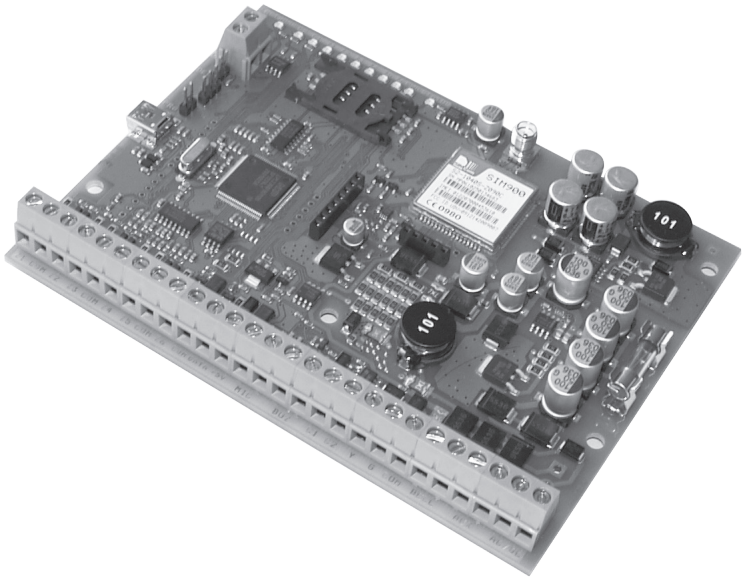
eldes



GSM ALARM AND MANAGEMENT SYSTEM

ESIM264

COMPLIES WITH EN 50131-1 GRADE 2, CLASS II REQUIREMENTS

CONTENTS

Safety instructions

Please read and follow these safety guidelines in order to maintain safety of operators and people around:

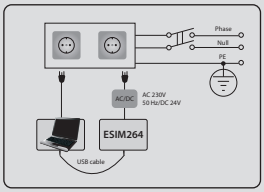
- GSM alarm & management system ESIM264 (later referenced as GSM alarm system ESIM264, ESIM264 alarm system, ESIM264 system, ESIM264, alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- DO NOT use the system in hazardous environment.
- DO NOT expose the system to high humidity, chemical environment or mechanical impacts.
- DO NOT attempt to personally repair the system.
- System label is on the bottom side of the device.

GSM alarm system ESIM264 is a device mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel.

The system must be powered by main 16-24V 50 Hz ~1.5A max or 18-24V ⎓ 1,5A max DC power supply which must be approved by LST EN 60950-1 standard and be easily accessible nearby the device. When connecting the power supply to the system, switching the pole terminals places does not have any affect.

Any additional devices linked to the system ESIM264 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

Main power supply can be connected to AC mains only inside installation room with automatic 2-pole circuit breaker capable of disconnecting circuit in the event of short circuit or over-current condition. Open circuit breaker must have a gap between connections of more than 3mm and the disconnection current 5A.



Mains power and backup battery must be disconnected before any installation or tuning work starts. The system installation or maintenance must not be done during stormy conditions.

Backup battery must be connected via the connection which in the case of breaking would result in disconnection of one of battery pole terminals. Special care must be taken when connecting positive and negative battery terminals. Switching the pole terminals places is NOT allowed.

In order to avoid fire or explosion hazards the system must be used only with approved backup battery.

The device is fully turned off by disconnecting 2-pole switch off device of the main power supply and disconnecting backup battery connector.

Fuse F1 type – Slow Blown 3A. Replacement fuses have to be exactly the same as indicated by the manufacturer.

If you use I security class computer for setting the parameters it must be connected to earth.

The WEEE (Waste Electrical and Electronic Equipment) marking on this product (see left) or its documentation indicates that the product must not be disposed of together with household waste. To prevent possible harm to human health and/or the environment, the product must be disposed on in an approved and environmentally safe recycling process. For further information on how to dispose of this product correctly, contact the system supplier, or the local authority responsible for waste disposal in your area.

Limited Liability

The buyer must agree that the system will reduce the risk of fire, theft, burglary or other dangers but does not guarantee against such events.
"ELDES UAB" will not take any responsibility regarding personal or property or revenue loss while using the system.
"ELDES UAB" liability according to local laws does not exceed value of the purchased system. "ELDES UAB" is not affiliated with any of the cellular providers therefore is not responsible for the quality of cellular service.

Manufacturer Warranty

The system carries a 24-month warranty by the manufacturer "ELDES UAB". Warranty period starts from the day the system has been purchased by the end user. The warranty is valid only if the system has been used as intended, following all guidelines listed in the manual and within specified operating conditions. Receipt must be kept as a proof of purchase date.
The warranty is voided if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or other force majeure factors.

Package Content

1. GSM Alarm System ESIM264.....qty. 1
2. Microphone.....qty.1
3. GSM Antenna .....qty. 1
4. Mini Buzzer. .....qty. 1
5. Battery Connection Wire.....qty. 1
6. User Manual. .....qty. 1
7. Resistor 5,6kΩ.....qty. 6
8. Resistor 3,3kΩ.....qty. 6

About User Manual

This document describes alarm system ESIM264 installation and operation. It is very important to read User Manual before start using the system.

CE

1. General Information

1.1 Functionality

ESIM264 – micro-controller based alarm system for houses, cottages, country homes, garages and other buildings, also capable of managing electrical appliances via cellular GSM/GPRS network. It can also be used as Intercom system.

The system can be used in the following applications:

- Property security;
- Alarm switch;
- Thermostat, heating and air-conditioner control, temperature monitoring;
- Lighting, garden watering, water pump and other electrical equipment control via SMS messages;
- Remote listening to what is happening in the secured area;
- Main 230V power status with SMS message;
- Two-way intercom device via GSM network.

1.2 Compatible Device Overview

Wired Devices		
Device	**Description**	**Max. Connectable Devices**
EKB2	LCD keyboard	4*
EKB3	LED keyboard	4*
EA1	Audio output module with 3,5mm jack	1**
EA2	Audio amplifier module 1W 8Ω	1**
EPGM1	16 zone and 2 PGM output expansion module	1
EPGM8	8 PGM output expansion module	1**
Wireless Devices		
Device	**Description**	**Max. Connectable Devices**
EWT1	Wireless transmitter-receiver extension with external antenna (access point)	1
EW1****	Wireless 2 zone and 2 PGM output expansion module	16***
EWP1****	Wireless PIR movement sensor	16***
EWD1****	Wireless magnetic door contact	16***
EWK1****	Wireless key-fob with 4 buttons	16***
EWS1****	Wireless indoor siren	16***
EWS2****	Wireless outdoor siren	16***

* - A mixed combination of EKB2 and EKB3 keyboards is supported. The combination can consist of up to 4 keyboards in total.
** - Only 1 of these modules can be connected at a time.
*** - A mixed combination of wireless devices is supported. The combination can consist of up to 16 wireless devices in total.
**** - EWT1 module for ESIM264 system is required to operate with the wireless devices.

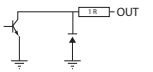
1.3 Default Parameters & Ways of Parameter Configuration

Main Parameters					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
SMS & EKB2 Menu Language	Depends on firmware version according to user's location	✓	✓	✓	✓
SMS Password	0000	✓	✓	✓	✓
User (Keyboard) Password 1	1111		✓	✓	✓
User (Keyboard) Password 2... 10	N/A		✓	✓	✓
Administrator Password	1470		✓	✓	✓
Duress Password	N/A		✓	✓	✓
SGS Password	N/A		✓	✓	✓
User 1... 5 Phone Number	N/A	✓	✓	✓	✓
Allow Only Preset Users	Enabled	✓	✓	✓	✓
Answer Call	Disabled				✓
Date & Time	N/A	✓	✓	✓	✓
Zones					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Zone Alarm Text	Z1 - Door sensor triggered, Z2 - Windows sensor triggered, Z3 - Fire sensor triggered, Z4 - Motion1 sensor triggered, Z5 - Motion2 sensor triggered, Z6 - Motion3 sensor triggered etc.	✓			✓
Entry Delay	15 seconds	✓	✓	✓	✓
On-Board Zone Delay	800 milliseconds				✓
EPGM1 Zone Delay	800 milliseconds				✓
On-board Z1 Zone Type	Delay		✓	✓	✓
Exit Delay	15 seconds	✓	✓	✓	✓
On-board Z2... Z12 Zone Type	Instant		✓	✓	✓
Keyboard Zone Type	Instant		✓	✓	✓
EPGM1 Zone Type	Instant		✓	✓	✓
Wireless Zone Type	Depends on the connected wireless device		✓	✓	✓
Virtual Zone Type	Follow			✓	✓
ATZ Mode	Disabled		✓	✓	✓
Zone Connection Type when ATZ Mode Disabled	Type 1		✓	✓	✓
Zone Connection Type when ATZ Mode Enabled	Type 4		✓	✓	✓
On-board Zone Status	Enabled	✓	✓	✓	✓
Keyboard Zone Status	Disabled	✓	✓	✓	✓
EPGM1 Zone Status	Enabled	✓	✓	✓	✓
Wireless Zone Status	Enabled	✓	✓	✓	✓
Virtual Zone Status	Disabled			✓	✓
Stay Mode for Particular Zone	Disabled		✓	✓	✓
Arm-Disarm by Zone	N/A		✓	✓	✓
Force Mode for Particular Zone	Disabled		✓	✓	✓
Tamper Name	Tamper 1, Tamper 2, Tamper 3, Tamper 4, Tamper 5, Tamper 6 etc.				✓
Chime	Enabled		✓	✓	✓
PGM Outputs					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
PGM Output Name	C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.	✓			✓
PGM Output Status	Disabled	✓	✓	✓	✓
EPGM8 PGM Output Status	Disabled	✓	✓	✓	✓
EPGM1 PGM Output Status	Disabled	✓		✓	✓
Wireless PGM Output Status	Enabled	✓	✓	✓	✓
Wireless PGM Output Type	Depends on the connected wireless device				✓
Automatic PGM Output Control 1... 16	Disabled			✓	✓
Automatic PGM Output Control Management	N/A				✓
Scheduler 1... 16	Disabled				✓
Turn ON/OFF PGM Output by Timer	N/A	✓			
EPGM8 Mode	Disabled		✓	✓	✓
Siren					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Siren Alarm Duration	1 minute	✓	✓	✓	✓
Bell Squawk	Disabled		✓	✓	✓
Siren ON if RF Signal is Lost	Disabled		✓	✓	✓

Periodic Info SMS, Alarm Notifications & Arm/Disarm Notifications					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Periodic Info SMS	Period – 1; Time - 11	✓	✓	✓	✓
Disable Call in Case of Alarm	Disabled		✓	✓	✓
Disable SMS in Case of Alarm	Disabled		✓	✓	✓
SMS to All Users in Case of Alarm	Disabled	✓	✓	✓	✓
Notification about Arming/Disarming	Enabled		✓	✓	✓
Notification about Arming/Disarming to All Users	Disabled	✓	✓	✓	✓
Temperature Limit Info, Main Power Status & iButton Key Mode					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Temperature Limit Info SMS	Enabled	✓	✓	✓	✓
Temperature Limit MIN Value	N/A	✓	✓	✓	✓
Temperature Limit MAX Value	N/A	✓	✓	✓	✓
Checking Main Power Status	Enabled	✓	✓	✓	✓
Main Power Failure Delay	30 seconds		✓	✓	✓
Main Power Restore Delay	120 seconds		✓	✓	✓
New iButton Key Mode	Disabled	✓	✓	✓	✓
Partitions					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Partition 0 Name	PART0		✓	✓	✓
Partition 1 Name	PART1		✓	✓	✓
Keyboard 1... 4 Partition	PART0		✓	✓	✓
Keyboard Partition Switch	Disabled		✓	✓	✓
Keyboard 1... 10 Password Partition	PART0		✓	✓	✓
User 1... 5 Partition	PART0		✓	✓	✓
iButton 1.. 10 Partition	PART0		✓	✓	✓
Monitoring Station					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
CID Mode	Disabled	✓	✓	✓	✓
CID Messages	All Enabled		✓	✓	✓
User Messages when CID Mode Enabled	All Disabled		✓	✓	✓
Account (Alarm System ID)	9999		✓	✓	✓
Monitoring Station Phone Number 1... 3 (Voice Calls)	N/A		✓	✓	✓
Call Attempts	3		✓	✓	✓
Monitoring Station Phone Number (CSD)	N/A		✓	✓	✓
CSD Attempts	3		✓	✓	✓
Server IP Address (GPRS)	0.0.0.0	✓	✓	✓	✓
DNS1 Server IP Address (GPRS)	N/A	✓	✓	✓	✓
DNS2 Server IP Address (GPRS)	N/A	✓	✓	✓	✓
Protocol (GPRS)	TCP	✓	✓	✓	✓
Server Port (GPRS)	20000	✓	✓	✓	✓
Local Port (GPRS)	N/A	✓	✓	✓	✓
APN (GPRS)	N/A	✓			✓
User (GPRS)	N/A	✓			✓
Password (GPRS)	N/A	✓			✓
Profile	Profile1	✓			✓
Primary Communication	GPRS Network		✓	✓	✓
Backup Communication 1... 3	N/A		✓	✓	✓
GPRS Attempts	3		✓	✓	✓
Delay Between Attempts	600 seconds		✓	✓	✓
Device ID (GPRS)	0000		✓	✓	✓
Test Period	180 seconds		✓	✓	✓
Additional Parameters					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
Event Log	Enabled		✓	✓	✓
Microphone Level	12		✓		✓
Speaker Level	85		✓		✓
GSM Loss Indication by PGM Output	N/A				✓
Message **ARMED** on EKB2 screen	Disabled				✓
GSM Loss Indication PGM Output Delay	180 seconds				✓

2. Technical Specifications

2.1 Electrical & Mechanical Characteristics

Electrical & Mechanical Characteristics	
Main Power Supply	16-24V 50 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current in Standby without External Sensors and Keyboard	Up to 80mA
Recommended Backup Battery Voltage, Capacity	12V; 1,3-7Ah
Recommended Backup Battery Type	Lead-Acid
Maximum Battery Charge Current	900mA
GSM Modem Frequency	850/900/1800/1900MHz
Number of Zones on Board	6 (ATZ mode: 12)
Nominal Zone Resistance	5,6kΩ (ATZ Mode: 5,6kΩ and 3,3kΩ)
Number of PGM Outputs on Board	4
PGM Output C1-C4 Circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum Commuting PGM Output Values	Voltage – 30V; Current – 100mA;
Siren Output when Activated	Connected to COM
BELL Maximum Siren Output Current	500mA
Auxiliary Equipment Power Supply Voltage	13,8V DC
Maximum Accumulative Current of Auxiliary Equipment and Siren	1A
+5V Maximum Current of Buzzer	150mA
Supply Voltage of Buzzer	5V DC
Dimensions	140x100x18mm
Operating Temperature Range	-20...+55^{0}C
Supported Temperature Sensor Model	Maxim®/Dallas® DS18S20, DS18B20
Maximum Cable Length for 1-Wire® Communication	up to 30 meters
Supported iButton® Key Model	Maxim®/Dallas® DS1990A
Supported Quantity of Keyboards	4 x EKB2 / EKB3
Maximum Cable Length for RS485 Communication	up to 100 meters
Wireless Transmitter-Receiver Frequency *	868 Mhz
Wireless Communication Range*	Up to 30m in premises; up to 150m in open areas
Maximum Number of Wireless Devices*	16
Event Log Size	1000 events
Maximum Supported Quantity of Zones	44
Maximum Supported Quantity of PGM Outputs	44
Communications	SMS, Ademco Contact ID®: Voice calls (GSM audio channel), GPRS network, RS485, CSD

* only for system ESIM264 with module EWT1

2.2 Main Unit, LED & Connector Functionality

Main Unit Functionality	
GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD	SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
ANTENNA	GSM antenna SMA type connector
MODULES (EWT1, EA1, EA2, EPGM8)	Additional module slots

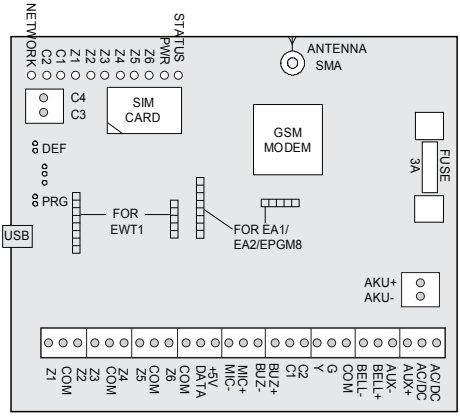


Fig. No.1

LED Functionality	
NETWORK	GSM network signal strength
C2, C1	PGM output C1, C2 status – on/off
Z1	Zone Z1 state – alarm/restore (ATZ mode: Z1 and Z7)
Z2	Zone Z2 state – alarm/restore (ATZ mode: Z2 and Z8)
Z3	Zone Z3 state – alarm/restore (ATZ mode: Z3 and Z9)
Z4	Zone Z4 state – alarm/restore (ATZ mode: Z4 and Z10)
Z5	Zone Z5 state – alarm/restore (ATZ mode: Z5 and Z11)
Z6	Zone Z6 state – alarm/restore (ATZ mode: Z6 and Z12)
PWR	Power supply status
STATUS	Micro-controller status

Connector Functionality	
Z1 - Z6	Security zones
COM	Common return contact for all zones
DATA	1-Wire® interface for iButton® key & temperature sensor connection
+5V	Temperature sensor power supply contact (+5V)
MIC-	Microphone negative contact
MIC+	Microphone positive contact
BUZ-	Mini buzzer negative contact
BUZ+	Mini buzzer positive contact
C1 - C4	PGM outputs
Y	RS485 interface for communication (yellow wire)
G	RS485 interface for communication (green wire)
COM	Common return contact
BELL-	Siren negative contact
BELL+	Siren positive contact
AUX-	Negative power supply contact for auxiliary equipment
AUX+	Positive power supply contact for auxiliary equipment
AC/DC	Main power supply contacts
AKU-	Backup battery negative contact
AKU+	Backup battery positive contact

2.3 Wiring Diagrams

2.3.1 General Wiring

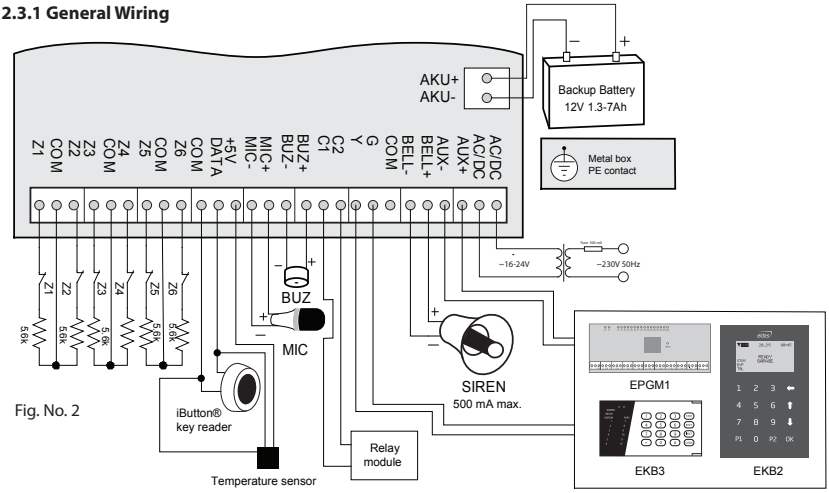
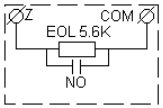


Fig. No. 2

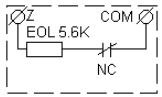
2.3.2 Zone Connection Types

Type 1



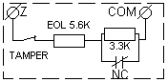
Normally open contact with 5,6KΩ end of line resistor

Type 2



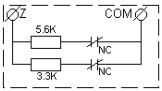
Normally closed contact with 5,6KΩ end of line resistor

Type 3



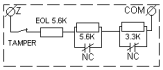
Tamper and 5,6KΩ end of line resistor and 3,3KΩ end of line resistor with normally closed contact

Type 4



ATZ Mode: 5,6KΩ end of line resistor and normally closed contact with 3,3KΩ end of line resistor and normally closed contact

Type 5



ATZ Mode: Tamper, 5,6KΩ end of line resistor, 5,6KΩ end of line resistor with normally closed contact and 3,3KΩ end of line resistor with normally closed contact.

Fig. No. 3

2.3.3 Siren

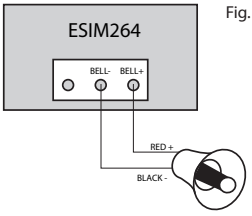
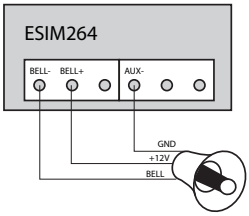


Fig. No. 4



NOTE: BELL- is the commuted contact intended for siren control.

2-wired siren

1. Connect positive siren wire (red) to **BELL+** contact.
2. Connect negative siren wire (black) to **BELL-** contact.

Self-contained siren

1. Connect negative **GND** siren wire to **AUX-** contact.
2. Controlling **BELL** siren wire must be connected to **BELL-** contact.
3. Connect positive **+12V** siren wire to **BELL+** contact.

2.3.4 iButton® Key Reader & Mini Buzzer

Supported iButton® Key Model: Maxim®/Dallas® DS1990A
The iButton® key reader can be installed with mini buzzer or separately. The mini buzzer is intended for audio indication of *Entry/Exit Delay* countdown providing short beeps.

1. Connect iButton® key reader contact wires to 1-Wire® interface: **COM** and **DATA** contacts respectively.
2. Connect mini buzzer negative contact wire to **BUZ-** and positive contact wire to **BUZ+.**
3. Additionally, a LED indicator for visual indication can be installed in parallel to mini buzzer or instead. Connect LED anode contact to **BUZ-** and cathode to **BUZ+**.

NOTE: The installation of mini buzzer is not necessary if EKB/EKB3 keyboard is used.

ATTENTION: The wire length for connection to 1-Wire® interface can be up to 30 meters max.

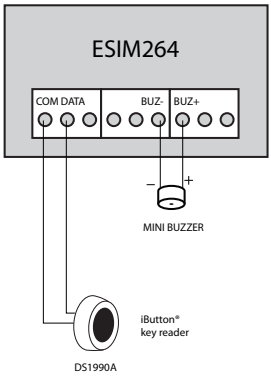


Fig. No. 5

2.3.5 Temperature Sensor & iButton® Key Reader

Supported iButton® Key Model: Maxim®/Dallas® DS1990A
Supported Temperature Sensor Model: Maxim®/Dallas® DS18S20, DS18B20

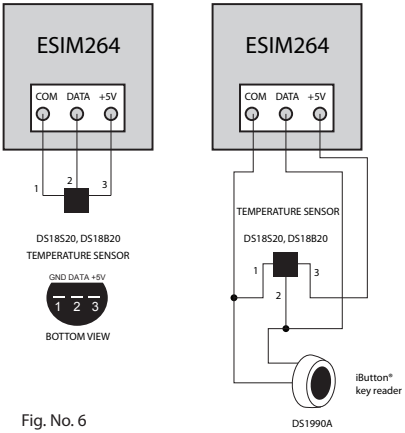


Fig. No. 6

1. Connect temperature sensor **1, 2, 3** contacts to 1-Wire® interface: **COM**, **DATA** and **+5V** contacts respectively.
2. When connecting iButton® key reader in parallel to temperature sensor, connect iButton® key reader contact wires to **COM** and **DATA** contacts respectively.

ATTENTION: The wire length for connection to 1-Wire® interface can be up to 30 meters max.

2.3.6 Relay Finder® 40.61.9.12 with Terminal Socket 95.85.3

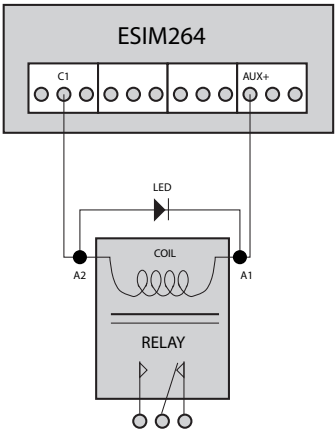


Fig. No. 7

1. Wire up relay **A2** contact to PGM output **Cx** and **A1** contact to **AUX+**.
2. In addition, connect LED **anode** contact to relay **A2** contact and **cathode** to **A1** contact.

2.3.7 Keyboards

Parallel Wiring

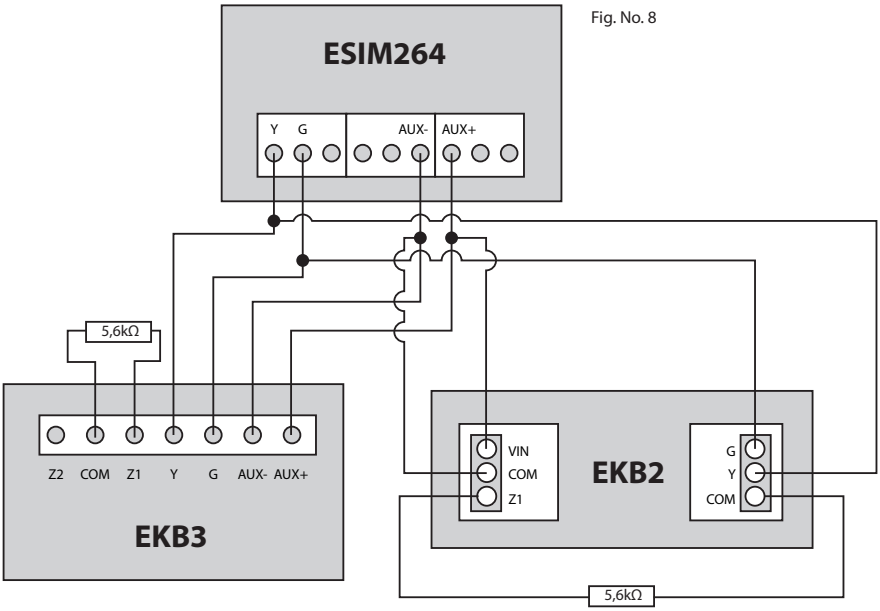


Fig. No. 8

ATTENTION: When wiring more than 1 keyboard, please, make sure that the set address of each keyboard is different.

NOTE: You may connect only 1 EKB2/EKB3 keyboard or a mixed combination of EKB2 and EKB3 keyboards. The combination can consist of up to 4 keyboards in total.

For more details, please, refer to chapters **7.1 EKB2 - LCD Keyboard** and **7.2 EKB3 - LED Keyboard**

Serial Wiring

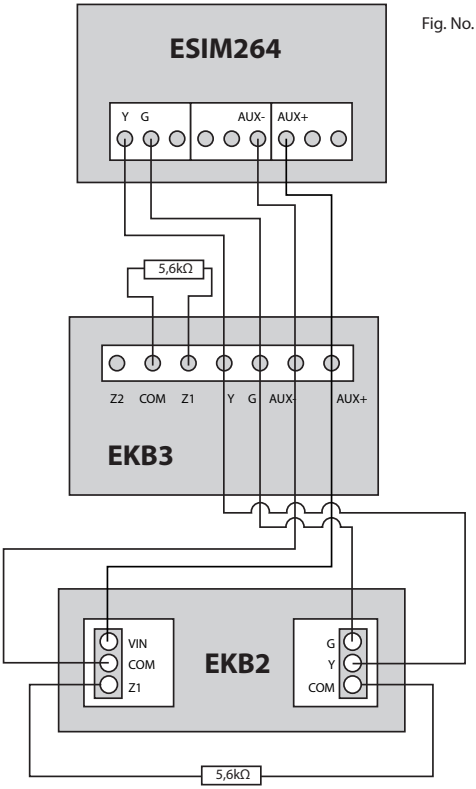


Fig. No. 9

ATTENTION: When wiring more than 1 keyboard, please, make sure that the set address of each keyboard is different.

NOTE: You may connect only 1 EKB2/EKB3 keyboard or a mixed combination of EKB2 and EKB3 keyboards. The combination can consist of up to 4 keyboards in total.

For more details, please, refer to chapters **7.1 EKB2 - LCD Keyboard** and **7.2 EKB3 - LED Keyboard**

3. Installation

The system can be installed only in a metal or non-flammable enclosure. When using the metal enclosure it is necessary to ground it using yellow/green colour cable. For the connection of 230V transformer use 3x0.75 mm^2 1 thread double isolated cable. The primary circuit of the transformer must be connected through 0.5A fuse. 230V power supply cables must not be grouped with low voltage cable group. For the connection of power supply and output connectors use 1 thread 2x0.75 mm^2 cable. For the connection of zone/PGM output connectors use 0.50 mm^2 1 thread cable.

1. Place the SIM card into the card holder and make sure that PIN code request is disabled. The PIN code can be disabled by inserting the SIM card into a mobile phone and following proper menu steps. There must be no SMS messages stored in the memory.

   ATTENTION: The system is NOT compatible with pure 3G SIM cards. Only 2G SIM cards and 3G SIM cards with 2G profile enabled are supported. For more details, please, contact your GSM operator.

2. Connect the antenna.
3. Install the mini buzzer close to iButton® key reader (if any) in order to hear alarm system arming and disarming countdown period. A LED can be used in parallel to mini buzzer, or both at once. ED1 is recommended for convenient installation.
4. Wire up the system according to the wiring diagrams. See chapter **2.3 Wiring Diagrams** for more details.
5. Connect the resistors and sensors to the system according to one of the selected zone connection types. See chapter **2.3.2 Zone Connection Types** for more details.
6. Connect the backup battery and main power supply (transformer).
7. The system starts up in less than a minute. LED **PWR** indicates main power supply status. LED **STATUS** should be blinking indicating successful micro-controller operation. In addition, the system sends an SMS message to a preset User 1 phone number.
8. System is ready for use.

The installation of iButton® key reader, EKB2/EKB3, EWK1 wireless key-fob is not mandatory. However it is recommended to have those devices installed as an emergency switch in case your mobile phone is switched off or missing.

To increase system reliability, it is recommended not to use prepaid SIM cards. The system would fail to send any messages upon depletion of prepaid account. In addition it is recommended to disable call forwarding and voice mail feature.

It is highly recommended to choose the same GSM cellular provider both for users and for ESIM264 system in order to assure fast and reliable SMS message delivery and phone call connection.

Even though alarm system ESIM264 installation process is not too complicated, we still recommend to perform it by a person with basic knowledge in electrical engineering and electronics to avoid any system damage.

4. Operation Description

4.1 Arming & Disarming

ESIM264 alarm system arming and disarming process can be performed:

- by entering a valid 1 out of 10 user (keyboard) passwords using EKB2/EKB3 keyboard;
- by making a free call to the system from any out of 5 preset user phone numbers;
- by sending an SMS message to the system from any out of 5 preset user phone numbers (possible to arm/disarm both system partitions at once);
- by touching 1 out of 5 iButton® keys to a reader;
- using EWK1 wireless key-fob;
- by violating/restoring a zone set up to operate under *Arm-Disarm by Zone* mode;
- using *EGR100* GPRS software at the monitoring station site.

The system initiates the *Exit Delay* countdown intended for user to leave the secured area when the system is being armed. During the countdown period the mini buzzer (if any) is providing short beeps and/or LED (if any) is providing illumination signals. By default, *Exit Delay* duration is 15 seconds. After the countdown is complete the system becomes armed and locks the configuration possibility by keyboard (if any). In case the user does not leave the secured area before the countdown is complete, the system switches to Stay mode if at least 1 zone is set up to operate under Stay mode. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the alarm system until the violated zone or tamper is restored. In case it is required to arm the alarm system despite the violated zone presence, the violated zone can be bypassed or set up to operate under *Force* mode.

The system initiates the *Entry Delay* countdown intended for system disarming after the user enters the secured area. The mini buzzer (if any) is providing short beeps and/or LED (if any) is providing illumination signals during the countdown period . By default, *Entry Delay* duration is 15 seconds. The system unlocks the keyboard (if any) after the user successfully performs the disarming process. The alarm will be caused in case the user does not disarm the alarm system during the *Entry Delay* countdown.

NOTE: There is no *Exit Delay* countdown when arming the alarm system by phone call, SMS message or *EGR100* GPRS software.

For more details, please, refer to chapter **5.4.5 Arming & Disarming the System.**

4.2 Zones

ESIM264 alarm system has 6 built-in on-board zones with expansion possibility for additional sensor connection. The number of zones can be expanded by:

- enabling the ATZ mode which doubles the on-board zone quantity;
- connecting EPGM1 - zone & PGM output expansion module;
- connecting the keyboards;
- adding the wireless devices;
- creating the virtual zones manually.

The maximum supported zone quantity is 44.

ESIM264 zones are classified by 5 categories:

Zone Category	Description	Max. Quantity of Zones per Device	Max. Quantity of Zones in Total
On-board Zones	Built-in wired zones of ESIM264 alarm system.	6/12*	6/12*
Keyboard Zones	Built-in wired zones of EKB2/EKB3 keyboard.	1	4
EPGM1 Zones	Built-in wired zones of EPGM1 - zone & PGM output expansion module.	16	16
Wireless Zones	Non-physical zones automatically created by connected wireless devices.	2**	32***
Virtual Zones	Non-physical zones intended for alarm activation by EWK1 wireless key-fob and manually created by the user using ELDES Configuration Tool.	32****	32****

* - 6 zone-mode is enabled by default. ATZ mode doubles the zone quantity and increases it to 12 in total.
** - Depends on the connected wireless device.
*** - Available only if no keyboard zones, EPGM1 zones and virtual zones are present.
**** - Available only if no keyboard zones, EPGM1 zones and wireless zones are present.

Any zone can be set up to operate under one of these types:

- **Follow** – *Follow* zone is inactive and alarm is not caused during *Entry/Exit Delay* countdown. In case of *Follow* zone violation before *Exit Delay* countdown the alarm is caused immediately. This zone type is usually used in case it is necessary to violate this zone in the secured area during *Entry/Exit Delay* countdown.
- **Instant –** After the system is armed, the alarm is caused instantly in case of Instant zone violation. This zone type is usually used for door, window and other sensors.
- **Delay** – In case of *Delay* zone violation the alarm is not caused for a set period of time - *Entry/Exit Delay* countdown. In case the zone of this type is not violated during arming process, the system enters into *Stay* mode. It is highly recommended to use this zone type at entrance/exit points of secured areas.
- **24H** – This zone type is intended for securing the areas which require monitoring *24/7*. In case of *24H* zone violation the alarm is caused even when the alarm system is disarmed.
- **Fire** – This zone type is intended for fire/smoke detectors and is always active. The alarm is caused even when the alarm system is disarmed. *Fire* zone alarm is pulse type (with pauses).
- **Silent** – *Silent* zone type operates in the same way as *24H* zone type, but in case of alarm the siren is not activated.

Any zone can be set up to operate under these modes:

- **Stay** – This mode enables the user to arm and disarm the alarm system while staying inside the secured area. The system goes into *Stay* mode in case the *Delay* zone is not violated during the *Exit Delay* countdown (the user does not leave the secured area). In case a zone operating under *Stay* mode is violated after the alarm system is armed, the alarm is not caused. *Stay* mode is not activated if the user leaves the secured premises during *Exit Delay* countdown or if none of the zones are configured to operate under *Stay* mode. This mode is not supported by virtual zones.
- **Force** - This mode allows the user to arm the alarm system even if the zone operating under *Force* mode is violated. This zone begins operating according to its' type and does not ignore violation after the system is armed and the zone is restored.
- **Arm-Disarm by Zone** – This mode allows to set up a zone for arming and disarming the alarm system when the zone gets violated and restored. This process is performed by providing a "low" level pulse longer than 3 secs. into the specified zone. It means that violating and restoring the zone leads to system arming and by repeating this action the system becomes disarmed. This mode can be set up for 1 on-board zone only.
- **Delay Zone becomes Instant in Stay Mode** - Every *Delay* zone can operate and act as *Instant* when the system is operating in *Stay* mode. When the alarm system is operating in normal mode, the *Delay* zone operates as described above.

For more details, please, refer to *ELDES Configuration Tool* software's HELP section and chapter **5.4.6 Zones.**

4.3 Programmable Outputs (PGM)

The system ESIM264 has 4 built-in on-board PGM outputs allowing to connect and control various electrical appliances: water pumps, heating, lighting, blinds etc. The number of PGM outputs can be expanded by:

- connecting EPGM8 - PGM output expansion module;
- connecting EPGM1 - zone & PGM output expansion module;
- adding the wireless devices.

The maximum supported PGM output quantity is 44.

ESIM264 PGM outputs are classified by 4 categories:

PGM Output Category	Description	Max. Quantity of PGM Outputs per Device	Max. Quantity of PGM Outputs in Total
On-board PGM Outputs	Built-in wired PGM outputs of ESIM264 alarm system.	4	4
EPGM8 PGM Outputs	Built-in wired PGM outputs of EPGM8 - PGM output expansion module.	8	8
EPGM1 PGM Outputs	Built-in wired PGM outputs of EPGM1 - zone & PGM output expansion module.	2	2
Wireless PGM Outputs	Non-physical PGM outputs automatically created by connected wireless devices.	2*	32**

* - Depends on the connected wireless device.
** - Available only if no EPGM1 PGM outputs and no EPGM8 PGM outputs are present.

For more details, please, refer to *ELDES Configuration Tool* software's HELP section and chapter **5.4.7 PGM Outputs.**

4.4 Wireless Devices

ESIM264 with installed EWT1 module operates as an access point for ELDES wireless devices: PIR movement sensor EWP1, expansion module EW1, sirens EWS1 & EWS2, magnetic door contact EWD1 and key-fob EWK1. Up to 16 ELDES wireless devices located at up to 30 meters (up to 150 meters in open areas) radius range from ESIM264 alarm system with EWT1 can be connected at a time. According to wireless device type and quantity the system adds wireless zones (RF zones) and wireless PGM outputs (RF outputs), therefore totally 32 wireless zones and/or 32 wireless PGM outputs can be added to the system. ELDES wireless connection operates at 868MHz non-licensed frequency. For more details, please, refer to chapter **8. ELDES Wireless Devices.**

4.5 RS485 Interface

ESIM264 has an RS485 interface supporting up to 4 EKB2 and/or EKB3 keyboards. This feature allows to install more than one alarm system control point in the secured area in order to be able to arm and disarm the alarm system at several entrance points.

The RS485 interface is also intended for EPGM1 module connection and data channel connection to monitoring station.

For more details, please, refer to chapter **7. Wired Devices.**

4.6 1-Wire® Interface

The implemented 1-Wire® interface enables the iButton® key reader connection to ESIM264. The system supports unlimited quantity of iButton® key readers. For more details, please, refer to chapter **7.7 iButton® Key Reader & Keys.**

1-Wire® interface is also intended for temperature sensor connection. Only 1 temperature sensor can be connected to ESIM264 system. For more details, please, refer to chapter **5.4.12 Temperature Change Notifications.**

In order to assure a stable signal between the connected iButton® reader/temperature sensor and 1-Wire® interface, the cable length must not exceed 30 meters.

4.7 Backup Battery, Main Power Failure & Memory

The system supports a backup battery maintaining system power supply in case of main power failure. In addition the implemented battery status feature checks the backup battery resistance once a day and sends an SMS report to all preset users on battery replacement in case more than 1,5Ω resistance is detected. This feature is permanently enabled and cannot be disabled manually.

NOTE: Backup battery is optional and does not come in standard package.

The configuration settings and event log records are stored in a built-in EEPROM memory, therefore even in case of full system shut down, the configuration and event log remains saved.

ATTENTION: It is forbidden to switch backup battery pole terminals places, otherwise this will lead to blown fuse.

For more details, please, refer to chapter **5.4.13 Main Power Supply Status Notifications.**

4.8 Communication with Monitoring Station

GSM alarm system ESIM264 supports data transmission to monitoring station by the following methods: Voice Calls (GSM audio channel), GPRS network, RS485 data channel or CSD (Circuit Switched Data). All of these data transmission methods can be set as primary or backup communication in any sequence order. For more details, please, refer to HELP section of *ELDES Configuration Tool* and chapter **9. Monitoring Station.**

4.9 GSM Loss Indication

ESIM264 alarm system features an indication when the GSM signal is lost. In case of such failure, the system not only turns off the **NETWORK** LED, but also turns on the specified PGM output if the GSM signal is lost for longer period than the set delay value. The PGM output is turned of once the GSM signal is restored. This feature can be configured using *ELDES Configuration Tool* software. For more details, please, refer to software's HELP section.

4.10 Partitions

ESIM264 supports 2 partitions (**PART0** - partition 0 & **PART1** - partition 1) dividing the alarm system into 2 separate system sections. Every system partition operates independently from each other, therefore this feature is useful for securing 2 different areas by using 1 alarm system unit. By default all users, zones, user (keyboard) passwords, keyboards, iButton® keys are assigned to partition 0. For more details, please, refer to chapter **5.4.16 Partitions.**

5. Configuration & Control

ATTENTION! In this user manual the underscore symbol "_" represents one <space> character. Every underscore symbol must be replaced by a single <space> character. There must be no <spaces> or other unnecesary characters at the beginning and at the end of the message. **XXXX** – 4-digit SMS password (the default SMS password is **0000** – four zeros).

The system configuration and control can be performed by sending SMS messages to ESIM264 phone number, using EKB2 keyboard, EKB3 keyboard, via USB or GPRS connection remotely using *ELDES Configuration Tool* software, which is recommended for quick and more convenient system configuration.

5.1 Primary System Configuration

1. Connect the main power supply and wait until **PWR** LED lights up.
2. The illuminated **NETWORK** LED indicates that the system successfully registered to GSM network.
3. Find the best GSM antenna position by following **NETWORK** LED indications in order to get the strongest GSM signal. Possible indications are mentioned in the table.
4. Set the language. See chapter **5.4.1 SMS Language** for more details.
5. Change the default SMS password. See chapter **5.4.2 Passwords** for more details.
6. Set the phone number for User 1. See chapter **5.4.3 User Phone Numbers** for more details.

NETWORK LED Indication	GSM Signal Strength
OFF	No GSM signal
Flashing every 3 sec.	Poor
Flashing every 1 sec.	Medium
Flashing several times per sec.	Good
Solid ON	Excellent

After completing these steps the system is ready for further configuration.

If you fail to receive an SMS reply from the system, please, check the SMS centre phone number.

Set SMS Centre Phone Number

SMS centre phone number is stored in a SIM card by the GSM operator, therefore if the SIM card has already been successfully used to send SMS messages from a mobile phone, then it is not necessary to change the SMS centre number.

SMS

SMS text:
0000_SMS_+37011111111
Example: 0000_SMS_+37069899992

5.2 Ways of System Configuration

SMS

In order to configure and control the system using SMS message, send the text command to the ESIM264 system phone number from one of the preset user phone numbers. The structure of SMS message consists of 4 digit SMS password (the default SMS password is **0000** – four zeros), the parameter and value. For some parameters the value does not apply, i.e. STATUS.

EKB2

The system configuration and control with EKB2 keyboard is performed by navigating throughout the menu section list displayed on LCD screen. To navigate in the menu path, touch ↓, ↑ keys to select the desired menu section and touch OK key to open the selected section. To enter a required value, use 0... 9 keys and touch OK key for value confirmation or cancel/go one menu section back by touching ← key. The value can be typed in directly by touching 0... 9 keys while highlighting the desired menu section. EKB2 menu type is "circle", therefore when the last section in the menu list is selected, you will be brought back to the beginning of the list after pressing the ↓ key. In this installation manual, the menu path is provided under "tree" view by starting at main screen view. Valid parameter values and range are indicated in brackets.

NOTE: Menu section **CONFIGURATION** is secured with administrator password. The default administrator password is **1470**.

EKB3

The system configuration and control with EKB3 keyboard is performed by activating the **Configuration Mode** using the administrator password (the default administrator password is **1470**) and entering a valid configuration command using the number keys (0... 9) and [#] key for confirmation. The indication of each pressed key is provided by zone red LEDs when entering a configuration command. The structure of standard configuration command is a combination of digits. EKB3 configuration command and valid parameter value range are indicated in brackets.

Configuration Mode

This command activates and deactivates the **Configuration Mode.**

EKB3

Enter administrator password:

[*xxxx#]

Value: xxxx – 4-digit adiministrator password.

EKB3 indications which are relevant during **Configuration Mode** are described in the table below.

Indication	Description
Red LED **ARMED** flashing	Configuration mode activated successfully.
Yellow LED **SYSTEM** flashing	Valid parameter is entered and waiting for value.
1 Long Beep	Non-existing command or parameter value entered.
3 Short Beeps	Command entered successfully.

NOTE: The system can be configured using one keyboard at a time only. Other connected keyboards become inactive in **Configuration Mode.**

CONFIGURATION TOOL

Software *ELDES Configuration Tool* is intended to work directly with ESIM264 alarm system, which can be connected to the computer via USB port or via GPRS connection remotely. This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use *ELDES Configuration Tool*, please, read user guide available in the software's HELP section.

ELDES Configuration Tool is freeware and can be downloaded from ELDES website at: www.eldes.lt

5.3 Remote System Configuration via GPRS Connection

Before configuring ESIM264 remotely via GPRS connection, make sure that:

- SIM card is inserted into ESIM264 device.
- Mobile internet service is enabled on the SIM card.
- Power supply is connected to ESIM264.
- Default SMS password is changed to a new 4-digit password;
- At least User1 phone number is set up.

5.3.1 Establishing Remote Connection Between ESIM264 System and Configuration Server

Initiate the Connection to ELDES Server

In order to activate a remote GPRS connection between ESIM264 system and ELDES configuration server, please, send the following SMS message from user phone number.

Upon the successful SMS message delivery, the system establishes a connection session for 20 minutes. An SMS reply, containing device IMEI number and confirming a successful connection establishment, is sent shortly.

SMS

SMS text:
XXXX_stconfig
Example: 1111_stconfig

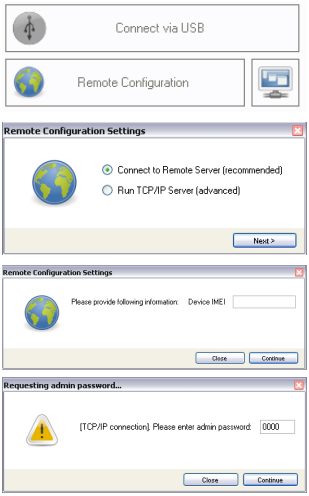
Initiate the Connection to Third-Party Server

In case it is necessary to establish a connection between ESIM264 system and a third-party configuration server, send the following SMS message.

SMS

SMS text:
XXXX_stconfig:IPaddress:Port
Value: Ipaddress – public IP address of third-party configuration server; Port – port number of third-party configuration server
Example: 1111_stconfig:62.80.115.102:4522

5.3.2 Connecting to ELDES Configuration Server using *ELDES Configuration Tool* Software



5.3.2.1 Run *ELDES Configuration Tool* software.

5.3.2.2 Press **Remote Configuration** button.

5.3.2.3 In the next window, select **Connect to Remote Server (recommended)** and press **Next** button.

5.3.2.4 Enter the received IMEI number in **Device IMEI** entry.

5.3.2.5 Press **Continue** button.

5.3.2.6 Upon the successfully established connection, the system prompts for an administrator password.

5.3.2.7 By entering a valid administrator password, the system grants access to full configuration remotely..

5.3.2.8 **Remote Configuration Management** window displays all performed configuration actions.

5.3.3 Ending the Configuration Process

Shut down the Connection with the Server

After the system configuration is complete, use one of the following methods to end the configuration process:
- Press Disconnect button and close *ELDES Configuration Tool* software;
- Wait for the system to reply with an SMS message confirming the end of the session;
- Shut down the connection with the server at any time by sending an SMS message.

SMS

SMS text:
XXXX_endconfig
Example: 1111_endconfig

5.4 Parameter Configuration Set (SMS, EKB2, EKB3)

5.4.1 SMS Language

Set SMS Language

This command sets the language for SMS message replies. The user is is allowed to switch between two languages only - the default language (depending on his/her location) and English.

EKB2 keyboard menu language depends on default language of the system firmware.

SMS

SMS text:
LL
Value: LL – system language, possible values – LT, RU, EN, EE, LV, CZ, SK, GR, FI
Example: EN

EKB2

Menu path:
OK → CONFIGURATION →PRIMARY SET →SMS LANGUAGE →LITHUANIAN / RUSSIAN / ENGLISH / ESTONIAN / LATVIAN / CZECH / SLOVAKIAN / GREEK / FINNISH

EKB3

Enter parameter 35 and language index number:
[3500#] - Lithuanian
[3501#] - Russian
[3502#] - English
[3503#] - Estonian
[3504#] - Latvian
[3505#] - Czech
[3506#] - Slovakian
[3507#] - Greek

NOTE: In order to change the SMS language in a configured system (after changing the SMS password), please, use *ELDES Configuration Tool* software.

5.4.2 Passwords

NOTE: All passwords consist of 4 digits. Non-numerical characters like letters, dots, colons, spaces are not allowed.

Set SMS Password

The 4-digit SMS password intended for system configuration and control by SMS messages. Manufacturer default SMS password is **0000** (four zeros) which is NECESSARY to change.

SMS

SMS text:
YYYY_PSW_XXXX
Value: YYYY – old 4-digit password, range - [0000... 9999]; XXXX – new 4-digit password, range - [0000... 9999]
Example: 0000_PSW_1111

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → PASSWORD → PSW FOR SMS → [XXXX]
Value: [XXXX] – 4-digit SMS password, range - [0000... 9999]

EKB3

Enter parameter 14 and SMS password:
[14xxxx#]
Value: xxxx – 4-digit SMS password, range - [0000... 9999]

Set User (Keyboard) Password

4-digit password intended for arming and disarming the alarm system using a keyboard. Up to 10 different user (keyboard) passwords can be set. Newly added user (keyboard) password is automatically assigned to the same partition as the keyboard. The default user (keyboard) password1 is **1111** and it is pre-assigned to partition 0.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → PASSWORD → KEYBOARD PSW → PSW [1... 10] → PASSWORD → [XXXX]
Value: [XXXX] – 4-digit user (keyboard) password, range - [0000... 9999]

EKB3

a) Enter parameter 63, old user (keyboard) password & new user (keyboard) password:
[63yyyyxxxx#]
Value: yyyy – old user (keyboard) password, range – [0000... 9999]; xxxx – new user (keyboard) password, range – [0000... 9999].

b) Enter parameter 15, user (keyboard) password number & new user (keyboard) password:
[15yyxxxx#]
Value: yy – user (keyboard) password number, range – [01... 10]; xxxx – new user (keyboard) password, range – [0000... 9999]

NOTE: The system does not allow to add a duplicate password.

Delete User (Keyboard) Password

This command erases a particular user (keyboard) password. It is possible to delete the password assigned to the same partition as the keyboard only.

SMS: N/A

EKB2: **Menu path:**
OK → CONFIGURATION → PRIMARY SET → PASSWORD → KEYBOARD PSW → REMOVE PSW → [XXXX]
Value: [XXXX] – 4-digit user (keyboard) password, range - [0000... 9999]

EKB3: **Enter parameter 65 & user (keyboard) password:**
[65xxxx#]
Value: xxxx – 4-digit user (keyboard) password, range - [0000... 9999]

See also chapter **5.4.16 Partitions.**

Set Administrator Password

The 4-digit administrator password providing access to system configuration. It is recommended to change the default admin password which is **1470**.

SMS: N/A

EKB2: **Menu path:**
OK → CONFIGURATION → PRIMARY SET → PASSWORD → ADMIN PSW → [XXXX]
Value: [XXXX] – 4-digit administrator password, range - [0000... 9999]

EKB3: **Enter parameter 16 & administrator password:**
[16xxxx#]
Value: xxxx – 4-digit administrator password, range - [0000... 9999]

Set Duress Password

This command assigns one of the user (keyboard) passwords which is used in case of alarm system disarm demanded by force. The system also sends a silent alert data message to monitoring station after system disarming using this password.

SMS: N/A

EKB2: **Menu path:**
OK → CONFIGURATION → PRIMARY SET → PASSWORD → KEYBOARD PSW → DURESS PSW → N/A / [1... 10]

EKB3: **Enter parameter 73 & user (keyboard) password number:**
[73xx#]
Value: xx – user (keyboard) password number, range - [01... 10]

Set Security Guard Service Password

This command assigns one of the user (keyboard) passwords which is used to notify the monitoring station about the arrival of security guards. The system transmits a data message to the monitoring station and disarms the alarm system after entering this password.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → PASSWORD → KEYBOARD PSW → SGS PSW → N/A / [1... 10]

EKB3

Enter parameter 74 & user (keyboard) password number:
[74xx#]
Value: xx – user (keyboard) password number, range - [01... 10]

5.4.3 User Phone Numbers

Set User Phone Number

The system supports up to 5 authorized phone number entries allowing system configuration and control by SMS. User 1 phone number is mandatory while other phone number entries are not necessary. All numbers must be entered starting with international country code e.g. 44[area code][local number]. The plus symbol is not necessary.

SMS

SMS text:
XXXX_NR1:YYYYYYYYYYYYYYY_NR2:VVVVVVVVVVVVVVV_ NR3:ZZZZZZZZZZZZZZZ_ NR4:UUUUUUUUUUUUUUU_NR5:NNNNNNNNNNNNNNN
Value: YYYYYYYYYYYYYYY – up to 15 digits user phone number
Example: 1111_NR1:441111111111

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5] → NUMBER → [XXXXXXXXXXXXXXX]
Value: [XXXXXXXXXXXXXXX] – up to 15 digits user phone number

EKB3

Enter parameter 17, user number & phone number:
[17xxYYYYYYYYYYYYYYY#]
Value: xx – user number, range – [1... 5]; YYYYYYYYYYYYYYY – up to 15 digits user phone number

Delete User Phone Number

This command erases the particular user phone number. The system will not allow erasing of the User 1 phone number. This number can only be modified.

SMS

SMS text:
XXXX_NR2:DEL_NR3:DEL_NR4:DEL_NR5:DEL
Example: 1111_NR3:DEL

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5] → NUMBER → OK → OK

EKB3

N/A

List User Phone Numbers

This feature allows to check the list of added user phone numbers to the system.

SMS

SMS text:
XXXX_HELPNR
Example: 1111_HELPNR

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5]

EKB3

N/A

See also chapter **5.4.16 Partitions.**

5.4.4 Date & Time

Set Date & Time

In order to receive SMS messages containing correct date and time, please, set date and time of the system.

SMS

SMS text:
XXXX_YYYY.MM.DD_HH:MM
Value: YYYY– year; MM – month, range – [01... 12]; DD – day, range - [01... 31]; HH – hours, range – [00... 23], MM – minutes, range – [00... 59].
Example: 1111_2011.12.15_13:45

EKB2

Menu path:
a) OK → DATE/TIME SET → [YYYY-MM-DD HH:MM]
b) OK → CONFIGURATION → PRIMARY SET → DATE/TIME SET → [YYYY-MM-DD HH:MM]
Value: YYYY– year; MM – month, range – [01... 12]; DD – day, range - [01... 31]; HH – hours, range – [00... 23], MM – minutes, range – [00... 59].

EKB3

Enter parameter 66, date & time:
[66yyyymmddhhmm#]
Value: yyyy– year; mm – month, range – [01... 12]; dd – day, range - [01... 31]; hh – hours, range – [00... 23], mm – minutes, range – [00... 59].

NOTE: When the alarm system is connected to a monitoring station the date and time are set automatically. The system retrieves this information from the monitoring station.

5.4.5 Arming & Disarming the System

Arm the System

This command arms the alarm system.

SMS: it is possible to arm system partition 0, partition 1 or both partitions at once despite the assigned partition to user phone number.

EKB2/EKB3: The default user (keyboard) password1 is **1111**. *Keyboard partition* switch feature allows to arm the system partitions one after another using 1 keyboard.

SMS text:
XXXX_ARM1 or XXXX_ARM1,2
Value: 1 - system partition 0; 2 - system partition 1
Example: 1111_ARM1,2

Enter user (keyboard) password:
[NNNNN]
Value: NNNNN - 4-digit user (keyboard) password

Enter user (keyboard) password:
[nnnnn]
Value: nnnnn - 4-digit user (keyboard) password

Disarm the System

This command disarms the alarm system.

SMS: it is possible to disarm system partition 0, partition 1 or both partitions at once despite the assigned partition to user phone number.

EKB2/EKB3: The default user (keyboard) password1 is **1111**. *Keyboard partition* switch feature allows to disarm the system partitions one after another using 1 keyboard.

SMS text:
XXXX_DISARM1 or XXXX_DISARM1,2
Value: 1 - system partition 0; 2 - system partition 1
Example: 1111_DISARM2

Enter user (keyboard) password:
[NNNNN]
Value: NNNNN - 4-digit user (keyboard) password

Enter user (keyboard) password:
[nnnnn]
Value: nnnnn - 4-digit user (keyboard) password

See also chapter **5.4.16 Partitions.**

Enable *Arm-Disarm by Zone*

This feature allows to set a zone for arming and disarming the alarm system when the zone gets violated and restored. Violating and restoring the zone leads to system arming and by repeating this action the system becomes disarmed. This mode can be set for 1 on-board zone only.

6-zone mode (ATZ mode disabled): a 5.6kΩ resistor is required for the set zone.

ATZ mode: a 5.6kΩ resistor is required for Z1-Z6 zones and additionally a 3.3kΩ resistor is required for Z7-Z12.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ZONES → ARM/DISARM BY ZONE → ZONE [1... 12]

EKB3

Enter parameter 34 & zone number :
[34xx#]
Value: xx – zone number, range – [01... 12]

Disable *Arm-Disarm by Zone*

This command disables *Arm-Disarm by Zone* mode.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ZONES → ARM/DISARM BY ZONE → N/A

EKB3

Enter parameter 34 & parameter status value :
[3400#]

See also chapter **2.3.2 Zone Connection Types**

5.4.6 Zones

NOTE: Colons, semi-colon characters, parameter names and/or values are not allowed in zone alarm texts, eg. PSW, STATUS, ON, OFF etc.

Set Zone Alarm Text

Each secured zone has an alarm text which is sent by SMS message in case of alarm. Manufacturer default zone alarm text: *Z1 - Door sensor triggered, Z2 - Windows sensor triggered, Z3 - Fire sensor triggered, Z4 - Motion1 sensor triggered, Z5 - Motion2 sensor triggered, Z6 - Motion3 sensor triggered etc.*

Alarm text can be edited by SMS or *ELDES Configuration Tool* software only. The length of zone alarm text for each zone can be up to 24 characters including <space> symbol.

SMS

SMS text:
XXXX_Z1:NewAlarmText;Z2:NewAlarmText;Z3:NewAlarmText;
Z4:NewAlarmText;Z5:NewAlarmText;Z6:NewAlarmText;Zn:NewAlarmText

EKB2

Menu path:
OK → CONFIGURATION → ZONES → WIRED ZONES → ZONE [1... 12] → NAME
OK → CONFIGURATION → ZONES → WIRELESS ZONES → RF ZONE [1... 16] → NAME
OK → CONFIGURATION → ZONES → KEYBOARD ZONES
→ [1ST... 4TH] KEYBOARD ZONE → NAME
OK → CONFIGURATION → ZONES → EPGM ZONES → EPGM ZONE [1... 16] → NAME

EKB3

N/A

List Violated Zones

This feature provides the list of violated zones.

SMS

Please, refer to chapter **5.4.9 Info SMS.**

EKB2

Menu path:
OK → VIOLATED ZONES → ZONE [1... 44]

EKB3

For violated zone Z1 - Z12 indication, please, check the zone LED indicators on EKB3 device. For violated high zone Z13 - Z44 indication, please, refer to chapter **6.1 Trouble Indication.**

NOTE: Due to security reasons it is recommended to restore the violated zone before arming the alarm system. In order to arm the alarm system despite violated zone presence, you can set tup the zone to operate under Force mode or bypass it.

List Violated Tampers

This feature provides the list of violated tampers.

SMS

The system notifies by SMS containing violated tamper number (unless tamper name is erased).

EKB2

Menu path:
TAMPERS -> TAMPER [1... 44]

EKB3

[CODE2]
For violated tamper 13 - 44 indication, please, refer to chapter **6.1 Trouble Indication.**

Set *Entry Delay*

Entry Delay is a period of time intended to disarm the alarm system after the user enters the secured area (after *Delay* zone is violated). The alarm will be caused in case the system is not disarmed during this period of time. By default, *Entry Delay* duration is 15 seconds and *Delay* zone is Z1.

SMS

SMS text:
XXXX_INOUT:YY:ZZ
Value: YY - *Entry Delay* duration in seconds, range - [0... 65535]; ZZ - *Exit Delay* duration in seconds, range - [0... 600]
Example: 1111_INOUT:25:14

EKB2

Menu path:
OK → CONFIGURATION → ZONES → WIRED ZONES → ZONE [1... 12] → ENTRY DELAY → [XXXXX]
OK → CONFIGURATION → ZONES → WIRELESS ZONES → RF ZONE [1... 16] → ENTRY DELAY → [XXXXX]
OK → CONFIGURATION → ZONES → KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → ENTRY DELAY → [XXXXX]
OK → CONFIGURATION → ZONES → EPGM ZONES → EPGM ZONE [1... 16] → ENTRY DELAY → [XXXXX]
Value: [XXXXX] – *Entry Delay* duration in seconds, range - [0... 65535]

EKB3

Enter parameter 54, zone number & entry delay duration:
[54xxyyyyy#]
Value: [XXXXX] – *Entry Delay* duration in seconds, range - [0... 65535]

Set *Exit Delay*

Exit Delay is a period of time intended for user to leave the secured area. The system begins the countdown after the arming process initiation. The default *Exit Delay* duration is **15** seconds.

SMS

XXXX_INOUT:YY:ZZ

Value: YY - *Entry Delay* duration in seconds, range - [0... 65535]; ZZ - *Exit Delay* duration in seconds, range - [0... 600]

Example: 1111_INOUT:25:14

EKB2

Menu path:

OK → CONFIGURATION → PRIMARY SETTINGS → EXIT DELAY → [XXX]

Value: [XXX]– *Exit Delay* duration in seconds, range – [0... 600]

EKB3

Enter parameter 72 & exit delay duration:

[72xxz#]

Value: xxx – *Exit Delay* duration in seconds, range – [0... 600]

Enable ATZ Mode

ATZ mode activates zone duplication increasing number of on-board zones from 6 to 12. By default ATZ mode is disabled.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → ATZ MODE → ENABLE

EKB3

Enter parameter 28 & parameter status value:

[281#]

Disable ATZ Mode

This command disables ATZ mode.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → ATZ MODE → DISABLE

EKB3

Enter parameter 28 & parameter status value:

[280#]

Set Zone Connection Type when ATZ Mode Disabled

Specify zone aconnection type when ATZ mode is disabled. Available types:

Type 1 – Normally open (NO) contact with 5,6KΩ end-of-line resistor.

Type 2 – Normally closed (NC) contact with 5,6KΩ end-of-line resistor

Type 3 – Tamper and 5,6KΩ end-of-line resistor and 3,3KΩ end-of-line resistor with normally closed (NC) contact

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ZONES → ZONE MODE NO ATZ → TYPE [1... 3]

EKB3

Enter parameter 38 & zone mode:
[381#] - Type 1
[382#] - Type 2
[383#] - Type 3

Set Zone Connection Type when ATZ Mode Enabled

Specify zone connection type when ATZ mode is enabled. Available types:

Type 4 – 5,6KΩ end-of-line resistor and normally closed (NC) contact with 3,3KΩ end-of-line resistor and normally closed (NC) contact.

Type 5 – Tamper and 5,6KΩ end-of-line resistor and 5,6KΩ end-of-line resistor with normally closed (NC) contact and 3,3KΩ end-of-line resistor with normally closed (NC) contact.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ZONES → ZONE MODE ATZ → TYPE [4... 5]

EKB3

Enter parameter 39 & zone mode:
[391#] - Type 4
[392#] - Type 5

See also chapter **2.3.2 Zone Connection Types.**

Disable Zone

This command disables a particular zone. By default, all on-board zones, EPGM1 zones and wireless zones are enabled.

SMS text:
XXXX_Zn:OFF
Value: Zn – zone number, range – [Z1... Z44]
Example: 1111_Z4:OFF

Menu path:
OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → STATUS → DISABLE
OK → CONFIGURATION → ZONES →
WIRELESS ZONES → RF ZONE [1... 16] → STATUS → DISABLE
OK → CONFIGURATION → ZONES →
KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → STATUS → DISABLE
OK → CONFIGURATION → ZONES →
EPGM ZONES → EPGM ZONE [1... 16] → STATUS → DISABLE

Enter parameter 52 & parameter status value:
[52xx0#]
Value: xx – zone number, range – [01... 44]

Enable Zone

This command enables a particular zone. By default, all keyboard zones and virtual zones are disabled.

Virtual zones can be enabled using *ELDES Configuration Tool* only.

SMS text:
XXXX_Zn:ON
Value: Zn – zone number, range – [Z1... Z44]
Example: 1111_Z3:ON

Menu path:
OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → STATUS → ENABLE
OK → CONFIGURATION → ZONES →
WIRELESS ZONES → RF ZONE [1... 16] → STATUS → ENABLE
OK → CONFIGURATION → ZONES → KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → STATUS → ENABLE
OK → CONFIGURATION → ZONES →
EPGM ZONES → EPGM ZONE [1... 16] → STATUS → ENABLE

Enter parameter 52 & parameter status value:
[52xx1#]
Value: xx – zone number, range – [01... 44]

Bypass Zone

Zone bypassing allows to temporally disable a particular violated zone.

SMS

N/A

EKB2

Menu path:
OK → BYPASS → BYPASS LIST [1... 3] → [ZONE 1... 44] → BYPASS

EKB3

Enter zone number & user (keyboard) password:
[BYPSxxyyyy#]
Value: xx – zone number, range – [01... 44]; yyyy – 4-digit user (keyboard) password

Bypass All Zones

This command allows to bypass all violated zones at once.

SMS

N/A

EKB2

Menu path:
OK → BYPASS → BYP VIOLATED ZONES

EKB3

N/A

Unbypass Zone

This command activates a particular bypassed zone.

Alternative way: Bypassed zones become active again after arming & disarming the alarm system.

SMS

N/A

EKB2

Menu path:
OK → BYPASS → [ZONE 1... 44] → UNBYPASS

EKB3

Enter zone number & user (keyboard) password:
[BYPSxxyyyy#]
Value: xx – zone number, range – [01... 44]; yyyy – 4-digit user (keyboard) password

Set Zone Type

Each zone can be set to operate under one of these types:

Follow – zone is inactive during *Entry/Exit Delay* countdown.

Instant – the alarm is caused instantly in case of zone violation.

24H – zone is always active, even when the system is disarmed.

Delay – inactive for a period of time dedicated to disarm the alarm system or leave the premises *(Entry/Exit Delay)*.

Fire – this zone is intended for smoke detectors and is always active, even when the system is disarmed.

Silent – operates in the same way as *24H* type, but siren is not activated during zone violation.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES →
WIRED ZONES → [ZONE 1... 12] → TYPE → FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
OK → CONFIGURATION → ZONES → WIRELESS ZONES →
RF ZONE [1... 16] → TYPE → FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
OK → CONFIGURATION → ZONES → KEYBOARD ZONES →
[1ST... 4TH] KEYBOARD ZONE → TYPE → FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
OK → CONFIGURATION → ZONES → EPGM ZONES →
EPGM ZONE [1... 16] → TYPE → FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT

EKB3

Enter parameter 53, zonos number & zone type number:

[53xx1#] - Follow
[53xx2#] - Instant
[53xx3#] - 24H
[53xx4#] - Delay
[53xx5#] - Fire
[53xx6#] - Silent

Value: xx – zone number, range – [01... 44]

Enable *Stay* Mode for a Specified Zone

Stay mode enables the users to arm and disarm the alarm system while staying inside the secured premises. The system goes into *Stay* mode in case the *Delay* zone is not violated during the *Exit Delay* countdown (the user does not leave the secured area) and the zones which are configured as *Stay* will not be secured. *Stay* mode is not activated if the user leaves the secured premises during *Exit Delay* countdown or if none of the zones are configured to operate under Stay mode. By default, this feature is disabled for all zones.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → STAY → ENABLE

OK → CONFIGURATION → ZONES → WIRELESS ZONES → RF ZONE [1... 16] → STAY → ENABLE

OK → CONFIGURATION → ZONES → KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → STAY → ENABLE

OK → CONFIGURATION → ZONES → EPGM ZONES → EPGM ZONE [1... 16] → STAY → ENABLE

EKB3

Enter parameter 56, zone number & parameter status value:

[56xx1#]

Value: xx – zone number, range – [01... 44]

NOTE: *Stay* mode becomes ineffective if the user leaves the secured premises during *Exit Delay* countdown.

Disable Stay Mode for a Specified Zone

This command disables *Stay* mode for a specified zone.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → STAY → DISABLE
OK → CONFIGURATION → ZONES → WIRELESS ZONES
→ RF ZONE [1... 16]→ STAY → DISABLE
OK → CONFIGURATION → ZONES → KEYBOARD ZONES
→ [1ST... 4TH] KEYBOARD ZONE → STAY → DISABLE
OK → CONFIGURATION → ZONES →
EPGM ZONES → EPGM ZONE [1... 16] → STAY → DISABLE

EKB3

Enter parameter 56, zone number & parameter status value:

[56xx0#]

Value: xx – zone number, range – [01... 44]

Enable *Force* Mode for a Specified Zone

Force mode allows the user to arm the alarm system even if the zone operating under *Force* mode is violated. This zone begins operating according to its' type and does not ignore violation after the system is armed and the zone is restored. By default, this feature is disabled for all zones.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → FORCE → ENABLE
OK → CONFIGURATION → ZONES → WIRELESS ZONES →
RF ZONE [1... 16]→ FORCE → ENABLE
OK → CONFIGURATION → ZONES → KEYBOARD ZONES
→ [1ST... 4TH] KEYBOARD ZONE → FORCE → ENABLE
OK → CONFIGURATION → ZONES → EPGM ZONES →
EPGM ZONE [1... 16] → FORCE → ENABLE

EKB3

Enter parameter 82, zone number & parameter status value:

[82xx1#]

Value: xx – zone number, range – [01... 44]

Disable *Force* Mode for a Specified Zone

This command disables *Force* mode for a specified zone.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → FORCE → DISABLE

OK → CONFIGURATION → ZONES → WIRELESS ZONES → RF ZONE [1... 16]→ FORCE → DISABLE

OK → CONFIGURATION → ZONES → KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → FORCE → DISABLE

OK → CONFIGURATION → ZONES → EPGM ZONES → EPGM ZONE [1... 16] → FORCE → DISABLE

EKB3

Enter parameter 82, zone number & parameter status value:

[82xx0#]

Value: xx – zone number, range – [01... 44]

Disable *Chime*

The mini buzzer connected to ESIM264, together with EKB2 and EKB3 buzzers provides three short beeps every time when any *Delay* zone is being violated. *Chime* feature applies even when alarm system is disarmed. By default, this feature is enabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → CHIME → DISABLE

EKB3

Enter parameter 32 & parameter status value:
[320#]

Enable *Chime*

This command enables *Chime* feature.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → CHIME → ENABLE

EKB3

Enter parameter 32 & parameter status value:
[321#]

List Zone & PGM Output Status

This feature provides the list of zone and PGM output statuses (enabled/disabled, turned on/off). In addition, the SMS message contains zone alarm texts, PGM output names and alarm system status (armed/disarmed).

SMS

SMS text:
XXXX_STATUS
Example: 1111_STATUS

EKB2

Menu path:
OK → CONFIGURATION → ZONES → WIRED ZONES → [ZONE 1... 12] → STATUS
OK → CONFIGURATION → ZONES → WIRELESS ZONES → RF ZONE [1... 16] → STATUS
OK → CONFIGURATION → ZONES →
KEYBOARD ZONES → [1ST... 4TH] KEYBOARD ZONE → STATUS
OK → CONFIGURATION → ZONES → EPGM ZONES → EPGM ZONE [1... 16] → STATUS
OK → CONFIGURATION → PGM OUTPUTS → PGM OUTPUTS → OUTPUT [1... 12] → STATUS
OK → CONFIGURATION → PGM OUTPUTS → RF OUTPUTS → RF OUTPUT [1... 32] → STATUS

EKB3

N/A

See also chapter **5.4.16 Partitions.**

5.4.7 PGM Outputs

NOTE: Space, colon, semi-colon characters, parameter names and/or values are not allowed in PGM output names, eg. PSW, STATUS, ON, OFF etc.

PGM Output Name

Each PGM output has a name. Manufacturer default PGM output names: C1 – **Controll1**, C2 – **Controll2**, C3 – **Controll3**, C4 – **Controll4** etc.

PGM output name can be edited by SMS or *ELDES Configuration Tool* software only. The length of each PGM output name can be up to 10 characters.

SMS

SMS text:
XXXX_Cn:NewOutputName
Value: Cn – PGM output number, range – [C1... C44]
Example: 1111_C3:Pump

EKB2

Menu path:
OK → CONFIGURATION → PGM OUTPUTS → PGM OUTPUTS → OUTPUT [1... 12] → NAME
OK → CONFIGURATION → PGM OUTPUTS → RF OUTPUTS → RF OUTPUT [1... 32] → NAME

EKB3

N/A

Turn ON PGM Output / Set PGM Output Startup Status (ON)

This command turns on a specified PGM output and sets its' status to ON on system startup.

SMS

SMS text:
XXXX_Cn:ON or XXXX_OutputName:ON
Value: Cn – PGM output number, range – [C1... C44]
Example: 1111_Pump:ON

EKB2

Menu path:
OK → CONFIGURATION → PGM OUTPUTS →
PGM OUTPUTS → OUTPUT [1... 12] → STATUS → ENABLE
OK → CONFIGURATION → PGM OUTPUTS →
RF OUTPUTS → RF OUTPUT [1... 32] → STATUS → ENABLE

EKB3

Enter parameter 61, PGM output number & parameter status value:
[61xx1#]
Value: xx – PGM output number, range – [01... 44]

Turn OFF PGM Output / Set PGM Output Startup Status (OFF)

This command turns on a specified PGM output and sets its' status to OFF on system startup.

SMS

SMS text:
XXXX_Cn:OFF or XXXX_OutputName:OFF
Value: Cn – PGM output number, range – [C1... C44]
Example: 1111_C2:OFF

EKB2

Menu path:
OK → CONFIGURATION → PGM OUTPUTS →
PGM OUTPUTS → OUTPUT [1... 12] → STATUS → DISABLE
OK → CONFIGURATION → PGM OUTPUTS →
RF OUTPUTS → RF OUTPUT [1... 32] → STATUS → DISABLE

EKB3

Enter parameter 61, PGM output number & parameter status value:
[61xx0#]
Value: xx – PGM output number, range -[01... 44]

Turn ON PGM Output by Timer

The system has an internal RTC (real time clock) allowing to set the timer for turning on a particluar PGM output at a set time.

SMS

SMS text:
XXXX_Cn:ON:HH.MM.SS or XXXX_OutputName:ON:HH.MM.SS
Value: Cn – PGM output number, range – [C1... C44], HH – hours, range – [00... 23], MM – minutes, range – [00... 59], SS – seconds, range [00... 59].
Example: 1111_C3:ON:13.23.48

EKB2

N/A

EKB3

N/A

Turn OFF PGM Output by Timer

This command allows to set the timer for turning off a particluar PGM output at a set time.

SMS

SMS text:
XXXX_Cn:OFF:HH.MM.SS or XXXX_OutputName:OFF:HH.MM.SS
Cn – PGM output number, range – [C1... C44], HH – hours, range – [01... 23], MM – minutes, range – [01... 59], SS – seconds, range [01... 59].
Example: 1111_Pump:OFF:14.50.22

EKB2

N/A

EKB3

N/A

NOTE: Value [00.00.00] is invalid

Enable Automatic PGM Output Control

The system supports up to 16 rules allowing to set automatic PGM output control by assigning it to a particular system event: arm/disarm, system alarm/restore, temperature changes, by scheduled date & time, particular zone alarm/restore in particular partition or in both partitions. By default all rules are disabled.

SMS

N/A

EKB2

N/A

EKB3

Enter parameter 49, rule number & parameter status value:
[49xx1#]
Value: xx – rule number, range – [01... 16]

Disable Automatic PGM Output Control

This command disables particular rule.

SMS

N/A

EKB2

N/A

EKB3

Enter parameter 49, rule number & parameter status value:
[49xx0#]
Value: xx – rule number, range – [01... 16]

NOTE: Automatic PGM output control can be fully configured using *ELDES Configuration Tool* software.

Enable EPGM8 Module Mode

The number of wired PGM outputs can be expanded to 12 by connecting EPGM8 - 8 PGM output expansion module. By default, EPGM8 module mode is disabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → USING EPGM8 → ENABLE

EKB3

Enter parameter 33 & parameter status value:
[3312#]

Disable EPGM8 Module Mode

This command disables EPGM8 module mode.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → USING EPGM8 → DISABLE

EKB3

Enter parameter 33 & parameter status value:
[3302#]

5.4.8 Siren

Set Siren Alarm Duration

In case of alarm the system activates the siren connected to alarm system (depending on zone type). By default siren alarm duration is **1** minute.

SMS

SMS text:
XXXX_SIREN:T
Value: T – siren alarm time in minutes, range – [0... 5]
Example: 1111_SIREN:4

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → ALARM TIME → [XX]
Value: [XX] – siren alarm duration in minutes, range - [1... 10]

EKB3

Enter parameter 10 & siren alarm duration:
[10xx#]
Value: xx – siren alarm time in minutes, range - [00... 10]

See Siren Alarm Duration

This command indicates the alarm duration set.

SMS

SMS text:
XXXX_SIREN
Example: 1111_SIREN

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → ALARM TIME

EKB3

N/A

Enable *Bell Squawk*

Bell Squawk feature enables the siren to provide short beeps everytime the alarm system is being armed. By default, this feature is disabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → BELL SQUAWK → ENABLE

EKB3

Enter parameter 29 & parameter status value:
[291#]

Disable *Bell Squawk*

This command disables *Bell Squawk* feature.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → BELL SQUAWK → DISABLE

EKB3

Enter parameter 29 & parameter status value:
[290#]

NOTE: *Bell Squawk* feature applies to wired sirens only.

Enable *Siren ON if RF Signal is Lost*

When the system is armed, the siren is activated in case of wireless connection loss between the alarm system and any wireless device. By default this feature is disabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → RF LOSS ALARM → ENABLE

EKB3

Enter parameter 76 & parameter status value:
[761#]

Disable *Siren ON if RF Signal is Lost*

This command disables *Siren* ON if RF *Signal is Lost* feature.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → SIREN SET → RF LOSS ALARM → DISABLE

EKB3

Enter parameter 76 & parameter status value:
[760#]

NOTE: The siren is always activated in case of alarm (depending on zone type), despite the status of *Siren* ON if RF *Signal* is Lost feature.

5.4.9 Info SMS

Info SMS

This SMS report provides information on alarm system status (armed/disarmed), GSM signal strength, man power supply status, temperature of secured area (if temperature sensor is used), zone state (alarm/restore).

SMS

SMS text:
XXXX_INFO
Example: 1111_INFO

EKB2

N/A

EKB3

N/A

Set Periodic Info SMS

The system periodically sends *Info SMS* to User 1 at the set period of time. By default this period is at 11:00 AM daily (period – 1, time - 11) .

SMS

SMS text:
XXXX_INFO:PP.TT
Value: [PP] – SMS sending period in days, range – [1... 99]; [TT] – SMS sending period in hours, range - [1... 23]
Example: 1111_INFO:4.16

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → INFO SMS SCHED → PERIOD → [PP]
OK → CONFIGURATION → PRIMARY SET → INFO SMS SCHED → TIME → [TT]
Value: [PP] – SMS sending period in days, range - [1... 99]; [TT] – SMS sending period in hours, range - [1... 23]

EKB3

Enter parameter 11, SMS sending time & period:
[11xxyy#]
Value: xx – SMS sending period in hours, range - [1... 23]; yy - SMS sending period in days, range - [1... 99]

Disable Periodic Info SMS

This command disables *Periodic Info SMS.*

SMS

SMS text:
XXXX_INFO:00.00
Example: 1111_INFO:00.00

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → INFO SMS SCHED → PERIOD → [0]
OK → CONFIGURATION → PRIMARY SET → INFO SMS SCHED → TIME → [0]

EKB3

Enter parameter 11 & parameter status value:
[110000#]

5.4.10 Alarm Notifications

Disable Call in Case of Alarm

In case of alarm, the system makes a phone call to User 1. The phone call is made to the next user in a row in case the previous user was unreachable (was „out of radio coverage" or provided engaged signal). By default, this feature is enabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
CALL/SMS SET → DIS CALL DUR ALM. → ENABLE

EKB3

Enter parameter 30 & parameter status value:
[301#]

NOTE: The system will not make a phone call to the next user in a row if the previous user was reachable, but did not answer or rejected the phone call.

Enable Call in Case of Alarm

This command enables phone calls in case of alarm.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → DIS CALL DUR ALM. → DISABLE

EKB3

Enter parameter 30 & parameter status value:
[300#]

Disable SMS in Case of Alarm

In case of alarm the system sends an SMS message to User 1. The SMS message is sent to the next preset user in a sequence in case the system does not receive a successful SMS message delivery confirmation in 20 seconds from the recipient. By default this feature is enabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → DIS SMS DUR ALM. → ENABLE

EKB3

Enter parameter 31 & parameter status value:
[311#]

Enable SMS in Case of Alarm

This command enables SMS messages in case of alarm.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → DIS SMS DUR ALM. → DISABLE

EKB3

Enter parameter 31 & parameter status value:
[310#]

Enable SMS to All Users Simultaneously in Case of Alarm

In case of alarm, the system simultaneously sends SMS messages to all preset users as the system does not require SMS message delivery confirmation. By default, this function is disabled.

SMS

SMS text:
XXXX_SMSALL:ON
Example: 1111_SMSALL:ON

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → SMS ALL → ENABLE

EKB3

Enter parameter 21 & parameter status value:
[211#]

Disable SMS to All Users Simultaneously in Case of Alarm

This command disables sending SMS messages to all users simultaneously in case of alarm.

SMS

SMS text:
XXXX_SMSALL:OFF
Example: 1111_SMSALL:OFF

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → SMS ALL → DISABLE

EKB3

Enter parameter 21 & parameter status value:
[210#]

5.4.11 Arm/Disarm Notifications

Disable *Arm/ Disarm* SMS

The system sends SMS message to User 1 after arming and disarming process (except - by phone call). This function disables this SMS message for a specified user. By default, this feature is enabled for all users.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5] → ARM/DISARM EVENT → DISABLE

EKB3

Enter parameter 75 & parameter status value:
[75zx0#]
Value: xx – user number, range – [1... 5]

NOTE: After arming or disarming the alarm system by phone call, the system sends SMS message to user who made a phone call only.

NOTE: By default, *Arm/Disarm* SMS is enabled for all users, but sent to User 1 only. However Users 2 - 5 can receive this SMS message as well after *Arm/Disarm SMS to All Users Simultaneously* is enabled.

Enable *Arm/ Disarm* SMS

This command enables *Arm/Disarm Event* SMS message.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5] → ARM/DISARM EVENT → ENABLE

EKB3

Enter parameter 75 & parameter status value:
[75xx1#]
Value: xx – user number, range – [1... 5]

Enable *Arm/Disarm SMS to All Users Simultaneously*

The system simultaneously sends SMS message to all users with *Arm/Disarm* SMS feature enabled, after arming and disarming process (by any method). By default, this feature is disabled.

SMS

SMS text:
XXXX_MASTER:ON
Example: 1111_MASTER:ON

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → INF ABOUT ARM/DARM → ENABLE

EKB3

Enter parameter 22 & parameter status value:
[221#]

Disable *Arm/Disarm SMS to All Users Simultaneously*

This command disables *Arm/Disarm SMS to All Users Simultaneously.*

SMS

SMS text:
XXXX_MASTER:OFF
Example: 1111_MASTER:OFF

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → INF ABOUT ARM/DARM → DISABLE

EKB3

Enter parameter 22 & parameter status value:
[220#]

5.4.12 Temperature Change Notifications

Disable *Temperature Limit Info SMS*

Temperature Limit Info SMS is sent to all preset users when temperature exceeds the min. or max. set temperature value. By default, this SMS message is enabled

The temperature is measured by temperature sensor connected to ESIM264 alarm system.

SMS

SMS text:
XXXX_TEMP:0:0
Example: 1111_TEMP:0:0

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → INFO SMS → DISABLE

EKB3

Enter parameter 50 & parameter status value:
[500#]

NOTE: Despite the status of *Temperature Limit Info SMS*, the temperature is always indicated in Info SMS content and displayed in EKB2 main screen view.

Enable *Temperature Limit Info SMS*

This command enables *Temperature Limit Info SMS.*

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → INFO SMS → ENABLE

EKB3

Enter parameter 50 & parameter status value:
[501#]

Set Temperature Limit Boundary – Min. Value

Set the value of minimum temperature limit boundary which causes *Temperature Limit Info SMS* to be sent to preset all users when the limit is exceeded.

SMS

SMS text:
XXXX_TEMP:min:max
Value: min - lowest temperature limit boundary in °C, range - [-55... 125]; max - highest temperature limit boundary in °C, range - [-55... 125]

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → TEMP. MIN → [XXX]
Value: [XXX] – lowest temperature limit boundary in °C, range - [-55... 125]
Keyboard keys P1 or P2 are used to enter minus symbol, e.g. -20

EKB3

Enter parameter 19 & temperature value:
[19x#]
Value: x - lowest temperature limit boundary in °C, range - [-55... 125]
00 stands for minus symbol, i. e. 0020 = -20

Set Temperature Limit Boundary – Max. Value

Set the value of maximum temperature limit boundary which causes *Temperature Limit Info SMS* to be sent to all preset users when the limit is exceeded.

SMS

SMS text:
XXXX_TEMP:min:max
Value: min - lowest temperature limit boundary in °C, range - [-55... 125]; max - highest temperature limit boundary in °C, range - [-55... 125]

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → TEMP. MAX → [XXX]
Value: [XXX] - highest temperature limit boundary in °C, range - [-55... 125]
Keyboard keys P1 or P2 are used to enter minus symbol, e.g. -20

EKB3

Enter parameter 20 & temperature value:
[20x#]
Value: x - lowest temperature limit boundary in °C, range - [-55... 125]
00 stands for minus symbol, i. e. 0020 = -20

See Temperature Limit Min. & Max Values

This command indicates the lowest. & highest temperature limit boundaries set.

SMS

SMS text:
XXXX_TEMP
Example: 1111_TEMP

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → TEMP. MIN
OK → CONFIGURATION → PRIMARY SET → TEMP SENSOR → TEMP. MAX

EKB3

N/A

5.4.13 Main Power Supply Status Notifications

Disable *Main Power Supply Status SMS*

After the main power is lost or restored, the system notifies all preset users by SMS message. By default this feature is enabled.

SMS

SMS text:
XXXX_M:OFF
Example: 1111_M:OFF

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
POWER STATUS → CHECK EXT. PWR ST → DISABLE

EKB3

Enter parameter 13 & parameter status value:
[130#]

Enable *Main Power Status SMS*

This command enables notifications about main power status.

SMS

SMS text:
XXXX_M:ON
Example: 1111_M:ON

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
POWER STATUS → CHECK EXT. PWR ST → ENABLE

EKB3

Enter parameter 13 & parameter status value:
[131#]

Set Main Power Failure Delay

This command allows to set main power failure delay time period notifying all preset users about external power supply loss events. If the power supply is restored during failure delay time period, the system will not notify the user (-s) about this event. By default, this time period is **30** seconds.

This parameter is useful when encountering temporary power supply failures.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
POWER STATUS → AC FAILURE DELAY → [XXXXX]
Value: [XXXXX] – main power failure delay in seconds, range - [0... 65535]

EKB3

Enter parameter 70 & duration in seconds:
[**70**x#]
Value: x – main power failure delay in seconds, range - [0... 65535]

Set Main Power Restore Delay

This command allows to set main power restore delay time period notifying all preset users about main power supply restore events. If the power supply is lost again during restore delay time period, the system will not notify the user (-s) about this event. By default, this time period is **120** seconds.

This feature is useful when encountering temporary power supply failures.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → PRIMARY SET → POWER STATUS → AC RESTORE DELAY → [XXXXX]

Value: [XXXXX] – main power restore delay in seconds, range - [0... 65535]

EKB3

Enter parameter 71 & duration in seconds:

[71x#]

Value: x – main power restore delay in seconds, range - [0... 65535]

5.4.14 Remote Listening

Remote Listening

This feature provides a possibility to listen to what is going on in the secured area where the alarm system with connected microphone is installed. After sending the SMS message the system calls back to the user and upon answering the call, user can listen to any sounds in the building. The phone call must be answered within 20 seconds otherwise the system ends the call and returns to previous state.

Alternative way 1: the system always makes a call to the user in case of alarm (unless this feature is disabled).

Alternative way 2: the system answers the phone call from a preset user phone number (if this feature is enabled). For more details on this feature, please, refer to *ELDES Configuration Tool* software's HELP section.

SMS

SMS text:

XXXX_MIC

Example: 1111_MIC

EKB2

N/A

EKB3

N/A

5.4.15 System Control from Any Phone Number

Disable *Allow Only Preset Users*

The system accepts control and configuration SMS messages from 5 preset user phone numbers only. By disabling this feature, the system will accept SMS messages from any user who knows the correct SMS password. By default, this feature is enabled.

SMS

SMS text:
XXXX_STR:OFF
Example: 1111_STR:OFF

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
PASSWORD → ALLOW ONLY PRS USR → DISABLE

EKB3

Enter parameter 12 & parameter status value:
[120#]

Enable *Allow Only Preset Users*

This command enables *Allow Only Preset Users* feature.

SMS

SMS text:
XXXX_STR:ON
Example: 1111_STR:ON

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
PASSWORD → ALLOW ONLY PRS USR → ENABLE

EKB3

Enter parameter 12 & parameter status value:
[121#]

5.4.16 Partitions

Set Keyboard Partition

System partition which every keyboard is assigned to. By default, new added keyboard is assigned to **partition 0.**

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
KEYBOARD PARTITION → KBRD [1... 10] → PARTITION [0... 1]

EKB3

Enter parameter 51, keyboard number & partition:
[51xxy#]
Value: xx – keyboard number, range – [01... 04]; y – partition, range – [0... 1]

Switch Between Keyboard Partitions

This feature allows to temporally switch between keyboard partitions. The partition is automatically switched back to the previous one in 3 minutes after the last key-touch/key-stroke. By default, this feature is disabled.

SMS

N/A

EKB2

Menu path:
P1 → PART[0... 1] | [custom name]

EKB3

Hold [*] key for 3 seconds and press [0] or [1] key.
Value: [0] key – partition 0; [1] key – partition 1.

Enable Keyboard Partition Switch

This command enables keyboard partition switch. By default this feature is disabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET →
KEYBOARD PARTITION → PARTITION SWITCH → ENABLE

EKB3

Enter parameter 77 & parameter status value:
[771#]

Disable Keyboard Partition Switch

This function disables keyboard partition switch.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → KEYBOARD PARTITION → PARTITION SWITCH → DISABLE

EKB3

Enter parameter 77 & parameter status value:
[770#]

Set User (Keyboard) Password Partition

System partition which every user (keyboard) password is assigned to. By default, newly added user (keyboard) password is assigned to partition 0.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → PASSWORD → KEYBOARD PSW [1... 10] → PARTITION → PARTITION [0... 1]

EKB3

Enter parameter 87, user (keyboard) password & partition:
[87xxxxy#]
Value: xxxxx - 4-digit user (keyboard) password, range - [0000... 9999]; y - partition, range - [0... 1]

Set User Partition

System partition which every user phone number (User 1 – User 5) is assigned to. By default, new added user phone number is assigned to partition 0.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → CALL/SMS SET → USER → USER [1... 5] → PARTITION → PARTITION [0... 1]

EKB3

Enter parameter 59, user number & partition:
[59xxy#]
Value: xx – user number, range – [01... 05]; y – partition, range – [0... 1]

Set Zone Partition

System partition which every zone is assigned to. By default, every zone is assigned to partition 0.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ZONES
→ WIRED ZONES → ZONE [1... 12] → PARTITION → PARTITION [0... 1]
OK → CONFIGURATION →
ZONES → WIRELESS ZONES → RF ZONE [1... 16] → PARTITION → PARTITION [0... 1]
OK → CONFIGURATION → ZONES → KEYBOARD ZONES → [1ST... 4TH]
KEYBOARD ZONE → PARTITION → PARTITION [0... 1]
OK → CONFIGURATION → ZONES → EPGM ZONES →
EPGM ZONE [1... 16] → PARTITION → PARTITION [0... 1]

EKB3

Enter parameter 57, zone number & partition:

[57xxy#]

Value: xx – zone number, range – [01... 44]; y – partition, range – [0... 1]

Set iButton® Partition

System partition which every iButton® key is assigned to. By default, new added iButton® key is assigned to partition 0.

SMS

N/A

EKB2

Menu path:

[0... 1]

EKB3

Enter parameter 60, iButton® key number & partition:

[60xxy#]

Value: xx – iButton® key number, range – [01... 05]; y – partition, range – [0... 1]

5.4.17 Additional Parameters

Disable *Event Log*

This feature enables to record all information about system configuration, system actions and information messages and to export it to .log file. The size of log file is up to **1000** records. By default, this feature is enabled.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → LOG SET → DISABLE

EKB3

Enter parameter 36 & parameter status value:
[360#]

Enable Event Log

This command enables *Event Log* feature.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → LOG SET → ENABLE

EKB3

Enter parameter 36 & parameter status value:
[361#]

Microphone Level

This command allows to set microphone connected to alarm system volume level. Default microphone volume level is **12**.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → GSM AUDIO → MIC LEVEL → [XX]
Value: [XX] – microphone volume level, range – [0... 15]

EKB3

N/A

Speaker Level

This command allows to set speaker connected to alarm system volume level. Default speaker volume level is **85**.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → PRIMARY SET → GSM AUDIO → SPEAKER LEVEL → [XX]
Value: [XX] – speaker volume level, range – [0... 100]

EKB3

N/A

Reset to Default Parameters

This command restores all device parameters to default values.
After this procedure all set phone numbers will be lost.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → RESET TO DEFAULT → [XXXX]
Value: [XXXX] – keyboard password

EKB3

Enter parameter 62 & administrator password:
[62xxxx#]
Value: xxxx – administrator password

6. Technical Support

6.1 Trouble Indication

EKB2

Message **TBL** displayed in the lower left side of the main screen view indicates presence of system troubles.
In order to find out more on the particular system problem, please, open menu section **TROUBLES**. The description on each system problem is indicated in the table below.

Menu path:

OK → TROUBLES → T [1... 6]

Trouble	Name	Description
TROUBLE 1	VIOLATED TAMPER	One or more tampers are violated.
TROUBLE 2	REPLACE BATTERY	Backup battery problem.
TROUBLE 3	AC FAILURE	Main power supply problem.
TROUBLE 4	TIME NOT SET	Date/time not set.
TROUBLE 5	HIZONES	One or more high zones (Z13 - Z44) are violated.
TROUBLE 6	GSM ERROR	GSM connection problem.

EKB3

Yellow LED **SYSTEM** indicates system troubles. **SYSTEM** LED indications are mentioned in the table below.

SYSTEM LED	Description
Illuminated continously	One ore more zones or tampers are violated; other system troubles
Flashing	One or more high zones are violated

In order to find out more on the particular system problem, please, enter command A. After this procedure the system will activate red zone LEDs for 15 seconds. The description on each LED indication is mentioned in the table below.

Zone LED	Description
1	One or more tampers are violated.
2	Backup battery problem.
3	Main power supply problem.
4	Date/time not set.
5	One or more high zones (Z13 - Z44) are violated.
6	GSM connection problem.

In order to find out which particular high zone is violated, please, enter command B.
In order to find out which particular tamper is violated, please, enter command C.

A. System trouble indication - enter command:
[CODE#]

B. Violated high zone indication – enter command:
[CODE1]

C. Violated tamper indication – enter command:
[CODE2]

The number of violated high zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

Example: LED #3 from section A is flashing and LED #8 from section B is illuminated continuously. According to the table below LED #8 is equal to number 18, therefore 18 + 3 = 21.

Result: Violated high zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (illuminated continously)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	Zone LED 11 = 36
Zone LED 6 = 6	Zone LED 12 = 42

6.2 Frequently Asked Questions

Question	Answer
1. Can ESIM264 operate as standalone device without SIM card inserted?	Yes, ESIM264 device can fully operate without any SIM card inserted. In this case you will not be able to configure and control the device by SMS and calls nor to receive any SMS reports and calls.
2. I am unable to arm the alarm system when one of the zones (some zones) is violated, although I was able to perform disarming. Is there a way to arm the alarm system while the zone is violated?	Due to security reasons it is recommended to restore the violated zone (-s) before arming the alarm system. However, you can set up the zone (-s) to operate under *Force* mode or use the *Bypass* feature it in order to arm the alarm system despite the violated zone (-s). Please, refer to chapter **5.4.6 Zones** for more details.
3. I have activated ATZ mode in *ELDES Configuration Tool* software, but I am unable to set the connection Type 5. Whenever I select Type 5 and press the "Write Settings" button it switches back to Type 4. What's wrong?	It appears that either ESIM264 firmware or the software is outdated. Please, upgrade the device firmware and download the latest *ELDES Configuration Tool* software version.
4. **When ESIM264 fully powers down my configura**tion becomes lost and I have to re-configure the device again. What's wrong?	This might have happened due to the jumper left on DEF pins or it is a hardware failure. Please, remove the jumper if it is present on DEF pins or contact your supplier for warranty service.
5. I have a smoke detector connected to ESIM264 system. How do I reset the smoke detector when the "Fire" zone is violated?	If the smoke detector is connected to one of the ESIM264 PGM outputs you can reset it by disabling and enabling back the PGM output. This can be performed by SMS, EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool* (please, refer to chapter **5.4.7 PGM Outputs**)
6. **What happens if I switch backup battery pole termi**nals places?	Switching backup battery pole terminals places is forbidden. Otherwise this will lead to blown fuse and ESIM264 alarm system will have to be repaired.
7. How do I disable SMS reports and calls in case of tamper violation when alarm system is disarmed?	The SMS reports on tamper violation can be disabled by erasing the tamper name of a particular tamper using *ELDES Configuration Tool*. However, due to security reasons it is not recommended to disable this feature.
8. Is any additional configuration necessary when connecting EPGM1 module after wiring is done accroding to EPGM1 user manual?	No additional configuration is required in order to make EPGM1 module operational.
9. Does the quantity of EPGM1 zones duplicate when ATZ mode is activated in the system?	No, the quantity of EPGM1 zones does not duplicate in ATZ mode as EPGM1 module does not support ATZ mode. Only ESIM264 zones duplicate in ATZ mode.
10. I have connected the EPGM1 module to ESIM264 system. The module LED indicators are on, but I am unable to receive any information on EPGM1 zone status after *XXXX_INFO* request. Why?	1. ESIM264 system firmware is outdated and does not support the EPGM1 module. Note that EPGM1 is supported in ESIM264 firmware v7.09.03 and later. Please, contact ELDES technical support and request for an updated firmware file. 2. *Info SMS* request does not indicate information on EPGM1 zones. Please, use *XXXX_STATUS* SMS request instead.
11. I connect the wired siren to ESIM264 and I hear a silent sound alarm even when the alarm system is disarmed. In case of alarm system alarm the siren provides a loud sound alarm as it should. Why?	Please, connect the resistor of 3,3 kΩ nominal to the BELL- / BELL+ contacts This should solve the problem.
12. I am using Windows operating system. The windows of ELDES Configuration Tool are not fully displayed and some parts are like cut-off. What's wrong?	a) For Windows 7 / Vista - Please, change the default window size view for Windows 7 interface. This can be done by clicking the right mouse button on the desktop and choosing the "Personalize" menu section, then navigating to "Display" section and selecting "Smaller size" option. b) For Windows XP - Please, change the default font size for Windows XP interface. This can be done by clicking the right mouse button on the desktop and choosing the "Properties" menu section, then navigating to "Appearance" section and setting "Font size" to "Normal". If the problem persists, please, navigate to the following window "Properties" → "Settings"→ "Advanced" → "General"→ set "DPI setting" to "Normal Size (96 DPI)".

Question	Answer
13. The buzzer remains active when I disarm the alarm system using the keyboard. Why?	The buzzer is intended for iButton indication only and it is not related to disarming process by keyboard.
14. One of wireless devices connected to ESIM264 system sends a tamper alarm from time to time, although no tamper was violated. Why?	This happens due to wireless connection loss. There might be several reasons: 1. ELDES wireless device is installed too close or too far from ESIM264 system. 2. Interference of other electronic equipment. 3. Physical interference (building walls, floors etc.) 4. Metal material interference.
15. I have connected a wired magnetic door sensor, but I receive tamper alarm instead of zone alarm. What's wrong?	This happens due to incorrect resistor connection. Please, refer to corresponding connection circuit according to the selected zone connection type (Type 1 – 5). See chapter **2.3.2 Zone Connection Types** for more details.
16. I disconnected the backup battery, but did not receive any SMS report on this event. How do I enable SMS report on backup battery disconnection?	This feature is permanently enabled and cannot be disabled manually. The system checks the backup battery resistance once a day and sends an SMS report to User 1 on backup battery expiration if more than 1,5Ω resistance is detected.
17. When I check system SIM card credit balance I see a lot of SMS delivery confirmation reports. How do I disable SMS delivery confirmation ESIM264 system?	Everytime an SMS message is sent to the user, the system must "know" that the message was successfully delivered. The only way to partly disable the SMS delivery report (for alarm notifications only) is to enable alarm SMS notifications to all users. This is useful when having only User1 phone number set up, as in case of alarm the system sends the alarm SMS to all preset users simultaneously, but does not require any SMS delivery report.
18. I have set zone alarm text and/or PGM output names containing some cyrillic and/or non-English characters. The alarm texts/PGM output names do not fully fit in the SMS message. What's wrong?	According to GSM standards 1 SMS message may consist of 160 latin alphabet/English characters max. If the message contains at least one non-latin/non-English character, the length of SMS message becomes at least half shorter, since those characters occupy more size of the SMS than the latin ones. It is reommended not to use any non-latin/non-English characters in zone alarm texts/PGM output names.
19. The configuration of added wireless key-fob EWK1 to ESIM264 system is not visible in ELDES Configuration Tool. What's wrong?	1. *ELDES Configuration Tool* version is too old. Please, update it. 2. The firmware version of EWT1 module is outdated. Note that EWK1 is supported in EWT1 firmware v16.4 and later. Please, return EWT1 module for replacement.
20. I am unable to run *ELDES Configuration Tool* - I receive error messages in Windows. Why?	Microsoft .NET Framework v3.5 is not installed in Windows system. Please, download this package from official Microsoft website free of charge and install it to your Windows system.
21. Info SMS report comes with wrong date and time. How do I correct it?	Please, set the correct system date and time using either *ELDES Configuration Tool*, EKB2, EKB3 or SMS message.

6.3 Troubleshooting

Indication	Possible reason
LED **PWR** is off	· No main power supply · Wiring done improperly · Blown fuse
LED **NETWORK** is off or solid on	· Missing SIM card · PIN code is enabled · SIM card is inactive · Disconnected antenna · GSM network signal too weak · Problems with GSM provider
LED **STATUS** solid on or solid off	· Microcontroller is not started due to electrical mains noise or static discharge
System does not send any SMS messages and/or does not ring	· SIM card account depleted · Incorrect SIM central number · No GSM network signal · User number is not preset (or control from unknown numbers disabled) · SIM card changed before disconnecting main power supply or backup battery

Received SMS message "Incorrect Format"	· Wrong syntax · Extra space symbol could be space left in SMS message
Missing temperature indication in Info SMS message	· Temperature sensor not connected · Temperature sensor broken · Connecting wires too long
24H and/or *Fire* zones do not work	· Specified zone must be enabled by SMS, *ELDES Configuration Tool*, EKB2 or EKB3
No sound during remote listening	· Microphone not connected · Improper microphone connection

6.4 Restoring Default Parameters

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Power up the device for 7 seconds.
4. Power down the device.
5. Remove short circuit from DEF pins.
6. Parameters restored to default.

6.5 Upgrading the Firmware using USB Cable

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Connect the device via USB cable to the PC.
4. Power up the device.
5. The new window must pop-up where you will find the .bin file. Otherwise open *My Computer* and look for *Boot Disk* drive.
6. Delete the .bin file found in the drive.
7. Copy the new firmware .bin file to the very same window.
8. Power down the device.
9. Unplug USB cable.
10. Remove short circuit from DEF pins.
11. Power up the device.
12. Firmware upgraded.

6.6 Upgrading the Firmware via GPRS Connection (FOTA)

FOTA

ESIM264 alarm system supports FOTA (firmware-on-the-air) feature. This allows to upgrade the firmware remotely via GPRS connection. Once the upgrade process is initiated, the system connects to the specified FTP server address where the firmware file is hosted and begins downloading and re-flashing the firmware. In order to initiate the upgrade process, please, send the following SMS message.

SMS text:
XXXX_fota:ftp-server-IP,port,firmware-file-name.bin,user-name,password

Value: ftp-server-IP - IP address of FTP server where ESIM264 firmware file is stored; port - port number of FTP server (usually - 21); firmware-file-name.bin - name of the firmware file; user-name - user name of FTP server login; password - password of FTP server login.

Example: 1111_fota:84.15.143.111,21,esim264fw.bin,eldesuser,eldespassword

ATTENTION: "ELDES UAB" does not run a FTP server and does not host the firmware files online. Please, contact ELDES technical support to request the latest firmware file: support@eldes.lt

NOTE: It is strongly recommended to restore default parameters after the firmware upgrade.

For product warranty repair service, please, contact your local retail store where this product was purchased.

If your problem could not be fixed by the self-guide above, please, contact your distributor or ELDES technical support by email support@eldes.lt . More up to date information about your device and other products can be found at the manufacturer's website www.eldes.lt

7. Wired Devices

7.1 EKB2 - LCD Keyboard

EKB2 is an LCD keyboard intended for using with ESIM264 alarm system.

Main EKB2 keyboard features:

- arms and disarms the alarm system
- enables and disables Stay mode
- configures system parameters
- displays system status information on LCD screen
- informs about system status via built-in mini buzzer

The system configuration is performed by accessing EKB2 menu and entering the required values. ESIM264 system allows to connect up to 4 EKB2 keyboards.

7.1.1. Technical Specifications

7.1.1.1 Electrical & Mechanical Characteristics

Power Supply	12-14V ⎓ 150mA max.
Maximum Keyboard Connection Cable Length	100 m.
Dimensions	133 x 89 x 19 mm
Range of Operating Temperatures	0...+55ºC

7.1.1.2 Keys funcionality

←	One menu level back / cancel
↑	Menu navigation – up
↓	Menu navigation – down
OK	Confirm (enter) value
0 .. 9	Value typing
P1	Keyboard partition switch / minus symbol for entering negative temp. value
P2	Minus symbol for entering negative temp. value

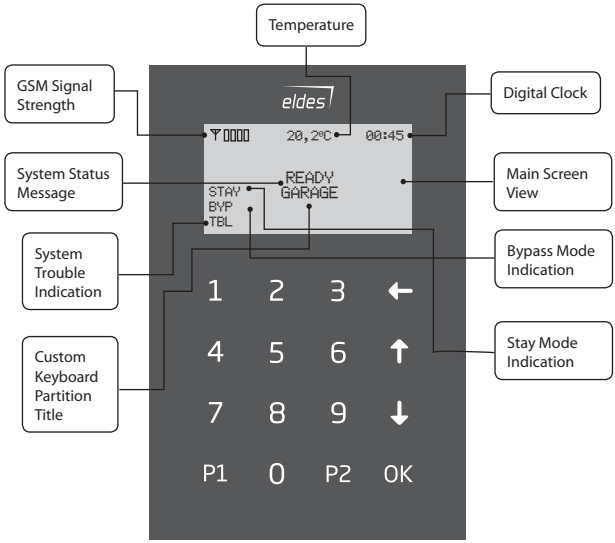


Fig. No. 10

7.1.1.3 Connector and Main Unit Functionality

Vin	Positive 12-14V ⎓ power supply contact
COM	Negative 12-14V ⎓ power supply contact
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common connector for Z1
Z1	Security zone connector
A0	Keyboard address pin
A1	Keyboard address pin
Buzzer	Mini buzzer providing sound signals
Tamper	Tamper-button for EKB2 enclosure status monitoring

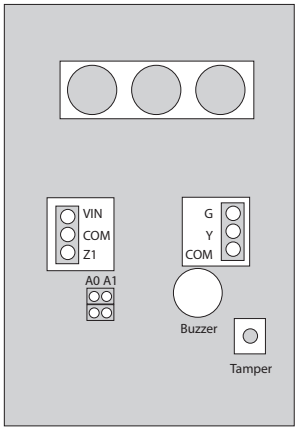


Fig. No. 11

7.1.1.4 Keyboard Address

A0 and A1 pins located on the back side of the keyboard are intended to set keyboard address. The keyboard address is set by putting the jumper (-s) on the pins. ESIM264 system allows to connect up to 4 EKB2 keyboards - each set under different address. Jumper combinations for different keyboard address configuration are indicated in the table below.

Jumper position	Address
A0 A1 	Keyboard 1
A0 A1 	Keyboard 2
A0 A1 	Keyboard 3
A0 A1 	Keyboard 4

The address of each connected keyboard is also indicated in *ELDES Configuration Tool* software.

7.1.2 Installation

1. Remove the screw located on the bottom side of the enclosure (see Fig. No. 12)
2. Detach keyboard holder from EKB2 keyboard by gently pulling the holder towards yourself (see Fig. No. 13).
3. Fix the keyboard holder on the wall using the screws. (see Fig. No. 14)
4. Disconnect ESIM264 main power supply and backup battery.
5. Wire up keyboard contacts to ESIM264 alarm system respectively – **Vin** to **AUX+**, **COM** to **AUX-**, **Y** to **Y**, **G** to **G**.
6. Z1 and COM contacts must be connected with resistor of 5,6kΩ nominal (see Fig. No. 12). As keyboard zone Z1 is disabled by default, it can be enabled by SMS, EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool*. Keyboard zone Z1 must be enabled and resistor connected even if the tamper button alone is required.
7. Set the keyboard address by putting the jumper on A0 and A1 pins (see chapter **7.1.1.4 Keyboard Address**).
8. Fix the keyboard into the holder.

   ATTENTION! Before fixing the keyboard into the holder, please, make sure that the tamper button is properly pressed (see Fig. No. 11).
9. Screw up the bottom side of the enclosure. (see Fig. No. 12)
10. Power up ESIM264 alarm system.
11. EKB2 keyboard is ready.

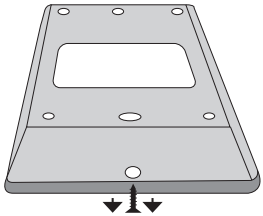


Fig. No. 12

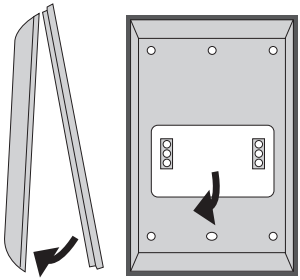


Fig. No. 13

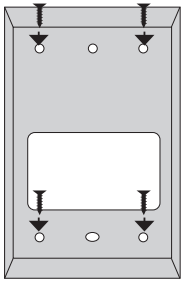


Fig. No. 14

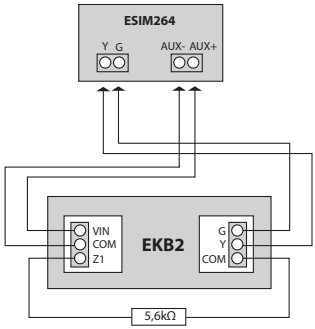


Fig. No. 15

7.1.3 Operation Description

EKB2 LCD screen is intended for displaying alarm system status messages and alerts. Message **READY** is displayed on the screen that no zones are violated or no troubles are present and the system is prepared for arming. Message **NOT READY** (and **TBL**) shows up in case of zone violation or if system troubles are present. The alarm system cannot be armed until the troubles are removed or violated zone (-s) is restored, bypassed or set up to operate under Force mode. The following troubles allow system arming when present:

- backup battery problem;
- main power supply failure;
- date & time not set;
- GSM connection problem.

The built-in mini buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration, one long beep – for invalid configuration. In addition, the mini-buzzer provides continuous short beeps in case of alarm.
EKB2 can be used even in dark premises as the LCD screen and keys are illuminated continuously. In case of alarm the keyboard illumination level is boosted and stays in this state until the system is disarmed. The illumination level lowers down in 3 minutes after the last key-touch while the system is disarmed.

7.1.3.1 EKB2 Zone & Tamper

Keyboard EKB2 has one built-in zone Z1 and one tamper button. By default, the keyboard zone Z1 is disabled. The keyboard zone can be enabled by SMS, EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool*. When Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM contacts must be connected with resistor of 5,6kΩ nominal.
The tamper button is intended for monitoring the enclosure status of EKB2, therefore the system causes alarm if the enclosure is illegally opened. Keyboard zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

7.1.3.2 Arming & Disarming

The arming and disarming process is performed by entering a valid user (keyboard) password. The default user (keyboard) password is **1111**.
When the system is being armed, the screen displays icon and initiates the *Exit Delay* countdown intended for user to leave the secured area. After the countdown is complete the system locks the keyboard menu, displays icon on the screen for 5 seconds and returns to the main screen view displaying **ARMED** message (optional feature).
After the user enters the secured area, the system begins the *Entry Delay* countdown intended to enter a valid user (keyboard) password. After the successful disarm process the system unlocks the keyboard menu and displays icon on the screen for 2 seconds. In case user does not enter a valid password during the countdown, the system causes alarm and displays the alarm message in the main screen view. The last alarm message stays displayed in the main screen view until a valid user (keyboard) password is entered. In addition, after 10 unsuccessful attempts to enter a password, the system disables the arming/disarming possibility for 2 minutes.

NOTE: Arming & disarming can only be performed using a keyboard password assigned to the same partition as the keyboard.

7.1.3.3 Keyboard Partition

Any EKB2 keyboard can be assigned to one of the two available system partitions. Every system keyboard assigned to different partition can operate independently from each other. The keyboard partition can be assigned:

- permanently - by EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool;*
- temporally - by EKB2 keyboard and EKB3 keyboard using keyboard partition switch feature. The partition automatically switches back to previous partition in 3 minutes after the last key-touch/key-stroke.

In order to find out the keyboard's partition, please, check the partition title displayed on the main screen view – **PART0** (partition 0) or **PART1** (partition 1). The partition title of up to 15 characters length can be customized using ELDES Configuration Tool software. For more details, please, refer to software's HELP section.

NOTE: The system can be configured using only one keyboard at a time regardless of the assigned keyboard partition. The displayed icon with message **CONFIGURATION MODE** on the screen indicates an inactive EKB2 keyboard while **CONFIGURATION MODE** stays activated on another keyboard of any partition.

NOTE: The configuration is disabled while any system partition is armed.

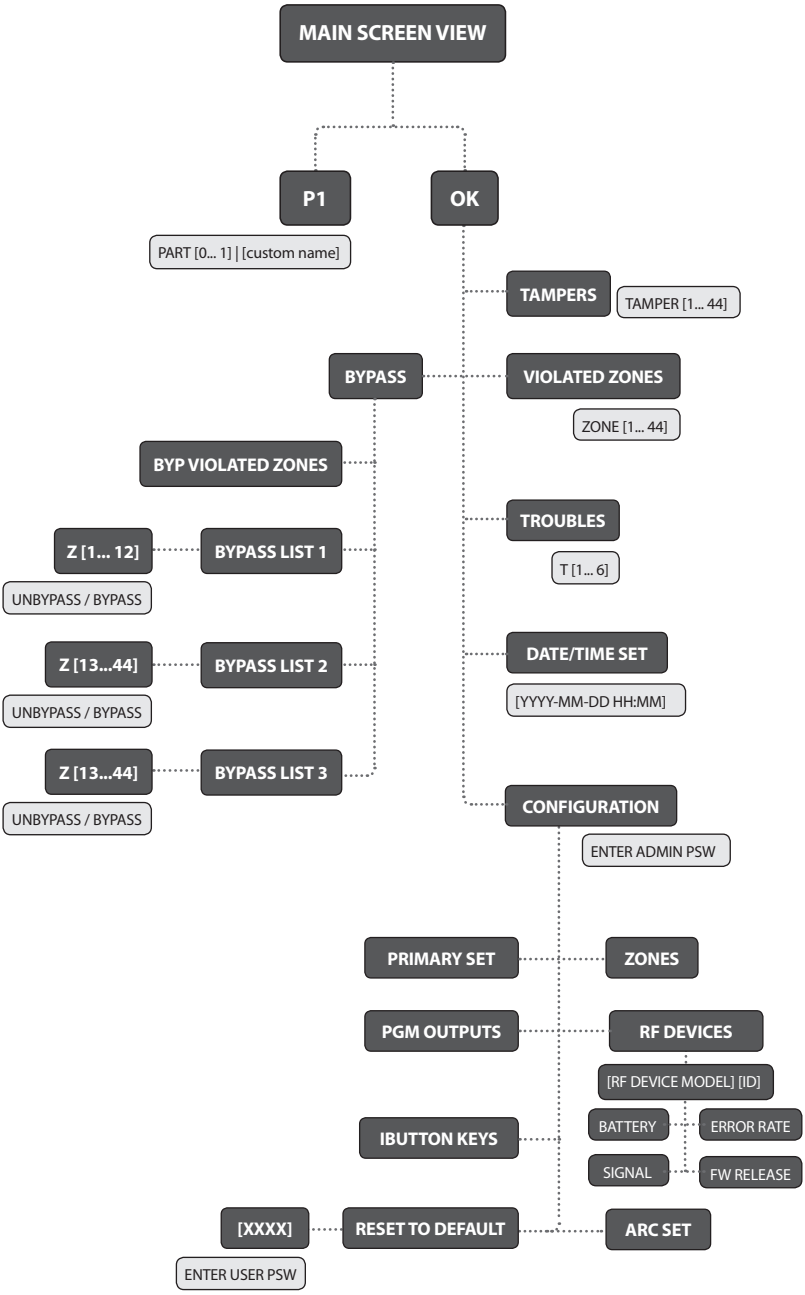
See also chapter **5.4.16 Partitions.**

7.1.3.4 Icons & Messages

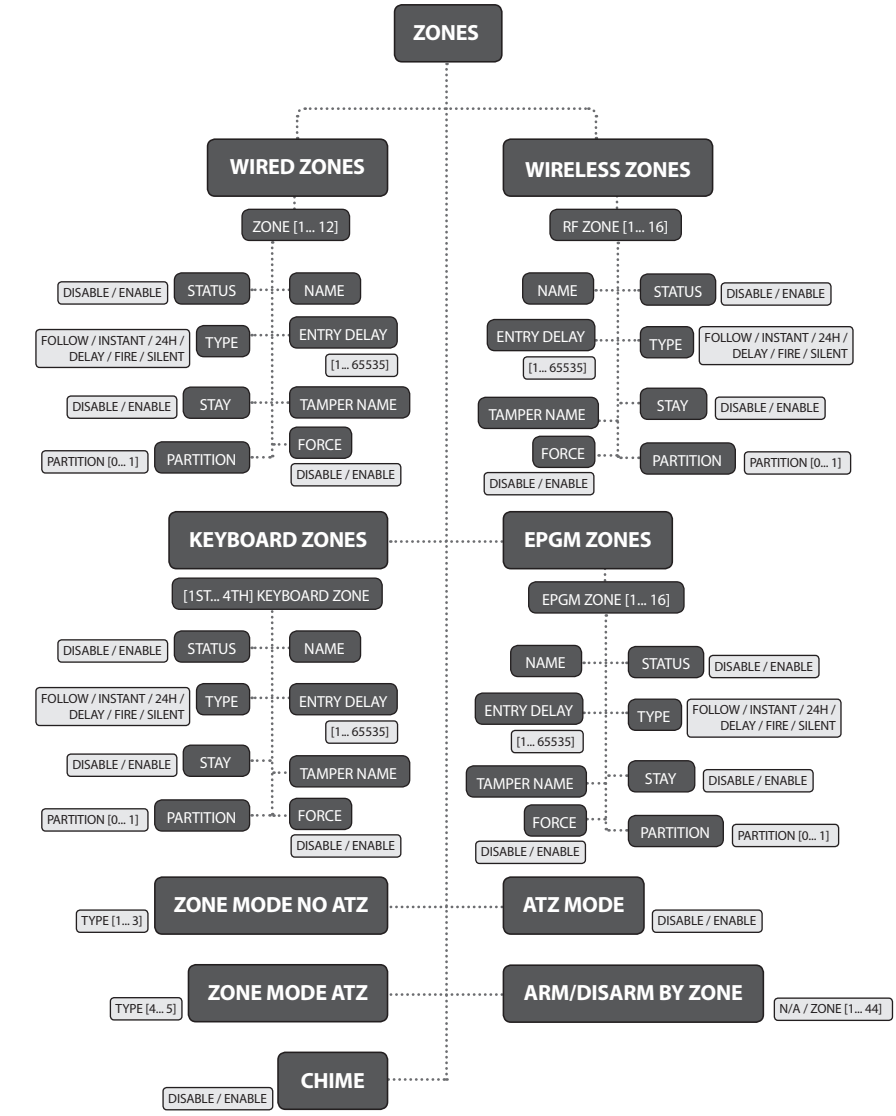
Icon / Message	Description
	*Delay* zone violated when system is disarmed.
	*Exit* Delay countdown initiated.
	System is armed and menu is locked.
	System is disarmed and menu is unlocked
 **+ CONFIGURATION MODE**	Configuration mode activated.
BURGLARY ALARM	*Delay, Instant* or *Follow* zone violated when system is armed.

Icon / Message	Description
24 ALARM	*24H* zone violated.
FIRE ALARM	*Fire* zone violated.
TAMPER ALARM	Tamper violated
READY	System is ready to be armed.
NOT READY	System is not ready to be armed – one or more zones / tampers violated.
ARMED	System is armed (optional feature).
STAY	*Stay* mode activated
BYP	One or more zones bypassed
TBL	One or more system troubles are present

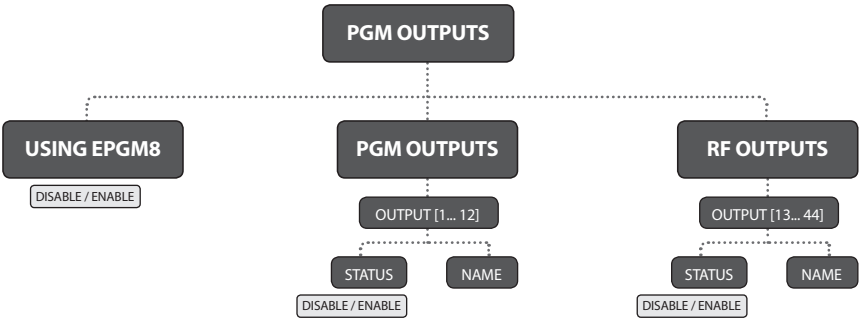
7.1.4 Menu Tree



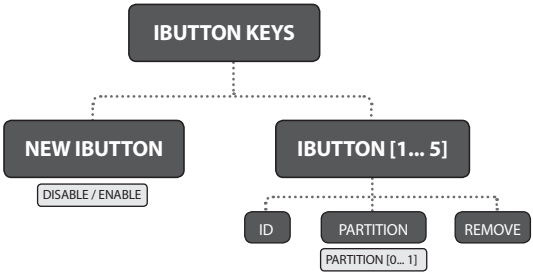

PRIMARY SET
CALL/SMS SET
USER [1... 5]
USER
SMS ALL
DISABLE / ENABLE
PARTITION
PARTITION [0... 1]
ARM/DISARM EVENT
DISABLE / ENABLE
NUMBER
[XXXXXXXXXXXXXXX]
INF ABOUT ARM/DARM
DISABLE / ENABLE
DIS SMS DUR ALM.
DISABLE / ENABLE
DIS CALL DURING ALM.
DISABLE / ENABLE
INFO SMS SCHED
PERIOD
[0... 99]
TIME
[0... 23]
TEMP SENSOR
TEMP. MIN
[-55... +125]
TEMP. MAX
[-55... +125]
INFO SMS
DISABLE / ENABLE
EXIT DELAY
[0... 600]
PASSWORD
DURESS PSW
N/A / [1... 10]
GBR PSW
N/A / [1... 10]
REMOVE PSW
[0000... 9999]
KEYBOARD PSW
PSW [1... 10]
PASSWORD
[0000... 9999]
PARTITION
PARTITION [0... 1]
PSW FOR SMS
[0000... 9999]
ALLOW ONLY PRS USR
DISABLE / ENABLE
ADMIN PSW
[0000... 9999]
SIREN SET
ALARM TIME
[1... 10]
BELL SQUAWK
DISABLE / ENABLE
RF LOSS ALARM
DISABLE / ENABLE
POWER STATUS
CHECK EXT. PWR ST
DISABLE / ENABLE
AC FAILURE DELAY
[0... 65535]
AC RESTORE DELAY
[0... 65535]
KEYBOARD PARTITION
PARTITION SWITCH
DISABLE / ENABLE
KBRD PARTITION
KBRD [1... 4] PARTITION
PARTITION [0... 1]
SMS LANGUAGE
LITHUANIAN / RUSSIAN / ENGLISH / ESTONIAN / LATVIAN / CZECH / SLOVAKIAN / GREEK
DATE/TIME SET
[YYYY-MM-DD HH:MM]
GSM AUDIO
MIC LEVEL
[0... 15]
SPEAKER LEVEL
[0... 100]
LOG SET
DISABLE / ENABLE

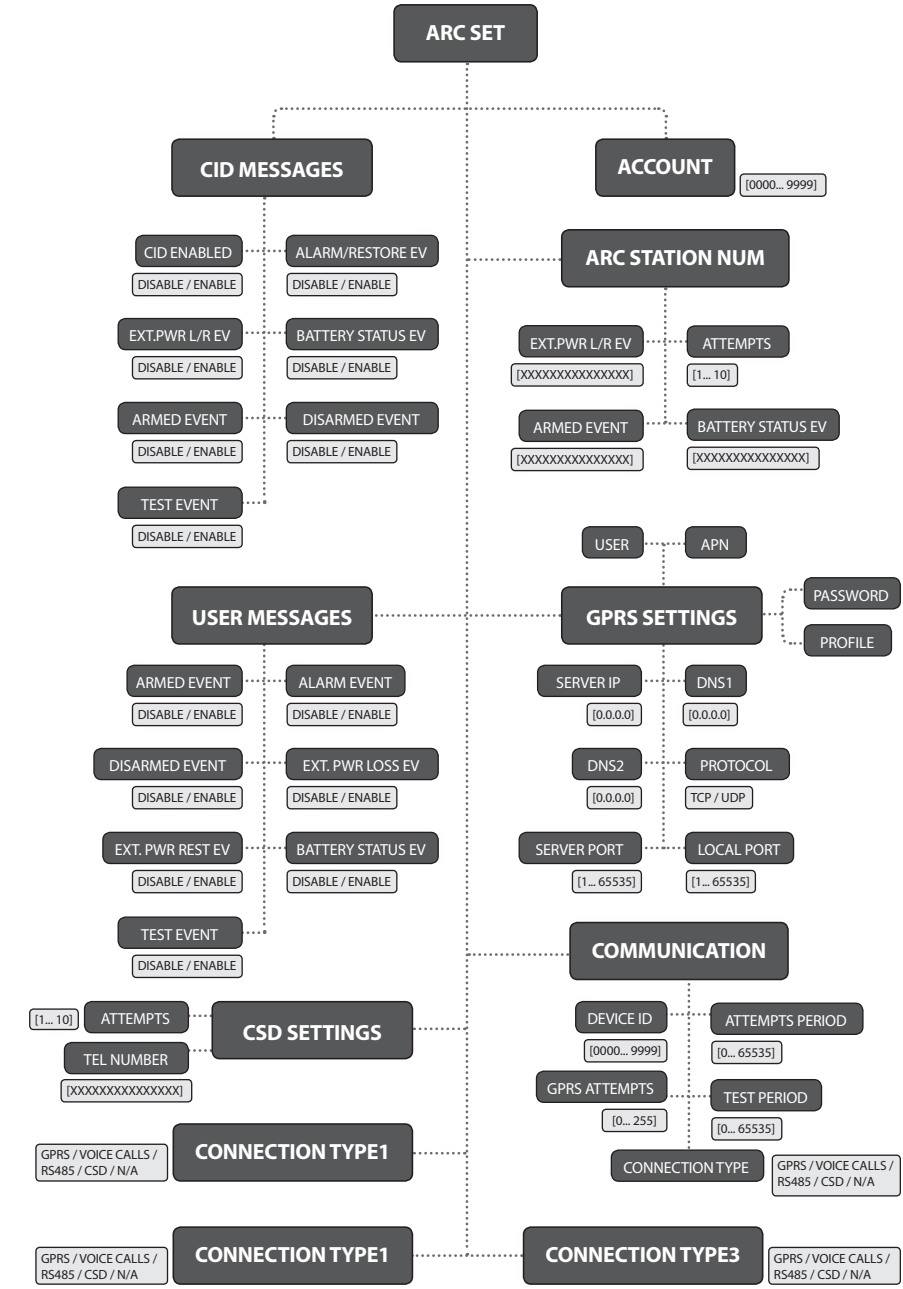

ZONES
WIRED ZONES
ZONE [1... 12]
STATUS
DISABLE / ENABLE
NAME
TYPE
FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
ENTRY DELAY
[1... 65535]
STAY
DISABLE / ENABLE
TAMPER NAME
PARTITION
PARTITION [0... 1]
FORCE
DISABLE / ENABLE
WIRELESS ZONES
RF ZONE [1... 16]
NAME
STATUS
DISABLE / ENABLE
ENTRY DELAY
[1... 65535]
TYPE
FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
TAMPER NAME
STAY
DISABLE / ENABLE
FORCE
DISABLE / ENABLE
PARTITION
PARTITION [0... 1]
KEYBOARD ZONES
[1ST... 4TH] KEYBOARD ZONE
STATUS
DISABLE / ENABLE
NAME
TYPE
FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
ENTRY DELAY
[1... 65535]
STAY
DISABLE / ENABLE
TAMPER NAME
PARTITION
PARTITION [0... 1]
FORCE
DISABLE / ENABLE
EPGM ZONES
EPGM ZONE [1... 16]
NAME
STATUS
DISABLE / ENABLE
ENTRY DELAY
[1... 65535]
TYPE
FOLLOW / INSTANT / 24H / DELAY / FIRE / SILENT
TAMPER NAME
STAY
DISABLE / ENABLE
FORCE
DISABLE / ENABLE
PARTITION
PARTITION [0... 1]
ZONE MODE NO ATZ
TYPE [1... 3]
ATZ MODE
DISABLE / ENABLE
ZONE MODE ATZ
TYPE [4... 5]
ARM/DISARM BY ZONE
N/A / ZONE [1... 44]
CHIME
DISABLE / ENABLE

MAIN SCREEN VIEW / OK / CONFIGURATION / PGM OUTPUTS



MAIN SCREEN VIEW / OK / CONFIGURATION / IBUTTON KEYS




ARC SET
CID MESSAGES
CID ENABLED
DISABLE / ENABLE
ALARM/RESTORE EV
DISABLE / ENABLE
EXT.PWR L/R EV
DISABLE / ENABLE
BATTERY STATUS EV
DISABLE / ENABLE
ARMED EVENT
DISABLE / ENABLE
DISARMED EVENT
DISABLE / ENABLE
TEST EVENT
DISABLE / ENABLE
ACCOUNT
[0000... 9999]
ARC STATION NUM
EXT.PWR L/R EV
[XXXXXXXXXXXXXXX]
ATTEMPTS
[1... 10]
ARMED EVENT
[XXXXXXXXXXXXXXX]
BATTERY STATUS EV
[XXXXXXXXXXXXXXX]
USER
APN
PASSWORD
PROFILE
GPRS SETTINGS
USER MESSAGES
ARMED EVENT
DISABLE / ENABLE
ALARM EVENT
DISABLE / ENABLE
DISARMED EVENT
DISABLE / ENABLE
EXT. PWR LOSS EV
DISABLE / ENABLE
EXT. PWR REST EV
DISABLE / ENABLE
BATTERY STATUS EV
DISABLE / ENABLE
TEST EVENT
DISABLE / ENABLE
SERVER IP
[0.0.0.0]
DNS1
[0.0.0.0]
DNS2
[0.0.0.0]
PROTOCOL
TCP / UDP
SERVER PORT
[1... 65535]
LOCAL PORT
[1... 65535]
COMMUNICATION
[1... 10]
ATTEMPTS
TEL NUMBER
[XXXXXXXXXXXXXXX]
CSD SETTINGS
DEVICE ID
[0000... 9999]
ATTEMPTS PERIOD
[0... 65535]
GPRS ATTEMPTS
[0... 255]
TEST PERIOD
[0... 65535]
CONNECTION TYPE
GPRS / VOICE CALLS / RS485 / CSD / N/A
GPRS / VOICE CALLS / RS485 / CSD / N/A
CONNECTION TYPE1
CONNECTION TYPE1
GPRS / VOICE CALLS / RS485 / CSD / N/A
CONNECTION TYPE3
GPRS / VOICE CALLS / RS485 / CSD / N/A

7.2 EKB3 - LED Keyboard

EKB3 is a LED keyboard intended for using with ESIM264 alarm system.

Main EKB3 keyboard features:

- arms and disarms the alarm system
- enables and disables *Stay* mode
- configures system parameters
- displays system status information by LED indicators
- informs about system status via built-in mini buzzer

The system configuration is performed by accessing EKB2 menu and entering the required values. ESIM264 system allows to connect up to 4 EKB3 keyboards.

7.2.1 Technical Specifications

7.2.1.1 Electrical & Mechanical Characteristics

Power Supply	12-14V ⎓ 150mA max
Maximum Keyboard Connection Cable Length	100 m.
Dimensions	140x100x18mm
Range of Operating Temperatures	-30...+55ºC

7.2.1.2 LED Funcionality

ARMED	Alarm system is armed /Configuration mode
READY	System is prepared for arming
SYSTEM	System troubles / valid command is being entered
BYPS	Zone bypass mode
1-12	Violated zone

7.2.1.3 Keys Functionality

[BYPS]	Zone bypass mode
[CODE]	Additional options - system trouble list / violated high zone indication / violated tamper indication
[*]	Configuration mode (when typed as a 1st character) / cancel command (when typed as a 2nd character) / keyboard partition switch (if enabled)
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[STAY]	(currently inactive)
[INST]	(currently inactive)

7.2.1.4 Connector Functionality

AUX+	Positive 12-14V ⎓ power supply contact
AUX-	Negative 12-14V ⎓ power supply contact
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common contact
Z1	Security zone
Z2	N/A

FRONT SIDE

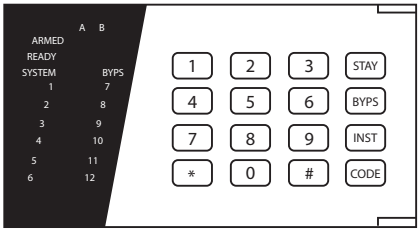


Fig. No. 16

BACK SIDE

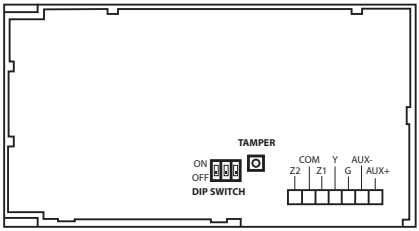


Fig. No. 17

7.2.1.5 Keyboard Address

DIP switches located on the back side of the keyboard are intended to set keyboard address. The keyboard address is configured by setting the DIP switch positions. ESIM264 alarm system allows to connect up to 4 EKB3 keyboards - each set under different address. DIP switch combinations for different keyboard address configuration are indicated in the table below.

Address Configuration

DIP Switch Position	Address
ON OFF 	Keyboard 1
ON OFF 	Keyboard 2
ON OFF 	Keyboard 3
ON OFF 	Keyboard 4

NOTE: Third switch is not active, therefore its' position is irrelevant.

The address of each connected keyboard is also indicated in *ELDES Configuration Tool* software.

7.2.2 Installation

1. Detach keyboard holder from EKB3 keyboard . Keyboard holder detach points are marked with arrows (see Fig. No. 18).

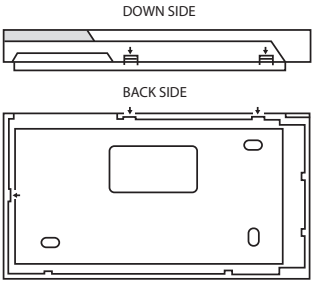


Fig. No. 18

2. Disconnect alarm system ESIM264 power supply and backup battery before connecting the wires.

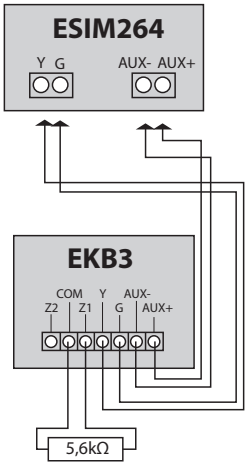


Fig. No. 19

3. Wire up keyboard contacts to ESIM264 alarm system respectively – **AUX+** to **AUX+, AUX-** to **AUX-**, **Y** to **Y**, **G** to **G**. (see Fig. No. 19).
4. Z1 and COM contacts must be connected with resistor of 5,6kΩ nominal (see Fig. No. 19). As keyboard zone Z1 is disabled by default, it can be enabled by SMS, *ELDES Configuration Tool,* EKB2 and EKB3 keyboard. Z2 contact is permanently inactive. Keyboard zone Z1 must be enabled and resistor connected even if the tamper button alone is required.
5. Set the keyboard address by combining DIP switch positions (see **7.2.1.5 Keyboard Address**).
6. Infix the keyboard into the holder (see Fig. No. 18).

ATTENTION! Before fixing the keyboard into the holder, please, make sure that the tamper is properly pressed (see Fig. No. 17).

7. Power up ESIM264 alarm system.
8. EKB3 keyboard is ready.

7.2.3 Operation Description

The green LED **READY** indicates that no zones are violated or no troubles are present and the system is prepared for arming. LED **SYSTEM** lights up or flashes in case of zone violation or if system troubles are present. The alarm system cannot be armed until the troubles are removed or violated zone (-s) is restored, bypassed or set up to operate under Force mode. The following troubles allow system arming when present:

- backup battery problem;
- main power supply failure;
- date & time not set;
- GSM connection problem.

The built-in mini buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the mini-buzzer provides continuous short beeps in case of alarm.
EKB3 keys have a LED back-light, therefore it is possible to use this keyboard even in dark premises. In case of alarm the keyboard back-light turns on and lasts until the system is disarmed. The back-light lasts for 3 minutes after the last key-stroke while the system is disarmed.

7.2.3.1 EKB3 Zone & Tamper

Keyboard EKB3 has one built-in zone Z1 and one tamper button. By default, the keyboard zone Z1 is disabled. The keyboard zone can be enabled by SMS, EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool*. When Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM contacts must be connected with resistor of 5,6kΩ nominal.
The tamper button is intended for monitoring the enclosure status of EKB3, therefore the system causes alarm if the enclosure is illegally opened. Keyboard zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

7.2.3.2 Arming & Disarming

The arming and disarming process is performed by entering a valid keyboard password. The default keyboard password is **1111**.
When the system is being armed, the red LED **ARMED** is illuminated continously and the system initiates the countdown, indicated by short beeps, intended for user to leave the premises. If the user does not leave the premises before the countdown is complete the system switches to *Stay* mode.
After user enters the secured premises, the system begins the countdown intended to enter a valid keyboard password. After the successful disarm process LED **ARMED** is switched off. In case user does not ener a valid keyboard password during the countdown, the system causes alarm and the LED of violated zone (-s) is illuminated continously.

NOTE: Arming & disarming can only be performed using a keyboard password assigned to the same partition as the keyboard.

7.2.3.3 Keyboard Partition

Any EKB3 keyboard can be assigned to one of two available partitions. Every system keyboard assigned to different partition can operate independently from each other. The keyboard partition can be assigned:

- permanently - by EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool;*
- temporally - by EKB2 keyboard and EKB3 keyboard using keyboard partition switch feature. The partition automatically switches back to previous partition in 3 minutes after the last key-touch/key-stroke.

In order to find out the keyboard's partition, please, check the position of illuminated LEDs **ARMED** and **READY**. If any of these LEDs is illuminated on the LED section A, the keyboard is assigned to partition 0, if on the B section – the keyboard is assigned to partition 1.

NOTE: The system can be configured using only one keyboard at a time regardless of the assigned keyboard partition. The flashing LED **SYSTEM** indicates an inactive EKB3 keyboard while **CONFIGURATION MODE** stays activated on another keyboard of any partition.

NOTE: The configuration is disabled while any system partition is armed.

See also chapter **5.4.16 Partitions.**

7.3 EPGM1 - Zone & PGM Output Expansion Module

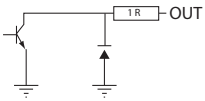
EPGM1 is a hardwired zone & PGM output expansion module intended for using with ELDES GSM alarm systems.

Main EPGM1 features:

- hardwired zone expansion adding 16 additional zones
- 2 PGM outputs for electrical appliance connection
- compatible with ESIM264

7.3.1 Technical Specifications

7.3.1.1 Electrical & Mechanical Characteristics

Power Supply	10-24V ⎓ 100mA max without Auxiliary Equipment.
Number of Digital Inputs	16
Nominal Resistance	5,6kΩ
Number of PGM Outputs	2
Maximum PGM Output Current	250 mA
PGM Output C1-C2 Circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum Commuting PGM Output Values	Voltage – 30V; current 250mA
Auxiliary Equipment Power Supply	13,8V ⎓ 500 mA max
Dimensions	118 x 47 mm
Range of Operating Temperatures	-20...+55°C

7.3.1.2 LED Functionality

C2, C1	PGM output C1, C2 status – on/off
Z1 - Z16	Zone Z1 - Z16 status – alarm/restore
STATUS	EPGM1 micro-controller status

7.3.1.3 Connector Funcionality

C1, C2	PGM outputs
Z1 - Z16	Security zones
AUX-	Negative 13,8V ⎓ power supply contact for auxiliary equipment
AUX+	Positive 13,8V ⎓ power supply contact for auxiliary equipment
Y	RS485 interface for communication (yellow wire)
G	RS485 interface for communication (green wire)
COM	Negative power supply contact
DC+	Positive power supply contact

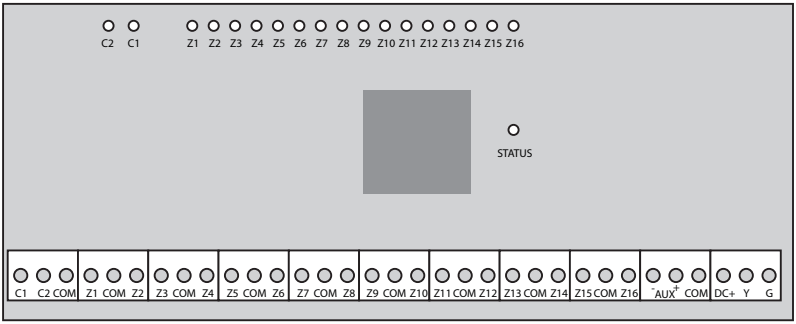


Fig. No. 20

7.3.1.4 Wiring Diagram

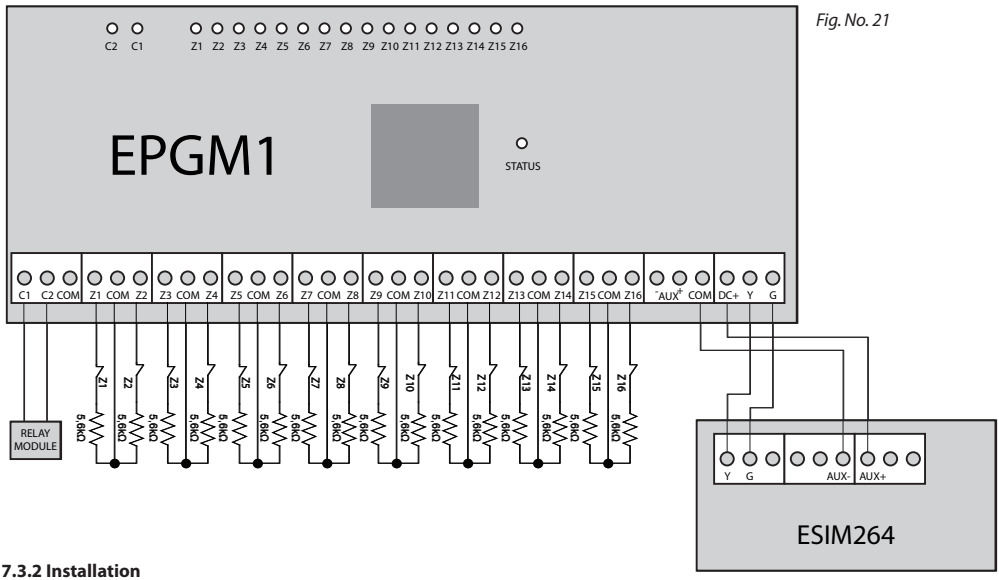


Fig. No. 21

7.3.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Connect EPGM1 DC+ contact to ESIM264 AUX+ contact, EPGM1 COM contact to ESIM264 AUX- contact. EPGM1 Y and G contacts must be connected to ESIM264 Y and G contacts respectively (see Fig. No. 21).
3. 3. Connect the resistors and sensors to EPGM1 module according to zone connection **Type 1**, **Type 2** or **Type 3.** See chapter **2.3.2 Zone Connection Types.**
4. Power up ESIM264 system.
5. Upon successful startup LED **STATUS** should be blinking indicating successful EPGM1 operation.
6. EPGM1 is ready for use with ESIM264 alarm system.

NOTE: ATZ mode is NOT supported for EPGM1 zones. ATZ mode is ineffective for EPGM1 zones when activated on ESIM264 alarm system.

7.4 EPGM8 - PGM Output Expansion Module

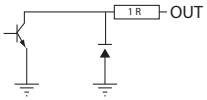
EPGM1 is a PGM output expansion module intended for using with ELDES GSM alarm system ESIM264. This module allows to connect up to additional 8 electrical appliances.

Main EPGM8 features:

- PGM output expansion adding 8 additional PGM outputs.
- compatible with ESIM264 alarm system

7.4.1 Technical Specifications

7.4.1.1 Electrical & Mechanical Characteristics

Power Supply	10-24V ⎓ 100mA max
Number of PGM Outputs	8
PGM Output D1-D8 Circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum Commuting PGM Output Values	Voltage – 30V; current 500mA
Dimensions	40 x 55 x 15 mm
Range of Operating Temperatures	-20...+55ºC

7.4.1.2 Connector Functionality

D1 - D8	PGM outputs
12V	Positive power supply contact
GND	Negative power supply contact

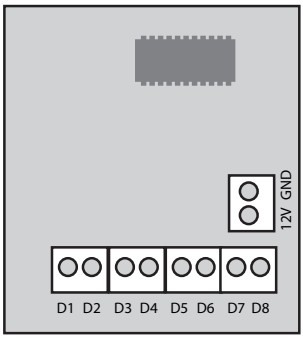


Fig. No. 22

7.4.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Insert EPGM8 pins into appropriate ESIM264 alarm system slots (see Fig. No. 23)

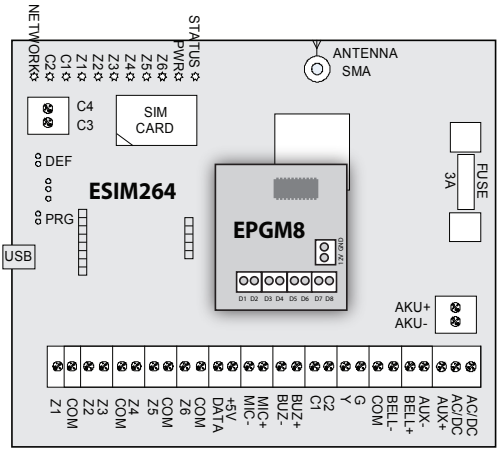


Fig. No. 23

3. Connect EPGM8 **12V** positive power supply contact with ESIM264 alarm system **AUX+** contact and EPGM8 GND contact with ESIM264 alarm system **AUX-** contact. (see Fig. No. 24).
4. Connect the electrical appliances to D1 – D8 PGM outputs. (see Fig. No. 24).

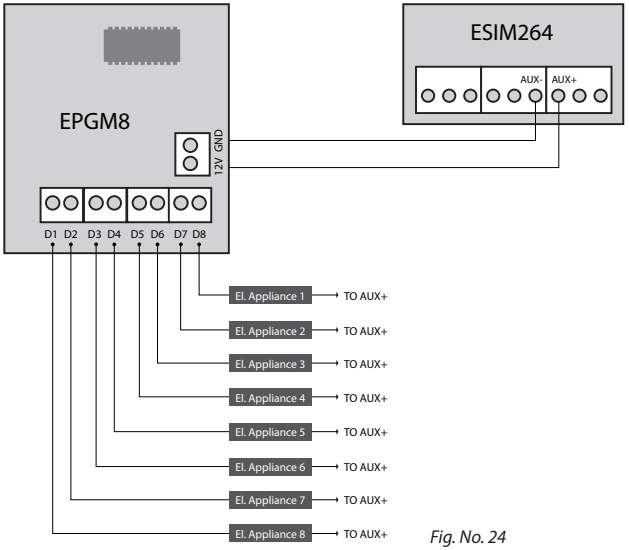


Fig. No. 24

5. Power up ESIM264 alarm system.
6. Enable EPGM8 mode using EKB2, EKB3 keyboards or *ELDES Configuration Tool* software. For more details, please, refer to software's HELP section or see chapter **5.4.7 PGM Outputs.**
7. EPGM8 is ready for use with ESIM264 alarm system.

7.5 EA1 – Audio Output Module

EA1 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA1 features:

- bi-directional voice conversation during a phone call
- possibility to connect headphones or desktop speakers

7.5.1 Technical Specifications

- 3,5 mm female jack
- Dimensions: 35 x 33 x 12 mm

7.5.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.

2. Insert EA1 pins into appropriate ESIM264 alarm system slots.

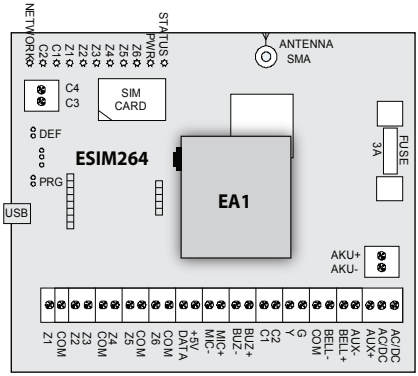


Fig. No. 25

3. Connect headphones or desktop speakers to EA1 3,5 mm female jack.

Fig. No. 26

4. Power up ESIM264 alarm system.
5. EA1 is ready for use with ESIM264 alarm system.

7.6 EA2 – Audio Output Module with Amplifier

EA2 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA1 features:

- bi-directional voice conversation during a phone call
- possibility to connect a speaker

7.6.1 Technical Specifications

- 1W 8Ω audio amplifier
- Dimensions: 41 x 40 x 24 mm

7.6.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.

2. Insert EA2 pins into appropriate ESIM264 alarm system slots.

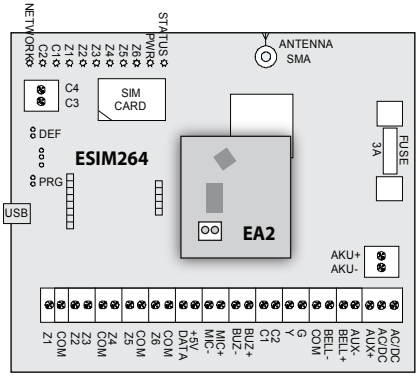


Fig. No. 27

3. Connect a speaker to EA2 Speaker contacts.

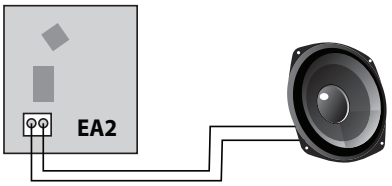


Fig. No. 28

4. Power up ESIM264 alarm system.

5. EA2 is ready for use with ESIM264 alarm system.

7.7 iButton® Key Reader & Keys

The iButton® key is a chip enclosed in a stainless steel tab usually implemented in a small plastic holder. Each iButton® key holds a unique identity code (ID) which is used for alarm system ESIM264 arming and disarming procedure.

Main features:

- Up to 5 iButton® keys per alarm system unit ESIM264.
- Communication via 1-Wire® interface.

7.7.1 Technical Specifications

7.7.1.1 Electrical & Mechanical Characteristics

Supported iButton® Key Model	Maxim®/Dallas® DS1990A
Communication Interface	1-Wire®
Maximum Cable Length for 1-Wire® Communication	up to 30 meters

7.7.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.

2. Connect iButton® key reader contact wires to 1-Wire® interface on ESIM264 alarm system: COM and DATA contacts respectively.

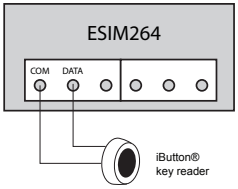


Fig. No. 29

3. Power up ESIM264 alarm system.

4. iButton® key reader is ready for use with ESIM264 alarm system.

7.7.3 Managing iButton® Keys

The procedure of adding an iButton® key to the system is performed by touching the iButton® key to the iButton® key reader when *New iButton® Key* mode is enabled (see Fig. No. 30). Alarm system ESIM264 supports up to 5 iButton® keys with different IDs.

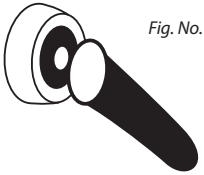


Fig. No. 30

NOTE: iButton® key1 ID can be added without *New iButton® Key* mode being enabled.

NOTE: When attempting to add the same iButton® Key ID twice, the system will consider this action as arming/disarming despite the *New iButton® Key* mode status.

Enable *New iButton® Key* Mode

This function enables *New iButton® Key* mode allowing to add the iButton® key IDs to the system. iButton® key1 can be added without *New iButton® Key* mode being enabled.

SMS

SMS text:
XXXX_IBPROG:ON
Example: 1111_IBPROG:ON

EKB2

Menu path:
OK → CONFIGURATION → IBUTTON KEYS → NEW IBUTTON → ENABLE

EKB3

Enter parameter 18 & parameter status value:
[180#]

Disable *New iButton® Key* Mode

This function disables *New iButton® Key* mode.

SMS

SMS text:
XXXX_IBPROG:OFF
Example: 1111_IBPROG:OFF

EKB2

Menu path:
OK → CONFIGURATION → IBUTTON KEYS → NEW IBUTTON → DISABLE

EKB3

Enter parameter 18 & parameter status value:
[181#]

Check iButton® Key ID

This function displays the added ID of a particular iButton® Key.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → IBUTTON KEYS → IBUTTON [1... 5] → ID

EKB3

N/A

Delete iButton® Key ID

If iButton® key is lost or stolen it is necessary to remove the key ID from the system.

SMS

SMS text:
XXXX_RESETIB
This feature removes ALL added iButton® key IDs at once.
Example: 1111_RESETIB

EKB2

Menu path:
OK → CONFIGURATION → IBUTTON KEYS → IBUTTON [1... 5] → REMOVE

EKB3

N/A

See also chapter **5.4.16 Partitions**

8. ELDES Wireless Devices

Main features:

- Up to 16 ELDES wireless devices per alarm system unit ESIM264 with EWT1 module installed.
- Two-way wireless communication.
- Supervised communication link with configurable self-test period.
- 4 wireless connection frequency modes.
- Maximum wireless connection range is 150 meters (in open areas).

NOTE: It is NOT RECOMMENDED to switch the frequency modes.

Add Wireless Device to the System

ELDES wireless device ID number is necessary in order to add the wireless device to the system. The device ID number is indicated on the outter or inner side of the wireless device enclosure.

SMS

SMS text:
XXXX_SET:yyyyyyyy
Value: yyyyyyyy – 8-digit wireless device ID number
Example: 1111_SET:535185D

EKB2

N/A

EKB3

N/A

NOTE: If you are unable to add a wireless device, please, restore the parameters of the wireless device to default and try again.

List Free Wireless Channels

The system supports up to 16 wireless channels intended for 16 wireless device connections. This feature allows to to check the list of free available wireless channels.

SMS

SMS text:
XXXX_STATUS_FREE
Example: 1111_STATUS_FREE

EKB2

N/A

EKB3

N/A

Replace Wireless Device

Both old and new device ID numbers are necessary in order to replace the wireless device. After successful replacement the configuration of the old wireless device is automatically applied to new device.

SMS

SMS text:
XXXX_REP:yyyyyyyy<zzzzzzzz
Value: yyyyyyyy – 8-digit old wireless device ID number; zzzzzzzz – 8-digit new device ID number.
Example: 1111_REP:535185D<41286652

EKB2

N/A

EKB3

N/A

Remove Wireless Device

The wireless device ID is necessary in order to remove the device from the system.

SMS

SMS text:
XXXX_DEL:yyyyyyyy
Value: yyyyyyyy – 8-digit wireless device ID number. *Example: 1111_DEL:535185D*

EKB2

N/A

EKB3

N/A

ATTENTION: In order to fully remove the device from the system, please, restore the parameters of ELDES wireless device to default AND remove it from the system. If the wireless device parameters are only reset to default or the device is only removed from the system, the wireless device (except EWK1) and the system attempts to exchange data packets every 10 seconds (attempts to keep wireless connection alive). This leads to faster battery discharge of battery-powered ELDES wireless devices.

Wireless Device Info

This command allows to retrieve the following information of a particular wireless device: wireless device battery level, wireless signal level, error rate (number of failed data transmission attempts in 10-minute period) and firmware version.

SMS

SMS text:
XXXX_RFINFO:Zn or XXXX_RFINFO:yyyyyyyy
Value: Zn - zone number of wireless device; yyyyyyyy - 8-digit wireless device ID
Example: 1111_RFINFO:8D2586B0

EKB2

OK -> CONFIGURATION -> RF DEVICES -> [RF DEVICE MODEL] [ID] -> BATTERY
OK -> CONFIGURATION -> RF DEVICES -> [RF DEVICE MODEL] [ID] -> SIGNAL
OK -> CONFIGURATION -> RF DEVICES -> [RF DEVICE MODEL] [ID] -> ERROR RATE
OK -> CONFIGURATION -> RF DEVICES -> [RF DEVICE MODEL] [ID] -> RF VERSION

EKB3

N/A

8.1 EWT1 - Wireless Transmitter-Receiver

Wireless transmitter-receiver EWT1 is an add-on module for ESIM264 system. It enables wireless transmission through alarm system ESIM264 and ELDES wireless devices, such as: wireless PIR movement sensors EWP1, wireless expansion modules EW1, wireless indoor sirens EWS1, wireless outdoor sirens EWS2, wireless magnetic door contacts EWD1 and wireless key-fobs EWK1.
EWT1 enables ESIM264 alarm system to connect up to 16 wireless devices at a time. Maximum wireless connection range is 150 meters (in open areas).

8.1.1 Technical Specifications

8.1.1.1 Electrical & Mechanical Characteristics

Wireless Transmitter-Receiver Frequency	868 MHz
Dimensions	68x38x18mm
Operating Temperature Range	-20...+55ºC
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Maximum Number of Wireless Devices	16

8.1.2 Installation

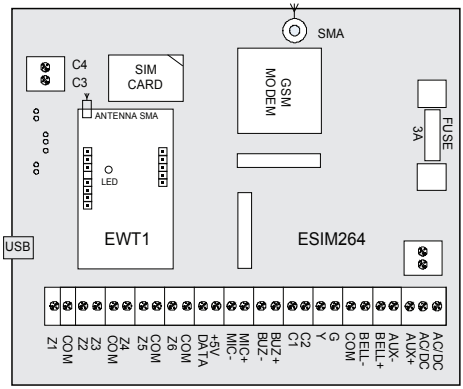


Fig. No. 31

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Insert EWT1 pins into appropriate ESIM264 slots as indicated in Fig. No. 31.
3. Mount the antenna to EWT1. It is not recommended to install the antenna inside the metal enclosure.
4. Power up ESIM264 system.
5. EWT1 is ready to use with ESIM264 system.

8.2 EW1 - Wireless Zone & PGM Output Expansion Module

Wireless expansion module EW1 is a wireless device with 2 zones and 2 PGM outputs. This expansion module connects to ELDES wireless alarm systems and enables wireless access for to 2 wired devices such as movement PIR sensors, magnetic door contacts etc. In addition it allows to connect and control up to 2 appliances, i.e. lighting, heating etc. After the wiring process to EW1 it is necessary to bind EW1 to the alarm system by sending a corresponding command via SMS message or using software *ELDES Configuration Tool*. It is possible to connect up to 16 EW1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

8.2.1 Technical Specifications

8.2.1.1 Electrical & Mechanical Characteristics

Power Supply	7-15V ⎓ 20mA max
Number of Zones	2
Number of PGM Outputs	2
Wireless Transmitter-Receiver Frequency	868 MHz
Range of Operating Temperatures	-20...+55ºC
Dimensions	38x60x12mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Maximum Commuting PGM Output Values	Voltage – 30V; current 500mA

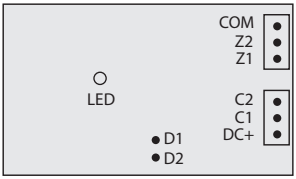
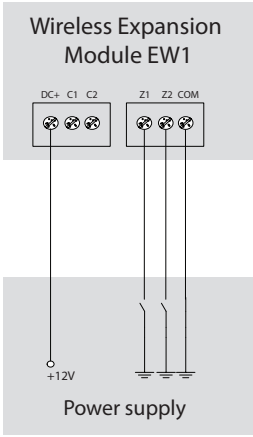


Fig. No. 32

Fig. No. 33



8.2.1.2 Connector & LED Functionality

COM	Common contact for power supply, zones, PGM outputs
Z2, Z1	Security zones
C2, C1	PGM outputs
DC+	Positive power supply contact
D1, D2	Pins for restoring default settings
LED	EW1 status

8.2.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Wire up EW1 as indicated in Fig. No. 33
3. Bind the device to ESIM264 alarm system. Use *ELDES Configuration Tool* software or send a corresponding SMS message. Please refer to software's HELP section or refer to installation manual of ELDES alarm system.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EW1 closer to ESIM264 alarm system device and bind anew.
5. EW1 module is ready for use.

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **8.2.4 Restoring Default Parameters** for more details.

8.2.3. EW1 Zones, PGM Outputs & Tamper

Upon successful EW1 module binding process, the system adds 2 wireless *Instant zones* intended for wired sensor connection and 2 wireless PGM outputs intended for electrical appliance connection and control.
The wireless connection loss between EW1 and ESIM264 alarm system leads to system alarm regardless of system being armed or disarmed. The system identifies this event as a tamper violation and sends alarm by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

8.2.4 Restoring Default Parameters

1. Disconnect EW1 power supply.
2. Short circuit (connect) pins D1 and D2.
3. Power up EW1 and wait until LED provides several short flashes.
4. Disconnect power supply.
5. Remove short-circuit from D1 and D2 pins.
6. Power up EW1.
7. Parameters restored to default.

8.3 EWP1 – Wireless PIR Movement Sensor

EWP1 is a wireless device with integrated PIR movement detector and operates with ELDES wireless alarm systems. The user only needs to switch on the EWP1 sensor and bind it to ESIM264 alarm system by sending a corresponding command via SMS message or using software *ELDES Configuration Tool*. User can also monitor temperature of the surrounding areas in real-time as EWP1 has a built-in temperature sensor.
It is possible to connect up to 16 EWP1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

8.3.1 Technical Specifications

8.3.1.1 Electrical & Mechanical Characteristics

Battery Type	ER14505 AA Lithium Thionyl Chloride
Battery Voltage; Capacity	3,6 V; 2,4 Ah
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 MHz
Range of Operating Temperatures	-10 ... +55°C
Dimensions	104x60x33mm
Detection Coverage Angle	90°
Maximum Detection Distance	10 meters
Compatible with Alarm Systems	ELDES Wireless
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas

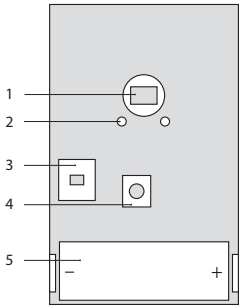


Fig. No. 34

* This operation time might vary in difference conditions.

1 – Motion detector
2 – LED indicators informing about status of PIR sensor EWP1
3 – TAMPER button automatically identifies when the box of sensor EWP1 is open or closed
4 – RESET button for reseting system parameters
5 – ER14505 3,6 V Lithium Thionyl Chloride battery

8.3.2 Installation

1. Choose the place where intrusion into the premises is the most probable and install the device. To avoid false triggers of the system do not install it in the following places:

   • directing the lens to direct sunlight, for example, to the window of the premises;
   • where there is a risk of sudden temperature alteration, for example, near a fireplace or heating system;
   • where there is an enlarged possibility of dust or air flow;
   • behind the curtain or some other cover blocking the detected zone.

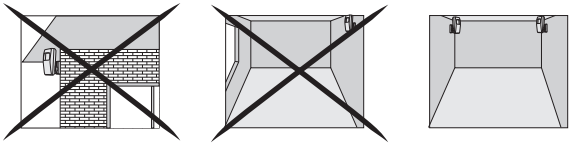


Fig. No. 35

2. Fix EWP1 sensors mounting holder with two screws to the wall and attach the sensor.
3. Bind the device to ESIM264 alarm system. Use a software *ELDES Configuration Tool* or send corresponding SMS messages. Please refer to software's HELP section or refer to chapter **8. ELDES Wireless Devices** for more details.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWP1 closer to alarm system device and bind anew.
5. EWP1 is ready to use.

8.3.3 EWP1 Zone & Tamper

Upon successful EWP1 sensor binding process, the system adds 1 wireless *Instant* zone intended for movement detection. By, default, the alarm is caused instantly if any movement is detected in coverage area of the sensor (when system is armed).
In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWP1 sensor:

- **By tamper button.** EWP1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWP1 is illegally opened, the tamper button becomes unpressed. This action is followed by alarm which is sent by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWP1 sensor and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

8.3.4 Battery Replacement

Only ER14505 AA Lithium Thionyl Chloride batteries should be used. Install only new, good quality and unexpired batteries. In order to replace old battery with a new one, open the case of EWP1 and remove the old battery. Then insert new ER14505 3,6V Lithium Thionyl Chloride battery.

ATTENTION: The battery must be removed if device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

ATTENTION: Using software *ELDES Configuration Tool* it is possible to watch the status of the battery in real-time.

8.3.5 Restoring Default Parameters

1. Remove any battery from EWP1.
2. Press and hold the RESET button.
3. Insert the battery back to EWP1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

8.4 EWD1 – Wireless Magnetic Door Contact

EWD1 is a wireless device with magnetic contact and panic button which is used to secure doors, windows or any other opening parts and it operates with ELDES wireless alarm systems. EWD1 is bind to ESIM264 alarm system by sending a corresponding command via SMS message or using software *ELDES Configuration Tool*. When EWD1 is connected to the system, two wireless zones are added. First wireless zone is used to monitor the magnetic contacts and the second wireless zone is for managing the panic button. By default panic button zone is configured as Silent zone and in case the panic button is pressed, the system causes silent alarm (no siren is activated).
It is possible to connect up to 16 EWD1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

8.4.1 Technical Specifications

8.4.1.1 Electrical & Mechanical Characteristics

Battery Type	CR2032 3V Lithium
Number of Batteries	1
Battery Operation time	15 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55ºC
Door Contact Dimensions	60x37x18mm
Magnet Dimensions	60x17x16mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

* This operating time may vary in difference conditions.

8.4.2 Installation

1. Open EWD1 enclosure and insert the battery (Fig. No. 36).

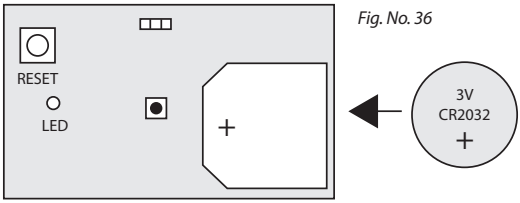


Fig. No. 36

2. Magnetic door contact consists of two parts: a magnet and a sensor. Sensor components are: a mounting part and the sensor. Magnet components are: a mounting part and the cover.

2.1 Fix the sensor mounting part with two screws on the door or window jamb.

2.2 Fix the magnet mounting part with two screws next to the sensor mounting part on door or window frame. How to fix the magnetic door contact correctly see Fig. No. 37. The distance between the magnet and the door contact must be no larger than 20 mm.

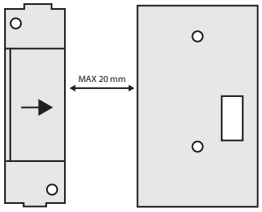


Fig. No. 37

2.3 The sensor should be attached to the fixed sensors mounting part. When attaching sensor pay attention to the tamper (micro switch) - it must be pressed.
2.4 The magnet cover should be attached to the fixed magnet mounting part.

NOTE: It is not recommend to fix EWD1 in other ways than with screws, e.g. with duck tape.
See Fig. No. 38 for the incorrect ways of fixing the magnetic door contact.

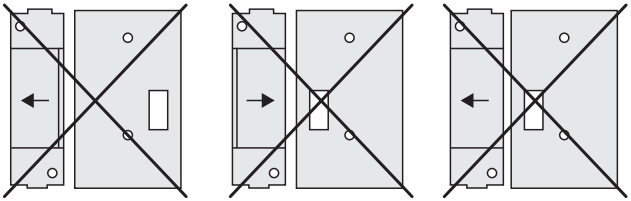


Fig. No. 38

3. Bind the device to ESIM264 alarm. Use a software *ELDES Configuration Tool* or send corresponding SMS messages. Please refer to software's HELP section or refer to chapter **8. ELDES Wireless Devices** for more details.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWD1 closer to alarm system device and bind anew.
5. EWD1 magnetic door contact is ready to use.

8.4.3 EWD1 Zones & Tamper

Upon successful EWD1 magnetic door contact binding process,the system adds 1 wireless *Instant* zone and 1 wireless *Silent* zone. The wireless zones are applied to the following EWD1 components respectively:

- **Magnetic contact -** by default, causing alarm if doors/windows is opened when system is armed.
- **Panic button** - by default, causing silent alarm instantly when pressed.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWD1:

- **By tamper button.** EWD1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWD1 is illegally opened, the tamper button becomes unpressed. This action is followed by alarm which is sent by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWD1 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

8.4.4 Battery Replacement

Only CR2032 3V Lithium batteries should be used. Install only new, good quality and unexpired batteries. In order to replace old battery with a new one, remove front cover of the magnetic door contact (see chapter **8.4.2 Installation**), carefully remove the device PCB and remove old battery. Then insert the new CR2032 3V Lithium battery.

ATTENTION: The battery must be removed if device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: Using software *ELDES Configuration Tool* it is possible to watch the status of the battery in real-time.

8.4.5 Restoring Default Parameters

1. Remove the battery from EWD1.
2. Press and hold the RESET button.
3. Insert the battery back to EWD1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

8.5 EWK1 - Wireless Key-Fob

Key-fob EWK1 – is a wireless device intended to arm and disarm ESIM264 alarm system, to open and close the gates or to control any other device connected to the alarm system. Wireless key-fob EWK1 is compatible with ELDES wireless alarm systems, therefore user can easily bind it to the alarm system using *ELDES Configuration Tool* software or sending a corresponding SMS command. EWK1 key-fob features four configurable buttons intended to operate according to individual needs. After the button is pressed, EWK1 internal buzzer's sound signal confirms a transferred command to ESIM264 alarm system via wireless connection. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button and holding it for 3 seconds. 3 short sound signals indicate a successfully carried out command while 1 long beep stands for failed command and feedback signal failure. By default one pair of buttons is already configured to arm and disarm the alarm system.

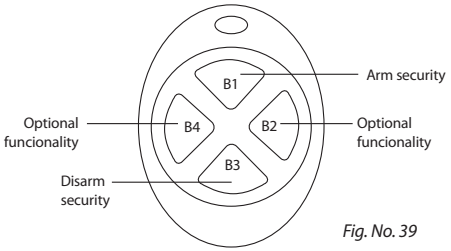


Fig. No. 39

The virtual zones of ESIM264 system are intended for EWK1 button configuration. Please, refer to software's *ELDES Configuration Tool* HELP section for more details.
It is possible to connect up to 16 EWK1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

NOTE: Fig. No. 39 reflects the default EWK1 button configuration. All key-fob buttons are configurable according to individual needs.

8.5.1 Technical Specifications

8.5.1.1 Electrical & Mechanical Characteristics

Battery Type	CR2032 Lithium
Battery Voltage; Capacity	3V; 240 mAh
Quantity of Batteries	1
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55ºC
Wireless Key-fob Dimensions	54 x 42 x 13 mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

* This operation time depends on different conditions and may vary.

8.5.2 Installation

1. Unscrew the EWK1 key-fob housing.

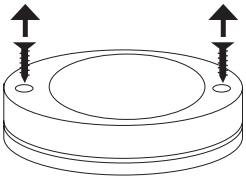


Fig. No. 40

2. Open EWK1 key-fob housing.

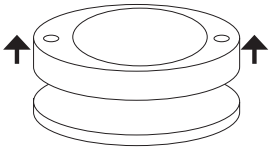


Fig. No. 41

3. Insert CR2032 battery provided in the EWK1 package.
Before inserting the battery, make sure that the battery's "+" sign is facing the outer side.

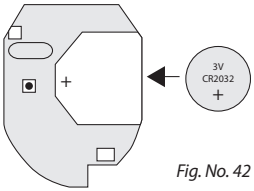


Fig. No. 42

4. Close and screw up the key-fob housing.

5. Bind the device to alarm system by sending a corresponding command via SMS message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to chapter **8. ELDES Wireless Devices** for more details.

6. After binding the device to the alarm system, press any EWK1 button several times.

7. EWK1 is ready to use.

ATTENTION: EWK1 wireless key-fob is supported from v16.4 firmware version of EWT1 wireless transmitter-receiver module. In order to find out the firmware version of EWT1 module, please, contact ELDES technical support: support@eldes.lt

8.5.3 EWK1 Zones (Panic Button)

EWK1 key-fob supports a *Panic Button* feature allowing to cause alarm at any time when the specified button is pressed. This feature can be configured using *ELDES Configuration Tool* by creating a virtual zone of *Silent* or *24H* type and assigning it to *Virtual Alarm* option. The *Panic Button* feature can be set up on any button of EWK1.

8.5.4 Battery Replacement

Only CR2032 3V Lithium batteries can be used for device powering. Install only new, good quality and not expired batteries. In order to replace the old battery with a new one, remove front cover of the EWK1 key-fob housing (see chapter **8.5.2 Installation**), carefully remove the PCB and remove the old battery. Then insert the new CR2032 3V Lithium battery.

ATTENTION: The battery must be removed when device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, only approved batteries can be used with the system. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only at special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: Using software *ELDES Configuration Tool* it is possible to watch the status of the battery in real-time.

8.5.5 Restoring Default Parameters

1. Remove the battery from EWK1 key-fob.
2. Press and hold B4 button.
3. Insert the battery back to EWK1.
4. Hold the button pressed until LED indicator provides several short flashes.
5. Release B4 button.
6. Parameters restored to default.

8.6 EWS1 – Wireless Indoor Siren

EWS1 is a wireless device with built-in siren speaker and operates with ELDES wireless alarm systems. EWS1 has to be bind to the alarm system by sending a corresponding SMS message or using software *ELDES Configuration Tool*. Upon successful EWS1 binding, the system adds one wireless zone and one wireless PGM output. The wireless zone is used to monitor the device (tamper - when the batteries are being removed) and the wireless PGM output is used to control the speaker. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS1 in order to save the battery power.

It is possible to connect up to 16 EWS1 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

8.6.1 Technical Specifications

8.6.1.1 Electrical & Mechanical Characteristics

Battery Type	1,5V Alkaline AA type
Number of Batteries	3
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55ºC
Dimensions	123x73x36mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

* This operation time might vary in difference conditions.

8.6.1.2 Main Unit & LED Functionality

RESET	Button for restoring default parameters
+ / -	Battery slots
LED	EWS1 status indication

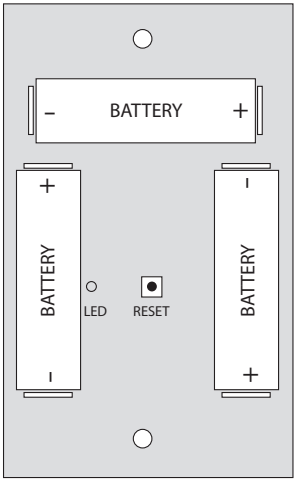


Fig. No. 43

8.6.2 Installation

1. Open EWS1 enclosure.

   Insert a thin flat-shaped screwdriver or any tool alike into the gap located on the back of the enclosure (see Fig. No. 44).

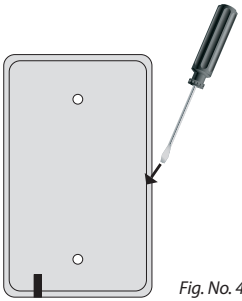


Fig. No. 44

Push the screwdriver down to the right carefully in order to detach the enclosure parts from each other (see Fig. No. 45)

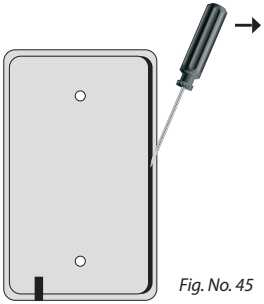


Fig. No. 45

2. Once the enclosure is opened, remove the plastic tab inserted between one of the battery terminals and battery slot contact (see Fig. No. 46).

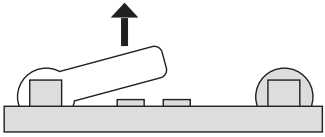


Fig. No. 46

3. Fix the siren on the wall using the screws (see Fig. No. 47).

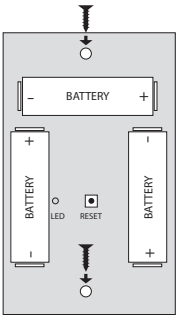


Fig. No. 47

4. Close EWS1 enclosure. No tools are required for this action.
5. Bind the device to the alarm system by sending a corresponding command via SMS message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to chapter **8. ELDES Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS1 closer to alarm system device and bind anew.,
7. EWS1 siren is ready for use.

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **8.6.5. Restoring Default Parameters** for more details.

8.6.3 EWS1 Zone, PGM Output & Tamper

Upon successful EWS1 indoor siren binding process,the system adds 1 wireless *Instant* zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS1 tamper control and the wireless PGM output is for siren control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. The wireless connection loss between EWS1 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS message and phone call to the user (-s) by default. The SMS message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

8.6.4 Battery Replacement

1. Open EWS1 enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS1
4. Insert the batteries into the battery slots.
5. Batteries replaced.

See chapter **8.6.2 Installation** for more details.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

8.6.5 Restoring Default Parameters

1. Remove any battery from EWS1.
2. Press and hold the RESET button.
3. Insert the battery back to EWD1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

8.7 EWS2 – Wireless Outdoor Siren

EWS2 outdoor siren is externally powered siren with integrated wireless module EW1. This wireless module EW1 connects to ELDES wireless alarm systems and managing EWS2 siren to work with alarm system. EWS2 is bind it to alarm system by sending a corresponding command via SMS message or using software *ELDES Configuration Too*l and configure zones and PGM outputs. The siren has a built-in battery and in case of power supply failure, it starts alarming. In case of alarm, the siren provides a sound alarm for one minute. This parameter can be configured. Please, refer to chapter **5.4.8 Siren** for more details.
EW1 module also has one unused zone and one unused PGM output. They can be used to connect variuos additional devices such as motion sensors, smoke detectors and etc (see chapter **8.2 EW1 - Wireless Zone & PGM Output Expansion Module**). For detailed information of siren configuration, please, refer to **Pyronix Decibell E** siren manual.
It is possible to connect up to 16 EWS2 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

8.7.1 Technical Specifications

8.7.1.1 EW1 Electrical & Mechanical Characteristics

Power Supply	7-15V ⎓ 150mA max
Number of Zones	2
Number of PGM Outputs	2
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55ºC
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Maximum Allowed Zone Voltage Values	0-30V
Maximum Allowed PGM Output Values	Voltage – 30V; current - 500mA

8.7.1.2 EW1 Connector & LED Functionality

COM	Common contact for power supply, zones, PGM outputs
Z2, Z1	Security zones
DC+	Positive power supply contact
D1, D2	Pins for restoring default settings
LED	EW1 status

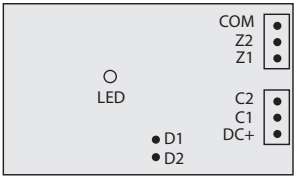


Fig. No. 48

8.7.1.3 Pyronix Decibell E Siren Connector Functionality

+12 V	Positive power supply contact
- 12 V	Negative power supply contact
BAT+	Positive battery contact
BAT-	Negative battery contact
SOUNDER+	Positive speaker contact
SOUNDER-	Negative speaker contact
BELL	Bell signal contact
STB	Strobe signal contact
TAMPER	Tamper
TAMPER	Tamper

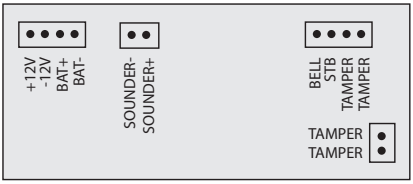
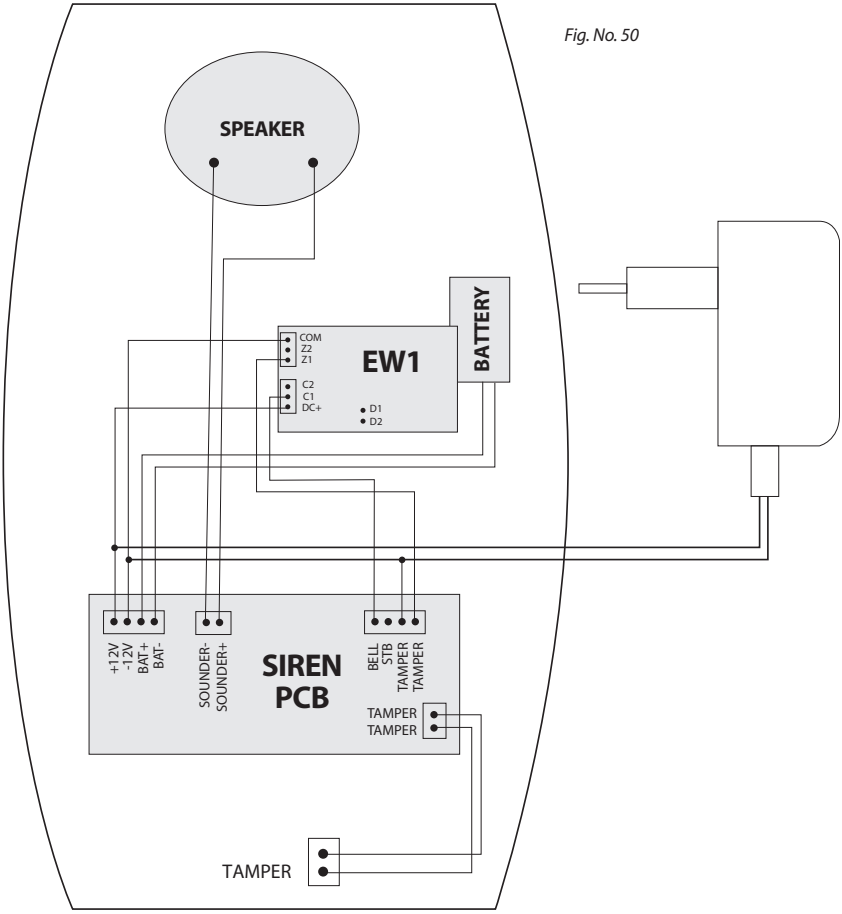


Fig. No. 49

8.7.2 Installation

Fig. No. 50



1. Connect the power supply and battery cables as shown in diagram (see Fig. No. 50).
2. Fix the siren to the wall.
3. Connect the power supply.
4. Bind EW1 device to alarm system by sending a corresponding command via SMS message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to chapter **8. ELDES Wireless Devices** for more details. If attempt to bind is unsuccessful, try to move siren EWS2 closer to central monitoring station and bind anew.
5. Disable EW1 zone Z2. Set EW1 PGM output C1 type to *Siren*.
6. EWS2 siren is ready to use.

8.7.3 Restoring Default Parameters

1. Disconnect EW1 power supply.
2. Short circuit (connect) pins D1 and D2.
3. Power up EW1 and wait untill LED provides several short flashes.
4. Disconnect power supply.
8. Remove short-circuit from D1 and D2 pins.
9. Power up EW1.
10. Parameters restored to default.

9. Monitoring Station

9.1 Basic Overview

The data transmission from ESIM264 alarm system to monitoring station can be carried out by one of the following communication methods at a time:

- GPRS Network;
- Voice Calls (GSM Audio);
- RS485 Interface;
- CSD (Circuit Switched Data).

The system supports 1 primary communication and up to 3 backup communications. All of the aforementioned communication methods can be set up as primary or backup in any sequence order by EKB2 keyboard, EKB3 keyboard and *ELDES Configuration Tool* software. For more details, please, refer to software's HELP section and chapter **9.3 Monitoring Station Parameter Configuration (SMS, EKB2, EKB3).**

ATTENTION: ESIM264 system is fully compatible with *Kronos NET/Kronos LT* monitoring station software for communication via GPRS network. When using different monitoring station software, *EGR100* GPRS software is necessary. *EGR100* is freeware and can be downloaded at www.eldes.lt

9.2 Event Messages

The event messages can either be transmitted to monitoring station alone or to monitoring station with duplication by SMS (user messages) to User1 phone number.

The following table provides the CID codes of events supported by ESIM264 alarm system:

Seq. No.	Contact ID® Code	Event Description	Duplication by SMS
1	1110	Fire Zone Alarm	✓*
2	3111	Fire Zone Restore	
3	1121	Armed by User (Duress Password)	✓**
4	3121	Disarmed by User (Duress Password)	✓**
5	1130	Burglary Alarm	✓*
6	3130	Burglary Restore	
7	1133	24H Zone Alarm	✓*
8	3133	24H Zone Restore	
9	1144	Tamper Alarm	✓
10	3144	Tamper Restore	
11	1146	Silent Zone Alarm	✓*
12	3146	Silent Zone Restore	
13	1158	Temperature Exceeded	✓
14	1159	Temperature Fallen	✓
15	1301	Main Power Loss	✓
16	3301	Main Power Restore	✓
17	1302	Wireless Sensor Low Battery	✓
18	1308	Device Shut Down	
19	1311	ESIM264 Backup Battery Fail	✓
20	1381	Wireless Signal Loss	✓***
21	3381	Wireless Signal Restore	
22	1401	Armed by User	✓
23	3401	Disarmed by User	✓
24	1456	Armed by User (Stay Mode)	✓**
25	3456	Disarmed by User (Stay Mode)	✓**
26	1463	Armed by User (SGS Password)	✓**
27	3463	Disarmed by User (SGS Password)	✓**
28	1602	Periodical Test	✓
29	1900	Device Started	✓

* - does not contain specific alarm type indication.
** - does not contain password type *Stay* mode indication.
*** - contains violated tamper number with a star "*" character.

9.3 Monitoring Station Parameter Configuration (SMS, EKB2, EKB3)

9.3.1 Main Parameters

Enable CID mode

This mode enables data transmission from alarm system ESIM264 to the monitoring station. By default, this mode is disabled.

SMS

SMS text:
XXXX_scnset:on

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → CID ENABLED → ENABLE

EKB3

Enter parameter 23 & parameter status value:
[231#]

Disable CID mode

This command disables CID mode.

SMS

SMS text:
XXXX_scnset:off

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → CID ENABLED → DISABLE

EKB3

Enter parameter 23 & parameter status value:
[230#]

Enable CID Messages

This command enables a particular CID message.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → CONTACT ID MSG → ALARM/RESTORE EV → ENABLE
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → EXT. PWR L/R EV → ENABLE
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → BATTERY STATUS EV → ENABLE
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → ARMED EVENT → ENABLE
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → DISARMED EVENT → ENABLE
OK → CONFIGURATION → ARC SET → CONTACT ID MSG → TEST EVENT→ ENABLE

EKB3

Enter parameter 24, event number & parameter status value:

[24011#] - Alarm/Restore Event
[24021#] - Main Power Loss/Restore Event
[24031#] - Backup Battery Status Event
[24041#] - Armed Event
[24051#] - Disarmed Event
[24061#] - Test Event

Enable User messages when CID mode enabled

User Messages allow to select particular SMS messages to be delivered to users when CID mode is enabled. By default, all *User Messages* are disabled.

Available User messages:

Alarm Event – SMS about alarm events.

Disarmed Event – SMS about disarm events.

Armed Event – SMS about arm events.

Main Power Loss Event – SMS about main power supply loss events.

Main Power Restore Event – SMS about main power supply restore events.

Backup Battery Status Event - SMS about low backup battery status.

Test Event - SMS with test information about the status of the device.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → USER MESSAGE → ALARM EVENT → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → ARMED EVENT → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → DISARMED EVENT → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → EXT. PWR LOSS EV → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → EXT. PWR REST EV → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → BATTERY STATUS EV → ENABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → TEST EVENT→ ENABLE

EKB3

Enter parameter 25, event number & parameter status value:

[25011#] - Alarm Event
[25021#] - Disarmed Event
[25031#] - Armed Event
[25041#] - Main Power Loss Event
[25051#] - Main Power Restore Event
[25061#] - Backup Battery Status Event
[25071#] - Test Event

Disable User Messages

This command disables particular *User Messages.*

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → USER MESSAGE → ALARM EVENT → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → ARMED EVENT → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → DISARMED EVENT → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → EXT. PWR LOSS EV → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → EXT. PWR REST EV → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → BATTERY STATUS EV → DISABLE
OK → CONFIGURATION → ARC SET → USER MESSAGE → TEST EVENT → DISABLE

EKB3

Enter parameter 25, event number & parameter status value:

[25010#] - Alarm Event
[25020#] - Disarmed Event
[25030#] - Armed Event
[25040#] - Main Power Loss Event
[25050#] - Main Power Restore Event
[25060#] - Backup Battery Status Event
[25070#] - Test Event

Account (Alarm System ID)

Account is an alarm system ID code required for identification by monitoring station. This ID code is transmitted via data message allowing the monitoring station to identify the alarm system device. The default Account ID **9999** must be changed.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → ACCOUNT → [XXXX]

Value: [XXXX] – 4 digit account ID code, range – [0000... 9999]

EKB3

Enter parameter 27 & account ID code

[27xxxx#]

Value: xxxx – 4 digit account ID code, range – [0000... 9999]

Set Primary Communication Type

Primary communication type for data transmission from the alarm system to monitoring station. Available types: GPRS Network, Voice Calls (GSM audio channel), RS485, CSD. By default the primary communication type is **GPRS network.**

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → COMMUNICATION → CONNECTION TYPE → GPRS / VOICE CALLS / RS485 / CSD / N/A

EKB3

Enter parameter 48 & connection type value:

[480#] - GPRS Network
[481#] - Voice Calls
[482#] - RS485
[483#] - CSD
[484#] - N/A

Set Backup Communication Type (-s)

This command sets the sequence order of backup communication types in case of primary communication failure. There can be up to 3 backup communications set in any sequence order.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → CONNECTION TYPE1 → GPRS / VOICE CALLS / RS485 / CSD / N/A
OK → CONFIGURATION → ARC SET → CONNECTION TYPE2 → GPRS / VOICE CALLS / RS485 / CSD / N/A
OK → CONFIGURATION → ARC SET → CONNECTION TYPE3 → GPRS / VOICE CALLS / RS485 / CSD / N/A

EKB3

Enter parameter 83, backup communication entry number & communication type value:

[83xx0#] - GPRS Network
[83xx1#] - Voice Calls
[83xx2#] - RS485
[83xx3#] - CSD
[83xx4#] - N/A

Value: xx - backup communication entry number, range - [01... 03]

Delay Between Attempts

This feature allows to set a delay period of time between data message sending attempts to monitoring station in case the initial attempt was unsuccessful. By default, this time period is **600** seconds.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → COMMUNICATION → ATTEMPTS PERIOD → [XXXXX]

Value: [XXXXX] – delay between attempts time period in seconds, range – [0... 65535]

EKB3

Enter parameter 69 & time period:

[69x#]

Value: x - delay between attempts time period in seconds, range – [0... 65535]

Test Period

Time period of data test message sending to monitoring station. This message is intended for alarm system status checking. The default test period is **180** seconds.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → COMMUNICATION → TEST PERIOD → [XXXXX]

Value: [XXXXX] – test time period in seconds, range - [1... 65535]

EKB3

Enter parameter 46 & test time period:

[46xx#]

Value: xx – test time period in seconds, range - [1... 65535]

9.3.2 GPRS Network Settings

Server IP address (GPRS)

Public IP address of the monitoring station. This parameter is intended for communication between the alarm system and monitoring station via GPRS network.

SMS
SMS text:
XXXX_setgprs:ip:0.0.0.0
Value: 0.0.0.0 – Server IP address digits

EKB2
Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → SERVER IP → [0.0.0.0]
Value: [0.0.0.0] – Server IP address digits

EKB3
Enter parameter 40 & Server IP address:
[40xxxxxxxxxxx]
Value: xxxxxxxxxxxx – Server IP address digits

DNS1 Server IP Address (GPRS)

Primary DNS server IP address.

SMS
SMS text:
XXXX_setgprs:dns1:0.0.0.0
Value: 0.0.0.0 – DNS1 IP address digits

EKB2
Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → DNS1 → [0.0.0.0]
Value: [0.0.0.0] – DNS1 IP address digits

EKB3
Enter parameter 41 & DNS1 IP address:
[41xxxxxxxxxx]
Value: xxxxxxxxxxx – DNS1 IP address digits

DNS2 server IP address (GPRS)

Secondary DNS server IP address.

SMS
SMS text:
XXXX_setgprs:dns2:0.0.0.0
Value: 0.0.0.0 – DNS2 IP address digits

EKB2
Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → DNS2 → [0.0.0.0]
Value: [0.0.0.0] – DNS2 IP address digits

EKB3
Enter parameter 42 & DNS2 IP address:
[42xxxxxxxxxx]
Value: xxxxxxxxxxx – DNS2 IP address digits

Server Port (GPRS)

Server port number for communication.

SMS text:
XXXX_setgprs:port:yyyyy
Value: yyyyy - server port number, range - [1... 65535]

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → SERVER PORT → [XXXXX]
Value: [XXXXX] – server port number, range - [1... 65535]

Enter parameter 44 & server port number:
[44x#]
Value: x – server port number, range - [1... 65535]

Local Port (GPRS)

Local port number for communication.

SMS text:
XXXX_setgprs:lport:yyyyy
Value: yyyyy - local port number, range - [1... 65535]

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → LOCAL PORT → [1... 65535]
Value: [XXXXX] – local port number, range - [1... 65535]

Enter parameter 45 & local port number:
[45x#]
Value: x – local port number, range - [1... 65535]

Protocol (GPRS)

User can switch between TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) communication protocol. The default protocol is **TCP**.

SMS text:
XXXX_setgprs:protocol:yyy
Value: yyy - communication protocol, range - [tcp - TCP protocol; udp - UDP protocol].

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → PROTOCOL → TCP / UDP

Enter parameter 43 & protocol type value:
[431#] - UDP protocol
[430#] - TCP protocol

APN (GPRS)

Access-point-name provided by GSM operator.
APN can be set and edited using *ELDES Configuration Tool* and SMS only.

SMS

SMS text:
XXXX_setgprs:apn:yyy
Value: yyy - Access-point-name provided by GSM operator.

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → APN

EKB3

N/A

User (GPRS)

User name provided by GSM operator.
User name can be set and edited using *ELDES Configuration Tool* and SMS only.

SMS

SMS text:
XXXX_setgprs:user:yyy
Value: yyy - User name provided by GSM operator.

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → USER

EKB3

N/A

Password (GPRS)

Password provided by GSM operator.
Password can be set and edited using *ELDES Configuration Tool* and SMS only.

SMS

SMS text:
XXXX_setgprs:user:yyy
Value: yyy - Password provided by GSM operator.

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → GPRS SETTINGS → PASSWORD

EKB3

N/A

Profile (GPRS)

Profile name for current GPRS configuration.

Profile name can be set and edited using *ELDES Configuration Tool* and SMS only.

SMS

SMS text:

XXXX_setgprs:profile:yyy

Value: yyy - profile name for current GPRS configuration.

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → GPRS SETTINGS → PROFILE

EKB3

N/A

GPRS Attempts

This command sets the number of data transmission attempts via GPRS network in case the initial attempt was unsuccessful. The default value is **3**.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → COMMUNICATION → GPRS ATTEMPTS → [XXX]

Value: [XXX] – number of GPRS attempts, range – [0... 255]

EKB3

Enter parameter 68 & number of GPRS attempts:

[68x#]

Value: x – number of GPRS attempts, range – [0... 255]

Device ID (GPRS)

The 4-digit ID code of the alarm system intended for system identification by *EGR100* software. This ID code is indicated as Unit ID in *EGR100* software.

This parameter can be set and edited using *ELDES Configuration Tool* and SMS only.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → COMMUNICATION → DEVICE ID → [XXXX]

Value: [XXXX] – 4 digit device ID code, range – [0000... 9999]

EKB3

Enter parameter 47 & Device ID code:

[47xxxx#]

Value: xxxx – 4 digit device ID code, range – [0000... 9999]

9.3.3 Voice Calls Settings

Set Monitoring Station Phone Number (Voice Calls)

The system supports up to 3 monitoring station phone numbers for communication with the alarm system via voice calls (GSM audio channel). Tel. Number 1 is mandatory, the other two are not necessary. All numbers must be entered starting with international country code e.g. 44[area code][local number]. The plus character is not necessary.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET

→ ARC STATION NUM → TEL. NUMBER [1... 3] → [XXXXXXXXXXXXXXX]

Value: [XXXXXXXXXXXXXXX] – up to 15 digits phone number

EKB3

Enter parameter 26, number of phone number entry & phone number

[26xxyyyyyyyyyyyyyyy#]

Value: xx – number of monitoring station phone number entry, range – [01... 03]; yyyyyyyyyyyyyy – up to 15 digits phone number

Delete Monitoring Station Phone Number (Voice Calls)

This command removes the selected monitoring station phone number.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → ARC STATION NUM → TEL. NUMBER [1... 3] → OK → OK

EKB3

N/A

Call Attempts

The system attempts to make additional calls to monitoring station telephone number in case the initial call fails. After all unsuccessful attempts, the system continues to make a call moving to the next preset monitoring station phone number in a row. After all unsuccessful call attempts to all phone numbers, the system returns to Tel. Number 1. By default, number of call attempts is **5**.

SMS

N/A

EKB2

Menu path:

OK → CONFIGURATION → ARC SET → ARC STATION NUM →ATTEMPTS → [XX]

Value: [XX] – number of attempts, range – [1... 10]

EKB3

Enter parameter 37 & number of attempts:

[37xx#]

Value: xx – number of attempts, range – [1... 10]

9.3.4 CSD Settings

Set Monitoring Station Phone Number (CSD)

The system supports 1 monitoring station phone number for communication with the alarm system via CSD connection. The number must be entered starting with international country code e.g. 44[area code][local number]. The plus character is not necessary.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ARC SET → CSD SETTINGS → TEL NUMBER→ [XXXXXXXXXXXXXXX]
Value: [XXXXXXXXXXXXXXX] – up to 15 digits phone number

EKB3

Enter parameter 85 & monitoring station phone number:
[85xxxxxxxxxxxxxxx#]
Value: xxxxxxxxxxxxxxx – up to 15 digits phone number

CSD Attempts

This command sets the number of CID data transmission attempts via CSD connection in case the initial attempt was unsuccessful. The default value is **3**.

SMS

N/A

EKB2

Menu path:
OK → CONFIGURATION → ARC SET→ CSD SETTINGS→ATTEMPTS → [XX]
Value: [XX] - number of CSD attempts, range - [0... 10]

EKB3

Enter parameter 84 & number of CSD attempts:
[84xx#]
Value: xx - number of CSD attempts, range - [00... 10]

For notes

For notes

Made in Lithuania.
www.eldes.lt