation of the signal strength is given in Table 2.6.

Table 2.6 – Gradation of the Wi-Fi signal level

Signal strength, dBm	Signal quality
< -81	Insufficient (possible loss of connection)
-80...-71	Minimally permissible (possible transmission delay of messages)
-70...-61	Sufficient
-60...-10	High

To determine the operation status of M-NET+ and M-WiFi modules, look at the LEDs located on the SCP board: HL2 for the MODULE1 connector, and HL1 for the MODULE2 (see Figures A.1 – A3, [Appendix A](#)). These indicators operate in pulse mode according to Table 2.7.

Table 2.7 – Operation modes of HL1 and HL2 indicators for M-NET+ and M-WiFi modules

Indicator operation mode	Status
No lights	Unset in the system
Blinks	Data exchange via Wi-Fi/Ethernet (from the CMS and/or Tiras CLOUD II)

Lights permanently	The module is connected and configured but cannot connect to the Internet
---------------------------	---



The SCP operates with only one of the M-NET + or M-WiFi modules simultaneously.

2.14 Working with the wireless devices

The SCP operates with the wireless devices if the M-X module is used. The gradation of the signal strength of the wireless devices is given in Table 2.8.

Table 2.8 – Gradation of the signal strength of the wireless devices

Signal strength, dBm	Signal quality
< -91	Insufficient (possible loss of connection)
-90...-80	Minimally permissible (possible transmission delay of messages)
-79...-70	Sufficient
-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 M-X module and choose a permanent place of operation with the best signal strength.

2.15 Complex inspection after installation



After installation of 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 recording of the settings and equipment malfunctions.

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

- 1) Make sure that the SCP transmits the messages listed below to the CMS and/or Tiras CLOUD II, alternately via each configured communication channel (each SIM card, M-NET+ or M-WiFi connection module):
 - control of the group(s) using each registered access ID of users;
 - transition to the "Armed mode" of each zone of the system;
 - generation of "Alarm" message in case of intrusion of each zone and interference into the body of the system device.
- 2) Make sure that the terminal connectors are connected to the battery contacts. Check the performance of the SCP and the system devices from the battery (main power should be turned off).
- 3) Remove tamper blocker jumpers (on those system devices where they are available).
- 4) After installation seal the device (if necessary). The cases of all keypads, modules and the SCP during operation should be closed.




For the SCP tamper detection, the options "The housing is opened" and "Break from wall tamper" (see 3.2.1) should be enabled. For system devices tamper detection, the "Tamper protection" option (see 3.2.1, 3.2.2) should be enabled.

2.16 System operability

As a result of the failure of any of the system devices, the level of protection decreases.

The devices installed outdoors (for example, outdoor sensors and sirens) are exposed to adverse environmental effects. During a thunderstorm as a result of atmospheric lightnings, devices that are connected to electrical systems are at risk of damage.

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 indicator on the keypad. It is necessary to respond to such a situation in time and to consult the system installer, if necessary.

3. SYSTEM CONFIGURATION

The SCP can be configured by means of:

- Windows PC/MacOS or Android device with installed oLoader II software (locally or remotely) – full configuration;
- connected display keypads – partial configuration.

3.1 Configuring the SCP by means of oLoader II software


oLoader II is a special software intended to configure the SCP. The Windows PC/MacOS versions are available for download on the manufacturer's website: tiras.technology in the "Products/Wired security systems/Software" section. The Android version is available in Google Play. A detailed description of the SCP settings in oLoader II software is given in section 3.2.

The SCP can be configured with the oLoader II software both locally (via cable connection) or remotely (via the Tiras CLOUD II service, if allowed in the SCP settings).

The software version of the SCP is displayed when the settings are downloaded from the SCP in the "Devices" tab in the "SCP" item.

3.1.1 Local SCP configuring using oLoader II software

The local connection of the SCP to Windows PC/MacOS or Android devices is carried out via the USB interface. To configure it, do the following:

- open the SCP's case, turn off the SCP's main power (230V), disconnect the terminals from the battery;
- connect a USB cable to the SCP and Windows PC or Android device using a USB-A/mini USB-B or USB-C (for version 3.7) cable to connect to the PC. For connecting to the Android device, two cables are used: USB-OTG/micro USB-B or USB-OTG/USB-C and USB-A/mini USB-B or USB-C (for version 3.7);
- launch the oLoader II software – the main window will be displayed;
- download settings from the SCP by clicking the "Configure locally" button in the menu, then click the "Open configuration from device" button;
- change settings;
- upload settings to the SCP by clicking the "Save in device " button (it may require entering the valid installer code, depending on the settings of the "Configuration protection with installer code" option);
- disconnect the USB cable (before disconnecting the USB cable from the PC or the Android device, the safe disconnection of the SCP (similar to the USB flash drive disconnection operation) **must be** performed).



To enable local control of the SCP, the Android device must support USB-OTG technology.



To reduce the Android device battery discharging, we strongly recommend disconnecting the Android device from the SCP during configuration editing. It is enough to connect during downloading the settings from the SCP and uploading them to the SCP.

To start the SCP, connect the terminals to the battery and turn on the 230 V power supply.



After changing the SCP's settings in the oLoader II software, when the SCP is turned on, all zones will have their initial state: "Entrance door", "Corridor", "Security" are disarmed, while "Panic button", "24h", "Universal input", "Tamper", "Anti-masking" – armed. Before changing the

configuration of the SCP, the authorized person must notify the users of the system that the configuration of the SCP will be changed, and the user groups will be disarmed.




After turning it on, the SCP will begin to accept the settings downloaded from the oLoader II software if the configuration is correct. During this process, the SIM1 and SIM2 indicators will blink rapidly (one by one). After receiving the configuration, the active SIM card indicator and (or) the GSM NET indicator will blink.

If after changing the configuration and the SCP turning on, the SIM1 and SIM2 indicators don't blink (as described above), and the GSM NET indicator blinks immediately, this means that the SCP has not accepted the new settings. In this case, you need to do the following:

- check the access to the 3rd level (see 3.2.10);
- make sure that the entered access code of the installer is correct;
- format the SCP flash drive to exclude its failure.

3.1.2 SCP default settings configuring in oLoader II software

To configure default settings in the SCP using the oLoader II software, do the following:

- connect a USB cable to the SCP and Windows PC/MacOS or Android device as described in section 3.1.1;
- launch the oLoader II software – the main window will be displayed;
- click the "Configure locally" button in the menu;
- click the "Create configuration" button;
- select the SCP and the required version;
- upload settings to the SCP by clicking the "Save in device " button (it may require entering the valid installer code, depending on the settings of the "Configuration protection with installer code" option);
- disconnect the USB cable (before disconnecting the USB cable from the PC or the Android device, the safe disconnection of the SCP (similar to the USB flash drive disconnection operation) **must be** performed);
- switch on the SCP.

After switching on, the SCP will set the default settings given in Table D.1 (Appendix D).

3.1.3 Reset of user access IDs

To reset user access IDs, do the following:

- open the SCP's case, turn off the SCP's main power (230V), and disconnect the terminals from the battery;
- connect the terminals to the battery, press and hold the "RESET" button, and press the "BAT START" button (see Figures A.1–A.3, [Appendix A](#)). After the GSM NET indicator starts lightning, the buttons can be released.

User access IDs will be changed to the default settings (see Table D.1, [Appendix D](#)), while other settings of the SCP remain unchanged.



If the "Configuration protection with installer code" (see 3.2.10) is enabled, then after resetting the user access IDs, the change of the SCP's settings using the oLoader II software will be possible by entering the default installer code (S/N of the SCP) while writing the settings (only if the installer code has not been changed after reset of the IDs).



After user access IDs resetting, we strongly recommend changing the default access IDs to enhance security.


3.1.4 Remote SCP configuring using oLoader II software

The remote configuration of the SCP is possible when it works with the Tiras CLOUD II service and Internet connection is available for Windows PC/MacOS or Android devices.

For remote configuration of the SCP, do the following:

- 1) launch the pre-installed oLoader II software – the registration window opens to create an account or log in;
- 2) create an account in the Tiras CLOUD II service or use an existing one;
- 3) install a SIM card with available Internet traffic in the SIM1 slot (while doing this, the SCP should be disconnected from the power supply).

SCP Orion NOVA L (LTE) can be connected to the Internet via the Ethernet channel. To do this, connect the SCP to the network equipment with automatic configuration (DHCP) via the ETHERNET connector on the board.

- 4) power on the SCP;
- 5) wait for registration in the mobile operator network and synchronization with the server (approximately 2 minutes);
- 6) add the SCP to the Tiras CLOUD II account within 10 minutes after powering on. For the SCP adding in the oLoader II software, do the following:
 - in the opened window, press the "+" button (add);
 - after opening the "Add device" window, you need to enter the following in the fields:
 - in the "Serial number" field – enter the 9-digit serial number of the SCP;
 - in the "Installer password" field – enter the default installer access code (9-digit serial number of the SCP);
 - in the "Object name" field – enter the name of the object (from 1 to 50 characters);
 - click the "Add" button.
- 7) select the required SCP from the list of objects and enter the valid installer code (after entering the installer code, the window with general parameters and the SCP's status will open);
- 8) press the "SCP setting" button, which will download the SCP settings to the software;
- 9) change the SCP settings;
- 10) upload the settings to the SCP by pressing the "Upload to device " button.

If the SCP **is disarmed** when it receives the configuration, it will reboot and accept the new configuration.

If the SCP **is armed** when it receives the configuration, it will accept the new configuration after disarming all the security system groups or after rebooting.

3.2 Description of the SCP settings

3.2.1 Devices

The SCP **Orion NOVA L (LTE)** supports operation with not more than 15 remote modules. The unique 9-digit serial numbers specified in user manuals are used for the identification of remote expansion and indication modules in the system. To add a remote module to the

system, specify its type and serial number in the appropriate settings in the oLoader II software.

When configuring the operation of the modules, specify additional parameters according to Tables 3.1 and 3.2.

Table 3.1 – The SCP settings

Parameter	Description
Zones	The SCP allows to add up to 250 zones to the system. This option allows to select zones of the SCP which will be used in the system.
Outputs	The SCP allows to add 6 outputs to the system (10 outputs when using two M-OUT2R modules). This option allows to select the outputs of the SCP that will be used in the system.
The housing is opened	This option allows to enable or disable the case intrusion tamper in the SCP.
Break from wall tamper	This option allows to enable or disable the software analysis of separation from the wall tamper on the SCP case.
MODULE 1/MODULE 2	In case of using the MODULE1 or MODULE2 slots for a communication module or an expansion module, specify its type. The available values are Do not use, M-OUT2R, M-X, M-WiFi, and M-NET+ (for Orion NOVA S/M (LTE)). It is not allowed to set two wireless expansion modules or M-WiFi and M-NET+ modules simultaneously.
M-X module settings	
Wireless zones	This option allows to select the wireless zones of the M-X module to be added to the system. The M-X module allows to add up to 64 wireless zones to the system. The number of zones corresponds to the number of detectors that can be assigned to them.
Communication test interval	This option allows to set the time interval of sending tests by wireless detectors to monitor communication: from 10 to 3600 seconds. If you change the intervals for testing communication with the detector from a longer to a shorter one, a loss of communication may occur before the device accepts the new setting.
Number of missed tests	This option allows to set the number of missed test messages to generate a message about a loss of communication with wireless detectors: from 3 to 20 tests.

Table 3.2 – Settings of remote expansion and indication modules

Parameter	Description
Title	Specify the device name in the system.
Device type	Select the device type: M-Z box, M-ZP mBox, M-OUT2R box, M-OUT8R, P-IND32.
Serial number	Specify the nine-digit device serial number for identification in the system.
Zones	Select zones of the remote expansion module to be added to the system. This option is available for the M-Z box and M-ZP mBox modules only.

Outputs	Select the outputs of the remote expansion module to be added to the system. This option is available for the M-ZP mBox, M-OUT2R box, and M-OUT8R modules only.
M-Z module use	Enable this option to use eight additional zones by connecting the M-Z module. This option is available for the M-ZP mBox module only.
M-OUT2R module use	This option allows to use two additional relay outputs by connecting the M-OUT2R module. This option is available for the M-ZP mBox module only.
Tamper control	This option allows to enable or disable the software analysis of the tamper protection for remote expansion module. When the SCP operates in accordance with Security Grade 2 or Security Grade 3 (see 3.2.10), this option is ignored and tamper protection is always enabled.
Display mode	This option is available for P-IND32 indication panel only. Select the indication mode of the panel indicators. The following values are available for selection: Zone status display – up to 32 zones can be selected, their status will be indicated on the panel indicators; Group status display – up to 32 groups can be selected, their status will be indicated on the panel indicators. The operating modes of the SCP indicators are described in Table D.2, Appendix D .

3.2.2 Keypads

The SPC supports operation with keypads. To identify the keypads in the system, their serial numbers are used. When adding keypads to the system, specify their type and serial number in the corresponding fields of the oLoader II software:

Maximum number of the keypads supported by the SCP depending on the SCP model is as follows:

- Orion NOVA S (LTE) – 4;
- Orion NOVA M (LTE) – 8;
- Orion NOVA L (LTE) – 12.

There are only 4 of the general number of supported keypads, however, the wireless keypads can be added.

When configuring the added keypads, specify additional parameters according to the table below.

Table 3.3 – Keypad settings

Parameter	Description
Title	Specify the name of the keypad in the system.
Keypad type	Select the keypad type: K-PAD4, K-PAD4+, K-PAD8, K-PAD8+, K-PAD16, K-PAD16+, K-PAD OLED, K-PAD OLED+, K-GLCD+, X-PAD (if M-X module is used).
Serial number	Specify the serial number of the keypad for identification in the system.
Permanent indication	If this option is enabled, the permanent indication (system status indicators and zones) of the selected keypad will be displayed without entering access ID.

Display mode	<p>This option allows to select displaying mode of keypad indicators. The following options are available:</p> <p>Zone status display – up to 4/8/16 zones (depending on the keypad type) can be selected, their status is displayed on the keypad indicators;</p> <p>Group status display – up to 4/8/16 groups (depending on the keypad type) can be selected, their status is displayed on the keypad indicators.</p>
Power indicator inverse mode	<p>If this option is enabled, then in case of absence of power supply faults in the system, the "Power" indicator on the keypad will be switched off. The option is configured if the "Permanent indication" option is enabled.</p>
Buzzer on input/output¹	<p>If this option is enabled, the keypad will generate an intermittent sound signal during an entry/exit delay in any zone of the "Entrance door" type, and a time countdown will be displayed on the display keypads.</p>
Buzzer on alarm¹	<p>If this option is enabled, the keypad will duplicate the sound of the siren by a built-in buzzer.</p> <p>If this option is enabled and the <u>Siren confirmation</u> option is enabled in one of the groups, then the keypad's sound confirmations will be similar to a wired siren.</p>
Tamper control	<p>This option allows to enable or disable the program analysis of the tamper protection of the keypad. When the SCP operates in accordance with Security Grade 2 or Security Grade 3, this option is ignored and tamper control is always enabled.</p>
Zones¹	<p>This option allows to select the keypad zones to be used in the system. All types of keypads except K-PAD4, K-PAD4+ and X-Pad allow adding two zones to the system. Keypad zones are added to the general list of zones (see 3.2.3).</p>
Outputs¹	<p>This option allows to add a keypad output to the system. All types of keypads except K-PAD4, K-PAD4+ and X-Pad allow to add one output to the system. Keypad outputs are added to the general list of outputs (see 3.2.4).</p>
Presence¹	<p>This option allows to select zones, in case of intrusion of which the keypad display and illumination will be switched on. You can select the following zones: "Entrance door", "Corridor", and "Security".</p>
Doorbell¹	<p>This option allows to select zones, in case of intrusion of which the keypad will generate 4 short beeps. You can select the following zones: "Entrance door", "Corridor", and "Security".</p>
Functional buttons	<p>The option allows to configure the functional buttons on the K-PAD series, K-GLCD+ and X-Pad keypads. The functional buttons can be assigned: turn on output, turn off output, toggle output, start script, stop script, show list of scripts. The "Show list of scripts" option is only available for K-GLCD+ and K-PAD OLED/OLED+.</p> <p>Outputs with operating mode "Controlled by user" and scripts with a method of launching by an unauthorized user are available for configuration.</p>

¹ Unavailable for X-PAD keypads.

Advanced settings for X-Pad wireless keypads	
Communication test interval	This option allows to set time interval for sending tests by wireless keypads to monitor communication. This option can be set from 10 to 3600 seconds. This option affects the keypad battery life.
Number of missed tests	This option allows to set the number of lost test messages to generate a keypad communication loss event. This option can be set from 3 to 20 tests.
Duration of bright illumination	After the set time expires, the keypad backlight will light at 50% brightness till the keypad enters pending mode. The time countdown starts after the last key press. This option can be set from 5 to 17 seconds.
Time to enter standby	This option allows to set the time interval for entering pending mode after the last key press on the keypad. The time is set from 5 to 20 seconds. In standby mode, there is no keypad backlight, and the status of the system and zones is not displayed on the indicators.
Sound when buttons are pressed	If this option is enabled, pressing the keys on the keypad will be accompanied by a buzzer.
Exit buzzer	If this option is enabled, the keypad will emit an intermittent sound signal during an exit delay in any zone of the "Entrance door" type.

3.2.3 Zones

Maximum number of zones in the system depends on the settings of the expansion modules and keypads, but it cannot exceed 250 for Orion NOVA L (LTE) and 64 for Orion NOVA S/M (LTE). Additional parameters can be set for each zone in the system according to the table below.

Table 3.4 – Zones settings

Parameter	Description
Title	Zone name in the system.
Zone type	<p>One of the following types must be selected for each zone:</p> <p>Guard – a zone ("Security" type) that can be armed or disarmed. When intruding into the armed zone of this type, the SCP generates an alarm and activates an external detector.</p> <p>Front door – a security zone ("Entrance door" type) with a time delay, which at the entrance to the premises should always be intruded first. From the moment of this zone intrusion, the entry delay countdown starts. After the entry delay expires, if the group has not been disarmed, the SCP generates an alarm.</p> <p>Hall – a security zone ("Corridor" type), which at the entrance to the premises should always be intruded after the "Entrance door" zone. In this case, the alarm is not formed by the SCP during the entry delay. In case of its intrusion before the Entrance door zone, the SCP generates an alarm immediately.</p> <p>24-hour – a zone ("24h" type) that is always armed. When intruding into the zone of this type, the SCP generates an alarm and activates an external detector. The zone is automatically rearmed by the time set in the "Auto arming delay" option after triggering, if the zone loop is in the normal state.</p> <p>Panic button – 24h zone, when it is intruded, the SCP generates an alarm without turning on the siren.</p> <p>Parametric input – 24h zone ("Universal input" type) which can operate in one of three modes: alarm, fault, info (see "Operation mode" option). In case of intrusion of the zone of this type, the siren does not turn on.</p>

	<p>Tamper zone – 24h zone ("Tamper" type), which is connected to the tamper contacts of detectors and other devices. An alarm signal is generated when attempting unauthorized interference in the device case to which that type of zone is connected. In case of the zone's intrusion, the SCP generates an alarm and activates an external siren (if armed groups are available in the system).</p> <p>Anti-mask zone – 24h zone ("Antimasking" type) used to connect detectors that support the detection of masking. In case of the zone's intrusion, the SCP generates an alarm and activates an external siren.</p>
Entry delay	<p>This option allows to set the entry delay from 0 to 90 seconds and is available for "Entrance door" type zones only.</p> <p>If during the entry delay the communication with the detector is lost, the tamper is activated and the "sabotage" event is generated. For the 2EOL zones, when the zone state is "Penetration alarm" with the loop resistance value within "0-2.2 kOhm" or above "10 kOhm" (see Table 2.2), the entry delay is canceled and alarms are generated on previously activated devices.</p>
Auto arming delay	<p>This option allows to set the time (from 1 to 300 seconds), after which the zone will be re-armed after the alarm, if the corresponding zone loop is in the normal state. The option is not available for the following types of zones: "Tamper" and "Antimasking".</p>
I'm at home	<p>When arming the group in the "I'm at home" mode, the zones with this option will not be armed. The option is only available for "Security" and "Corridor" zones.</p>
Security of common premises (dependent zone)	<p>The option is available only for the zones configured as "Entrance door" and "Corridor". When enabled, this zone is indicated as a dependent one. It is not allowed to create groups only with dependent zones.</p>
Disarming with CMS	<p>Those zones for which this option is enabled will be disarmed upon receipt of the corresponding command from the CMS. This option is available only for zones configured as "Entrance door", "Corridor", and "Security".</p>
Notification to the CMS	<p>If this option is disabled, the messages in this zone will not be transmitted to the CMS. The option is available only for "Universal Input" type zones in the "Alarm" and "Fault" modes.</p>
Notification on Tiras CLOUD II	<p>If the option is disabled, Tiras CLOUD II will not be notified from this zone. The option is available only for "Universal Input" type zones in the "Info" mode.</p>
Operation mode	<p>The option is configured for "Universal input" type zones. Depending on the value in this option, zone intrusion will be processed by the SCP differently. One of the following options can be selected:</p> <p>Alarm – when a zone is intruded, the SCP generates an alarm. This mode can be used to connect fire detectors;</p> <p>Fault – in case of zone intrusion, the SCP forms a fault in this zone. This mode can be used to monitor the state of the connected automation;</p> <p>Info – zone intrusion in this mode does not lead to the formation of an alarm or fault. Events in the zone are not transferred to the CMS. This operation mode can be used to control a group via a key fob using a script.</p>
2EOL	<p>The option must be enabled for zones with 2EOL connection type. This option is available for the zones of the SCP, M-Z Box and M-ZP mBox modules. This option is not available for "Tamper", "Antimasking", and "Universal input" zone types (in the "Info" and "Fault" modes).</p>
Advanced settings for wireless detectors	
Serial number	<p>A 10-digit ID of the wireless detector for its identification in the system. This parameter is set for the zones of the M-X module only.</p>

Communication test interval	Interval for sending tests by wireless detectors to monitor communication. This parameter can be set from 10 to 3600 seconds. This parameter affects the detector battery life. This parameter is available for the zones of the M-X module only.
Number of missed tests	The number of lost test messages to generate a detector communication loss event. This parameter can be set from 3 to 20 tests. This parameter is available for the zones of the M-X module only.
Sensitivity	Motion sensor sensitivity setting: high, medium, and low. This parameter is set for the following detectors: X-Motion, X-Motion+, and X-Motion Alarm.
Constantly active motion sensor	If the option is enabled, the motion sensor will detect the intrusion immediately after receiving a command from the SCP. If the option is disabled, after receiving a command from the SCP, the motion sensor will detect the intrusion after its activation (~ in 30 seconds). Permanently active motion sensor reduces the detector battery life. This parameter is set for the following detectors: X-Motion, X-Motion+, and X-Motion Alarm.
Light indication of alarms	If the option is enabled, the detector's LED indicator will light up shortly when the detector is alarmed. This parameter is set for the following detectors: X-Motion, X-Motion+, X-Shift, and X-Shift+.
Wired connection	If this option is enabled, the SCP will analyze the status of an additional detector (with NC contacts) connected to the X-Shift or X-Shift+ detector terminals.

3.2.4 Outputs

Maximum number of outputs in the system depends on the SCP and keypads settings but cannot exceed 128 for Orion NOVA L (LTE), 32 for Orion NOVA M (LTE), and 16 for Orion NOVA S (LTE).

The outputs are controlled using the keypads and Control NOVA II software. The outputs are configured using the oLoader II software.

The output assigning to the keypad's functional buttons is as follows:

- to set the output operating mode as "Controlled by user";
- to assign the output to one of the keypad's functional buttons (F1, F2, F3).

The output assigning to a user control by means of the Control NOVA II software is as follows:

- to set the output operating mode as "Controlled by user";
- to assign the output to the user.

Additional parameters for each output in the system can be set according to the table below.

Table 3.5 – Outputs settings

Parameter	Description
Title	Output name in the system.
Outputs operating mode	When configuring, one of the following operating modes can be selected for each of the outputs:

	<p>By script – the output is activated and deactivated only when a certain script is running. Outputs in this operating mode can be selected when configuring script actions.</p> <p>Confirm arming – the output is activated for the time specified in the "Confirmation glowing time" option, after receipt of the confirmation from the CMS for all zones arming in the group for which it is configured. The output in this operating mode can be selected when configuring groups. Operating modes of the "Confirmation" indicator are given in Table C.1, Appendix C.</p> <p>Controlled by user – output operating mode, in which control authorities can be gained to users of the system (using keypads, readers, and Control NOVA II software). The output in this operating mode can be selected when assigning users.</p> <p>Siren – the output in this operating mode is activated when an alarm occurs for the time specified in the "Alarm sounding time" option ("General settings" → "Security settings").</p> <p>+ 12V – the output in this operating mode is activated when the SCP is turned on and can be used to power the devices connected to it.</p> <p>Siren and " +12V" operating modes are available only for the following outputs: SIR – the SCP, OUT1, OUT2 – M-ZP mBox module.</p> <p>SGM – the output in this operating mode is activated when patrolling is turned on and deactivated when patrolling is confirmed, or patrolling time expires. The output in this operating mode can be selected when configuring scripts.</p>
<p>Connection type of output</p>	<p>The type of connection is selected in this parameter. Transistor outputs can operate in one of the following modes:</p> <p>Remote LED – the output intended for direct LED connection (see Figure 2.10, a).</p> <p>Open collector – when activated, the output switches to the ground (see Figure 2.10, b);</p> <p>This parameter is available only for outputs: "Q1", "Q2" – the SCP, "Q1", "Q2" – M-ZP mBox module, "Q1" – keypads.</p>

3.2.5 Groups

Maximum number of groups in the system is as follows:

- Orion NOVA S (LTE) – 16;
- Orion NOVA M (LTE) – 32;
- Orion NOVA L (LTE) – 128.

Additional parameters for each group in the system can be set according to the table below.

Table 3.6 – Groups settings

Parameter	Description
Title	The group name in the system.
Zones	This option allows to select zones for each group that will be part of it. The following zones can be selected: "Security", "Entrance door", and "Corridor". The group cannot include zones of the "Corridor" type if the "Entrance door" type zones are not available.
"Confirmation" outputs	The outputs can be selected for each group that will operate in the confirmation mode when arming the group. The outputs operating in the "Confirm arming" mode are available for selection.

Exit delay	For each group, if it includes the "Entrance door" type zone, the delay is set from 10 to 90 seconds.
Quick arming	If the option is enabled , during exit delay the group will immediately be armed after the return of the "Entrance door" type zone to the normal state.
Arming delay from reader	If the option is enabled, when the group is armed with the TM reader, the "Exit delay" option (if it is configured) is enabled.
Confirmation by siren	If the option is enabled, the confirmation of arming from the CMS will be accompanied by the activation of the siren (one short signal), while the confirmation of disarming will be accompanied by the activation of the siren (two short signals).
Displaying group status on "Guard" indicator on first access level	If the option is enabled, the "Security" indicator at the 1 st access level on all keypads for which the "Permanent indication" option is enabled and works according to Table D.4 in Appendix D . At the 2 nd access level (after entering the access code), the "Security" indicator displays the status of the group that is controlled according to Table D.4 in Appendix D .
Access limitation from keypads	This option allows to select the keypads from which the control of the group will be prohibited. If no keypad is selected in the parameter, then the control of the group will be possible from all the keypads available in the system.

3.2.6 Scripts

Maximum number of scripts that can be created in the system is as follows:

- Orion NOVA L (LTE) – 64;
- Orion NOVA S/M (LTE) – 16.

Additional parameters for scripts can be set according to the table below.

Table 3.7 – Scripts settings

Parameter	Description
Title	The script name in the system.
Script run	
Manually	Authorized user Unauthorized user Do not allow manual launch
On schedule	The option allows to configure the script run on schedule
Conditions time	The option allows to choose the time when the conditions will be checked: any time (by default) or you have an opportunity to customize time or period.
Run conditions Option allows to set three conditions and logic: "All came true" or "At least one true"	
Conditions "Group"	In alarm Guarded Guarded in "I'm home" mode Guarded with confirmation from CMS Ready for arming during set time interval

	Guard off Exit delay started Ready to guard during the time If several groups are selected, the additional logic is available: "All groups" or "At least one"
Conditions "Zone"	In alarm Guarded Guarded with confirmation from CMS Guard off Enter delay started Not disturbed (in norm) Disturbed If several zones are selected, the additional logic is available: "All zones" or "At least one"
Conditions "SCP"	Start of the SCP SCP has been notified of the air alarm launch SCP has been notified of the air alarm clearance
Conditions "Connection"	No connection Connection restored Available for communication with: CMS, Tiras CLOUD II, Ethernet, Wi-Fi, remote modules (RS-485), wireless devices.
Conditions "Power supply"	No power supply – Battery or 230V Power supply restored – Battery or 230V Defective battery: discharged, low capacity, absent, charger fault Discharged battery
Conditions "Housing"	Housing opened Housing closed
Conditions "Temperature"	Below the set value Above the set value
Execute The option allows to set the number of the main actions of the script are executed (1-100 or infinite) The maximum number of actions – 16.	
Execute	Set under guard – select groups and arm mode (In normal mode, In "I am home" mode, With entrance time). Unset from guard – select groups. Toggle guard status – select groups. Delay – type of delay (Fixed or Random) and time. Turn on – select outputs. Turn off – select outputs. Toggle – select outputs. Start script – select script. Stop script – select script. Send a notification to the CMS – select message type (Fault, Alarm, Info) and event (Door is not released).
Stop conditions	

Option allows to set three conditions and logic: "All came true" or "At least one true"	
Conditions time	The option allows to select the time when the conditions will be checked: any time (by default) or you have an opportunity to customize time or period.
Conditions	All actions are completed Launch conditions are no longer valid Timeout On schedule Another termination condition - all run conditions except " Start of the SCP".
Final actions	
Set of actions is similar "Execute". Maximum number of actions - 3.	
Messages	
Automatic start/stop notification	This option allows to enable or disable sending messages about script run and stop.

3.2.7 Security guard monitoring (SGM)

The SGM scripts reduce the influence of the human factor in the process of security and duty and give an opportunity to monitor performance of the security guard's responsibilities, including the guard's presence at the post or bypassing the guarded object.

Maximum number of SGM scripts to be created - 7.

Setting up the SGM script

The SGM scripts are set up using the oLoader II software. After going to the SGM tab, click "+" for the script configuration window to appear. Following the instructions, it is necessary to enter a script name, select a guard duty schedule, control type of the guard's work, indication of the patrol mode, the guard's actions, and the recipient of the SGM results.

Table 3.8 - SGM script settings

Parameter	Description
Title	A SGM script name, maximum 40 characters.
Guard duty schedule	Days of the security guard monitoring: <ul style="list-style-type: none"> ▪ Daily - duty monitoring will be carried out on all days from Monday to Sunday. ▪ On weekends - duty monitoring will be carried out only on Saturdays and Sundays. ▪ On weekdays - duty monitoring will be carried out from Monday to Friday. ▪ Own schedule - allows selecting specific days of the week for duty monitoring. The time range of security guard monitoring: <ul style="list-style-type: none"> ▪ From - hours and minutes ▪ To - hours and minutes. If nothing is selected, the SGM will last until the beginning of the next day.
Control of the guard's work	Modes to monitor guard's work: <ul style="list-style-type: none"> ▪ Regular - sets a fixed time interval after which the security guard will be requested to <u>confirm the fulfillment of duties</u>. ▪ Unexpected - randomly generates the time interval after which the request for confirmation of the guard's duties will be made. To generate a random time, the time range is set to "Not more than" and "Not less than". The value "Not more than" must be less than "Not less than". If two values are the

	<p>same, then the random generation of time does not occur, and the interval of requests for confirmation of the guard's duties will be fixed.</p> <p>The unexpected mode enhances monitoring as it does not allow the security guard to leave the guarded object for a long time because he does not know when he will be requested to confirm his duties.</p>
Indication of the beginning of control for the guard	The operating mode of the output must be SGM to use it to indicate the start of patrol mode. All outputs with the SGM operating mode can be selected when setting up the script.
Guard needs to make	<p>The patrol duration is set to 10 minutes by default. If necessary, you can change it, but keep in mind that this time should not exceed the patrol frequency.</p> <p>The option allows to select the following ways to confirm patrolling:</p> <ul style="list-style-type: none"> ▪ Break zone – it is enough to break a zone for a short time and then restore it. The zone type must be pre-configured as "Universal Input" with the "Info" operating mode. Notification transmission on Tiras CLOUD II must be disabled. 10 zones are the maximum allowed to configure for one SGM script. ▪ Authorize on the keypad – enter the password and press the # button or authorize with a key/card (see 5.7 for key/card settings). The number of keypads for selection is limited by the SCP model. Regardless of the number of selected keypads, 10 users are the maximum allowed to assign. <p>Both ways can be used simultaneously.</p>
Notify about the result of the service	<p>The option allows to select the following notification options:</p> <ul style="list-style-type: none"> ▪ Security company – if the patrol is successful, an information message will be sent to the CMS, and if the patrol failed, an alarm message will be sent to the CMS. ▪ The owner of the object – a user with administrator privileges or an installer with administrator privileges who will receive the results of successful and failed patrols. <p>You can use both notifications at the same time or do not use any of them.</p>

SGM script operation

SGM will start automatically according to the time specified in the schedule. The patrol mode will start immediately after monitoring, as indicated by the blinking of the LED which is previously connected to the configured output. During the patrol mode, the guard must confirm the fulfillment of his/her duties by breaking the zone for a short time and then restoring it or by authorization using the keypad or both. After confirmation, the LED blinking stops indicating a successful patrol. Also, the LED blinking stops if the patrol time has expired, and the guard has not confirmed his/her duties indicating a failed patrol. The results of successful and failed patrols will be sent to the owner of the object or security company, or to no one at all, depending on the settings.

The patrol mode will be activated at fixed or random intervals throughout the entire period of SGM. The duration and frequency of the patrol mode depend on the settings of the SGM script.

If the SCP is restarted during the SGM period, the patrol mode is activated immediately after time synchronization.

The software updates during the SGM period will be installed if the next patrol mode is more than 10 minutes away.

SGM status menu

The menu allows to view the status of the guard's duties confirmation from the display keypads. It is available to administrators, installers, and users¹. The menu can be used only

¹ The menu is available only to those users who have been added to confirm patrolling using keypad authorization.

during the patrol period. The status of the guard's duties confirmation is displayed in square brackets. The [+] symbol indicates the confirmation, while the [] symbol indicates that the confirmation has not occurred.

3.2.8 Users

Maximum number of users:

- Orion NOVA L (LTE) – 128;
- Orion NOVA S/M (LTE) – 64.

Installer and Administrator users have specific rights as described in the table below.

Table 3.9 – Users settings

Parameter	Description
Name	Username in the system.
User role	<p>Administrator – the main user of the system, who has the rights to manage groups and automation. The administrator can change the users and scripts settings, as well as block the installer access to the SCP. As a rule, this type of user is assigned to the owner of the object.</p> <p>Installer – the user who can change system settings (if allowed by the administrator). The installer can also manage groups and automation. As a rule, this type of user is assigned to an employee of the organization that installs and maintains the SCP.</p> <p>Installer with administrator rights – the user who configures the system remotely or locally and has full administrator privileges. This type is assigned to the main user of the system. It can be both the owner of the object and the employee of the maintaining company.</p> <p>User – a type of user who can manage groups and automation.</p>
Access type	<p>Local – allows the user to control the system using keypads, readers, and radio key fobs, but forbids the control using the Control NOVA II software.</p> <p>Remote – allows the user to control the system using the Control NOVA II software, but forbids the control using keypads, readers, and radio key fobs.</p> <p>Full – this value combines local and remote access permissions.</p>
Authority	<p>Arming alarm – allows to arm groups but does not allow to disarm them.</p> <p>Arming/disarming – allows both to arm and to disarm groups added to the user.</p> <p>Bypass of unassembled zone – allows the groups of the zones to be armed if there is one unassembled zone in the group (only with display keypads or the Control NOVA II software).</p> <p>Ignore faults – allows the group to be armed in case of a fault in the system. When working with the SCP, the fault overriding is required according to Security Grade 2 or Grade 3.</p>
Access code	A combination up to 12 digits used by the user to control the system. When reading the settings from the SCP, the valid user codes are displayed as "*".
Key/card	A combination of a TM/NFC key used by the user for authorization in the system. When reading settings from the SCP, all valid keys/cards combinations are displayed as "*".

Attack code	A combination from 1 to 12 digits or a combination of a TM key reader. By entering any of them, the user gets all the privileges that are available, 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.
Groups	This option allows to select the applicable privileges from the general list of groups in the system.
24h zones	This option allows to select those zones from the general list of configured 24h zones ("Panic button", "24h", "Universal Input", "Tamper", "Antimasking") for which a user will receive messages (SMS, check call in case of alarm, notification via the Control NOVA II software).
Scripts	This option allows to select those scripts from the general list of scripts that have the following ways to run: "From the 1 st access level" or "From the 2 nd access level".
Outputs	This option allows the user to select those outputs from the general list of outputs that are configured to work in "Controlled by user" mode and can be managed by the user.
Access code main action	This option allows to select one group, one output, or one script from the list of user controls (groups, outputs, and scripts) that will be immediately available for control after entering the access code using the keypad.
Key/card main action	This option allows to select one group, one output, or one script from the list of user controls (groups, outputs, and scripts) that will be immediately available for control after reading a key/card.
Use X-Key	This option allows to configure the user's X Key wireless key fob to control the status of one of the groups and generate an attack message. One key fob can be assigned to only one user. To add a key fob, specify its ID.
Keyfob group	This option allows to select one group from the list of user groups that can be controlled using the user-assigned key fob.
Management without prior authorization (fast action)	Enabling this option allows to arm/disarm the security group when controlling the keypad and manage outputs and scripts skipping the stage of viewing their status, that is, the action is performed after entering the access code and pressing the # button once. The option is not available for "Installer" and "Administrator" user types.
Access limitation from keypads	In this parameter, the user can select the keypads available in the system from which user authorization will be prohibited. If no keypad is selected in the parameter, user authorization will be possible from all keypads available in the system.
Phone number	The user's mobile phone number for sending SMS messages set in the following format: 0671234567 or +380671234567.
Check call	The option is available only in autonomous operating mode of the SCP. 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.

SMS settings	<p>To set SMS notifications, the following options must be enabled:</p> <p>Send SMS about arming/disarming – permission to send SMS about the status of groups that can be controlled by the user.</p> <p>Send service SMS¹ – permission to send SMS about system alarms (interference with the enclosure of the SCP/system devices) and faults.</p> <p>Send SMS about alarms – permission to send SMS about alarms available in the groups and zones assigned to the user.</p> <p>Send SMS about outputs control – permission to send SMS about activation/deactivation of outputs controlled by the user.</p> <p>The list of SMS notifications that can be sent to the user phone numbers is shown in Table D.5, Appendix D.</p>
---------------------	---

3.2.9 Communication settings

The communication settings include the settings of the CMS, SIM cards, M-NET+ and M-WiFi communicators, as well as Tiras CLOUD II.

Table 3.10 – CMS settings

Parameter	Description
Device operating mode	<p>Autonomous mode – the SCP operating mode, in which no messages are transmitted to the CMS. In this mode, the SCP transmits messages about the system status to the Control NOVA II software, by SMS messages and makes check calls to the specified phone numbers of the user.</p> <p>Central monitoring station mode (NOVA protocol) – an operating mode, when the SCP transmits messages to MISTO or MOST CMSs using the NOVA protocol.</p> <p>Console mode (Sur-Gard protocol (Contact ID)) – an operating mode, when 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 D.6, Appendix D.</p> <p>In the CMS mode, in addition to the CMS, the SCP can transmit information about the system status to the Control NOVA II software and by SMS messages to the specified user phone numbers.</p>
CMS	This option allows to select one of the following CMSs for the SCP connection: "MOST" and "MISTO Security Platform". This option is only configured for "NOVA" protocol.
Encryption algorithm	This option allows to select one of the following encryption algorithms for exchange between the SCP and the CMS: "DES" and "AES". The parameter is only configured for "MISTO Security Platform". The selected encryption algorithm must match the encryption algorithm in the object card on the CMS.
Hidden number	This option allows to provide additional crypto protection when the SCP operates with MISTO or MOST using NOVA protocol. The entered value must match the hidden number in the object card on the CMS.
Object number in Sur-Gard (Contact ID) protocol	A 4-digit number used to identify the object when the SCP operates with the CMS using "Sur-Gard protocol" (Contact ID). The entered value must match the object number in the object card on the CMS.
Test message interval (main connection channel)	This option allows to set test message sending interval ranging from 30 to 990 seconds to control the main communication channel with the CMS.

¹ SMS notification about system alarms (penetration into the SCP's case or system devices) is sent to the Administrator only.

Test message interval (alternate connection channel)	This option allows to set test message sending interval ranging from 60 to 3600 seconds to control an alternative communication channel with the CMS. The parameter can be enabled only when the SCP operates on two communication channels. This parameter is only available in "NOVA" protocol.
Generation time of "CMS connection malfunction" message	This option allows to set time (after a fault detection), after which the SCP generates a message of data exchange with the CMS fault. We strongly recommend setting the parameter value equal to the test message control interval in the object card on the CMS.
CMS addresses	This option allows to set up to 3 addresses for transmission to the CMS. The address setting includes the IP address (or domain name) and the CMS port. The transition between the addresses of the CMS is carried out on priority automatically.
Hide CMS settings	If this option is enabled, when reading the configuration from the SCP, all settings for operation with the SCP will be hidden. If you need to change any hidden parameter, all the settings for operation with the CMS must be set again.

Table 3.11 – SIM-cards settings

Parameter	Description
Using SIM	If this option is enabled , the SCP checks the SIM card availability in the corresponding slot.
Roaming	If this option is enabled , roaming is allowed for the SIM card.
Access point name	For each SIM card to be used, an Internet access point (determined by the mobile operator) must be specified.
PIN-code	SIM card security code. If PIN code for the SIM card is disabled, the field should be empty.
Balance check code	The combination is used to check the SIM card account using the keypad menu, by default - *111#.
Number check code	The combination is used to define the SIM card number using the keypad menu, by default - * 161 #.
Username	A username for registration in the mobile operator's network. This field is optional.
Password	Password for registration in the mobile operator's network. This field is optional.
Automatic operator selection	Enabling the option allows to set the MCCMNC binding code for each SIM card to a specific mobile operator network (5 or 6 digits). If this option is enabled , the MCCMNC field must be filled in for each SIM-card.

Table 3.12 – Ethernet settings¹

Parameter	Description
DHCP protocol	If the option is enabled , the SCP will receive IP address and other Ethernet network settings automatically. If the option is disabled , the SCP will use the Ethernet network settings entered in the fields: IP address of SCP, Subnet Mask, Gateway IP address, DNS1, DNS2.
IP-address of SCP	IP address of the SCP in the Ethernet network.
Gateway IP-address	The IP address of the local computer network router with access to the Global Internet network.
Subnet mask	Ethernet subnet mask.
DNS1 and DNS2	IP addresses of DNS servers (for the domain name use).

¹ Orion Nova L (LTE) has a built-in Ethernet module.

SCP MAC address	This parameter is displayed when loading settings from the SCP and not available for editing.
------------------------	---

Table 3.13 – Settings of Wi-Fi communication module M-WiFi

Parameter	Description
Wi-Fi access point name	The name of the Wi-Fi access point. From 1 to 31 characters (available characters: 0-9, A-Z).
Wi-Fi password	Wi-Fi APN password. From 8 to 31 characters (available all ASCII characters).

Table 3.14 – Settings of Tiras CLOUD II service

Parameter	Description
Connection with Tiras CLOUD	<p>Connection with Tiras CLOUD II service for remote control and monitoring of the object status. The following options are available:</p> <p>Turned off – the SCP does not connect to the Tiras CLOUD II service.</p> <p>Only by cellular communication – the SCP connects via the GSM/LTE (it requires at least one configured SIM card).</p> <p>Only by Ethernet (Wi-Fi) – the SCP connects via a local computer network (Ethernet or Wi-Fi).</p> <p>Through all available communication channels – the SCP connects via the main communication channel – Ethernet/Wi-Fi. When the main communication channel is lost, the SCP connects via an alternative communication channel – GSM/LTE.</p>
Informing users	<p>User notification about system events and faults in Control NOVA II software.</p> <p>Complete – information about system events and faults is sent to all users of the system.</p> <p>Partial – information about system events and faults is sent to system users with the Administrator and Installer privileges only.</p>

3.2.10 Setting of system parameters

Table 3.15 – Configuring system parameters

Parameter	Description
Device language	The language of the display keypads' menu, SMS, and event log: Ukrainian, Russian, and English are available.
Alarm sounding time	Alert sound duration that can be configured from 10 to 900 seconds.
Confirmation glowing time	The time for exit activation is configured for the "Confirmation" mode when receiving the confirmation of the group arming from the CMS. It can be configured within from 10 to 300 seconds.
Deny enter in 3rd access level	If the option is enabled , the SCP will not accept both the configuration file (locally and remotely) and the installer access code from the keypad. There will be no opportunity to update the SCP firmware using the CMS.
Enable SMS sending	If the option is disabled , the users of the system will not be notified via SMS messages.
Enable lower speed of transition between SCPs and keypads	The option must be enabled to reduce interference in case of unsatisfactory quality of the communication between the SCP and the keypad.
Use external GSM antenna	If the option is disabled , the SCP uses the built-in GSM antenna. If the option is enabled , the SCP uses an external GSM antenna connected to the SMA connector.
Ignore GSM channel jamming	If the option is enabled , the SCP does not generate a GSM jamming event. This option is used for objects where false GSM jamming events generation is caused by interference from third-party equipment.

Auto SCP firmware update	<p>The SCP can independently check the availability of the firmware updates. The SCP can download and install it. The following options are available:</p> <p>Turned off – the SCP will not automatically download and install the firmware update.</p> <p>Turn on only through Ethernet/Wi-Fi – If an update is available, the SCP will automatically download and install the firmware update, in case the communication with Tiras CLOUD II via Ethernet or M-WiFi is enabled.</p> <p>Turn on through Ethernet/Wi-Fi/cellular communication – If an update is available, the SCP will automatically download and install the firmware update, in case the communication with Tiras CLOUD II is available regardless of the type of the communication channel.</p>
Time zone of SCP	This option allows to select time zone for setting the SCP time depending on its territorial location.
Battery type	<p>The SCP supports two types of batteries. Depending on the installed battery, select one of the following parameters:</p> <ul style="list-style-type: none"> ▪ Lead-acid battery; ▪ Lithium iron phosphate battery.
Charging optimization	This option allows to avoid quick battery aging, while charging to a maximum capacity may be limited.
Fast charging	This option allows to increase the battery charging current. Consider it when calculating the total current consumption.
Configuration protection with installer code¹	<p>If the option is enabled, when configuring the SCP, it is necessary to enter the valid installer code for the SCP to accept the new settings.</p> <p>If the option is disabled, oLoader II software does not require the installer code.</p>
Enable permanent confirmation LED glow¹	If the option is enabled , then the " Confirmation glowing time " option is not configured, while the confirmation indicators light permanently.
Enable alarm formation on alarm zones violation during input delay¹	<p>The option is enabled – if the "Security" zone is intruded during the entry delay, the SCP immediately generates alarm (to the CMS and Tiras CLOUD II).</p> <p>The option is disabled – if the "Security" zone is intruded during the entry delay, the alarm will be transmitted (to the CMS and Tiras CLOUD II) when the entry delay expires (if no disarming occurred).</p>
Number of events of the same type	This option allows to limit the number of messages of the same type (from 5 to 100) generated in the event log of the SCP and to the CMS. If 100 events are selected, then 230V and battery faults are not limited.

3.3 Check call

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

If the "Check call" option is enabled in the user settings and the user phone number is specified, the SCP calls to the specified user phone number in case of alarm generation. Check call is made without voice message playback. For check calls and SMS messages, the same phone number specified in the user settings is used.

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

The SCP identifies the check call as **successful**, if the user **rejects the call**, otherwise it is considered that the user does not receive the call, and the SCP repeats attempts. The maximum number of attempts to dial one user per one alarm – 3. If the SCP fails to reach the user, it will try again after calling the remaining users, but not earlier than in 5 minutes (the

¹ This option is unavailable for Security Grade 2 or Grade 3.

interval between attempts to connect to one user).

In case of other events transmitted to Tiras CLOUD II or via SMS during the check calls, they are sent in regular mode. If the call to the user phone number is in progress when such an event occurs, it is not interrupted (the attempt is made in full).



The call caused by tampering the system devices is made only to the users of Installer and Administrator types (if the "Check call" option is enabled).

4. INSTALLER OPERATION WITH KEYPADS

To allow the installer's access to the functions of the SCP from the keypad, disable the "Deny enter in 3rd access level" option (see 3.2.9).

Display keypads allow the installer:

- to review the system status;
- to control groups (arm/disarm) and automation;
- to review the SGM scripts;
- to change one's own access IDs (see 4.1.1);
- to change the settings of groups (see 4.4), wireless devices (see 4.4), scripts, device language (see 4.5), and options of keypads (see 4.6);
- to enable "Zones testing" option (see 4.7);
- to check communication quality with connected devices;
- to restart the SCP (see 4.9);
- to check and download firmware updates (see 4.10);
- to restore default settings (see 4.11);
- to format flash memory drive in the SCP (see 4.12);
- to review the current communication state with the CMS and Tiras CLOUD II (see 4.14);
- to run USSD requests (see 4.15).

LED keypads allow the installer:

- to partially review the system status;
- to control groups (arm/disarm) and automation;
- to change one's own access IDs (see 4.1.2);
- to assign wireless devices and review the signal quality (see 4.4);
- to enable "Zones testing" option (see 4.7);
- to restart the SCP (see 4.9);
- to restore default settings (see 4.11);
- to format flash memory drive in the SCP (see 4.12);
- to view the signal strength of the GSM network and/or Wi-Fi (see 4.14).

When operating with display keypads, the ▲ and ▼ buttons are used for navigation between items. To select one of them, press the ● button. To return to the previous menu, press the ◀ button (or *).

After entering the installer code from the display keypad, the main installer menu is displayed. The items of this menu are given in Table 4.1. If the installer has control elements, after entering the installer code the keypad menu to control these elements is displayed. To return to the main menu, press the ◀ button (or *).

Table 4.1 – The installer main menu

No	Menu section ¹	Purpose
1	ALARMS	List of alarms that have been generated since the previous viewing of this menu item
2	FAULTS	List of faults that have been generated since previous viewing of this menu item
3	SECURITY	List of groups available for control
4	AUTOMATICS	List of outputs and scripts available for control
5	SGM	List of available SGM scripts
6	CODE CHANGE	Allows the installer to change one's own access IDs
7	SETTINGS	List of additional installer settings
8	COMMUNICATION STATUS	Opens the menu item where the current state of communication with the CMS and Tiras CLOUD II can be viewed, as well as the signal strength of the active SIM card or Wi-Fi
9	USSD-REQUEST	Allows the installer to make USSD requests from configured SIMs to receive service information from a mobile operator
10	ABOUT DEVICE	Displays the current firmware version of the SCP and its serial number

4.1 Change of the installer access IDs

The installer can change one's own access IDs using keypads, the oLoader II and Control NOVA II software.

4.1.1 Change of access IDs using display keypads

To change the **access code**, do the following:

- 1) Enter the valid access code on the keypad and press the # button;
- 2) Select the section "CODE CHANGE" in the main menu;
- 3) Select the "ACCESS CODE" item;
- 4) Enter a new access code and press the # button;
- 5) Re-enter the new code and press the # button.

To change the **key/card ID**, do the following:

- 1) Enter the valid access code on the keypad and press the # button;
- 2) Select the section "CODE CHANGE" in the main menu;
- 3) Select the "KEYFOB/CARD" item;
- 4) Attach the key/card to the reader;
- 5) Re-attach the key/card to the reader.

To change the **attack code**, do the following:

- 1) Enter the valid access code on the keypad and press the # button;
- 2) Select the section "CODE CHANGE" in the main menu;
- 3) Select the "HOLD-UP CODE" item;
- 4) Enter a new attack code and press the # button;
- 5) Re-enter the new attack code and press the # button.

4.1.2 Change of access IDs using LED keypads

To change the **access code**, do the following:

- 1) Enter the valid access code # 1 # (the ✓ indicator starts blinking once per second);

¹ Depending on the settings of the SCP and the current system status, some sections of the main menu may be missing.

- 2) Enter a new access code and press the # button (the ✓ indicator starts blinking twice per second);
- 3) Re-enter the new access code and press the # button.

To change the **key/card ID**, do the following:

- 1) Enter the valid access code # 15 # (the ✓ indicator starts blinking once per second);
- 2) Attach the key/card ID to the reader (the ✓ indicator starts blinking twice per second);
- 3) Re-attach the key/card ID to the reader.

To change/assign the **attack code**, do the following:

- 1) Enter the valid access code # 2 # (the ✓ indicator starts blinking once per second);
- 2) Enter a new attack code and press the # button (the ✓ indicator starts blinking twice per second);
- 3) Re-enter a new attack code and press the # button.

Successful change of access ID is confirmed by four short sound signals of the keypad buzzer. If the ID change failed (if the re-entered combination does not match or the entered ID is already used), there is one long sound signal.

4.1.3 Change of access IDs using oLoader II software

To change **access IDs**, do the following:

- 1) Read the configuration from the SCP or create a new one;
- 2) Go to the "Users" tab;
- 3) Open the installer settings and select the required access ID;
- 4) Enable the "Change" option;
- 5) Enter a new combination of ID;
- 6) Save settings in the SCP.



When downloading the configuration with the new installer access code, the installer code that was used before changing the SCP settings must be entered.

4.2 SETTINGS section of the main menu



Entering the "SETTINGS" menu item is not available if the "Security", "Entrance door", or "Corridor" zones are armed.

When working with display keypads, the installer gets access to the **"SETTINGS"** section of the main menu (see Table 4.2). When selecting this section, there is the menu with the items given in Table 4.2.

Table 4.2 – SETTINGS installer setup menu

No	Menu section ¹	Purpose	Described in
1	GROUPS	This option allows to view the list of groups available for creating, deleting, and editing (change name, add/delete zones, set the confirmation outputs and additional options).	sec. 4.3
2	WIRELESS DEVICES	This option allows to view the list of assigned wireless devices, as well as start the mode for assigning new devices. The menu item	sec. 4.4

¹ Depending on the settings of the SCP and the current status system, some menu items may not be available.

		is available if the M-X module is installed.	
3	LANGUAGE MENU	This option allows to change the language of the SCP and SMS messages.	sec. 4.6
4	KEYPAD'S OPTIONS	This option allows to configure additional keypad settings, such as "Doorbell", "Brightness", "Night light", and "Presence".	sec. 4.7
5	ZONES TESTING	This option allows to view the mode giving an opportunity to check the performance of the connected detectors.	sec. 4.8
6	DEVICE CONTROL	This option allows to control the communication line between the SCP and each of the connected devices via RS-485.	sec. 4.9
7	RESTART SCP	This option allows to restart the SCP without powering it off.	sec. 4.10
8	UPDATE FIRMWARE	This option allows to update the built-in firmware for the SCP, keypads and expansion modules.	sec. 4.11
9	DEFAULT SETTINGS	This option allows to restore default settings on the SCP.	sec. 4.12
10	FLASH MEMORY FORMATTING	This option allows to format the USB flash drive of the SCP in case of damage (viruses when connected to the PC, neglection of the SCP safe disconnection from the PC, etc.)	sec. 4.13
11	EOL CALIBRATION	This option allows to calibrate the EOL resistors of the SCP when using detectors with EOL resistance in range from 1 kΩ to 7.5 kΩ.	sec. 4.14

4.3 Group settings

When selecting the "GROUPS" section, the menu with the list of already created groups and the "NEW GROUP" item are displayed. When creating a new group, or selecting an existing one, the setup menu is displayed, containing the items given in Table 4.3.

Table 4.3 – Group setting menu

No	Menu section	Purpose
1	NAME	This option allows to edit a group name.
2	ZONES	List of zones that are included or can be included in the group.
3	EXIT TIME	This option allows to set the exit delay duration (within the range of 10-90 seconds) when arming a group of zones. The menu item is not available when arming groups that do not include the "Entrance Door" zone.
4	CONFIRMATION OUTPUTS	This option allows to choose outputs with "Confirm arming" mode for displaying the status of this group.
5	ADDITIONAL OPTIONS	This option allows to enable a confirmation of the group arming/disarming by a siren. "Quick setting" mode is available for the groups that contain the "Entrance door" zone.
6	ACCESS RESTRICTION	This option allows to restrict access to group control from keypads.
7	DELETE GROUP	This option allows to delete a group.

When selecting the "NAME" item, the dialog box for editing the group name is displayed (see Figure 4.1).

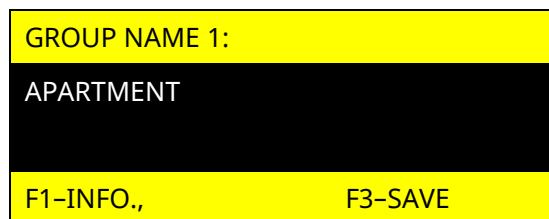


Figure 4.1 – A dialog box for group name editing

For example, to erase the default group name "Group name 1", it is necessary to press the # button for the cursor indicating an editable character to appear. The position of the cursor changes when the # and * buttons are pressed. The symbols are entered using the "0

... 9" buttons on the keypad touchpad (the list of characters is available when button is pressed, and it is displayed on the keypad display). When pressing the "F2" button, the selected character is deleted.

When selecting the "ZONES" item, the list of zones available in the system, such as the "Entrance door", "Corridor", and "Security", is displayed (see Figure 4.2).

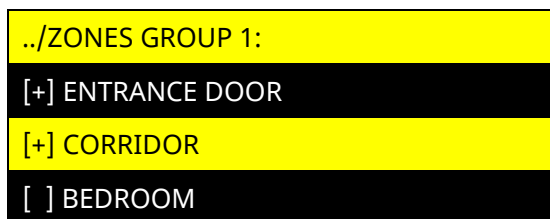


Figure 4.2 – A dialog box for zone selection belonging to the group

The symbol "[+]" means that the zone belongs to the group, while the symbol "[]" means that the zone does not belong to the group.



The group cannot include zones of the "Corridor" type if there are "Entrance door" zones.

When selecting the "EXIT TIME" item, the dialog box is opened allowing to edit the time given for leaving the premises when the group is armed (see Figure 4.3).

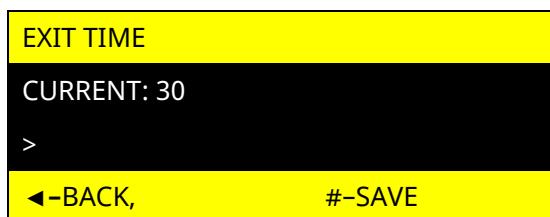


Figure 4.3 – A dialog box for selecting confirmation outputs for the group

The dialog box shows the current exit delay. With the "0" - "9" buttons, the installer enters a new exit delay time. When the # button is pressed, the current time is replaced with a new one.

When selecting the "CONFIRMATION OUTPUTS" item, the list of available outputs configured for the "Confirm arming" mode is displayed (see Figure 4.4).

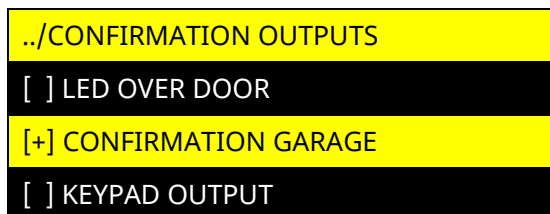


Figure 4.4 – A dialog box for choosing confirmation outputs for the group

The symbol "[+]" means that the output is used to confirm the group arming, while the symbol "[]" means that the output is not used to confirm the group arming.

When selecting the "ADDITIONAL OPTIONS" item, the dialog box with the list of additional group settings is displayed (see Figure 4.5).

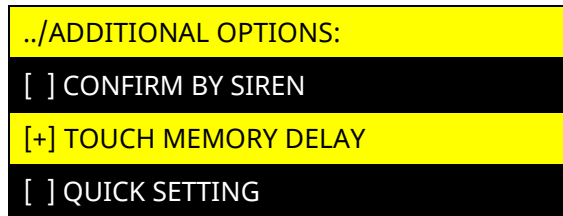


Figure 4.5 – A dialog box for additional group options

The symbol "[+]" means that this option is enabled for the group, while the symbol "[]" means that this option is not enabled for the group.

The "TOUCH MEMORY DELAY" and "QUICK SETTING" options are available only for the groups including the "Entrance door" zone.

When selecting the "ACCESS RESTRICTION" item, the dialog box with the list of available keypads is displayed (see Figure 4.6).

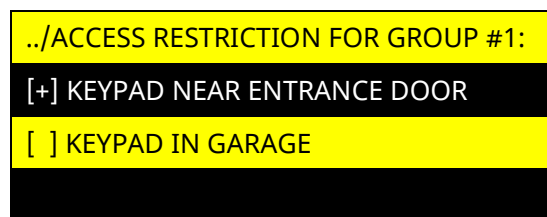


Figure 4.6 – A dialog box for keypad selection to restrict access to the group

The symbol "[+]" is used to mark the keypad that cannot be used to control the group. If **no keypad is marked** with the "[+]" symbol, there is **no access restriction** from the keypads (the group can be controlled from any keypad in the system).

When selecting "DELETE GROUP" item, the installer must confirm group deleting by pressing the # button, or cancel this action by pressing the ← button (see Figure 4.7).

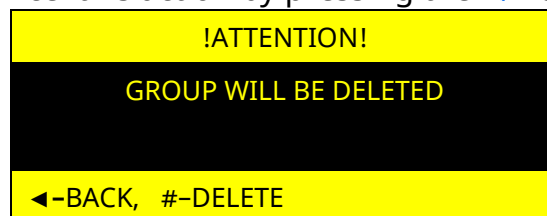


Figure 4.7 – A dialog box for the group deletion

4.4 Tiras wireless devices

4.4.1 Wireless devices setting

When selecting the "WIRELESS DEVICES" section, the options described in Table 4.4 are displayed. The item is accessible only if the M-X module is available in the system.

Wireless devices:

- **X-Shift** – wireless opening detector (for window 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-Pad** – wireless keypad;
- **X-Key** – wireless key fob;
- **X-Siren** – wireless siren;

- **X-Water** – wireless water leak detector;
- **X-Cover S** – wireless radio signal repeater.

Table 4.4 – Wireless devices setting menu

№	Menu section	Purpose
1	ASSIGNED	This item displays a list of assigned wireless devices.
2	ACTIVATION	This item displays the list of wireless devices with entered serial numbers. The opportunity to delete a serial number is included.

When selecting "ASSIGNED" section, the options listed in Table 4.5 are displayed. This section is available only if there are activated wireless devices.

Table 4.5 – ASSIGNED menu section

№	Menu item	Purpose
1	ZONES	This item displays the list of the activated wireless devices: X-Motion, X-Motion+, X-Motion Alarm, X-Shift, X-Shift+, and X-Water. It is possible to view the status of each wireless device or unassign it.
2	KEY FOBS	This item displays the list of the activated X-Key wireless key fobs. It is possible to view the key fob status and unassign it.
3	KEYPADS	This item displays the list of the activated X-PAD wireless keypads. It is possible to view the keypad status or unassign it.
4	SIRENS	This item displays the list of the activated X-Siren wireless outdoor sirens. It is possible to view the siren status or unassign it.
5	REPEATERS	The item displays the list of the activated X-Cover S repeaters. It is possible to view the repeater status or unassign it.

When selecting the "ZONES" item, the list of zones with the activated wireless devices is displayed (see Figure 4.8).

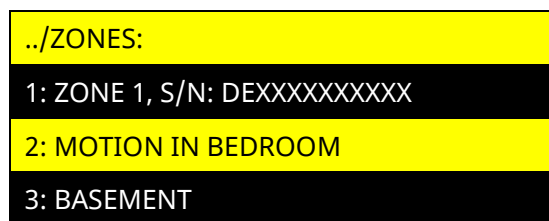


Figure 4.8 – Zones with activated wireless devices

When selecting one of the zones, the installer can view the status of its wireless device and unassign it from the zone (see Figure 4.9). For X-Key, the "STATUS" item is unavailable.

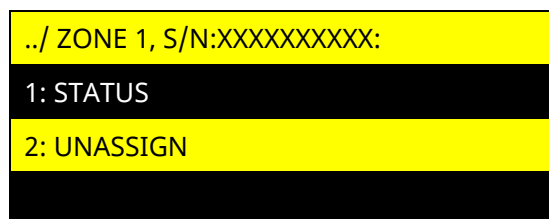


Figure 4.9 – View of wireless devices status and unassigning

When selecting the "STATE" item, the following wireless device information is displayed:

- serial number;
- type of wireless device;
- communication status;
- communication quality;
- signal strength (in dBm);
- temperature (in °C);

- battery charge status;
- firmware version.

An example of displaying the wireless device status is shown in Figure 4.10. Information is available if the wireless device has "Online" communication status.

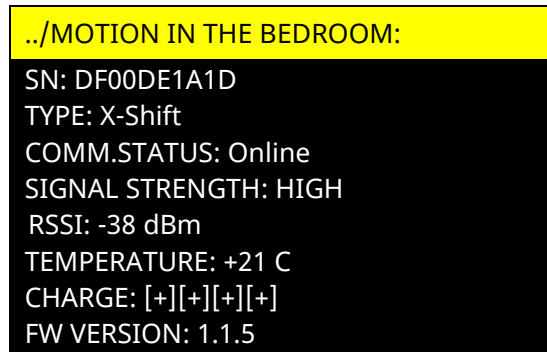


Figure 4.10 – Wireless device status window

When selecting "UNASSIGN" item, the installer can confirm the unassigning of the wireless device by pressing the # button or cancel the action by pressing the ◀ button. After unassigning the wireless device, it appears in the "ACTIVATION" section. The wireless device serial number (see 3.2.3) is also removed from the settings.

When selecting "KEY FOBS" item, the list of activated X-Key key fobs is displayed (see Figure 4.11).

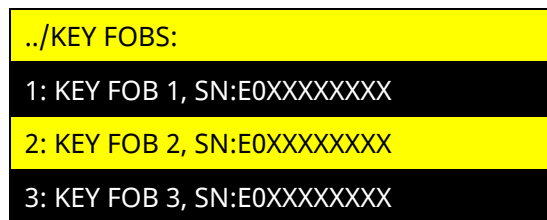


Figure 4.11 – Enabled X-Key fobs

When selecting "UNASSIGN" item, the installer can confirm the unassigning of the key fob by pressing the # button or cancel the action by pressing the ◀ button. After unassigning the key fob, it appears in the "ACTIVATION" section. The key fob serial number (see 3.2.3) is also removed from the settings.

When selecting "KEYPADS" item, the list of activated X-Pad keypads is displayed (see Figure 4.12).

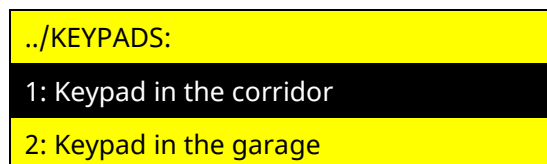


Figure 4.12 – Enabled X-Pad keypads

When selecting one of the keypads, the installer can view its status and unassign it (see Figure 4.13).

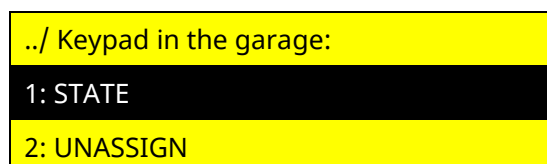


Figure 4.13 – View of wireless devices status and unassigning

When selecting "STATE" item, the X-Pad keypad information is displayed:

- serial number;
- type of wireless device;
- communication status;
- communication quality;
- signal strength (in dBm);
- temperature (in °C);
- battery charge status;
- firmware version.

An example of displaying the X-Pad status is shown in Figure 4.14. Information is available if the X-Pad has "Online" communication status.

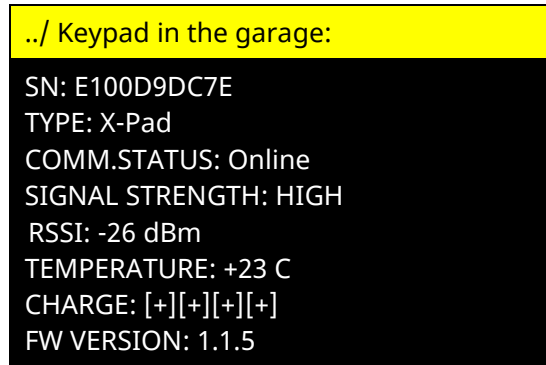


Figure 4.14 – X-Pad status window

When selecting "UNASSIGN" item, the installer can confirm the unassigning of the X-Pad by pressing the # button or cancel the action by pressing the ◀ button. After unassigning the X-Pad, it appears in the "ACTIVATION" section. The X-Pad serial number (see section 3.2.3) is also removed from the settings.

When selecting "ACTIVATION" section, the options listed in Table 4.6 are displayed. This section is available only if there are unassigned wireless devices.

Table 4.6 – ACTIVATION menu

No	Menu item	Purpose
1	ZONES	The item displays the list of unassigned X-Motion, X-Motion+, X-Motion Alarm, X-Shift, X-Shift+, and X-Water detectors.
2	KEY FOBS	The item displays the list of unassigned X-Key fobs.
3	KEYPADS	The item displays the list of unassigned X-Pad keypads. It is possible to view the status of each keypad or unassign it.
4	SIRENS	The item displays the list of unassigned X-Siren devices.
5	REPEATERS	The item displays the list of unassigned X-Cover S repeaters.

The "ACTIVATION" section items of "WIRELESS DEVICES" menu are shown in Figure 4.15.

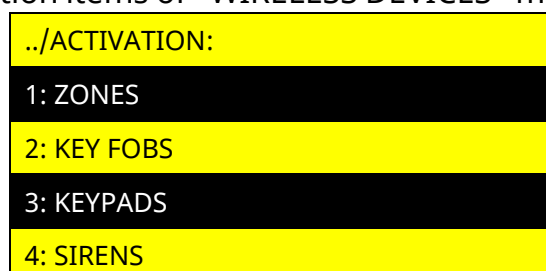


Figure 4.15 – The list of unassigned wireless devices ready for activation

4.4.2 Steps for adding wireless devices

Every wireless detector should be added to the SCP settings. The detector addition is conducted after the assignment and activation processes are performed sequentially:

1. **Assigning** the device to the SCP using **oLoader II** software (zones, key fobs, keypads, sirens, and repeaters settings: enter a name, serial number, add a zone to the group, set test intervals, etc.) or **Control NOVA II** software (enter the serial number of the detector/keypad/key fob/siren/repeater for the previously created wireless zone/keypad/key fob/siren/repeater in oLoader II software).
2. After successful assignment of the detector to the SCP, the wireless device should be **activated** (start, exchange of settings, and enabling of the operating mode from the SCP).

To activate the wireless device, the activation mode on the SCP should be enabled, then activation mode on the wireless device should be enabled. The activation mode of the SCP is enabled from the Control NOVA II software, display keypad, LED keypad (wired) and at the start of the SCP (with pre-assigned wireless devices). It is also possible to activate the wireless devices without pre-entered serial number from the display keypad.



When changing the communication test intervals with the detector from a larger value to a smaller one, the detector can generate a loss of communication message till the new setting is accepted.

The Activation mode is unavailable if there are armed groups in the system and/or if there are unassigned wireless devices.

To activate the wireless devices, it is necessary to enable the Activation mode on the SCP, then short press the "Start" button for each wireless device (for X-Key – any button).

Step 1. Assign the required wireless devices or create wireless zones/keypads/key fobs/sirens/repeaters without entered serial numbers.

Step 2. Enable the ACTIVATION mode on the SCP:

- **Control NOVA II software¹:** open the menu "☰ → System → Wireless devices", select the required wireless device from the list and click "ACTIVATE" (with a pre-entered serial number) or "ADD" (without a pre-entered serial number). Then follow further instructions on the screen.
- **oLoader II software:** open the menu "Devices ☐", select the required wireless device from the list and click "Activate" (with a pre-entered serial number) or "Add" (without a pre-entered serial number). Then follow further instructions on the screen.
- **Display keypad²:** authorize and open the menu "SETTINGS → WIRELESS DEVICES", select the "ACTIVATION" section. If the activation is conducted without prior assigning (without a pre-entered serial number of the wireless device in the SCP), then select the required zone to which this device will be assigned.
- **LED keypads (wired):** to enter the Activation mode, use the following combination:

installer access code # 4 #



Activation mode cannot be activated on the SCP from the X-PAD keypad.

¹ Users with the "INSTALLER" privileges can "ADD" or "ACTIVATE" wireless devices.

² Users with the "INSTALLER" privileges can "ADD" or "ACTIVATE" wireless devices.

- **When the SCP is running:** in the Activation mode, the M-X module indicator inserted in the MODULE1 / MODULE2 slot flashes at a frequency of 1 Hz. Activation mode is enabled for one minute for each wireless device. After activating one device, a minute for activation of another one starts. After activating the last wireless device, the Activation mode is disabled.

Step 3. Enable the Activation mode for the wireless device. To enable the Activation mode, remove the wireless device from the bracket and press the "Start" button (any button for X-Key). Confirmation of transition to the Activation mode is shown in Table 4.7.

Table 4.7 – Indication in Activation mode

Device	Description of indication
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Cover S	Flashing up to six times with green LED
X-Pad	Up to six sound signals of buzzer accompanied by flashes of red zone state LEDs
X-Key, X-Siren	Flashing up to six times with a red LED
X-Water, X-Motion Alarm	Sounding up to six times of buzzer

Step 4. Response from the wireless device. Table 4.8 shows the indication of the wireless devices with successful and failed activation.

Table 4.8 – The activation result

Device	Successful activation and adding of the SCP	Activation failed	
		The device is out of range of the wireless network, or the SCP is turned off or not in "Activation" 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	One short flash and sound signal	One long flash	Two long flashes
X-Key	Three short flashes of green LED	One long flash of green LED	Two long flashes of green LED
X-Siren	Three short flashes	One long flash and sound signal	Two long flashes and sound signal
X-Water, X-Motion Alarm	Three sound signals of buzzer	One sound signal of buzzer	Two sound signals of buzzer

4.4.3 Description of the device addition algorithm

Adding the wireless devices using Control NOVA II software

To add a wireless device to the zone/key fob/keypad/siren/repeater using Control NOVA II software: after authorization, the installer or administrator should open the menu "☰ → System → Wireless devices" and select a required wireless device from the list, and "ACTIVATE" (with pre-entered serial number) or "ADD" (without a pre-entered serial number).

Then the installer or administrator should follow further instructions on the screen.

Adding X-Shift, X-Shift+, X-Motion, and X-Motion+

To add the wireless devices (X-Shift, X-Shift+, X-Motion, X-Motion+) to the zone with a serial number specified in the settings, select the menu "ACTIVATION → WIRELESS DEVICES" on the display keypad. To enable, press the "Start" button on the back of the wireless device. After a short button press, the LED indicator of the wireless device (if inactivated) flashes up to six times, the device is automatically added to the zone with the serial number in its settings. If the wireless device is successfully activated, the zone is automatically moved from the "ACTIVATION" section to the "ASSIGNED" section and the wireless device will confirm the successful activation by triple flashing of the detector's LED indicator.

For adding the wireless device to the zone that does not have a serial number in the settings, select a zone from the list (the window shown in Figure 4.16 will appear) and press the "Start" button on the wireless detector. When you switch on the wireless device, it will be automatically activated and appear in the "ZONES" item.

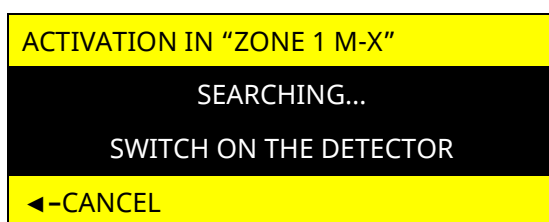


Figure 4.16 – A dialog box for detector searching

For adding the wireless device from the LED keypad (wired), enter the command:

installer access code # 5 #

Then press the "Start" button on the wireless device with a one-second delay.

The adding mode is also automatically activated after the SCP start, which is confirmed by the flashing of the HL LED indicator on the SCP board. Only after the HL indicator starts flashing, press the "Start" button on the detector with a one-second delay.

In both cases, after successful activation of the wireless device, its LED indicator flashes three times being accompanied by a sound signal.

Adding X-Water and X-Motion Alarm

Adding these detectors is similar to the one described above. The only difference is that X-Water and X-Motion Alarm do not have light indication.

After short pressing the "Start" button, the wireless detector (if inactivated) sounds up to six times and is automatically added to the zone with a pre-entered serial number. In case of successful activation, three sound signals are generated.

Adding X-Key key fobs

The "ACTIVATION" menu of the display keypad allows to activate the X-Key key fobs to the SCP with a pre-entered serial number of the key fob. To activate the X-Key, press any button while the key fob is within range of the M-X module transceiver. If the X-Key is successfully activated, the key fob is automatically moved from the "ACTIVATION" section to the "ASSIGNED" section.

If it is necessary to add X-Key, but there is no serial number in the settings of the wireless device, select the key fob from the list (as shown in Figure 4.17) and press any button on X-Key - X-Key LED indicator will flash and X-Key will be automatically added.

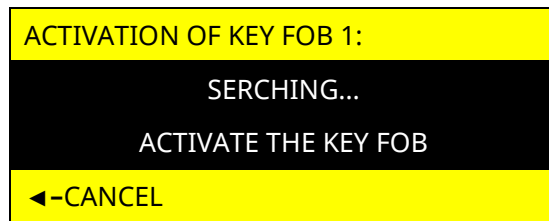


Figure 4.17 – A dialog box for key fob searching

For adding the key fob from the LED keypad (wired), enter the command:

installer access code # 4 #

Then press any button on the X-Key key fob.

The adding mode launches with the SCP start automatically which is confirmed by the HL LED indicator flashing on the SCP board. Only after the HL LED indicator starts flashing, it is necessary to press the "Start" button on the key fob with a one-second delay.

After successful key fob activation, its green LED flashes three times.

To add the key fob in the "Panic button" mode, set this mode for the required zone and follow the steps similar to the steps of adding X-Shift, X-Shift+, X-Motion, and X-Motion+ wireless detectors. In the "Panic button" mode, any button press is interpreted by the SCP as a "Panic button" alarm.

To use the key fob in automation, it can be added to the zone of the "Universal Input" type. Using the oLoader II software, you can assign the key fob to the zone as described above for the wireless detectors and activate the X-Key key fob.

Adding X-Pad

X-Pad can be added to the SCP using the display keypad. The keypad serial number must be specified in the SCP settings. To activate the keypad, remove the back cover and press the "Start" button on X-Pad. When pressing the "Start" button, it is activated automatically if its serial number is specified in the settings. If the keypad is successfully activated, it is automatically moved from the "ACTIVATION" section to the "ASSIGNED" section.

For adding the keypad with no serial number specified in the SCP settings, select it from the list (as shown in Figure 4.18) and switch on the keypad. When the keypad is switched on, it will be automatically activated and appear in the "ASSIGNED" section.

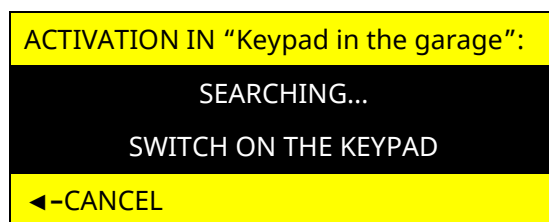


Figure 4.18 – A dialog box for keypad searching

To add the wireless keypad from the LED keypad (wired), enter the command:

installer access code # 4 #

Then press the "Start" button on the wireless keypad board.

The adding mode is also activated automatically after the SCP start, which is confirmed by the HL LED indicator flashing on the SCP board. Only after the HL indicator starts flashing, press the "Start" button on the keypad with a one-second delay.

In both cases of adding, successful activation of the keypad is indicated by triple sound signals.

Adding X-Siren

X-Siren can be added to the SCP using the display keypad. The siren serial number must be specified in the SCP settings. To activate the siren, remove the back cover and press the "Start" button on the X-Siren. When pressing the "Start" button, it is automatically activated if its serial number is specified in the settings. If the siren is successfully activated, it is automatically moved from the "ACTIVATION" section to the "ASSIGNED" section.

For adding the siren with no serial number in the SCP settings, select it from the list and switch on the siren. When the siren is switched on, it will be automatically activated and appear in the "ASSIGNED" section.

To add the siren from the LED keypad (wired), enter the command:

installer access code # 4 #

Then press the "Start" button on the siren with a one-second delay.

The adding mode is also automatically activated after the SCP start, which is confirmed by the HL LED indicator flashing on the SCP board. Only after the HL LED indicator starts flashing, press the "Start" button on the siren with a one-second delay.

In both cases of adding, successful activation of the siren is indicated by triple flashing of the LED indicator and a sound signal.

To exit the Adding mode, press any button or wait for 10 minutes.

Adding X-Cover S

X-Cover S can be added to the SCP using the display keypad. The repeater's serial number must be specified in the SCP settings. To activate the repeater, press the "Start" button on the X-Cover S. When pressing the "Start" button, it is automatically activated if its serial number is specified in the settings. If the repeater is successfully activated, it is automatically moved from the "ACTIVATION" section to the "ASSIGNED" section.

For adding the repeater with no serial number in the SCP settings, select it from the list and switch on the repeater. When the repeater is switched on, it will be automatically activated and appear in the "ASSIGNED" section.

To add the repeater from the LED keypad (wired), enter the command:

installer access code # 4 #

Then press the "Start" button on the repeater with a one-second delay.

The adding mode is also automatically activated after the SCP start, which is confirmed by the HL LED indicator flashing on the SCP board. Only after the HL LED indicator starts flashing, press the "Start" button on the repeater with a one-second delay.

In both cases of adding, successful activation of the repeater is indicated by triple flashing of the LED indicator.

To exit the Adding mode, press any button or wait for 10 minutes.

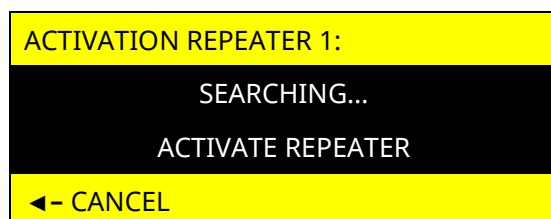


Figure 4.19 – A dialog box for repeater searching



The activation of wireless devices requiring amplification is conducted in the range of the M-X module.

4.4.4 Wireless device unassigning

There are three ways to delete the wireless device from the system: 1) using the display keypad in the "WIRELESS DEVICES" menu; 2) using the "Start" button; 3) using the Control NOVA II software.

Unassigning the wireless device using the Control NOVA II software

The wireless device can be unassigned by the administrator or installer. To unassign the wireless device using the Control NOVA II software, open the "WIRELESS DEVICES" menu, select the required wireless device from the list and press the "DELETE" button. There are two options for deletion:

1. **"Temporary deletion"** – the wireless device resets its settings to default ones and switches off (if it is within the range of the M-X module transceiver), the serial number remains in the settings allowing to activate the wireless device.
2. **"Delete completely"** – the zone/keypad/key fob/siren/repeater is deleted from the settings and the wireless device resets its settings to default ones after receiving the command and switches off (if it is within the range of the M-X module). For X-Key unassigning, press any button. After unassigning, the wireless device will confirm the received command (see Table 4.9).

Unassigning the wireless device using the display keypad

Unassigning the wireless device using the display keypad is available only for users with "Installer" privileges. To unassign the wireless device using the display keypad, open the "WIRELESS DEVICES" menu, select the required active wireless device and select "UNASSIGN"¹. The wireless device will be unassigned when there is a test message or alarm (such as tamper alarm). For X-Key unassigning, press any button. After unassigning, the wireless device will confirm the received command (see Table 4.9).

Unassigning the wireless device using the "Start" button

For the X-Key unassigning, press the **□** and **△** buttons simultaneously and hold them (5 s) until you see a long flash of the red indicator, then release the **□** and **△** buttons. For the next two seconds (while the red indicator flashes), shortly press the **X** button.

To unassign X-Shift, X-Shift+, X-Motion, X-Motion+, X-Motion Alarm, X-Water, X-Pad, and X-Siren, press and hold the "Start" button until the LED indicator flashes twice or you hear two sound signals of the buzzer.

The indication when unassigning using the display keypad and the "Start" button is given in Table 4.9.

Table 4.9 – Indication when unassigning using the display keypad and the "Start" button

Device	Successful unassigning	Unassigning only on the wireless device side (if there is no communication between the SCP and the wireless device)
X-Shift, X-Shift+, X-Motion,	Two long flashes	One long flash

¹ Corresponds to deletion.

X-Motion+, X-Cover S		
X-Pad, X-Siren	Two long flashes with sound signal of buzzer	One long flash with sound signal of buzzer
X-Key (after pressing the button)	Two long flashes of green LED	One long flash of green LED
X-Water, X-Motion Alarm	Two long sound signals of buzzer	One long sound signal of buzzer

4.4.5 Switching on the wireless device

To switch on the wireless device, remove the wireless device or keypad from the bracket and press the "Start" button. Indication of successful switching on the activated wireless device is shown in Table 4.10.

Table 4.10 – Switch-on indication of the activated wireless device

Device	Indication
X-Shift, X-Shift+, X-Motion, X-Motion+, X-Siren, X-Cover S	Three short flashes
X-Pad	Three sound signals of buzzer, pause, one more sound signal
X-Motion Alarm, X-Water	Three short sound signals of buzzer

4.4.6 Switching off the wireless device

To switch off the wireless device, press and hold the "Start" button until the second short flash (the first flash indicates pressing the "Start" button). Indication of successful switching off the activated wireless device is shown in Table 4.11.

Table 4.11 – Switch-off indication of the activated wireless device

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 sound signal of buzzer

4.4.7 Features of the wireless devices

X-Key

When pressing the "Panic button", the alarm message about the attack on the user is transmitted to the Control NOVA II software of all the 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, hold it from 0.3 to 2 seconds, and release the button. Then the LED indicator on the added key fob flashes one of the following colors:

- **green** – the command has been transmitted;

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

After successful transmission of the command, the indicator flashes with an interval of 1 s, confirming the command execution:

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

There is no indication of the command execution for the "Panic button" and for repeating the previous command. The key fob configured as the "Panic button" sends an attack message when any button is pressed.

X-Motion

To ensure long battery life, X-Motion forms 5 alarms per security session by default. The detector will react to the motion after re-arming or automatic arming. The number of alarms from the detector is configured via the oLoader II software. If the "Constantly active motion sensor" option is disabled, after receiving the arming command, X-Motion needs 30 seconds for the PIR sensor to start detecting motion.

X-Motion+

The break sensor can operate in one of three sensitivity levels and can be configured in the oLoader II software. Be careful with the microphone connection cable because it can be easily damaged when replacing the battery (CR123A).

X-Motion Alarm

X-Motion Alarm has a built-in siren, which can be switched off to preserve the detector battery life.

Setting the built-in siren includes the following options:

- The "Signal volume" option has four levels of siren volume.
- The "Autonomous notification" option can operate in three modes:
 - "When motion is detected" – activates the siren if the armed detector detects motion and the communication with the SCP is lost.
 - "When opening the case" – activates the siren if the detector is armed, its enclosure is opened, and communication with the SCP is lost.
 - "In case of loss of communication with SCP" – activates the siren if the detector is armed and has no communication with the SCP. Once the mode is enabled, it is necessary to set the duration of communication loss that triggers the activation of the siren.

X-Shift

After mounting and fixing, the detector should be calibrated. Calibration should be performed with the windows/doors closed. This feature is available in the Control NOVA II software. When the detector is correctly installed and the command has been received, the message is sent to the Control NOVA II software to indicate a successful calibration.

The magnet can be placed on the right or left side of the detector, parallel to its axis. The detector with a magnet may be placed in a horizontal position. The maximum magnet installation distance depends on the surface material where the detector is installed (the distance on metal surfaces is reduced by about 3 times).

An additional wired magnetic contact detector or remote LED can be connected to X-Shift. To do this, open the X-Shift enclosure, connect an additional magnetic contact detector (opening sensor) to the terminals in the middle of the enclosure and enable the "Wired connection" option in the oLoader II software, selecting one of the available modes: "Wired magnetic contact detector" or "Remote LED". In the oLoader II software, this option is enabled for each X-Shift individually.

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 strokes" option is enabled, the alarm is generated only if the sensor detects more than one shock.

X-Pad

Do not leave any objects on the touch screen of the keypad when it is switched on, as this may affect its correct operation.

Before entering the access code on the activated keypad, it is necessary to press any button (for 1 s) to "wake up the keypad", then you will hear a multi-tone sound signal.

X-Siren

The X-Siren has a 12V terminal block for connecting the external power supply. To connect the siren to an external power supply, it is necessary to make a hole for the cable in a specially designated place in the bracket.

To run the siren on the external power supply, enable the "External power supply" option in the oLoader II software.

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 "Water leak confirmation" 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.

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 1²: Add a repeater and new wireless devices.

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

²The SCP allows to pre-assign wireless devices, a repeater and configure the wireless devices for amplification. During activation, the wireless devices will receive the necessary settings and start working with repeaters. After that, you need to perform steps 4 and 5 described above.

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 M-X module 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.

You can assign the wireless device, immediately set it for amplification, and then perform its activation. After successful activation in the range of the M-X module, 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 M-X module 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 M-X module 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 job within the range of the M-X module. The X-Key works only with the repeater it is assigned to.

4.5 Language menu

In this item, the language of the display keypad menu can be configured, as well as the language of SMS messages sent to user phone numbers. The options available for selection are as follows: UKRAINIAN, RUSSIAN, and ENGLISH (see Figure 4.20). To change the language, select the option using the ▲ and ▼ buttons and click the ● button.

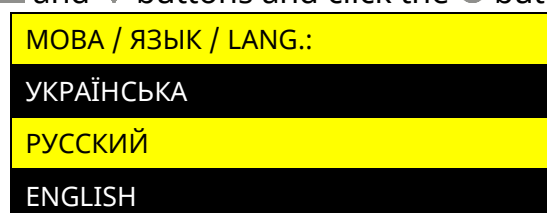


Figure 4.20 – A dialog box for language selection

4.6 Keypad options

This setting item displays the list of keypads added to the system (see Figure 4.21).

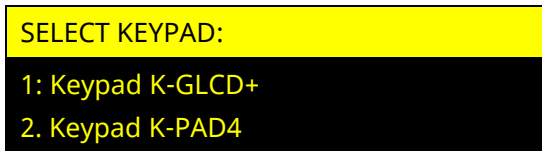


Figure 4.21 – A dialog box for keypad setting

After selecting the desired keypad, the display shows the options available for configuration (see Figure 4.22). If there is only one keypad in the system, you will immediately enter the settings for its options.



Figure 4.22 – A dialog box for keypad setting

4.6.1 Doorbell

This option allows to switch on the built-in keypad buzzer (4 short sound signals), when intruding the zones specified in its settings.

To enable the option, click the ● button on the "SWITCH ON" item. After enabling, select the required zones (the list shows the available zones of the following types in the system: "Entrance door", "Corridor, and "Security"). To the left of each zone, there is the symbol "[+]" or "[]" indicating whether the option is enabled for this zone or not respectively.

To disable the option, go to the "DISABLE" item and click the ● button.

4.6.2 Presence

This option allows to switch on (for one minute) the display (if available) and the keypad backlight, when the zones specified in its settings are intruded.

To enable the option, click on the ● button in the "SWITCH ON" item. After enabling, select the required zones (the list shows the available zones of the following types in the system: "Entrance door", "Corridor", and "Security"). To the left of each zone, there is the symbol "[+]" or "[]" indicating whether the option is enabled for this zone or not respectively.

To disable the option, go to the "DISABLE" item and click the ● button.

4.6.3 Night light



The "Night light" option is available only for the K-GLCD+ keypad.

The option allows to illuminate the wall indication of the K-GLCD+ keypad for a specified period (for example, to illuminate a corridor at night). This option is enabled and disabled in the oLoader II software in the "SMART Light" section. After enabling, set the time interval of the night light and the light colour (see Figure 4.23).

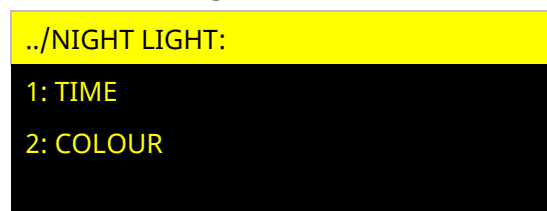


Figure 4.23 – A dialog box for the "Night light" option setting

After selecting the "TIME" item, the display shows the current time interval of the night light and allows to set a specific time interval (see Figure 4.24).

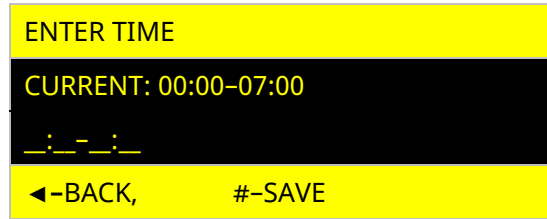


Figure 4.24 – A dialog box for the setting the time of "Night light" option

The operation period is set in 24-hour format. To clear the entered values, press the **F2** button. To save the settings, press the **#** button. To cancel, press the **<-** button.

In the "COLOUR" item, you can change the colour of the wall indication. The available colours are white, blue, aquamarine, deep blue, violet, and green-gray. The "SET CUSTOM" option allows to customize the colour of the wall indication.

4.7 Zone testing



Changing the zone status in the "Zones testing" mode affects only the indication in this menu and is not transmitted to the CMS, Tiras CLOUD II, and SMS, the check call is not made, nor scripts are run, or the siren is activated.

4.7.1 Testing using the display keypads

This item displays the system zones (see Figure 4.25). The device zones are navigated by means of the **<**, **>** and **▲**, **▼** buttons (if the device has more than 8 zones). To move to the zones of the next device (the SCP, keypad, and expansion module), use the **▲** and **▼** buttons.

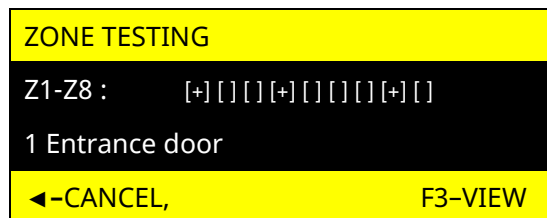


Figure 4.25 – A dialog box for zone testing

If the zone is "NORM", it is marked by the "[]" symbol. If the zone is "NOT NORM", it is marked by the "[+]" symbol.

With the **F3** button, zone display mode can be changed. In the "Last intrusions" mode, three last zone intrusions that were recorded after the testing mode start are displayed (see Figure 4.26).

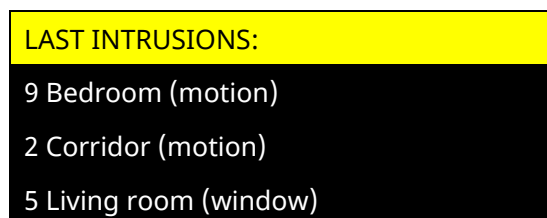


Figure 4.26 – "Last intrusions" testing mode

The "Not tested" mode displays the list of zones not transited from "NORM" to "NOT NORM" state after the testing mode start (see Figure 4.27). After the untested zone intrusion, the symbol "[+]" appears near its name. After restoration, the zone disappears from the list.

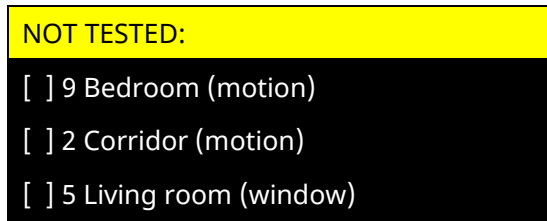


Figure 4.27 – "Untested zone" testing mode

When running "Zones testing" mode from one keypad, it runs on all the keypads in the system, while the system state control is currently unavailable. To exit the menu, press the * button or the ← button.

4.7.2 Zone testing using the LED keypads

To start zone testing mode, enter the following combination on the keypad:

installer access code # 0 #

In "Zones testing" mode, the zones indicators in the "NOT NORM" status flash red. The indicator number corresponds to the zone number in the system. To exit "Zones testing" mode, click the * button on the keypad from which the testing mode was enabled.

4.8 Device control (RS-485)

When selecting this item, the display will show the list of available devices (keypads and expansion modules connected via RS-485 interface), as shown in Figure 4.28.

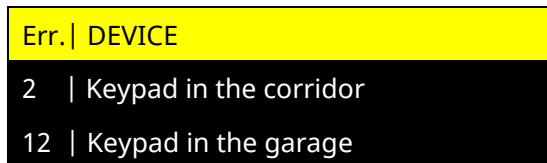


Figure 4.28 – A dialog box for device control menu

In the "Error" column near each device, the number of lost data packets (per 1000 last) between the SCP and each of the devices is displayed. If the number of lost packets is more than 10, it is necessary to ensure that the device connection meets the requirements given in Section 2.

To exit the menu, press the * button or the ← button.

4.9 SCP restart

After the SCP restart, the current settings and event log will be saved. Table 4.12 describes the steps you need to take to restart the SCP.

Table 4.12 – SCP restart

Keypad type	Description of actions for restarting
Display	Go to the "SCP RESTART" item and press the 5● button
LED	Enter the combination: installer access code # 13 # installer access code #



If the SCP restart was performed during the process of downloading the firmware update, downloading the firmware update must be initiated again.

4.10 Firmware update

When selecting the "FIRMWARE UPDATE" item, the following options are displayed (see

Figure 4.28): AUTOMATIC UPDATE, UPDATE TO BETA and DEVICES. Each of them is described in detail in this section.

Figure 4.29 shows the "Firmware update" menu

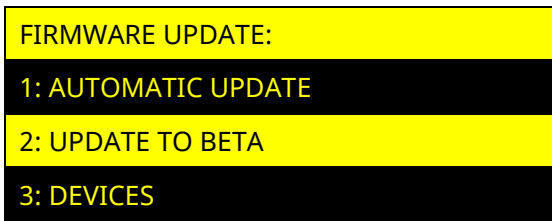


Figure 4.29 – A dialog box for the firmware update

4.10.1 Automatic update

The "Automatic update" option allows the SCP, connected and assigned modules and keypads to independently check the availability of the firmware update (once a day), download and install it (if there are no armed groups in the system and power supply faults). The automatic update is set according to Table 4.13.

Table 4.13 – Menu for setting automatic firmware update

Parameter	Description
Off	The SCP will not automatically download and install the firmware update
On	If the firmware update is available, the SCP will automatically download and install it, if there is a connection with Tiras CLOUD II, regardless of the type of communication channel
Only via Ethernet/Wi-Fi	If the firmware update is available, the SCP will automatically download and install it, if there is a connection with Tiras CLOUD II via Ethernet or Wi-Fi

4.10.2 Update to beta version

The "Update to beta" option allows to early access to updates by the "On" or "Off" value (see Figure 4.30).

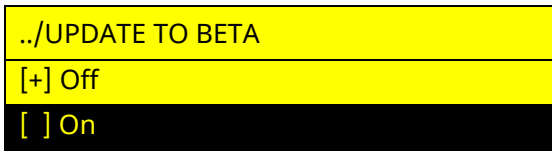


Figure 4.30 – A dialog box for the "Update to beta" menu

The "Update to beta" option is set according to Table 4.14.

Table 4.14 – Menu for setting update to beta version

Parameter	Description
Off	The device will not check for updates with early access
On	If the update with early access is available and automatic firmware update is enabled, the SCP will automatically download and install it. If automatic update is disabled, the update with early access will be available from the display keypad menu



By enabling the "Update to beta" option, the user can gain early access to test software updates. Such updates may contain some shortcomings, and by enabling this option the user should confirm that he/she understands and accepts the possible risks.

TIRAS-12 LTD is not responsible for the possible consequences of using test system updates.

4.10.3 Devices

When selecting the "DEVICES" item, you will get to the list of the SCP and devices assigned to it (keypads and expansion modules connected via RS-485 interface).

In the "SCP" item, you can check for updates (see Figure 4.31).

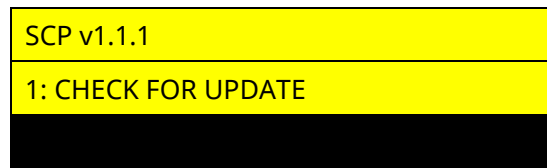


Figure 4.31 – SCP updates menu

Check for updates

When selecting the "CHECK FOR UPDATE" item, the display will show the message with the checking progress status. This item is available for assigned keypads and modules. If the current firmware version is installed in the SCP, keypads or modules, the notification "NO UPDATES FOUND" is displayed. If a newer firmware version is available, the notification "DOWNLOAD" and the firmware version number is displayed.

To download the update, select the required firmware version. After that, the download loading process starts displaying the percentage of the download progress. When the download is complete, the notification "UPDATE DOWNLOADED" is displayed. To install the downloaded update, click the # button to restart the SCP and launch the automatic software installation process. To ensure an uninterruptible power supply during the update installation, the SCP must be connected to the battery and 230 V network. The installation process takes approximately 2 minutes.

When updating the firmware of the SCP, current settings remain unchanged.

Manual update of keypads and expansion modules firmware

The firmware update of the assigned keypads and expansion modules is available when there is a HEX update file for the corresponding system device (supporting the update option) on the USB flash drive of the SCP.

After choosing the keypad or expansion module, the notification "START UPDATE TO v x.x?" is displayed.



Before updating keypad and expansion module firmware, make sure there are no connection faults with them.

To install the update, click the # button. Then the notification "FIRMWARE IS UPDATING, DO NOT SWITCH OFF POWER" is displayed. When the update process is completed, the updated keypad will restart. The notification "UPDATING COMPLETED SUCCESSFULLY" is displayed on the keypad.

If the update file is absent, the notification "UPDATE FILE NOT FOUND" is displayed.


4.11 Default settings



When the default settings are restored, all the settings of the SCP differing from the default ones will be lost. All data about the SCP in the Tiras CLOUD II service will be cleared; the SCP will be deleted from all accounts in the Control NOVA II software.

4.11.1 Restoring default settings using display keypads

When selecting "DEFAULT SETTINGS" in the SETTINGS section, the following notification is displayed on the keypad: "!! WARNING !! CHANGING DEFAULT SETTINGS" and the F3 button to

confirm the action and the  button to return to the previous menu. When the **F3** button is pressed, the SCP is restarted and switched on with the restored default settings (see Table D.1, [Appendix D](#)).

4.11.2 Restoring default settings using LED keypads

To restore the default settings of the SCP using the LED keypads, enter the following combination on the keypad:

installer access code # 5 # installer access code #

After entering the combination, the device is restarted and switched on with the restored default settings (see Table D.1, [Appendix D](#)).

4.12 Formatting the SCP flash-memory drive

Formatting the SCP flash memory drive is required when the file system of the SCP flash memory drive or the configuration file of the SCP ("Config") stored on this drive is damaged (for example when infected by viruses during configuration using the PC).



It is forbidden to format the SCP flash drive using Android devices.

4.12.1 Formatting the SCP flash drive using display keypads

When selecting "**FLASH MEMORY FORMATTING**" in the "SETTINGS" section, the notification "FORMATTING..." is displayed on the keypad. When the formatting process is completed, the keypad returns to the home screen. A "Config" file with the current settings of the SCP will be created on the SCP flash drive.

4.12.2 Formatting the SCP flash drive using LED keypads

To format a flash drive, enter the following combination on the keypad:

installer access code # 14 # installer access code #

The successful combination entering is confirmed by four short sound signals of the keypad buzzer. After the formatting process is completed, the "Config" file with the current SCP settings is created on the flash drive.

4.12.3 Formatting the SCP flash drive using the "Reset" button on the SCP board

To format the flash drive, press the "Reset" button for 5 seconds in the operating mode of the SCP. When this process is completed, the "Config" file with the current SCP settings is created on the flash drive. The process of the "Config" file creation is accompanied by flashing SIM1 and SIM2 indicators on the SCP.



When formatting the flash drive, the SCP settings are saved, but all the files on it are deleted (including exported event log files, firmware files, etc.).

4.13 Calibration of EOL resistors

The calibration option allows to use detectors with EOL resistors in the range from 1 kΩ to 7.5 kΩ. The option is available only for the zones loop connected to the SCP. The calibration is started for all the zones simultaneously.

The calibration requires all the SCP zones to be in normal state (without alarms). The calibration for each zone is performed separately, so it is possible to use detectors with different EOL resistors.

4.13.1 Calibration of EOL resistors via LED keypads

To calibrate the EOL resistor, enter the following combination on the keypad:

installer access code # 16 # installer access code #

Successful combination entering and the beginning of the calibration of the EOL resistors is confirmed by one short sound signal of the keypad buzzer. The zone status indicators of the calibrated zones lit green. The zone status indicators of the uncalibrated zones lit red being accompanied by one long sound signal of the keypad buzzer.

4.13.2 Calibration of EOL resistors via display keypads

When selecting the "EOL CALIBRATION" item in the "SETTINGS" section, the notification "START EOL CALIBRATION?" will appear on the keypad display with the # button to confirm the action and the ← button to return to the previous menu. After pressing the # button and successfully calibrating the EOL resistors, the notification "EOL CALIBRATION COMPLETED" will appear on the keypad display and the ← button to return to the previous menu. If the EOL resistors are not calibrated successfully, the list of uncalibrated zones will appear on the keypad display (see Figure 4.32).

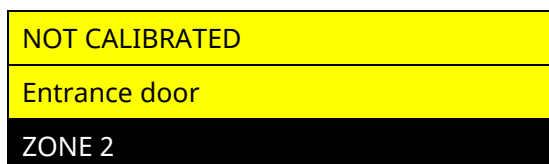


Figure 4.32 – The "NOT CALIBRATED" menu



When calibrating the EOL resistor less than 3 kΩ, the operation time from the battery will be reduced.

4.14 Communication status

4.14.1 Checking the communication status on the display keypads

When selecting the "COMMUNICATION STATUS" section in the main menu of the installer, the current communication with the CMS and (or) Tiras CLOUD II status is displayed (see Figure 4.33).

The "CMS" item displays information about the current communication channel for the SCP communication with the CMS (indicates the communication module or SIM card number and the CMS address), as well as the information about the availability of each configured communication channel (the symbol "[+]" indicates a working communication channel, while the symbol "[]" – a faulty one). When the SCP is working autonomously or when the CMS settings are hidden, the "CMS" item is not displayed.

In the "TIRAS CLOUD" item, the communication module or SIM card number for communication with Tiras CLOUD II is specified. When "Connection with Tiras CLOUD II" option is disabled, the "Tiras CLOUD" item is not displayed.

In the "LEVEL" item, the Wi-Fi signal level (according to Table 2.5) or the active SIM-card (see Table 2.3) is indicated. In case of no configured SIM-cards and M-WiFi module, the "LEVEL" item is not displayed.

"SIM1" or "SIM2" item displays the phone number of the active SIM card.

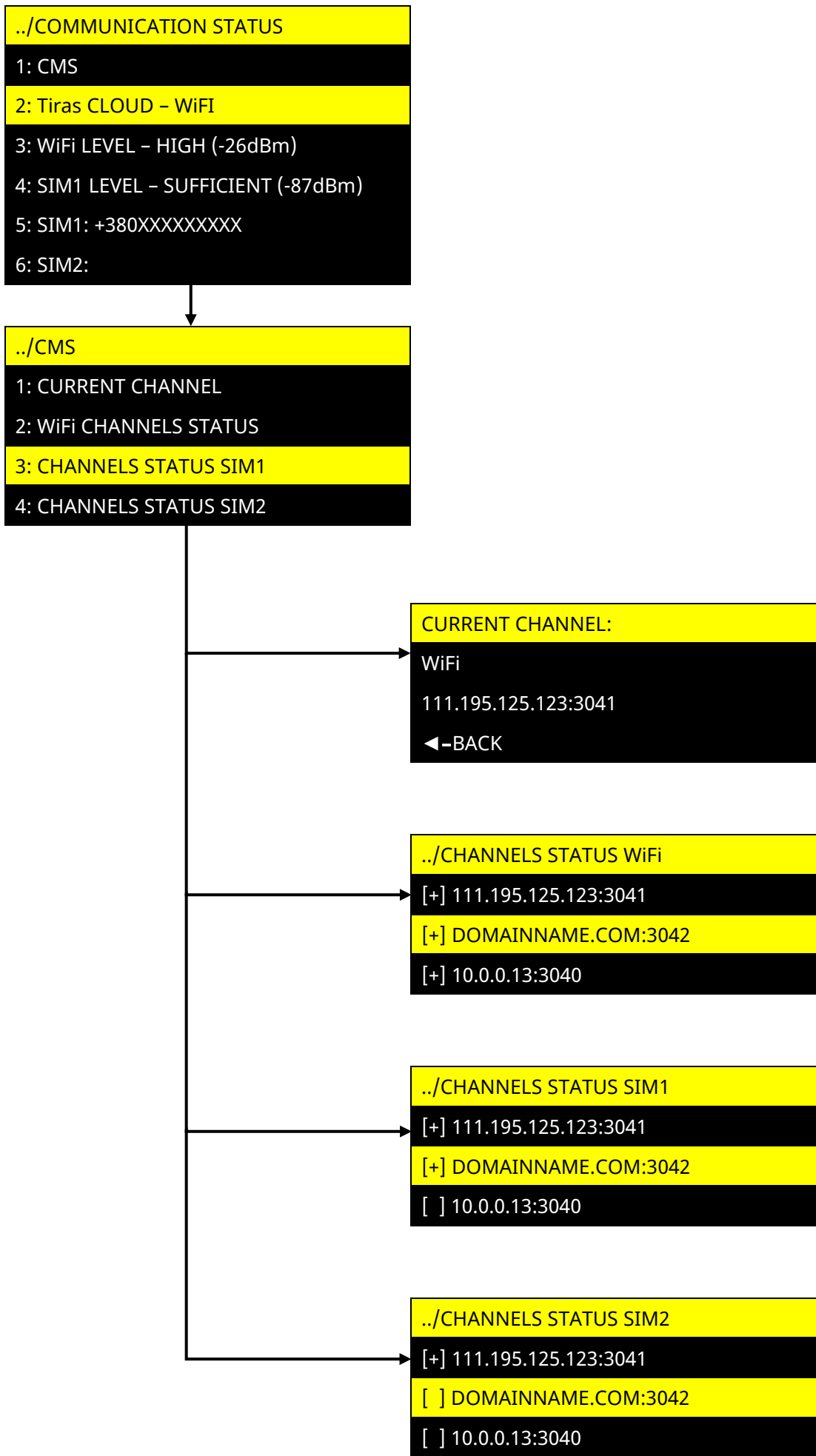


Figure 4.33 - "COMMUNICATION STATUS" menu

4.14.2 Checking the communication status using the LED keypads

Using the LED keypads, the installer can check the signal strength of the Wi-Fi and GSM/LTE networks.

Viewing 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, the keypad indicators 1-4 will display the signal strength of the Wi-Fi network as shown in Table 4.15.

Table 4.15 – Display 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, wrong password, etc.)

Viewing the GSM/LTE signal strength

To view the current **GSM/LTE** signal strength, enter the following combination:

installer access code # 12 #

After entering the combination, the keypad indicators 1-4 will display the GSM/LTE signal strength of the active SIM-card as shown in Table 4.16.

Table 4.16 – Display of the GSM/LTE 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 changing a SIM card or losing registration)

4.15 USSD-request



To enable USSD-requests running, at least one SIM-card should be set.

When selecting the "USSD-REQUEST" section, the installer is asked to select the SIM-card for request running (see Figure 4.34). If only one SIM card is configured, a dialog box for entering the USSD code opens immediately.

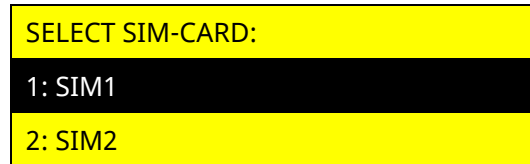


Figure 4.34 – A dialog box for selecting a SIM-card to run a USSD request

The "ENTER USSD-REQUEST" dialog box (see Figure 4.35) displays the field for entering the USSD code and the **F1** button to get additional information, and the **F3** button to run the USSD-request.

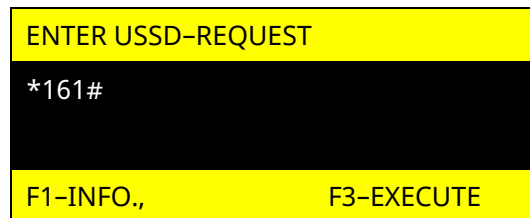


Figure 4.35 – A dialog box for entering the USSD code

To enter the USSD code, use the following buttons: "0" - "9" - to type text, * - LEFT, # - RIGHT, ← - EXIT, **F2** - DELETE, **F1** - INFO., **F3** - EXECUTE.

With the help of USSD-requests, the installer can get information about the status of the SIM-card account, as well as other information from the mobile network operator. The list of USSD codes and their values is provided by the mobile operator. If there are no configured SIM cards, the "USSD-REQUEST" section is not displayed.

5. SCP CONTROL

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

There are four access levels to the SCP functions:

1st access level – access for any person. The access code is not required. Alarms and warning indications on the keypad are available (the **i** indicator) at the 1st access level unless the permanent indication mode is set. Also, at the 1st access level, the scripts can be run from the display keypads if they are pre-configured.

2nd access level – access level for system users, requiring the access code. The 2nd access level displays the system status on the keypad indicators (see Table D.4, Appendix D). The users with the 2nd access level can control the elements added to their settings (groups arming/disarming, output states control, and the scripts running).

3rd access level – access level for the users of the Installer type allowing to change all the SCP settings.



The users of Administrator type can grant/deny access to the 3rd level.

4th access level – access level for the manufacturer; the manufacturer can make changes to the devices, equipment design, and firmware.

5.1 System control via keypads

The SCP supports display keypads K-GLCD+, K-PAD OLED (see Figure 5.1) or K-PAD OLED+, and LED keypads of the following types: K-PAD4, K-PAD4+, K-PAD8, K-PAD8+, K-PAD16, K-PAD16+, and X-PAD (see Figure 5.2).

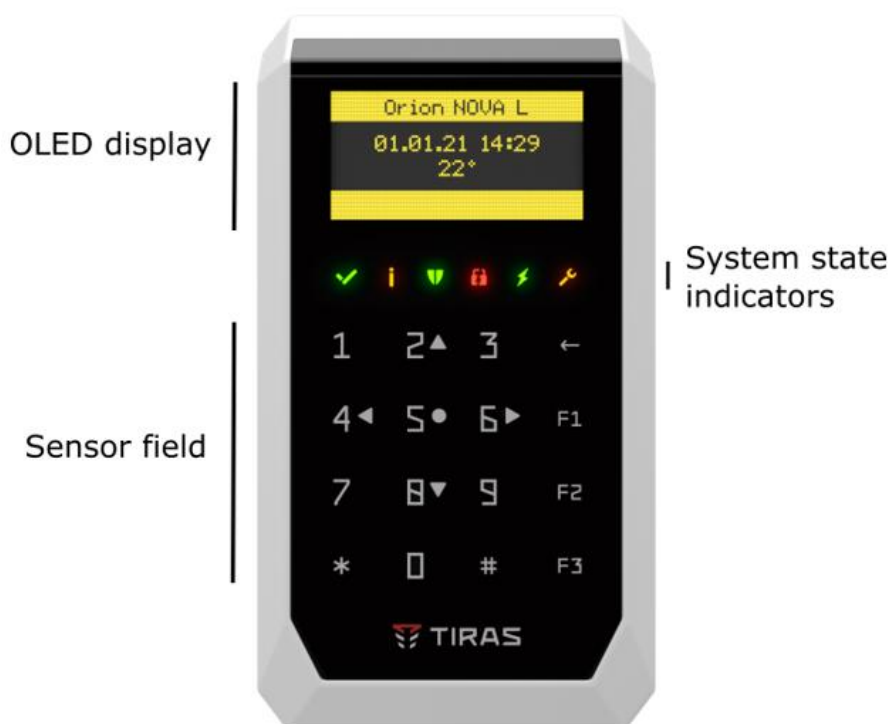


Figure 5.1 – K-PAD OLED



Figure 5.2 – K-PAD8/X-PAD

The SCP control using the keypads is available after the user authorization which requires entering the valid access code and pressing the # button. User authorization is confirmed by four short sound signals of the keypad buzzer, after which the indicators on the keypad display the current state of the system (see Table D.4, Appendix D).

Entering the invalid access code is indicated by one long sound signal of the buzzer. If the invalid access code (including TM) is entered four times in a row, all the connected keypads and readers are blocked for 90 seconds, the corresponding message on password selection event is sent to the CMS and Control NOVA II software.

Table 5.1 – Groups or zones status indication on LED keypads

Groups or zones status indication on LED keypads		
Indicator state	Zone state	Group state
No lights	The zone is disarmed	All zones of the group are disarmed
Flashing red (once)	Entry delay in zone	Unviewed alarms in any zone of the group
	The zone is violated and is in alarm	
Flashing red (double)	Unviewed memory of alarms in zones	-
Lights red	Viewed alarm in the zone	Viewed group alarm
	The zone is violated and cannot be armed	
Flashing green	Exit delay for "Entrance door" or "Corridor" is counted down	Group exit delay is counted down
Lights green	Armed zone	Group or part thereof is armed



When using the keypad in the "Permanent indication" mode, its current consumption increases, thus reducing the system operating time from the battery.

When controlling the SCP by display keypads, after entering the access code and pressing the # button, the user enters the 2nd access level menu (see Figure 5.3).

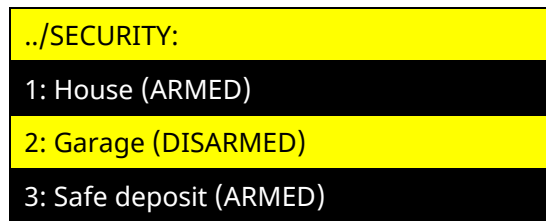


Figure 5.3 – The 2nd access level menu on the display keypads

The keypad display contains four text lines. Top line contains the menu or submenu name. Next three lines contain menu items navigated by means of the ▲ and ▼ buttons – the selection cursor goes to the next or the previous menu item. To select the menu item, press the ● button. To return to the previous menu, press ◀ or *.

5.1.1 Sound indication of keypads

Each keypad is equipped with a buzzer, which generates a sound signal for certain events in the system or keypad actions. The buzzer operating modes are described in Table 5.2.

Table 5.2 – Sound signals of keypads buzzer and their description

Sound	Meaning
1 short beep	Press the button on the keypad
1 long beep	Denial
1 long repeating sound signal	Keypad is blocked
4 short beeps	Action confirmation
4 short duplicate signals	Entry/exit delay
Permanent beep	Alarm

5.2 Groups arming and disarming

5.2.1 Group arming

To arm the group, do the following:

1) before arming, close all the doors and windows in the protected premises. Make sure that the group is ready to be armed with your control device;

2) if the protected group does not contain the zones with delay ("Entrance door", "Corridor"), it is required to leave the premises being armed and close the entrance door.

If the control device of the SCP is inside the protected premises, the zones with delay ("Entrance door", "Corridor") must be configured for the correct group arming. The zones with delay may remain intruded during the exit delay;

3) initiate arming (depending on the SCP). If the group does not have zones with delay, it will be armed immediately.

If the control device of the SCP is inside the premises, then the user must leave the room and close the entrance door during the exit delay. After the exit delay expires or after all zones return to the normal state, the group becomes armed. The corresponding message is sent to the CMS about the arming of the specified zones. Upon receipt of the confirmation from the CMS, the remote confirmation LEDs configured for the armed group will flash within the time specified in the SCP settings.



Depending on the load of the CMS and the communication channel with the CMS, the interval between the arming and the receipt of the corresponding confirmation from the CMS ranges from 1 to 20 seconds.



If after the exit delay expiration, at least one zone of the "Entrance door" or "Corridor" type, which are the part of the arming group, is intruded, then arming of all zones of this type will not be carried out. The relevant zone indicators and the "Security" indicator (see Table 5.1) will flash green. In this case, it is necessary to eliminate the cause of the failure and repeat the attempt.



If one group has common zones or is part of another group, when arming the first group, the second one will be "Partial armed". To switch the group from "Partial armed" to "Armed" mode, disarm this group and then arm it again. The confirmation LED will light if all zones of the group or the "Entrance door" are armed. The "Confirmation by siren" option will be enabled when all zones of the group are armed.

5.2.2 Group disarming

If the control device of the SCP is inside the protected premises, do the following to disarm the group:

- 1) open the entrance door – the entry delay starts. The buzzer will sound on the keypads for which the sound indication is set (see Table 2.3);
- 2) during the entry delay, disarm the group of zones using control device.

If the control device of the SCP is outside the premises, just disarm the group using the control device.

5.2.3 Group arming in "I'm at home" mode

"I'm at home" mode allows to protect the object perimeter (entrance doors, windows, fences, etc.) ignoring the intrusion in the user-selected zones inside the object.

In "I'm at home" mode, the group can be armed using the keypad, reader, or Control NOVA II software if there is at least one zone with the enabled "I'm at home" option.

Arming using keypads and readers. To arm in the "I'm at home" mode, initiate the group arming and during the exit delay do not intrude zones of the "Entrance door" type. After the exit delay expires, all zones of the group will be armed, except for the zones such as "Corridor" and "Security" configured in the "I'm at home" mode.

Arming using the Control NOVA II software. To arm in the "I'm at home" mode, after authorization in the object, click on the "I'm at home" icon near the required group. All zones of the group will be armed, except for the "Corridor" and "Security" zones configured in the "I'm at home" mode.

If the group is armed in the "I'm at home" mode, when the "Entrance door" zone is intruded, the siren is turned on without delay, the alarm is generated immediately.



The group comprising the zones with the enabled "I'm at home" option must contain zones with delay ("Entrance door"). In case there are no such zones, the "I'm at home" mode will be ignored.

5.2.4 Groups arming/disarming using display keypads

The control of groups using the display keypad is possible after the user's authorization (entering the valid access code and pressing the # button). After authorization, the system enters the 2nd access level with four short sound signals and the corresponding menu is displayed on the keypad.

If there is only one group in the user settings, or the control of a certain group is specified in the user's access code main action, after authorization, the control menu for this group is displayed (see Figure 5.4).

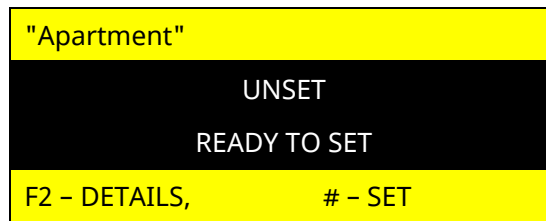


Figure 5.4 – Group control menu

The group menu is displayed on the keypad:

- the upper line contains the name of the group;
- the second and third lines display the current group states (the possible states of the group are given in Table 5.3);
- the fourth line contains a hint for possible user actions.

Table 5.3 – Possible group states

No	Group state	Description of the group state and possible user actions
1	SET	All zones of the group are armed. Pressing the # button will disarm the group.
2	SET (CMS)	All zones of the group are armed; confirmation from the CMS is received. Pressing the # button will disarm the group.
3	PARTIAL ARMED	Some zones of the group are armed. Pressing the # button will disarm the group. By pressing the F2 button, the user can browse the list of armed zones. To transition in the "ARMED" mode, disarm this group and arm again.
4	READY TO SET	All zones in the group are normal. Pressing the # button will arm the group.
5	INTRUDED	More than one zone of the "Security" type in the group is not normal. It is impossible to arm the group. By pressing the F2 button, the user can view the list of zones that are not normal. When the # button is pressed, the group of zones will not be armed.
6	ALARM	One, several, or all groups of the zone are in alarm mode. By pressing the F2 button, the user can view the list of zones that are in alarm mode.
7	EXIT TIME, COMPLETED IN: [time to end in seconds]	The group with delay zones ("Entrance door", "Corridor") is armed. When the * button is pressed, the user can quit the 2 nd access level (the keypad buzzer will be turned off), the group will continue arming. When the user presses the # button, the user can complete the exit delay - the group becomes armed.

If there are several user groups in the user settings and there are no control elements in the user's access code main action, after the authorization, the SECURITY menu with the list of user groups is displayed on the keypad (see Figure 5.3). When selecting the group from the list, the SCP menu is displayed (see Figure 5.4).

Quitting the 2nd access level occurs when the # button is pressed if it leads to the group arming or disarming, or when the ← button is pressed in the user main menu, or automatically after 10 seconds of user inactivity. It is accompanied by four short sound signals. All the indicators except "i" (if there is a fault or alarm not viewed by the user) on the keypad turn off, in case the "Permanent indication" option is disabled for the keypad.



If the "Quick Action" option is enabled for the user, the group status viewing is skipped, the group is armed/disarmed after one click on the # button.

5.2.5 Group arming/disarming using LED keypads

At the 1st access level, the keypad zone indicators display the current state of the system zones/groups specified in the keypad settings in case the "Permanent indication" option is enabled for the keypad. If the "Permanent indication" option is disabled for the keypad, the indicators of system state and zones/groups on the keypad at the 1st access level are switched off permanently.

To control the group using the LED keypad, enter the following combination:

access code # #



Using LED keypads, the user can control the groups added to their settings. If there are several groups for this user, the user will control the group selected in the "Access code main action" option, the first group in the list of groups added to the user or several groups if after authorization 0 and number of the group were entered. If it is required to control several groups separately by one user, you should create users in the system for each group.

After entering the valid access code and clicking on the # button, there will be four short sound signals (entering the 2nd access level). If the keypad **operates in the "Permanent indication" mode**, after entering the 2nd access level, the display mode of the zone/group indicators will not change, the indicators will display the status of zones/groups specified in the keypad settings (see Table 5.1). In case **the "Permanent indication" mode is disabled** in the keypad settings, after entering the 2nd access level, the zone/group indicators on the keypad will display the current state of the group zones (the indicator number corresponds to the zone number in the group). If the user has been assigned such zones as 24h, Panic button, Universal input, Tamper, Anti-masking, their status will also be displayed on the indicators of the keypad zones (after group zones).

▼ indicator at the 2nd access level displays the status of the controlled group:

- **lights green** (ARMED) – all zones of the group are armed. When the # button pressed again, the group will be disarmed;
- **no lights** (DISARMED) – if the ✓ indicator lights green, the group is ready for arming. When the # button pressed again, the group will be armed.

Exit from the 2nd access level occurs when the user presses the # button if it leads to the group arming or disarming or automatically after 10 seconds of inactivity. It is accompanied by four short sound signals. All indicators except "i" (if there is an unviewed fault or alarm by the user) on the keypad disappear, if the "Permanent Indication" is disabled for the keypad.



If the "Quick Action" option is enabled for the user, the group status viewing stage is skipped, the group is armed/disarmed after one click on the # button.

5.2.6 Group arming/disarming with single code using LED keypads

The users can control several groups with single code using LED keypads if the "Quick action" option is disabled. The users can control groups added to their settings. The groups are controlled by their system-wide numbers.

To arm/disarm the group, enter the following combination on the LED keypad:

user access code # 0 system-wide group number # #

After the user is authorized, the status of the first user-configured group is displayed on the status indicators of the zones/groups (if "Permanent indication" option is enabled). After

entering **0** and the system-wide group number, and pressing the **#** button, the zone/group status indicators will display the status of the selected group if the "Permanent indication" option on the keypad is disabled. Press the **#** button again to change the status of the group.



*After user authorization, entering **0** and system-wide group number and pressing the **#** button, the indication of the zone/group on the keypad is similar to the control of one group from the LED keypad (see 5.2.5).*

Press the **#** button again to change the status of the group.



*If "Permanent indication" option is enabled, the indication of zones/groups does not change after entering **0**, system-wide group number and pressing the **#** button.*

5.2.7 Group arming/disarming using Touch Memory (TM) / Card readers

The groups can be controlled with TM or card readers by attaching a key/card to a reader. In this case, the group is armed or disarmed, depending on its previous state.

If the reader is located in the area covered by the security detectors, then for the correct group arming, the zones with delay should be set in it, and the "Arming delay with reader" option must be enabled.



The group status can be displayed using outputs that operate in the "Confirm arming" or "By script" modes. The indication in the "Confirm arming" mode is described in Table C.1, [Appendix C](#).

5.2.8 Group arming/disarming using radio key fobs

The groups are controlled with key fobs by pressing the button on the key fob aimed to arm or disarm the zone of "Universal Input" type. By arming or disarming this zone, the script is run with the appropriate running method, which performs the control of the group on behalf of the user specified in the action settings.

The group status can be displayed using outputs that operate in the "Confirm arming" or "By script" modes. The indication in the "Confirm arming" mode is described in Table C.1, [Appendix C](#).

5.2.9 Group arming/disarming using X-KEY

The groups are controlled with key fobs by pressing the  button ("Tiras logo") to arm the group, the **X** button to disarm it, and the  button to arm the group in the "I'm at home" mode. The key fob has protection against false presses; to execute the command, press the button from 0.3 to 2 seconds and release, then the LED indicator on the added key fob flashes one of the following colors:

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

After successful transmission of the command, the LED indicator shortly flashes three times with a green indicator with an interval of 1 s, confirming the execution of the command and shortly flashes three times with a red indicator if the command execution is prohibited.

The indication of the command execution is not available for the "Panic button" and when repeating the previous command.







5.3 Prevention of the group arming



The SCP can prevent group arming unless the user has the appropriate privileges. Prevention of the group arming can be performed in the cases described in Table 5.4.

Table 5.4 – Possible cases of arming prevention

Reason for prevention	Method of elimination
A user does not have the privileges to arm the group	You must provide the user with the appropriate privileges for group arming
Penetration in the system device enclosure	For group arming, you must eliminate the existing interference
One intruded zone of the "Security" type is available in the group ¹	For group arming, you must provide the user with the "OVERRIDE ZONE" rights. Zone overriding can be performed only when arming the group using display keypads or Control NOVA II software
Several intruded zones of the "Security" type are available in the group ¹	In this case, group arming is impossible. You must restore intruded zones and repeat arming
Any fault in the system when the SCP is set to work according to Security Grade 2	If the SCP operates according to Security Grade 2, in case of faults, the group arming can only be performed by users with the "Override the faults" rights
Any fault in the system when the SCP is set to work according to Security Grade 3	For Security Grade 3, in case of faults in the system, the group arming is impossible.

5.4 Alarm and fault handling using keypads

The keypads allow users to view alarms and faults available in the system. When an alarm or fault is detected, the  indicator starts blinking on the keypads. After the user is authorized from the keypad, the  indicator starts blinking in case there is a fault in the system and the  indicator starts blinking in case of a user-related alarm. If the  indicator blinks at the 1st access level, but after the user's authorization, the  or  indicator does not blink or light up which means that the user does not have the rights to view the fault or alarm (for example, alarm in the zone that is absent in the groups or 24h zones 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 SCP enclosure or an alarm in the armed zone). After handling all the alarms, the  indicator turns off.

After viewing all the system faults, the  indicator lights up. When all faults are handled, the  indicator turns off.



When controlling the group status (arming, disarming, and partial arming) by 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.

5.4.1 Alarm handling using display keypads

To handle alarms by display keypads, the user must be authorized (enter the access code and press the # button). After authorization, the user should enter the main user menu (see Figure 5.5).

¹ It is impossible to bypass an unassembled zone of the "Front door" type.

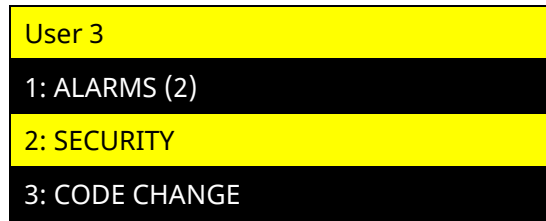


Figure 5.5 – User main menu

If user-related alarms are available in the system, the "Alarms" menu will appear in the main menu with the number of alarms in brackets. After selecting this section, the keypad display will show the list of alarms (zone alarms, penetration in the enclosure of the system devices). The alarm list can be navigated with the help of the ▲ and ▼ buttons. After viewing the list of all alarms and returning to the main menu, the "Alarms" section disappears (if active alarms are absent) or continue to be displayed (if active alarms still remain (after handling active alarms, the "Alarms" menu automatically disappears and the 🚨 indicator turns off)). The user can also view alarms after disarming the group by clicking the # button (see Figure 5.6).

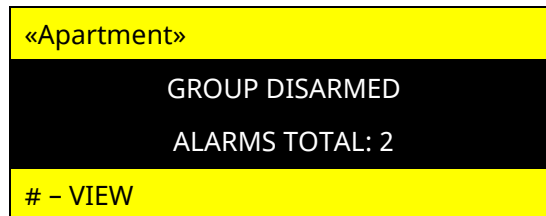


Figure 5.6 – Viewing alarms

5.4.2 Fault handling using display keypads

To handle the faults using display keypads, a user should authorize (enter the access code and press the # button). After authorization, go to the main user menu (see Figure 5.7).

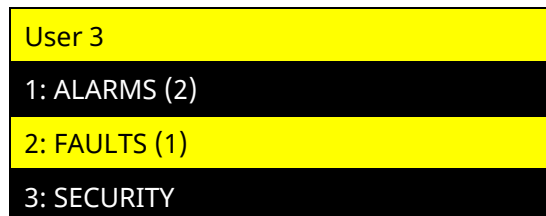




Figure 5.7 – User main menu


In case of faults, the "Faults" section is displayed in the user main menu with the number of faults in brackets. After selecting this section, the list of faults is displayed on the keypad display (the list of possible faults is shown in Table 5.5). The user can view the list of faults using the ▲ and ▼ buttons. After viewing the list of all active faults, the 🛠 indicator lights up. After handling all the faults, the "Faults" menu automatically disappears, and the 🛠 indicator turns off.

5.4.3 Alarm handling using LED keypads

To handle alarms with the LED keypad, the user must be authorized (enter the access code and then press the # button). If active user-related alarms are available in the system, the 🚨 indicator will blink red once. If the memory of alarms is set, the 🚨 indicator blinks red twice. In case of alarm in the zone, the indicator of the appropriate zone in alarm blinks together with the 🚨 indicator. In case of the "Penetration" 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 turns off if there are no active alarms in the system or flashes if active alarms still remain (after active alarms are handled, the  indicator turns off automatically). All the alarms are automatically cleared after disarming the group.

5.4.4 Fault handling using LED keypads

In case of any fault in the system, the  indicator blinks once after user authorization. To enter the handling mode, enter the following combination on the keypad:

access code # 3 #

(the  indicator starts blinking 4 times per second)

In the faults viewing mode, the next fault is displayed by pressing the # button. When viewing the faults, the zone indicators on the keypad display one of the current faults (see Table 5.5). After viewing the last fault, the system turns to the first fault. When all faults are viewed, the "" indicator starts to light continuously (if uneliminated faults are available) or turns off (if all faults are eliminated). To exit the Fault viewing mode, press the * key.

If a user tries to enter the Fault handling mode when faults are absent, buzzer will generate a long beep; entering the Fault handling mode is forbidden.

Table 5.5 – Faults that can be analyzed in the system

Fault name	Reasons for formation	Zone indicators state			
		● - lights ○ - no lights			
		1	2	3	4
No 230 V	Formed by the SCP in the case when the main power supply of 230 V is lost (within 10 minutes).	●	○	○	○
Battery discharged	Formed by SCP when the battery voltage decreases below 11.5 +/-0.2 V.	○	●	○	○
No battery	Formed by SCP in case of no voltage on the battery terminals.	●	●	○	○
Siren fault	Formed by SCP in case of siren loop fault.	○	○	●	○
Output fault	Formed by SCP at short circuit of + 12V outputs.	●	○	●	○
No connection with CMS	Formed by SCP in case of communication with CMS fault on all of the configured communication channels.	○	●	●	○
No 230 V of expansion devices	Formed by the expansion module when 230 V power supply is lost (within 10 minutes).	●	●	●	○
Expansion device battery is discharged	Formed by the expansion module when the voltage at the battery terminals of the expansion module below 11 +/-0.2 V.	○	○	○	●
No battery in the expansion device	Formed when the battery of the expansion module faults.	●	○	○	●
Low keypad power	Formed by keypad at decreasing it power supply voltage to 9 V.	○	●	○	●
Low expansion module power	Formed by expansion modules at decreasing it power supply voltage to 9 V.	●	●	○	●
Fault of expansion module siren	Formed by SCP at open circuit of the expansion module siren.	○	○	●	●
Fault of expansion device output	Formed at a short circuit of outputs + 12V of the expansion module.	●	○	●	●
No connection with keypad	Formed by the SCP when the connection with keypad is lost.	○	●	●	●

No connection with expansion module	Formed by SCP when the connection with expansion module is lost.	•	•	•	•
No connection with wireless detector	Formed by the SCP in case of no connection with the wireless detector.	Not shown on LED keypads			
Wireless device battery is discharged	Formed by a wireless device if its battery is discharged.				
Fault in the zone of "Universal input» type in the «Fault» mode	Formed in the case of intruded zones such as "Universal Input" in the "Faults" mode.				

5.5 Control of automatics

The user can control different devices (heating, lighting, water supply, etc.) connected to the outputs of the system devices.

Control of the outputs can be carried out in two ways:

1. At the 1st access level:
 - functional buttons (change of output states, script start/stop);
2. At the 2nd access level:
 - by the user (change of the output state to the opposite one);
 - using a script (due to the conditions set in the script).

5.5.1 Output control and script running using functional buttons of display keypads



Any user who is not registered in the system and has physical access to the keypad can change the outputs state and start or stop scripts using the F1, F2, F3 functional buttons.

To control an output or script, simply press the functional button to which the output or script is assigned and follow the instructions on the keypad display.

You can assign an output or script to one of the functional buttons using the oLoader II software:

- To assign an output, you need to set its operating mode to "Controlled by user", then select the desired keypad in the "Devices → Keypads" section and assign the output to one of the functional buttons in the "Functional buttons" tab. When assigning the output, select the action that will occur when the functional button is pressed. The following options are available for selection: "Turn on output"; "Turn off output"; "Toggle output".
- To assign a script, the method of manual script run should be set as "Unauthorized user", then it is necessary to select the desired keypad in the "Devices → Keypads" section and assign the script to one of the functional buttons in the "Functional buttons" tab. When assigning the script, select the action that will occur when the functional button is pressed. The following options are available for selection: "Show list of scripts"; "Start script"; "Stop script".

5.5.2 Output control and script running using display keypads

If the user has one or more outputs to control and/or one or more scripts to run, the main menu contains the "AUTOMATICS" item (see Figure 5.8).

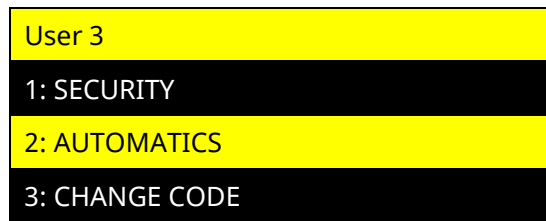


Figure 5.8 – User main menu

This section shows the list of outputs and scripts available to the user to control/run (see Figure 5.9).

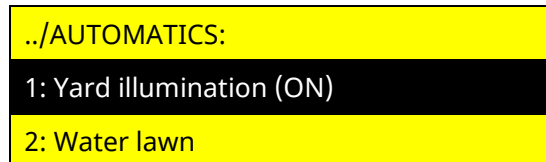


Figure 5.9 – "Automatics" section of the main menu

The current state (ON/OFF) of each output is indicated near its name. When the ● button is pressed, the state of the selected output changes to the opposite.

By clicking on the ● button in the script, user can open a dialog box and run it (see Figure 5.10). To run the script, click on the # button.

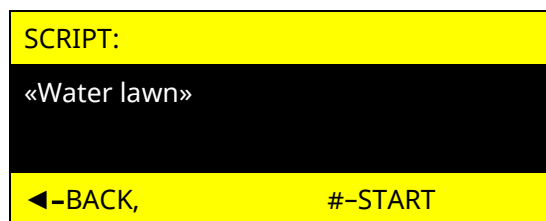


Figure 5.10 – A dialog box for script running

5.5.3 Output control and script running using functional buttons of LED keypads



Any user who is not registered in the system and has physical access to the keypad can change the outputs state and start or stop scripts using the F1, F2, F3 functional buttons.

To control the output or script, simply press the functional button to which the output or script is assigned.

For assigning the output or script to the functional buttons using the oLoader II software, see section 5.5.1. Please note that the "Show list of scripts" option is not available for LED keypads.

5.5.4 Output control using LED keypads

Using the LED keypad, the user can control the status of one output that is added to the settings. For this purpose, control of output must be configured as "Access code main action".

To control the output, enter the **access code # #** on the keypad, the output state will change to the opposite (ON/OFF).



If the "Quick Action" option is enabled for the user, the output state can be controlled by a single # button press.

5.5.5 Script running using LED keypads

Using the LED keypad, the user can run one script that is added to the settings. For this purpose, the script must be configured as "Access code main action".

To run the script, enter the following combination on the keypad:

access code ##



If the "Quick Action" option is enabled for the user, the script runs by single press of the # button.

5.5.6 Output control using readers

Using the reader, the user can control the status of one output added to its settings. For this purpose, the output control must be configured as "Access code main action".

The output control is carried out by attaching the key/card to the reader, the output state will change to the opposite one (ON/OFF).

5.5.7 Script running using readers

Using the reader, the user can run a single script added to its settings. For this purpose, the script must be configured as "Access code main action". To run the script, attach the key/card to the key/card reader.

5.6 Remote control and monitoring

Control NOVA II software for Android or iOS mobile devices is intended for remote control and monitoring of the object status. The connection of the software to the SCP is carried out via the Tiras CLOUD II service.

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



The use of Tiras CLOUD II services (remote control, SCP firmware update, etc.) increases the amount of Internet traffic used by the SCP. We strongly recommend using a cell 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 Tiras CLOUD II services).

The Control NOVA II software allows to perform the following:

- control the group status (arming/disarming).
- notify about alarms, faults, etc.;
- monitor the system status in real-time mode;
- control the outputs state;
- script run;
- view the event log;
- administrators and installers can invite other users to control the system;
- view videos from the added video monitoring cameras at the premises;
- change user access code.

5.6.1 Control NOVA II installation, first run, and update

The Control NOVA II software can be installed from the store (Google Play for Android, App Store for iOS). For the correct operation of this software, it is necessary to provide all permissions it requires during installation or during the operation. To run Control NOVA II software, select the appropriate icon in the main menu of the mobile device. The language of the software (Ukrainian, Russian, or English) is automatically set according to the language settings of the mobile device. If the Google Play or App Store settings do not have permission to automatic updates, you will receive the corresponding notification about the available

updates (after the release of the new software version).

5.6.2 Account registration

To register the account, do the following:

- open the software and click on "Register";
- add a user photo from camera or gallery (optional);
- enter a username in the "Name" field (at least 1 character);
- enter a valid user e-mail in the "E-mail" field;
- enter a valid user phone number in the format +380XXXXXXXXXX in the "Phone number" field;
- enter the password in the "Password" field (minimum 6 characters);
- enter the same password as in the previous step in the "Password (again)" field;
- agree to the terms and conditions;
- click on "Register".

After clicking on "Register", a dialogue box for confirmation code from an SMS message is displayed (if the dialogue box is not displayed, the activation is executed immediately). Control NOVA II software reads the code from the SMS message automatically and goes to the next step. In some cases, when the SMS message code does not appear in the field automatically, you should enter it manually.



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

After successful SMS verification of the phone number, the confirmation of the account registration in the Control NOVA II software is sent to your email. To confirm the account registration, open the email on the mobile device specified during registration. You should open the email and follow the link that will confirm the registration and open the software.

5.6.3 Authorization

After completing registration, log in to your account:

- enter the email specified during registration;
- enter the password specified during registration;
- click on the "Login" button.

5.6.4 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 can invite other users.

Before adding the SCP to the account, it is necessary to enable registration mode (lasts 10 minutes). After enabling registration mode, do the following:

- In the "Objects" dialogue box, click on 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 administrator or installer access code.
- In the "Object name" field, enter the name of the object (from 1 to 50 characters).
- If the mobile device has a fingerprint scanner, you may optionally enable the "Use of fingerprint scanner" option. Note that when entering the object for the first time, the user should enter the access code for Control NOVA II software to remember and associate it with the fingerprint.

- Select the user type (administrator or installer) that adds the object to the account (the user access code must match the chosen type).
- Add a photo of the object from a camera or a gallery (optional).
- Click on the "Add" button.



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

If the data has been filled correctly, after clicking on the "Add" button, the SCP will be added to the "Objects" window.

5.6.5 Adding SCP to user accounts

After adding the SCP to the account, the administrator can view the list of system users and their data in the "Settings/Users" item. The user data is obtained from the device settings and displayed for viewing only. In this item, the user can link the user account to the Control NOVA II software with the user of the SCP. For this purpose, do the following:

- select the required system user (the user must have full or remote access);
- click on the button of an envelope shape;
- enter user e-mail and click "OK".

If the user has entered the e-mail that is not registered in the Control NOVA II software, he or she will be emailed the invitation letter with the offer to register in the Control NOVA II software. After account registration and user authorization, the SCP will be added to the list of its objects automatically.

If the user has entered the e-mail that is registered in the Control NOVA II software, the SCP will be added to the list of objects of the given user automatically.



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

5.6.6 Push notifications

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

Alarms – sent when alarms (interference, intrusion, etc.) are generated in the system, which the user has the rights to view;

Faults – sent when faults are detected in the system (no 230 V, battery discharged, etc.);

Arm/Disarm – sent when controlling the status of the groups added to the user;

Automation – sent when controlling the state of automation (script run, outputs control) added to the user;

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

Push notifications about alarms have a specific sound signal. All the push notifications received by the software are stored in the notification center. By clicking on the notification, the Control NOVA II software launches.



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

Some problems with receiving push notifications may appear in the following cases:

- 1) Energy-saving mode is enabled (for example, Stamina on Sony devices).
- 2) The user does not have any activated Google account on the device.
- 3) The 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" section in the device settings).
- 5) The background running of the Control NOVA II software is restricted.
- 6) The device is not connected to the Internet.
- 7) Authorization is not performed in the object at the first launch of the Control NOVA II software.
- 8) When closing the Control NOVA II software, the account was logged out.



The notification sounds (including alarms) from the Control NOVA II software can be interrupted by notifications from other applications on the mobile device (calls, SMS, etc.).

5.6.7 Adding IP cameras to the Control NOVA II software

The Control NOVA II software gives an opportunity to connect IP cameras (regardless of the manufacturer) supporting the RTSP protocol. The administrator or installer with administrator rights can do that.




RTSP (real-time streaming protocol) is the protocol used for viewing video streams from IP-cameras remotely.

Before adding the 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 the camera or on the manufacturer's website);
- contact your Internet provider and find out whether it provides an external static IP address;
- configure the network equipment (port forwarding, IP address for the camera);
- configure the camera (using the manufacturer's guide);
- create an RTSP link to the video stream (usually the RTSP link format is specified in the manufacturer's documents or the camera's web interface);
- add the camera to the Control NOVA II software.

Adding the camera to the Control NOVA II software is completed by entering the RTSP link to the video stream in the object settings.

To add the camera, do the following:

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

- go to the "Settings" section and select "Users";
- select the user to whom the access to the camera should be granted and select "Video monitoring" in its settings;
- select cameras that the user can view (after selecting the camera, the user will see the "Video monitoring" tab in the "Control" section).

5.7 Assign/Change of access IDs

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



Users with enabled "Quick Action" option cannot change their own access IDs using keypads.

5.7.1 Change of access ID using display keypads

To change **access code**, it is necessary to:

- 1) enter the access code on the keypad and press the # button;
- 2) go to the user main menu (see Figure 5.11);

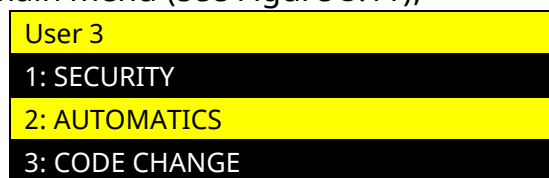


Figure 5.11 – User main menu

- 3) select the "CODE CHANGE" menu item using the ▼ and ▲ buttons;
- 4) select the "ACCESS CODE" item;
- 5) enter a new access code and press the # button;
- 6) repeat the new access code and press the # button.

To change **one's own key/card**, it is necessary to:

- 1) enter the valid access code on the keypad;
- 2) select the "CODE CHANGE" section in the main menu;
- 3) select the "KEYFOB/CARD" item;
- 4) attach the key/card to the reader;
- 5) re-attach the key/card to the reader.

To change/assign the **attack code**, it is necessary to:

- 1) enter the valid access code on the keypad;
- 2) select the "CODE CHANGE" section in the main menu;
- 3) select the "HOLD-UP CODE" item;
- 4) enter a new attack code and press the # button;
- 5) repeat the new attack code and press the # button.

5.7.2 Change of the access IDs using LED keypads

To change the **access code**, it is necessary to:

- 1) enter the valid access code # 1 # (the ✓ indicator starts blinking 1 time per second);
- 2) enter a new access code # (the ✓ indicator starts blinking 2 times per second);
- 3) enter the new access code again.

To change/assign a **key/card**, it is necessary to:

- 1) enter a valid access code # 15 # (the ✓ indicator starts blinking 1 time per

- second);
- 2) attach the key/card to the reader # (the ✓ indicator starts blinking 2 times per second);
 - 3) re-attach the key/card to the reader.

To change/assign the **attack code**, it is necessary to:

- 1) enter the valid access code # 2 # (the ✓ indicator starts blinking 1 time per second);
- 2) enter a new attack code # (the ✓ indicator starts blinking 2 times per second);
- 3) repeat the new attack code.

Successful change of the access ID is confirmed by four short sound signals of the keypad buzzer. In case the change of access and attack codes using LED keypads fails (the entered and re-entered combinations do not match, or the entered code is already used), you will hear one long sound signal.



After the administrator or installer authorization using the default access code on the keypad, the latter will immediately switch to the access code changing mode. To change the access code, enter a new access code (4 digits) and then press the # button, repeat the entered code, and press the # button again.

5.7.3 Change of the access code with the Control NOVA II software

To change one's own access code, do the following:

- enter the object;
- click the ☰ icon in the upper left corner;
- go to the "Settings" section;
- select "Access code";
- click on the "Change access code" item (the virtual keypad will appear);
- enter the valid access code and press the # button (confirm);
- enter a new access code and press the # button (confirm);
- repeat the new access code and press the # button (confirm).

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

6. ADMINISTRATOR OPERATIONS WITH KEYPADS

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

Using the display keypads, the administrator can do the following:

- arm/disarm groups;
- view the system status;
- control the outputs status and run scripts;
- view the SGM scripts;
- view and export the event log;
- check the balance of the active SIM-card in autonomous mode;
- enable the SCP registration mode in Control NOVA II software;
- delete the SCP data on the Tiras CLOUD II service;
- create users and change their settings;
- create scripts and change their settings;
- change the system menu language;
- enable or disable the installer access;
- enable or disable keypad option setting.

Using the LED keypads, the administrator can do the following:

- arm/disarm groups;
- view the system status;
- control the outputs state and run scripts;
- change one's own access IDs;
- export event log;
- enable the SCP registration mode in Control NOVA II software;
- delete the SCP data on the Tiras CLOUD II service;
- enable or disable the installer access.

6.1 Administrator operation with display keypads

After the administrator authorization using the display keypad, the main menu with sections is displayed (see Table 6.1).

Table 6.1 – Administrator main menu

No	Main menu section	Purpose
1	ALARMS ¹	List of alarms (zone alarms and penetrations) fixed since the previous viewing of this section
2	FAULTS ¹	List of faults fixed since the previous viewing of this section
3	SECURITY ²	List of groups available for control
4	AUTOMATICS ²	List of available options for outputs and scripts control
5	SGM ²	List of available SGM scripts

¹ Tabs are available in the main menu if there are active or unviewed alarms or faults in the system.

² The items are displayed according to the user rights and SCP operation mode.

6	CODE CHANGE	This option allows the administrator to change one's own access IDs
7	SETTINGS	This option allows to change the settings of users, scripts, system menu language, installer access, keypads
8	EVENT LOG	This option allows to view events occurring in the chronological sequence (alarms, faults, arming, disarming, etc.)
9	EXPORT EVENT LOG	This option allows to create events log file in txt-format on USB flash drive of the SCP
10	CHECK BALANCE ¹	This option allows to check the balance of the configured SIM-cards
11	ACTIONS WITH Tiras CLOUD	This option allows to enable the registration mode to add the SCP to Control Nova II user accounts, as well as to clear the SCP data on the Tiras CLOUD II server
12	ABOUT DEVICE	Displays the current firmware version of the SCP and its serial number

6.2 "Settings" section

Using the display keypads, the administrator can access the "Settings" section of the main menu (Table 6.2). When selecting this section, the menu with the following items is displayed.

Table 6.2 – Settings section of the main menu

No	Menu item	Purpose
1	USERS	List of users available in the system. This option allows to create new users and delete existing ones, as well as to configure their rights and settings
2	LANGUAGE MENU	This option allows the administrator to change the system menu and SMS message language
3	INSTALLER ACCESS	The administrator grants (or denies) the permission to enter the 3 rd access level – the access for users of the installer type.
4	KEYPAD'S OPTIONS	This option allows to configure additional keypad settings, such as "Doorbell", "Brightness", "Night light" and "Presence".

6.2.1 User settings

By selecting the "**USERS**" item, the administrator opens the menu, which displays the list of users of the system and the "NEW USER" item. When creating a new user or choosing an existing one, the user opens the user's menu, which contains items as shown in Table 6.3.

Table 6.3 – User settings menu

No	Menu item	Purpose
1	NAME	This option allows to edit the username
2	USER TYPE	This option allows to select the user type
3	ACCESS TYPE	This option allows to select the user access type
4	AUTHORITY	This option allows to select user rights
5	CODES	This option allows to change access IDs
6	GROUPS	This option allows to choose to which groups this user will be able to apply his/her rights
7	24 HOUR ZONES	This option allows to choose 24h zones about which the user will receive notifications and view their status
8	SCRIPTS	List of scripts configured to be run from the 1 st and 2 nd access levels, to allow a user to run them

¹ The items are displayed according to the user rights and SCP operation mode.

9	OUTPUTS	List of outputs configured as "Controlled by user" to be run by user
10	PHONE NUMBER	This option allows to specify or change the user phone number
11	SMS	This option allows to select events for user SMS notification
12	MAIN ACTION	This option allows to choose the main control element for the user when authorizing with the access code or key/card
13	QUICK ACTION	This option allows to enable or disable quick action (arming without reviewing system status)
14	CHECK CALL ¹	This option allows to enable or disable the check call option for an individual user
15	ACCESS RESTRICTION	This option allows to specify the keypad forbidden for user authorization
16	KEY FOB	This option allows to select one of the key fobs and define a group to control it
17	DELETE	This option allows the administrator to delete the user

By selecting the "**NAME**" item, the Username editing dialog box is displayed (see Figure 6.1).



Figure 6.1 – Username editing dialog box

The cursor highlights an editable character. The cursor position changes by pressing the ◀ and ▶, or #, * buttons. To input characters the "0..9" buttons located on the keypad touchpad are used (the list of characters available upon button pressing is displayed on the keypad display). To delete selected character, press the F2 button. To get a hint, press the F1 button. To save the entered name, press the F3 button.

By selecting the "**USER TYPE**" item, the list of possible user types is displayed (Table 6.4). The selected user type is indicated by the "[+]" symbol.

Table 6.4 – Types of users

No	Menu item	Purpose
1	INSTALLER WITH ADMINISTRATOR RIGHTS	The installer with Administrator rights can change the SCP settings using the keypad or oLoader II software (if allowed by the administrator), as well as control system elements (arm/disarm groups, control outputs, run scripts) and change the specified SCP settings using keypads.
2	ADMINISTRATOR	This option allows to control system elements (arm/disarm groups, control outputs, run scripts) and change the specified SCP settings using keypads.
3	INSTALLER	This option allows to control system elements (arm/disarm groups, control outputs, run scripts). The installer can change the settings of the SCP using keypads or oLoader II software (if allowed by the administrator).
4	USER	This option allows to control system elements: arm/disarm groups, control outputs, run scripts.

By selecting the "**ACCESS TYPE**" item, the list of the possible types of user access is displayed (see Table 6.5). The selected user access type is indicated by the "[+]" symbol.

¹ The item is available only if the control panel is operating in autonomous mode.

Table 6.5 – Types of user access

No	Menu item	Purpose
1	LOCAL	This option allows the user to control the system using keypads, readers and key fobs, but forbids control from the Control NOVA II software
2	REMOTE	This option allows the user to control the system using the Control NOVA II software, but forbids control using keypads, readers and key fobs
3	FULL	This option allows the user to control the system using keypads, readers, and key fobs, as well as the Control NOVA II software

By selecting the "**AUTHORITY**" item, the list of user rights is displayed. Each right is marked with the "[+]" or "[]" symbol indicating whether this privilege is included for the user or not respectively. Table 6.6 lists the rights that can be assigned to users.

Table 6.6 – User rights

No	Menu item	Purpose
1	SETTING	This option allows to arm groups
2	UNSETTING ¹	This option allows to disarm groups
3	FAULTS OVERRIDING	This option allows to arm groups in case of faults in the system
4	ZONES INHIBITING ²	This option allows to arm the group in case of one intruded zone in the group

By selecting the "**CODES**" item, the administrator can change access IDs for the selected user, following the displayed hints.

By selecting the "**GROUP**" item, the list of groups configured in the system is displayed (see Figure 6.2).

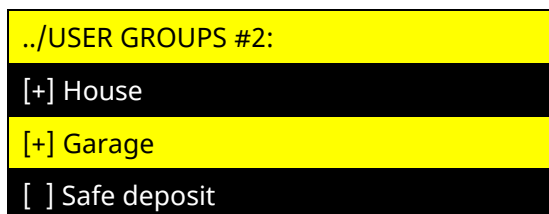


Figure 6.2 – A dialog box for user group selection

The symbol "[+]" or "[]" near each group means the permission or prohibition to control this group by selected user respectively.

By selecting the "**24 HOUR ZONES**" item, the list of the following zone types is displayed: 24h, Panic button, Universal input, Tamper, Anti-masking configured in the system (see Figure 6.3).

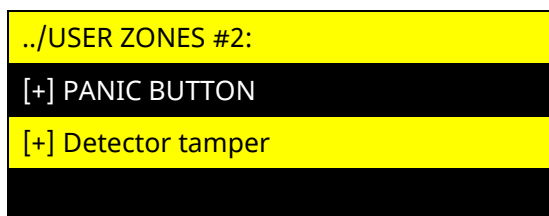


Figure 6.3 – A dialog box for user zone selection

The symbol "[+]" indicates the zones from which the user receives alarms and can view their status.

By selecting the "**SCRIPTS**" item, the list of scripts with the following run methods is displayed: "By user of the 1st access level" and "By user of the 2nd access level" configured in

¹ When selecting DISARMING, the ARMING rights will be activated automatically.

² A group with the unassembled zone type "Front Door" cannot be armed.

the system (see Figure 6.4).

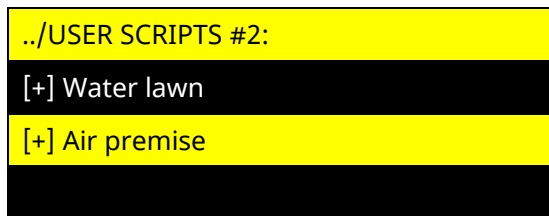


Figure 6.4 – A dialog box for user scripts selection

The [+] symbol marks the scripts that can be run by the user.

By selecting the "**OUTPUTS**" item, the list of outputs with the "Controlled by user" mode is displayed (see Figure 6.5).

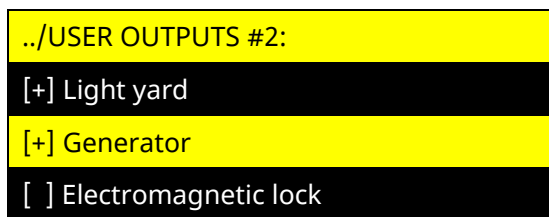


Figure 6.5 – A dialog box for user outputs selection

The "[+]" symbol indicates the outputs that can be controlled by the user.

By selecting the "**PHONE NUMBER**" item, the dialog box for editing a user phone number is displayed (see Figure 6.6).

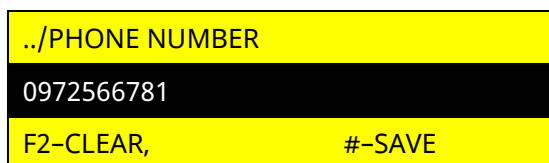


Figure 6.6 – A dialog box for editing a user phone number

A phone number may be in the format "+ 380XXXXXXXXX" or "0XXXXXXXXX". Characters are entered using the "0" to "9" buttons. To erase the whole row, click on the F2 button. To save the entered number, click on the # button.

By selecting "**SMS**", the list of events that can be sent in SMS messages is displayed (see Table 6.7). The "[+]" or "[]" symbol near each event type indicates the permission or prohibition for sending SMS messages for this event type respectively. SMS messages about groups and alarms arming/disarming are sent if they occur in the groups added to the user. The list of SMS messages that can be sent to users is shown in Table D.5, [Appendix D](#).

Table 6.7 – SMS notification

No	Menu item	Purpose
1	ALARMS	User SMS notification about intrusions in zones
2	GROUP SETTING/UNSETTING	User SMS notification about arming/disarming of the groups assigned to user
3	SYSTEM EVENTS	User SMS notification about faults or penetration in the device case (for Administrator only)
4	OUTPUTS CONTROL	User SMS notification about activation/deactivation of outputs assigned to user

By selecting the "**MAIN ACTION**", the "ACCESS CODE" and "KEY/CARD" options become available for selection. For each of these access IDs, the administrator can select one controlled item available for the user: group, output or script (see Figure 6.7). When authorizing with the appropriate ID using the keypad or reader, the item selected in this

setting will be immediately available for control.

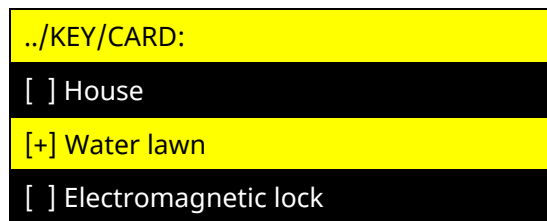


Figure 6.7 – A dialog box for user main action settings

The "**QUICK ACTION**" option allows to control the group and outputs or run the script by skipping the stage of system status viewing, i.e. the action is performed after entering the access code and one # button pressing. The option is **not configurable** for the users of installer and administrator type. When clicking on the ● button on "QUICK ACTION" item, the option is enabled or disabled, depending on the previous state (ENABLE/DISABLE).

When the ● button is pressed on the "**CHECK CALL**" item, the option is enabled or disabled, depending on the previous state (ENABLE/DISABLE).



During the check call, it is difficult to work with the Control NOVA II software (monitoring and control). We do not recommend enabling "Check call" option for more than 5 users.

By selecting the "**ACCESS RESTRICTION**" item, the list of available keypads is displayed (see Figure 6.8).

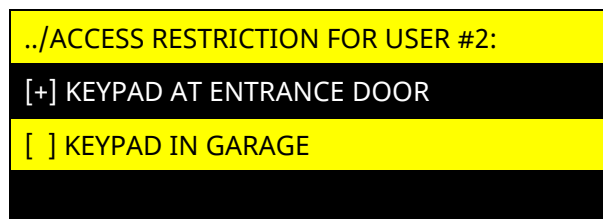


Figure 6.8 – A dialog box for keypad selection for access restriction

The "[+]" symbol marks the keypads by means of which the user authorization will be forbidden. If no keypad is marked with this symbol, the user can operate with any keypad in the system.

In the "**KEY FOB**" item, the user can select one key fob from the list of assigned X-Key key fobs not added to any user. Also, the user can select one group, which will be controlled by this key fob.

By selecting the "**DELETE**" item, the system will require the confirmation of the user deletion by pressing the # button.



The single Administrator and (or) Installer user cannot be deleted.

6.2.2 Menu language

By selecting "**LANGUAGE MENU**" item, the following dialog box is displayed (see Figure 6.9) allowing to configure the menu language of the display keypads and the language of SMS messages sent to user phone numbers. The following options are available for selection: "УКРАЇНСЬКА", "РУССКИЙ", and "ENGLISH". To change the language, select the values with the ▲ and ▼ buttons and press the ● button.

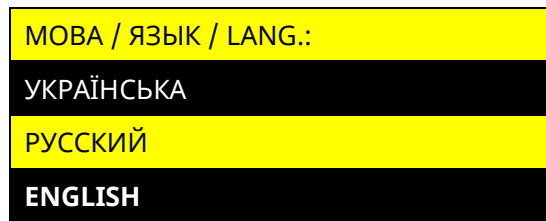


Figure 6.9 – A dialog box for language menu selection

6.2.3 Installer access

The administrator can restrict the installer's access to the system. If the installer access is denied (the option is disabled), no user of the Installer type will be able to log in from the keypad or change the SCP settings using the oLoader II software (locally and remotely). Also, the user will not be allowed to update the SCP software with the CMS.



To gain the Installer privileges to change the settings of the SCP using the oLoader II software and ability to authorize in the system from the keypads, the "Installer access" option should be enabled.

Setting the installer access from display keypads

By selecting "INSTALLER ACCESS", in the "SETTINGS" section of the main menu, the current value of the parameter is displayed (see Figure 6.10). Press the # button to enable or disable the setting.



Figure 6.10 – Installer Access option

Setting the installer access from LED keypads

To view the current status of the parameter, enter the following combination on the keypad:

administrator access code # 8 #

(the indicator ✓ starts blinking 1 time per second).

Zone 1 indicator displays the status of the option:

- lights green – installer access is enabled;
- lights red – installer access is disabled.

Changing the parameter value can be done by pressing the # button (each press changes the state). To exit the parameter setting mode, press the * button.

6.2.4 Keypad options

This settings item displays the list of keypads added to the system. After selecting the required keypad, the display will show the options available for setting (see Figure 6.11). If there is only one keypad in the system, you will immediately enter the settings of its options.

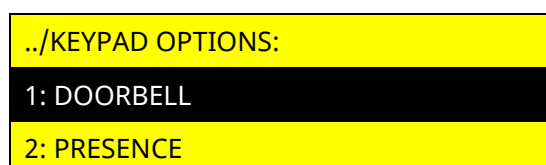


Figure 6.11 – Keypad options dialog box

The "DOORBELL" option allows to turn on the built-in keypad buzzer (4 short sound signals) in case of the intrusion of the zones specified in its settings.

To enable the option, click the ● button on the "ENABLE" item. After enabling, the administrator can select zones (the list of the available zones in the system is displayed: "Entrance door", "Corridor", and "Security"). The "[+]" or "[]" symbol near each zone indicates whether the option is enabled or disabled for this zone respectively.

To disable this option, place the cursor on the "DISABLE" item and press the ● button.

The "PRESENCE" option allows to turn on (for one minute) the display and illumination of the keypad key field, if the zone specified in this option is intruded.

To enable this option, click on the ● button in the "ENABLE" item. After enabling, administrator can select zones (the list of the available zones in the system is displayed: "Entrance door", "Corridor", and "Security"). The "[+]" or "[]" symbol near each zone indicates whether the option is enabled or disabled for this zone respectively.

To disable the "PRESENCE" option, place the cursor on the "DISABLE" item and press the ● button.

6.3 Event Log

By selecting the "EVENT LOG" item in the main administrator menu, the administrator can view the list of the events that have occurred in the system. The events are arranged in chronological order (the latest events are at the top of the list). The user can navigate the event log with the ▲ and ▼ buttons. For a detailed view of the selected event, click the ● button.

The list of events that will be recorded in the event log in case of their occurrence and a brief description of the reasons for their generation are given in Table D.7, [Appendix D](#)



The event log can store up to 1000 events. After exceeding this number, the oldest events are replaced by new ones.

6.4 Event log export

The administrator can export the event log to a txt-file on the USB flash drive of the SCP. The user can copy or view it by connecting the SCP to the PC. After exporting the event log, the "EXP_LOG.TXT" file will be created on the USB flash drive of the SCP, containing the information about the date and time of export, model, firmware version, serial number of the SCP, the list of the events recorded in the SCP.

6.4.1 Event log export by display keypads

To export the event log, select the "EXPORT EVENT LOG" section in the administrator's main menu. To start the export process, press the # button (see Figure 6.12). When the event log is exported, the "LOG EXPORTED" message will be displayed on the keypad display.

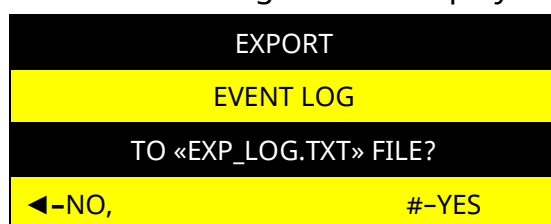


Figure 6.12 – Event log export

6.4.2 Log export with LED keypads

To export the event log, enter the following combination on keypad:

administrator access code # 9 #

6.5 Balance checking

After choosing the "**CHECK BALANCE**" item in the main administrator menu, the system offers to select the SIM card for the account checking (see Figure 6.13). If SIM card is used, the balance checking dialog box is displayed immediately (see Figure 6.14).

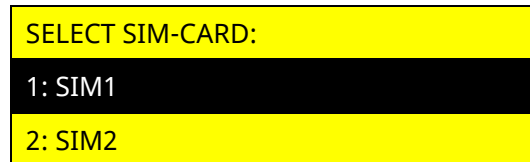


Figure 6.13 – Select the SIM card to check a balance

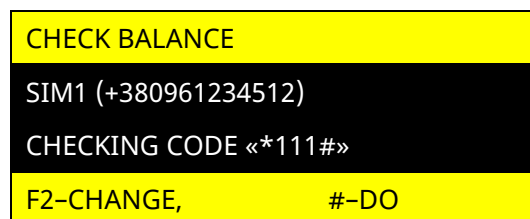


Figure 6.14 – Balance checking dialog box

The dialog box displays the number of the SIM card installed in the SCP and the USSD code for checking the balance. This code can be changed. To execute the USSD request, click on the # button. To change the USSD code, press the F2 button, enter a new USSD code, and press the F3 button to save it.



Balance checking is available only with the autonomous operating mode of the SCP.

6.6 SCP registration mode

Enabling the registration mode is required to add the SCP to the Tiras CLOUD account using Control NOVA II or oLoader II software.

After enabling the registration mode (and after turning on the SCP), within 10 minutes users of the Administrator and Installer types can add the SCPs to their accounts (if the data in the Control NOVA II software has been entered correctly).

To enhance the system security, the users are prohibited from adding the SCP to the Tiras CLOUD accounts using Control NOVA II or oLoader II software if the SCP registration mode has not been enabled by the system administrator, or if more than 10 minutes have passed since the registration mode enabling (or the SCP start).



When adding the object, any fault (invalid access code, incorrectly specified user type, no rights for remote control, etc.) resets the 10-minute permission, so it is necessary to re-enable the registration mode of the SCP. Also, in case of enabling the registration mode by restarting the SCP, the user should wait at least for a minute after turning on the SCP before adding the object to the account.

6.6.1 Enabling the registration mode from display keypads

To enable the registration mode, select the "**ACTIONS with Tiras CLOUD**" section in the administrator's main menu and select the "**REGISTRATION MODE**" item. The administrator

will be prompted to enable the SCP registration mode by clicking the # button (see Figure 6.15).

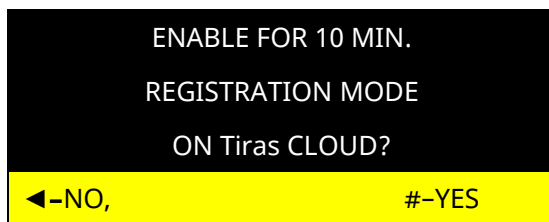


Figure 6.15 – Enabling the SCP registration mode

6.6.2 Enabling the registration mode from LED keypads

To enable the registration mode, enter the following combination on the keypad:

administrator access code # 7 #

6.7 Deleting the SCP data from the Tiras CLOUD II server

The administrator can delete the SCP data stored in the Tiras CLOUD II service (the SCP serial number, event log, etc.). If this SCP is in the accounts of the Control NOVA II users, it will be also deleted.

6.7.1 Deleting the SCP data from display keypads

To delete the data, select the "**ACTIONS with Tiras CLOUD**" section in the administrator's main menu and select the "**DELETE DATA**" item. The display shows the warning in Figure 6.16. Press the **F3** button to delete the data.



Figure 6.16 – Deleting control data on Tiras CLOUD

6.7.2 Deleting the SCP data from LED keypads

To delete data, enter the following combination on keypad:

administrator access code # 6 # administrator access code #

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

6.8 About device

In the "ABOUT DEVICE" section (see Figure 6.17), the administrator can view the current version of the SCP firmware and its serial number.

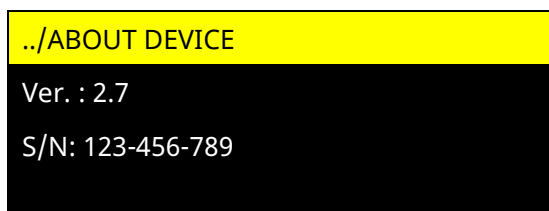


Figure 6.17 – "About Device" menu

APPENDIX A

Orion NOVA L (LTE)

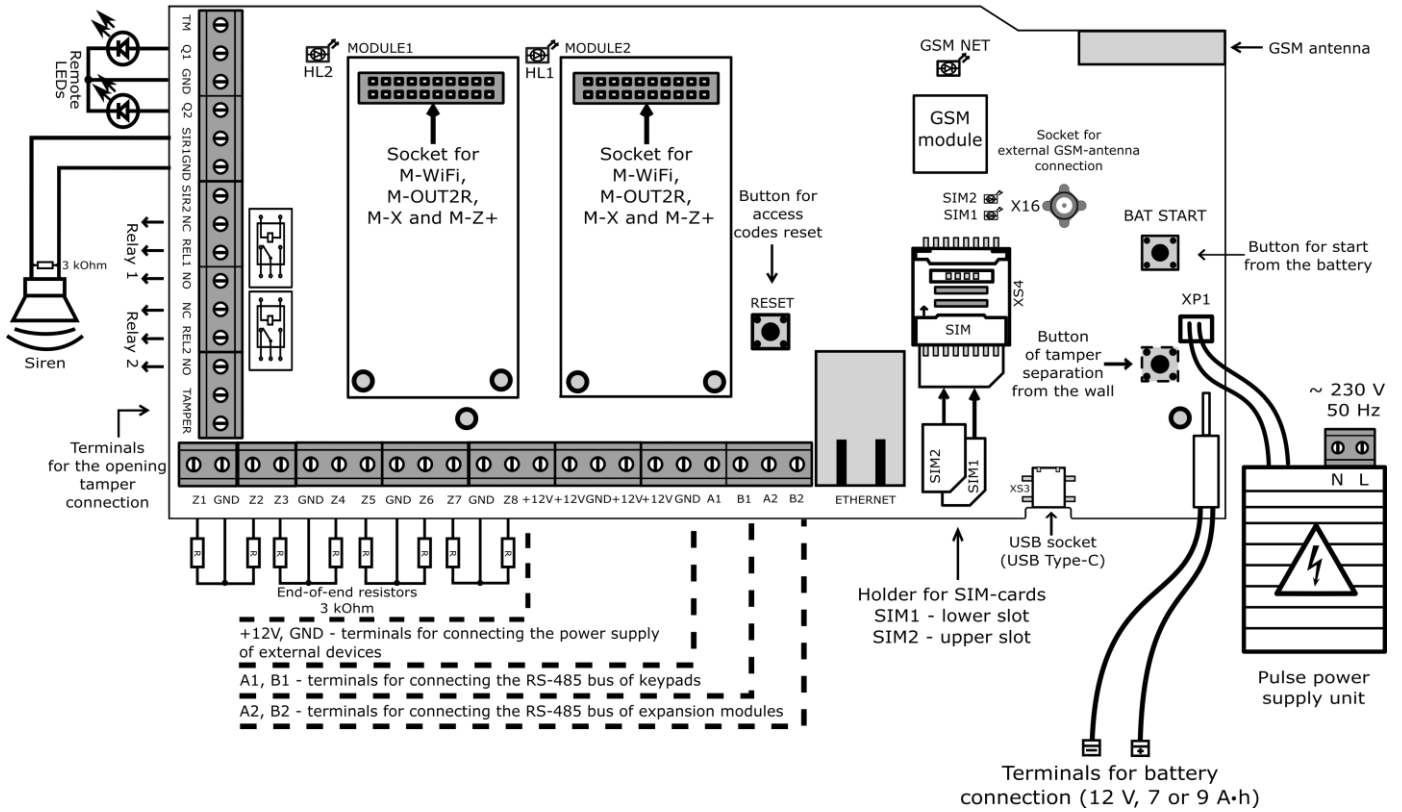


Figure A.1 – Electrical connection scheme for the SCP Orion NOVA L (LTE)

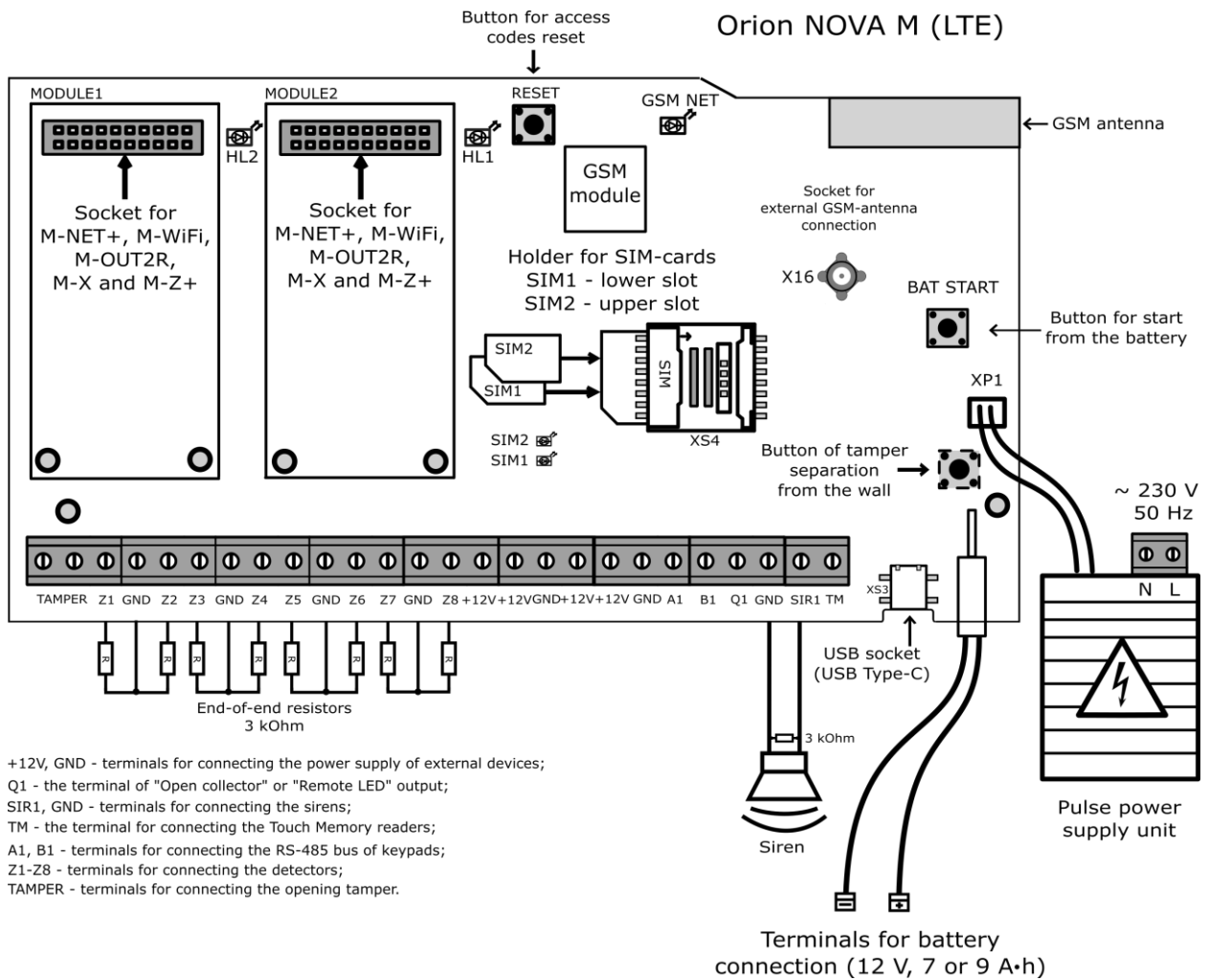


Figure A.2 – Electrical connection scheme for the SCP Orion NOVA M (LTE)

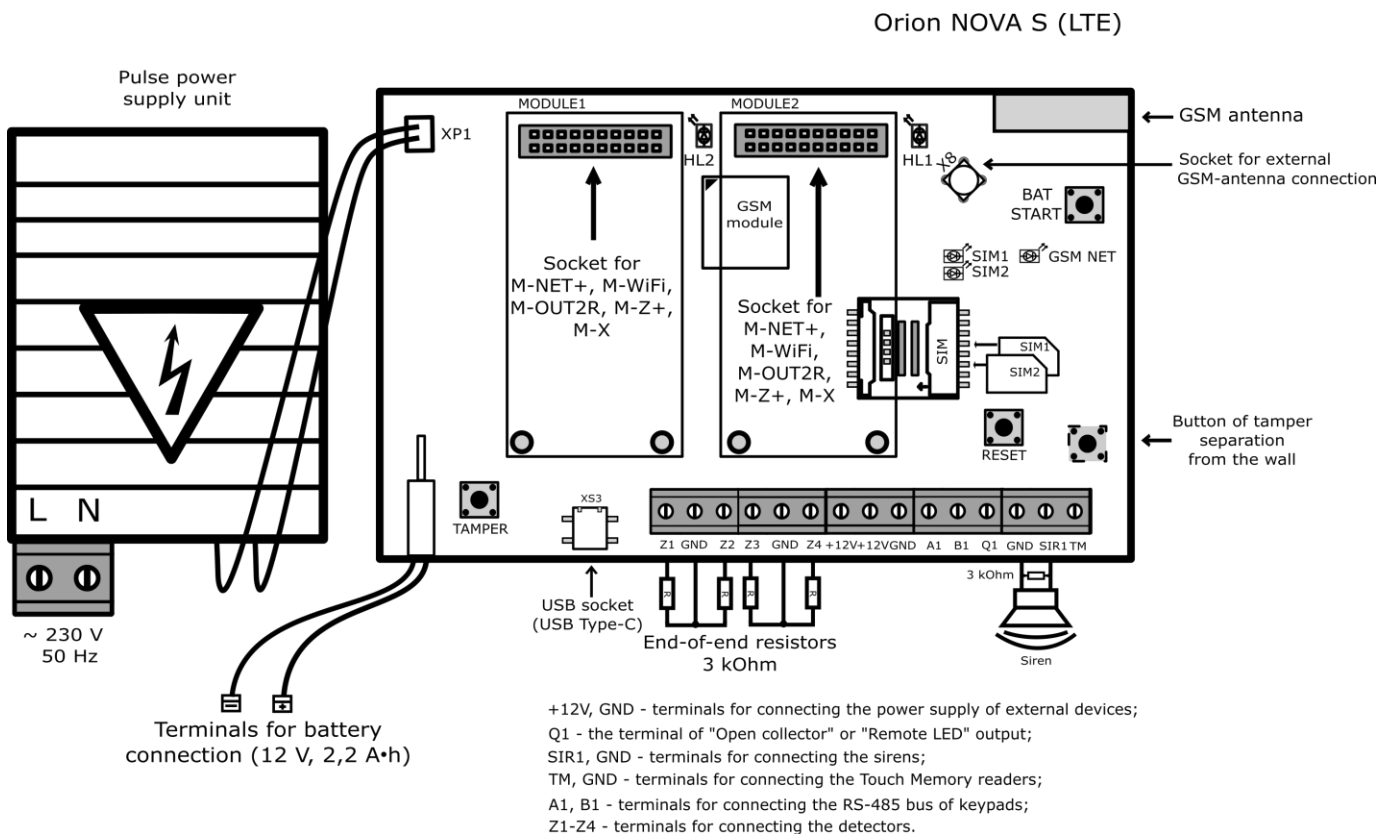


Figure A.3 – Electrical connection scheme for the SCP Orion NOVA S (LTE)

APPENDIX B

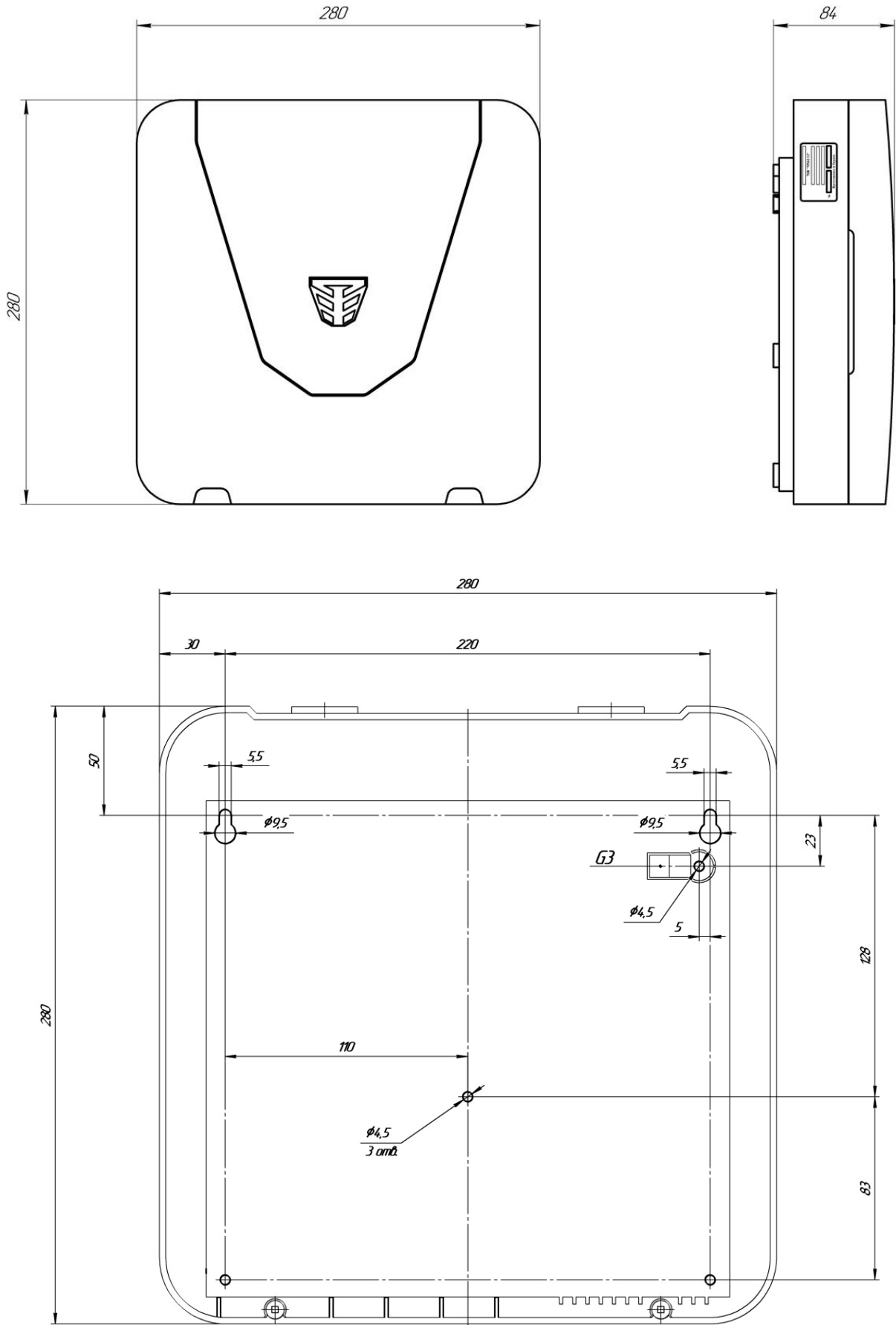


Figure B.1 - Mounting dimensions of the SCP Orion NOVA L/M (LTE)

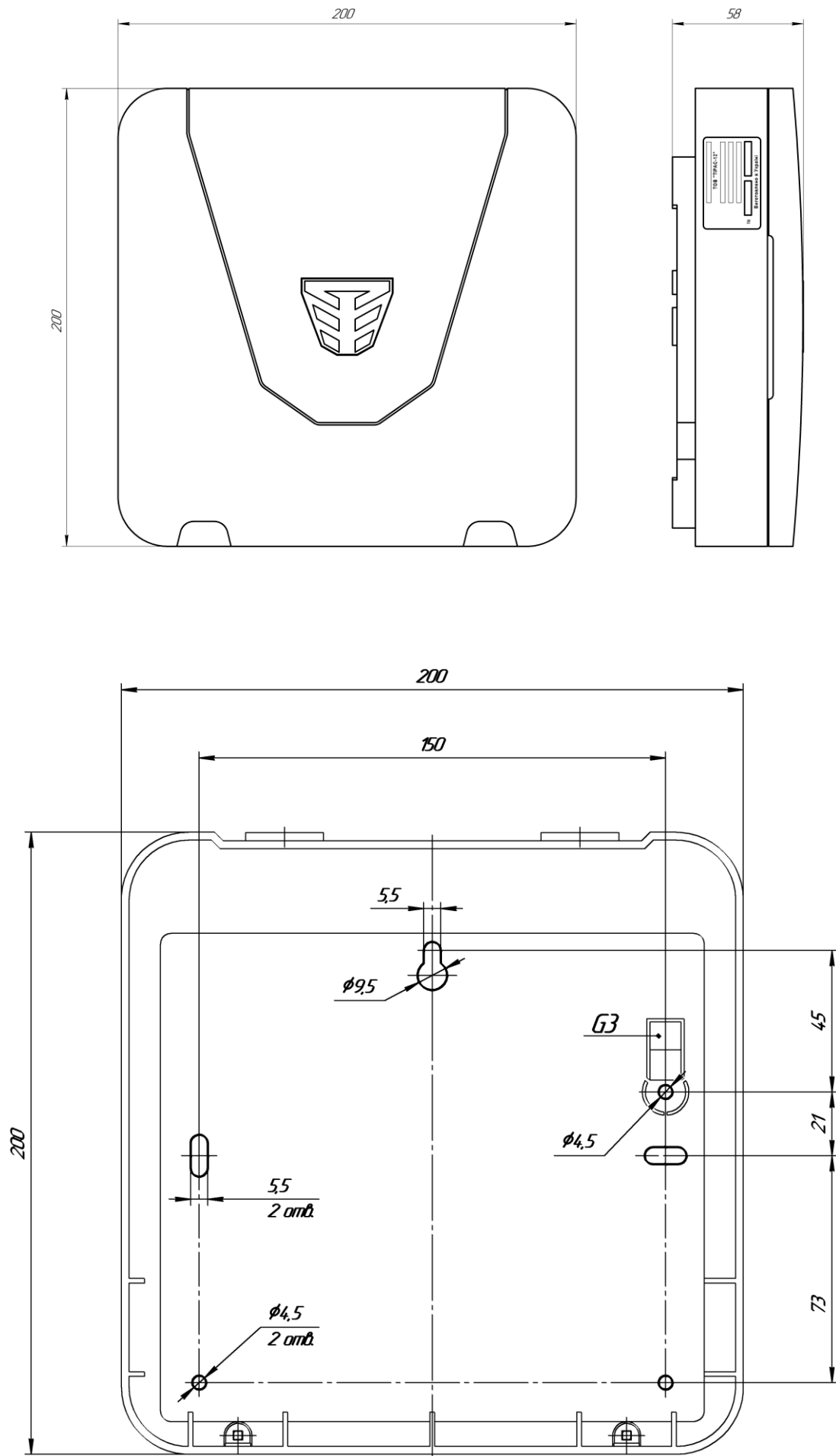


Figure B.2 - Mounting dimensions of the SCP Orion NOVA S (LTE)

APPENDIX C

Table C.1 – Description of the operation mode of the "Confirmation" indicator

Group status	Permanent confirmation enabled	Permanent confirmation disabled (status during the set lighting time)
Group disarmed	No lights	No lights
Entry delay	Blinks with the frequency of 1 Hz	Blinks with the frequency of 1 Hz
Unsuccessful arming	4 times blinking	4 times blinking
The group is armed, no confirmation from CMS	No lights	No lights
All zones or at least all zones of the "Entrance door" type of the group are armed; there is confirmation from the CMS	Light permanently	Lights within the set time
Entry delay	Blinks with the frequency of 1 Hz	Blinks with the frequency of 1 Hz
Group in alarm	Blinking 4 times per second	Not lights

APPENDIX D

Table D.1 – Default settings

Section	Settings
Devices	No devices
Keypads	No keypads
Zones	Zone 1 – Entrance door, entry delay – 30 seconds (Additional options – disabled); Zone 2 – Corridor (Additional options – disabled); Zones 3...16 – Security (Additional options – disabled).
Outputs	Q1, Q2 – confirmation outputs for group No. 1, connection type of output – Remote LED; SIR – Siren; REL1, REL2 – By script.
Groups	One group (zone 1...8), exit delay – 30 seconds; Confirmation by siren – disabled; Quick arming – disabled; Arming delay from reader – disabled.
Automatics	No scripts
Users	User No. 1 <ul style="list-style-type: none"> ▪ Name – no data; ▪ User role – installer, with administrator rights; ▪ Access type – full; ▪ Authority – Arming/disarming, bypass of unassembled zone, ignore faults; ▪ Access IDs: <ul style="list-style-type: none"> ▫ Access code – 9 digits of the serial number of the SCP (without hyphens); ▫ Key/card, attack code – no data; ▪ Groups, outputs, scripts – no data.
Working with SCP	Device operating mode – autonomous mode.
SIM cards	SIM cards – configured SIM1 with an access point – Internet.
Tiras CLOUD II	Connection with Tiras CLOUD II – through all communication channels.
System settings	<ul style="list-style-type: none"> ▪ Device language – Ukrainian; ▪ Alarm sounding time – 90 seconds; ▪ Confirmation glowing time – infinitely; ▪ Deny enter in 3rd access level – disabled; ▪ Enable SMS sending – disabled; ▪ Enable lower speed of transition between SCP and keypads – disabled; ▪ Auto SCP firmware update – turn on through Ethernet/Wi-Fi/cellular communication; ▪ Time zone of SCP – Europe/Kiev; ▪ Security class – do not analyze; ▪ Configuration protection with installer code – disabled; ▪ Enable permanent confirmation LED glow – enabled; ▪ Enable alarm formation on alarm zones violation during input time – enabled; ▪ Number of events of the same type – 50.

Table D.2 – Description of indicators operation for P-IND32 indication panel











Indicator	Purpose
 Fault	Flashes yellow in case of any fault in the system
 Alarm, intrusion	Flashes red in case of any alarm in the system
 Line	Lights green in case of communication with SCP is normal or flashes 1 time per second in case of communication fault
 Power	Lights green - P-IND32 indication panel power supplying is normal
Zones/group indicator	Display current status of zones or groups (depending on the setting of the "Display mode" option)

Table D.3 – Display of zones or groups status by P-IND32 indicators and keypad indicators

Indicator status	Zone status	Group status
No light	Zone is disarmed	All zones of the group are disarmed
	Panic button zone in alarm	
Lights red	Zone is intruded	Any zone of the group is intruded
	Zone is in norm, but there is an unviewed alarm in the system	Any zone of the group is in norm
Flashes red	Zone entry delay is activated	Alarm of any zone of the group
	Alarm in zone	
Lights green	Zone is armed	All or part of zones of the group are armed
Flashes green	Exit delay is counted down for the "Entrance door" or "Corridor" zone	The group exit delay is counted down

When pressing the **TEST** button on the P-IND32, the audible indication that was activated when an alarm occurs in the system is disabled, as well as the memory of alarms is cleared.

Table D.4 – Operating modes of keypad system status indicators

Indicator	Access level	Does not light	Blinks	Lights
 Attention	I	There are no alarms and faults in the system	There are unviewed alarms and (or) faults	All available alarms and faults are viewed
	II, III	There are no user-related alarms and faults	There are user-related unviewed alarms and (or) faults	All available user-related alarms and faults are viewed
 Ready	II, III	Group arming is prohibited	Indication of the steps of the access IDs changing	In the controlled group, all zones are in normal mode (zones with a delay may be intruded), no faults
 Security	I	All zones of groups for which the "Display group status in the Security" indicator in the first level of access" option is enabled – disarmed	Armed one or more (but not all) zones of groups for which the "Display group status in the Security" indicator in the first level of access" option is enabled – partial arming	All zones of the groups for which the "Displaying the status of the group in the Security" indicator on the first level of access" option is enabled are armed
	II, III	The controlled group is disarmed	Entry/exit delay is enabled	The controlled group is armed
 Alarm ¹	I	There are no alarms	Unviewed group alarm and (or) tamper alarm	All alarms are viewed (alarm of group or 24h zone, tamper alarm)
	II, III	There are no user-related alarms	Blinks once – unviewed group alarm and (or) tamper alarm Blinks twice – unviewed memory of alarms (group alarm and (or) tamper alarm)	All alarms are viewed (alarms of group, tamper alarms)
 Fault	I	There are no faults	There are unviewed faults	All faults are viewed
	II, III	There are no user-related faults	There are unviewed user-related faults	All user-related faults are viewed
 Power	I, II, III	Power of all devices is normal ²	Power fault of any device in the system	Power of all devices is normal

¹ The "Alarm" indicator does not display the activation of zones with the "Panic Button" type at the 1st access level.

² The "Power" indicator will not light up when it is set in inverse mode.

Table D.5 – List of SMS-messages, which can be sent to the user phone number

Event	SMS-message type¹
Alarm in zone	DD.MM <u>HH:MM</u> ALARM, ALARM TYPE, "Zone Name"
Arming	DD.MM <u>HH:MM</u> "Group Name" SET, "Username"
	DD.MM <u>HH:MM</u> "Group Name" SET FROM CMS
	DD.MM <u>HH:MM</u> "Group name" SET (automatically)
Disarming	DD.MM <u>HH:MM</u> "Group Name" UNSET, "Username"
	DD.MM <u>HH:MM</u> "Group Name" UNSET FROM CMS
Output activation	DD.MM <u>HH:MM</u> SWITCHING ON "Output Name", "Username"
Output deactivation	DD.MM <u>HH:MM</u> SWITCHING OFF " Output Name", "Username"
Penetration (tamper)	DD.MM <u>HH:MM</u> SCP TAMPER ALARM
	DD.MM <u>HH:MM</u> TAMPER ALARM OF "Keypad Name"
	DD.MM <u>HH:MM</u> TAMPER ALARM OF "Name of the module"
Power supply 230 V of SCP fault	DD.MM <u>HH:MM</u> POWER 230V FAULT, SCP
Power supply 230 V of SCP is normal	DD.MM <u>HH:MM</u> POWER 230V SCP OK
SCP battery fault	DD.MM <u>HH:MM</u> BATTERY FAULT
No battery	DD.MM <u>HH:MM</u> MISSING SCP BATTERY
SCP battery is normal	DD.MM <u>HH:MM</u> BATTERY SCP OK

Note.

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

¹ If there are no element names in the system (zones, groups, keypad outputs, etc.), the system-wide numbers and element names are written in the text of the SMS message.

Table D.6 – 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 zone overriding	Arming	E570_00_(overridden zone number)	
3	Group disarming	Disarming	E401_(group number)_ (user number)	
4	Alarm in zone (open/short circuit) type: security, entrance door, corridor, 24h, universal input (in alarm mode)	Alarm	E130_00_(zone number)	
5	Panic button alarm (open/short circuit)	Alarm	E120_00_(zone number)	
6	Intrusion in 2EOL type zone: wireless	Alarm	E137_00_(zone number)	
7	Intrusion of the zone type: tamper, anti-masking	Alarm	E130_00_(zone number)	
8	SCP tamper alarm: penetration, separation	Alarm	E140_00_000	
9	Keypad tamper	Alarm	E341_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
10	Expansion module tamper	Alarm	E341_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
11	Entering the user attack code	Alarm	E423_00_000	
12	Keypad blocking	Alarm	E461_00_000	
13	System error	Fault	E303_00_000	
14	Universal input fault (in "Fault" mode)	Fault	E370_00_(zone number)	
15	SCP battery is missing	Fault	E311_00_000	
16	SCP battery is discharged	Fault	E302_00_000	
17	SCP battery low capacity	Fault	E309_00_000	
18	No 230 V power supply of SCP	Fault	E301_00_000	
19	Output fault	Fault	E312_00_000	
20	Siren output failure	Fault	E321_00_000	
21	GSM module power supply failure	Fault	E353_00_000	
22	SCP jamming	Fault	E353_00_000	
23	Low power voltage of keypad	Fault	E300_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
24	Communication fault with keypad	Fault	E330_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
25	Low power voltage of expansion module	Fault	E300_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
26	Communication fault with expansion module	Fault	E330_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
27	Expansion module battery is missing	Fault	E311_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
28	Expansion module battery is discharged	Fault	E302_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
29	No power supply of expansion module	Fault	E301_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
30	Expansion module output fault	Fault	E312_00_000	
31	Expansion module siren output fault	Fault	E321_00_000	
32	Unsuccessful arming	Fault	R457_(group number)_ (user number)	
33	Low power voltage of the wireless detector	Fault	E384_00_(zone number)	
34	Communication fault with wireless detector	Fault	E380_00_(zone number)	

35	Normal condition of zones: Security, Entrance door, Corridor, 24h, Universal input (alarm mode) is restored	Restoring	R130_00_(zone number)	
36	Intrusion in wireless 2EOL type zone restored	Restoring	R137_00_(zone number)	
37	Normal condition of Panic button restored	Restoring	R120_00_(zone number)	
38	Zone is restored: tamper, antimasking	Restoring	R130_00_(zone number)	
39	Universal input in the "Fault" mode restored	Restoring	R370_00_(zone number)	
40	SCP battery is restored	Restoring	R311_00_000	
41	230V power supply is restored	Restoring	R301_00_000	
42	SCP output restored	Restoring	R312_00_000	
43	SCP siren output restored	Restoring	R321_00_000	
44	SCP tamper restored	Restoring	R140_00_000	
45	GSM module power supply restored	Restoring	R353_00_000	
46	Jamming is eliminated	Restoring	R353_00_000	
47	Keypad power supply restored	Restoring	R300_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
48	Keypad tamper restored	Restoring	R341_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
49	Communication with keypad restored	Restoring	R330_00_(501-512)	501-512: the number of the keypad in the system from 1 to 12, respectively
50	Expansion module power supply restored	Restoring	R300_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
51	Expansion module tamper restored	Restoring	R341_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
52	Communication with expansion module restored	Restoring	R330_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
53	Expansion module battery restored	Restoring	R311_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
54	230 V power supply of expansion module restored	Restoring	R301_00_(601-615)	601-615: the number of the expansion module in the system from 1 to 15, respectively
55	Expansion module output restored	Restoring	R312_00_000	
56	Expansion module alarm output restored	Restoring	R321_00_000	
57	Wireless detector power supply restored	Restoring	R384_00_(zone number)	
58	Communication with the wireless detector restored	Restoring	R380_00_(zone number)	
59	Switching on SCP	Informative	R308_00_000	
60	Switching off SCP	Informative	E308_00_000	
61	Change of the SCP settings	Informative	E429_00_000	
62	SCP firmware update	Informative	E306_00_000	
63	Change of user access ID	Informative	E462_00_(user number whose code was changed)	
64	User access ID changed by the administrator	Informative	E462_00_(user number whose code was changed)	
65	Periodic test messages	Test	E602_00_000	

Table D.7 – The list of records that can be recorded in the event log

Event	Reason for appearance
"Group name GROUP ARMING INITIATED by "User name" USER	User has armed the group
"Zone number" ZONE ARMING by "User name" USER	Arming zones (initiated by the user)
"Zone number" ZONE OVERRIDE by "User name" USER	User has overridden the intruded zone during the arming procedure
VIEWING FAULTS by "User name" USER	The user has reviewed all faults during the arming procedure
"Group name GROUP DISARMING INITIATED by "User name" USER	User has disarmed the armed group
"Zone number" ZONE DISARMING by "User name" USER	Disarming zones (initiated by the user)
"Zone number" ZONE ARMING FROM CMS	Arming zones by the CMS operator
"Zone number" ZONE DISARMING FROM CMS	Disarming zones by the CMS operator
"User name" USER CODE CHANGING	User has changed one's access/attack code
"User name" USER CODE CHANGING by "User name" USER	Administrator has changed one's access IDs
"Administrator name" USER ADDED "User name" USER	Administrator has created a new user
"Administrator name" USER DELETED "User name" USER	Administrator has deleted the user
"User name" USER CHANGED SETTINGS	Change the settings of the SCP by the user
ATTACK, "User name" USER	Attack code entered by the user
ENTRY DELAY TIME THROUGH "Zone name" ZONE	Armed Entrance Door zone is intruded
ALARM IN ZONE (Zone number) "Zone name"	1) Intrusion in the Corridor or Security armed zone 2) During the entry delay, the zone of Entrance door type was not disarmed
ALARM IN PANIC BUTTON # (Zone number) "Zone name"	Alarm in the Panic button zone
RESTORING PANIC BUTTON # (Zone number) "Zone name"	Automatically rearming of Panic button zone in 180 seconds after physical restoring.
REARMING ZONE # (Zone number) "Zone name"	1) Automatic rearming of a 24h zone in 180 seconds after physical restoring 2) Deactivation of the Universal Input zone
FAULT IN ZONE # (Zone number) "Zone name"	Activation of Universal Input Zone
No communication with the wireless detector in (Zone number) "Zone name"	Communication loss with wireless detector
A low battery in with wireless detector in (Zone number) "Zone name"	Battery discharge in wireless detector
TAMPER ALARM OF SCP	Activation of SCP tamper
TAMPER ALARM OF SCP RESTORED	SCP tamper restored
TAMPER ALARM OF "Keypad name"	Activation of keypad tamper
TAMPER ALARM OF "Keypad name" RESTORED	Keypad tamper restored
TAMPER ALARM OF "Module name"	Activation of module tamper
TAMPER ALARM OF "Module name" RESTORED	Module tamper restored
ALARM (time and date) TRANSMITTED TO CMS	Alarm message was successfully transmitted to the CMS
NO BATTERY OF SCP	The battery of the control panel is absent or the voltage on its terminals is less than 10.5V
LOW BATTERY OF SCP	The voltage on the terminals of the SCP battery has dropped less 11.2 V
BATTERY OF SCP IS NORMAL	The voltage on the terminals of the SCP battery has increased to 11.2 V
SCP MAIN POWER SUPPLY FAULT	SCP main power supply (230 V) fault
SCP MAIN POWER SUPPLY RESTORED	SCP main power supply (230 V) restored
FAULT OF 12V OUTPUT	Fault of SCP "+12V" output
FAULT OF 12V OUTPUT RESTORED	Fault of SCP "+12V" output restored

FAULT OF "SIR" OUTPUT	Fault of SCP "SIR" output
FAULT OF "SIR" OUTPUT RESTORED	Fault of SCP "SIR" output restored
FAULT OF GSM TRANSCEIVER	Power voltage of GSM transceiver is lower than normal
FAULT OF GSM TRANSCEIVER RESTORED	Power voltage of GSM transceiver restored
FAULT OF COMMUNICATION WITH CMS	No response from the CMS within the set time
COMMUNICATION WITH CMS RESTORED	Got response from the CMS after the loss of communication
GSM-SIGNAL JAMMING	GSM signal jamming detected
GSM-SIGNAL JAMMING RESTORED	GSM signal jamming eliminated
FAULT OF COMMUNICATION WITH "Device name"	Communication with external device fault
FAULT OF COMMUNICATION WITH "Device name" RESTORED	Communication with external device restored
ACCESS RESTRICTION ("Keypad name" keypad)	Keypad has been locked after unsuccessful attempts to enter the code
POWER OF "Device name" IS LOW	Power supply voltage of external device dropped below 9.0V
POWER OF "Device name" RESTORED	Power supply voltage of external device restored
NO BATTERY IN "Module name"	The expansion module battery is absent or voltage at its terminals is less than 10.5 V
BATTERY FAULT IN "Module name", DISCHARGED	The voltage at the terminals of the expansion module battery decreased to 11.2 V
BATTERY IN "Module name" RESTORED	The voltage at the terminals of the expansion module battery increased higher 11.2 V
FAULT OF 230 V POWER SUPPLY IN "Module name"	No 230 V power supply of the expansion module
230 V POWER SUPPLY IN "Module name" RESTORED	230 V power supply of expansion module restored
FAULT OF SIR OUTPUT IN "Module name"	Expansion module "SIR" output fault
FAULT OF SIR OUTPUT IN "Module name" RESTORED	Expansion module "SIR" output restored
FAULT OF 12V OUTPUT IN "Module name"	Expansion module "12V" output fault
FAULT OF 12V OUTPUT IN "Module name" restored	Expansion module "12V" output restored
SYSTEM FAULT	Failed to process data. Automatic restart of the SCP.
SCP START	Switching on of the SCP or restart it by the installer from the display keypad
TIME SYNCHRONIZATION WITH CMS	SCP synchronized its time with the CMS
TIME SYNCHRONIZATION WITH TIRAS CLOUD	SCP synchronized its time with the Tiras CLOUD II server
RESTORE DEFAULT SETTINGS	Factory settings were set by the installer by the keypad menu
RESTORE SAVED SETTINGS	A system error occurred causing the saved settings to be restored
SCP FIRMWARE IS UPDATED TO "New version number"	SCP firmware has been updated to the specified version
FIRMWARE UPDATING ERROR, FILE IS DAMAGED	Failed to update SCP firmware

APPENDIX E

Table E.1 – Subsection numbers for LED keypads

Number¹ (Subsection)	Function	Admin	Installer	User
0	Enable zone testing mode	-	+	-
1	Change one's own access code	+	+	+
2	Change the attack code	+	+	+
3	Faults viewing	+	+	+
4	Enable the Wireless Devices Adding mode	-	+	-
5	Reset to default settings [# installer code]	-	+	-
6	Delete data on Tiras CLOUD II [# admin code]	+	-	-
7	Enable the Tiras Cloud II registration mode	+	-	-
8	Restriction of access to the installer	+	-	-
9	Export event log	+	-	-
10	Display the wireless devices signal strength	-	+	-
11	Display the Wi-Fi signal strength	-	+	-
12	Display the GSM signal strength	-	+	-
13	Restart the SCP [#installer code]	-	+	-
14	Flash drive formatting [#installer code]	-	+	-
15	Change one's own key/card	+	+	+
16	EOL calibration [# installer code]	-	+	-

¹ Inputting format: [access code # number #]. For subsections 6,14,16: [access code # number # access code]

Edited: 09.07.2025



tiras.technology

CONTACTS OF THE MANUFACTURER:

Tiras-12 LTD

Ukraine, Vinnytsia, Khmelnytskoho Shose lane 2, building 8

If 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