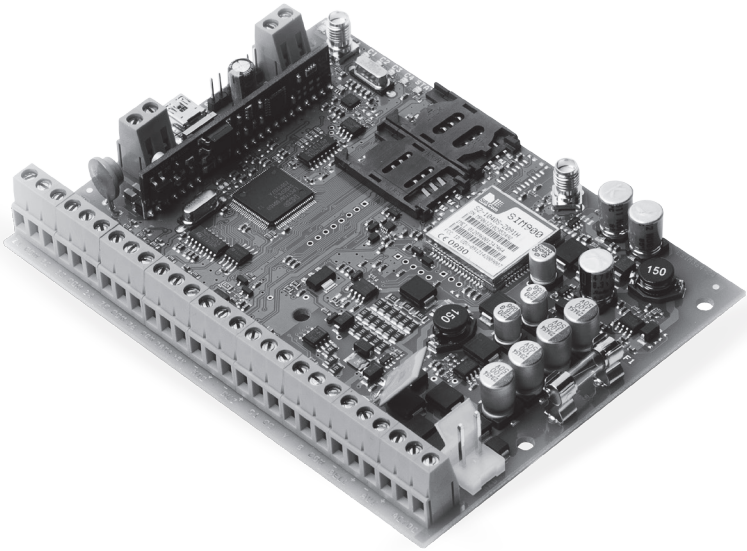


eldes

ESIM364

GSM ALARM AND MANAGEMENT SYSTEM

INSTALLATION MANUAL

COMPLIES WITH EN 50131-1 GRADE 3, CLASS II REQUIREMENTS

Installation Manual v1.7
Valid for ESIM364 v02.10.01 and up

Safety instructions

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

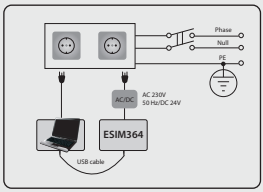
- GSM alarm & management system ESIM364 (also referenced as alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- 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 ESIM364 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 Hz1.5A max or 18-24V ⎓ 1,5A max 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 ESIM364 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

The 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 (0.12in) 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.

Contents

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

Item	Quantity
1. ESIM364	1
2. Microphone	1
3. SMA antenna	2
4. Buzzer	1
5. Back-up battery connection wire	1
6. User manual	1
7. Resistors 5,6kΩ	12
8. Resistors 3,3kΩ	6
9. Plastic standoffs	4

About Installation Manual

This document describes detailed installation and operation process of alarm system ESIM364. It is very important to read the installation manual before starting to use the system.

1. GENERAL INFORMATION

1.1. Functionality

ESIM364 – 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.

Examples of using the system:

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

1.2. Compatible Device Overview

Wired Devices		
Device	**Description**	**Max. Connectible Devices**
EKB2	LCD keypad	4*
EKB3	LED keypad	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	2
ELAN3-ALARM	Ethernet communicator	1
EPGM8	8 PGM output expansion module	1**

Wireless Devices		
Device	**Description**	**Max. Connectible Devices**
EW2	Wireless 2 zone and 2 PGM output expansion module	16*****
EWP2	Wireless motion detector	32***
EWD2	Wireless magnetic door contact/shock sensor/flood sensor	32***
EWK1****	Wireless keyfob with 4 buttons	5***
EWK2****	Wireless keyfob with 4 buttons	5***
EWS3	Wireless indoor siren	32***
EWK2A****	Wireless keyfob with 1 button	5***
EWS2	Wireless outdoor siren	32***
EKB3W	Wireless LED keypad	4***
EWF1/EWF1CO	Wireless smoke/CO detector	32***
EWR2	Wireless signal repeater	4***

* - A mixed combination of EKB2 and EKB3 keypads is supported. The combination can consist of up to 4 keypads in total.
** - Only 1 of these modules can be connected at a time if the module slots are implemented in ESIM364 unit.
*** - A mixed combination of wireless devices is supported. The combination can consist of up to 32 wireless devices in total.
**** - A mixed combination of EWK1, EWK2 and EWK2A keyfobs is supported. The combination can consist of up to 5 keyfobs in total.
***** - EW2 creates 4 wireless zones, therefore the max. number of connectible EW2 devices is 16 if no keypad zones, no EPGM1 and no virtual zones exist in the system's configuration.

1.3. Default Parameters & Ways of Parameter Configuration

Main Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
User 1... 10 name	N/A				✓
User 1... 10 phone number	N/A	✓	✓	✓	✓
User 1... 10 partition	Partition 1		✓	✓	✓
User 1...10 - call in case of alarm	Enabled		✓	✓	✓
Allow control from any phone number	Disabled	✓	✓	✓	✓
SMS password	0000	✓	✓	✓	✓
SMS language	Depends on the firmware				
Partition 1 name	PART1				✓
Partition 2 name	PART2				✓
Partition 3 name	PART3				✓
Partition 4 name	PART4				✓
Partition 1... 4 exit delay	15 seconds	✓	✓	✓	✓

GSM signal loss indication - delay	180 seconds				✓
GSM signal loss indication – activate output	N/A				✓
Dual SIM management – SIM card switch	Disabled				✓
Dual SIM management – try to find operator for a maximum of	3 time (s)				✓
Dual SIM management – send SMS/call via	Currently in use SIM				✓

Main Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Passwords/Codes					
Installer's code	1470		✓	✓	✓
Duress code	N/A		✓	✓	✓
SGS code	N/A		✓	✓	✓
Passwords/codes format	4-digit				✓
Prompt additionally for master code when configuring via keypad/software	Disabled				✓
Master code	1111		✓	✓	✓
Master code name	N/A				✓
Master code partition	Partition 1, Partition 2, Partition 3, Partition 4		✓	✓	✓
User code 2... 30	N/A		✓	✓	✓
User code 2... 30 name	N/A				✓
User code 2... 30 partition	Partition 1		✓	✓	✓
Faults					
Main power loss	Enabled				✓
Low battery	Enabled				✓
Battery dead or missing	Enabled				✓
Battery failed	Enabled				✓
Siren failed	Enabled				✓
Tamper alarm	Enabled				✓
Date/time not set	Enabled				✓
GSM connection failed	Enabled				✓
GSM antenna failed	Enabled				✓
Wireless antenna failed	Enabled				✓
Keypad lost	Enabled				✓
Notifications					
System armed - User 1... 10	Enabled		✓	✓	✓
System armed - SMS delivery report	Enabled		✓	✓	✓
System disarmed – User 1... 10	Enabled		✓	✓	✓
System disarmed – SMS delivery report	Enabled		✓	✓	✓
General alarm – User 1... 10	Enabled		✓	✓	✓
General alarm – SMS delivery report	Enabled		✓	✓	✓
Main power loss/restore – User 1... 10	Enabled		✓	✓	✓
Main power loss/restore – SMS delivery report	Enabled		✓	✓	✓
Battery failed – User 1... 10	Enabled		✓	✓	✓
Battery failed – SMS delivery report	Enabled		✓	✓	✓
Battery dead or missing – User 1... 10	Enabled		✓	✓	✓
Battery dead or missing – SMS delivery report	Enabled		✓	✓	✓
Low battery – User 1... 10	Enabled		✓	✓	✓
Low battery – SMS delivery report	Enabled		✓	✓	✓
Siren fail/restore – User 1... 10	Disabled		✓	✓	✓
Siren fail/restore – SMS delivery report	Disabled		✓	✓	✓
Date/time not set – User 1... 10	Disabled		✓	✓	✓
Date/time not set – SMS delivery report	Disabled		✓	✓	✓
GSM connection failed – User 1... 10	Disabled		✓	✓	✓
GSM connection failed – SMS delivery report	Disabled		✓	✓	✓
GSM antenna fail/restore – User 1... 10	Disabled		✓	✓	✓
GSM antenna fail/restore – SMS delivery report	Disabled		✓	✓	✓

Tamper alarm/restore - User 1... 10	Enabled		✓	✓	✓
Tamper alarm/restore - SMS delivery report	Enabled		✓	✓	✓
Keypad loss/restore - User 1... 10	Enabled		✓	✓	✓
Keypad loss/restore - SMS delivery report	Enabled		✓	✓	✓
Temperature info - User 1... 10	Enabled		✓	✓	✓
Temperature info - SMS delivery report	Enabled		✓	✓	✓
System started - User 1... 10	Enabled		✓	✓	✓
System started - SMS delivery report	Enabled		✓	✓	✓
Periodical info - User 1... 10	Enabled		✓	✓	✓
Periodical info - SMS delivery report	Enabled		✓	✓	✓
Wireless signal loss - User 1... 10	Enabled		✓	✓	✓
Wireless signal loss - SMS delivery report	Enabled		✓	✓	✓
Unable to arm - User 1... 10	Enabled		✓	✓	✓
Unable to arm - SMS delivery report	Enabled		✓	✓	✓
Send to all users simultaneously - all notifications	Disabled		✓	✓	✓
Time Synchronization					
Time synchronization over GSM network	Disabled				✓
Phone number of the currently inserted SIM card	N/A				✓
Synchronization frequency	30 days				✓
Event Log					
Event log	Enabled	✓	✓	✓	✓

Zones					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
On Board					
Z1... Z6 zone name	Zone1... Zone6	✓			✓
Z1 type	Delay		✓	✓	✓
Z1... Z6 zone status	Enabled	✓	✓	✓	✓
Z2... Z6 type	Instant		✓	✓	✓
Z1... Z6 delay, ms	800 milliseconds				✓
Z1... Z6 - Stay	Disabled		✓	✓	✓
Z1... Z6 - Force	Disabled		✓	✓	✓
Z1... Z6 Tamper name	Tamper1... Tamper6				✓
Delay-type zone - entry delay	15 seconds	✓	✓	✓	✓
Z1... Z6 partition	Partition 1		✓	✓	✓
Z1... Z6 - Shared	Disabled				✓
Z1... Z6 - audio track	N/A				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓
Tamper 1... 6 status	Enabled				✓
Delay becomes Instant in STAY mode	Disabled				
Chime	Enabled		✓	✓	✓
ATZ mode	Disabled		✓	✓	✓
Arm-disarm by zone No1... No4	N/A		✓	✓	✓
Zone connection type	Type 1		✓	✓	✓
EPGM1 Module					
Zone name	Zone X	✓			✓
Zone status	Enabled	✓	✓	✓	✓
Type	Instant		✓	✓	✓
Delay, ms	800 milliseconds				✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone - entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓

Tamper status	Enabled				✓
Audio track	N/A				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓
Tamper status	Enabled				✓
Wireless Devices					
Zone name	Zone X	✓			✓
Zone status	Enabled	✓	✓	✓	✓
Type	Depends on the connected wireless device model		✓	✓	✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone - entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Audio track	N/A				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓
Tamper status	Enabled				✓
Keypads					
Zone name	Zone X	✓			✓
Zone status	Disabled	✓	✓	✓	✓
Type	Instant		✓	✓	✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone - entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Audio track	N/A				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓
Tamper status	Enabled				✓
Virtual Zones					
Zone name	Zone X				✓
Zone status	Disabled			✓	✓
Type	Instant			✓	✓
Force	Disabled			✓	✓
Delay-type zone - entry delay	15 seconds			✓	✓
Partition	Partition 1			✓	✓
Shared	Disabled				✓
Cross-Zone/Intelli-Zone	N/A				✓
Confirmation Timeout	20 seconds				✓
Tamper status	Enabled				✓

PGM Outputs					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
On Board					
C1... C4 output name	Controll1... Controll4	✓			✓
Status	Turned OFF	✓	✓	✓	✓
Using module EPGM8	Disabled		✓	✓	✓
EPGM1 Module					
Output name	ControllX	✓			✓
Status	Turned OFF	✓	✓	✓	✓
Wireless Devices					
Output name	ControllX	✓			✓

Type	Depends on the connected wireless device model				✓
Status	Turned OFF	✓	✓	✓	✓

MS Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Management					
MS mode	Disabled	✓	✓	✓	✓
Account	9999		✓	✓	✓
GSM & SMS – attempts	5		✓	✓	✓
GSM & SMS – tel. number 1... 3	N/A		✓	✓	✓
PSTN – treat PSTN call as user call	Disable				✓
PSTN – attempts	5		✓	✓	✓
PSTN – tel. number 1... 3	N/A		✓	✓	✓
CSD – attempts	5		✓	✓	✓
CSD – tel. number 1... 5	N/A		✓	✓	✓
IP Server 1... 3 – IP attempts	3		✓	✓	✓
IP Server 1... 3 – test period	180 seconds		✓	✓	✓
IP Server 1... 3 – protocol	UDP	✓	✓	✓	✓
IP Server 1...3 – unit ID	0000		✓	✓	✓
IP Server 1... 3 – communication protocol	EGR100		✓	✓	✓
IP Server 1... 3 – server IP	0.0.0.0	✓	✓	✓	✓
IP Server 1... 3 – server port	20000	✓	✓	✓	✓
Communication - primary	IP Server 1		✓	✓	✓
Communication – backup 1... 5	N/A		✓	✓	✓
Delay after last communication attempt	600 seconds		✓	✓	✓
SIA IP protocol settings - encryption	Disabled				✓
SIA IP protocol settings – encryption key	0000				✓
SIA IP protocol settings – account prefix	N/A				✓
SIA IP protocol settings – receiver number	N/A				✓
SIA IP protocol settings – Contact ID ping	Disabled				✓
SIA IP protocol settings – data message	Event: 1602, partition: 01, user/zone: 000				✓
Data Messages					
Burglary alarm/restore – code	130				✓
Burglary alarm/restore – status	Enabled		✓	✓	✓
Main power loss/restore – code	301				✓
Main power loss/restore – status	Enabled		✓	✓	✓
Armed/disarmed by user – code	401				✓
Armed/disarmed by user – status	Enabled		✓	✓	✓
Test event – code	602				✓
Test event – status	Enabled		✓	✓	✓
Battery failed – code	309				✓
Battery failed – status	Enabled		✓	✓	✓
Battery dead or missing – code	311				✓
Battery dead or missing – status	Enabled		✓	✓	✓
Tamper alarm/restore – code	144				✓
Tamper alarm/restore – status	Enabled		✓	✓	✓
Silent zone alarm/restore – code	146				✓
Silent zone alarm/restore – status	Enabled		✓	✓	✓
Kronos ping – code	602				✓
Kronos ping – status	Enabled		✓	✓	✓
System started – code	900				✓
System started – status	Enabled		✓	✓	✓
24H zone alarm/restore – code	133				✓
24H zone alarm/restore – status	Enabled		✓	✓	✓
Fire zone alarm/restore – code	110				✓
Fire zone alarm/restore – status	Enabled		✓	✓	✓
Low battery – code	302				✓
Low battery – status	Enabled		✓	✓	✓
Temperature exceeded – code	158				✓

Temperature exceeded – status	Enabled		✓	✓	✓
Temperature fallen – code	159				✓
Temperature fallen – status	Enabled		✓	✓	✓
Wireless signal loss/restore – code	381				✓
Wireless signal loss/restore – status	Enabled		✓	✓	✓
Disarmed by user (duress code) – code	121				✓
Disarmed by user (duress code) – status	Enabled		✓	✓	✓
Armed/disarmed by user (SGS code) – code	463				✓
Armed by user (SGS code) – status	Enabled		✓	✓	✓
Armed/disarmed in STAY mode – code	456				✓
Armed/disarmed in STAY mode – status	Enabled		✓	✓	✓
Siren fail/restore – code	321				✓
Siren fail/restore – status	Disabled		✓	✓	✓
Date/time not set – code	626				✓
Date/time not set – status	Enabled		✓	✓	✓
GSM connection failed – code	358				✓
GSM connection failed – status	Enabled		✓	✓	✓
GSM antenna fail/restore – code	359				✓
GSM antenna fail/restore – status	Disabled		✓	✓	✓
System shutdown – code	414				✓
System shutdown – status	Enabled		✓	✓	✓
Keypad fail/restore – code	330				✓
Keypad fail/restore – status	Enabled		✓	✓	✓
GPRS connection lost – code	354				✓
GPRS connection lost – status	Enabled		✓	✓	✓
Zone bypass – code	570				✓
Zone bypass – status	Enabled		✓	✓	✓

Control / Scheduler					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
PGM output control 1... 16	Disabled				✓
Scheduler 1... 16	Disabled				✓
Additional conditions	Disabled				✓

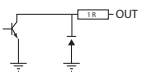
Peripheral Devices					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Keypads					
Keypad 1... 4 partition	Partition 1		✓	✓	✓
Show armed status in keypad	Disabled				✓
Keypad partition switch	Disabled		✓	✓	✓
EKB3 mode	2 partitions				✓
Wireless keypads - partition	Partition 1		✓	✓	✓
Wireless keypads – backlight timeout	10 seconds				✓
Wireless keypads – bell	Disabled				✓
Siren					
EWS2 LED	Enabled		✓	✓	✓
Bell squawk	Disabled		✓	✓	✓
Activate siren if wireless device is lost	Disabled		✓	✓	✓
EWS3 fire alarm LED	Disabled		✓	✓	✓
EWS3 alarm LED	Disabled		✓	✓	✓
Bell squawk enabled if arming in STAY mode	Disabled		✓	✓	✓
Temperature Sensors					
Temperature sensor 1... 8 name	N/A	✓			✓
Temperature sensor 1... 8 min. temperature	0	✓	✓	✓	✓
Temperature sensor 1... 8 max. temperature	0	✓	✓	✓	✓
Primary	No.1	✓	✓	✓	✓

Secondary	No.2	✓	✓	✓	✓
iButton Keys					
iButton key name	N/A				✓
iButton key partition	Partition 1		✓	✓	✓
Allow adding new iButton keys	Disabled	✓	✓	✓	✓

System					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Management					
Mains power loss delay	30 seconds		✓	✓	✓
Mains power restore delay	120 seconds		✓	✓	✓
Alarm duration	1 minute	✓	✓	✓	✓
Wireless channel	Depends on firmware				✓
Periodic test	Every 1 day at 11:00	✓	✓	✓	✓
Microphone level	12		✓		✓
Speaker level	85		✓		✓
Service mode	Disabled	✓	✓	✓	✓
ELDES Cloud Services					
ELDES Cloud Services	Disabled	✓			✓
Server address	ss.eldes.lt	✓			✓
Port	8082	✓			✓
Ping period	180 seconds	✓			✓
Time zone	N/A				✓
Communication	Via GPRS network				✓
GPRS Settings					
SIM1... SIM2 APN	N/A	✓			✓
SIM1... SIM2 user name	N/A	✓			✓
SIM1... SIM2 password	N/A	✓			✓
DNS1	N/A	✓	✓	✓	✓
DNS2	N/A	✓	✓	✓	✓

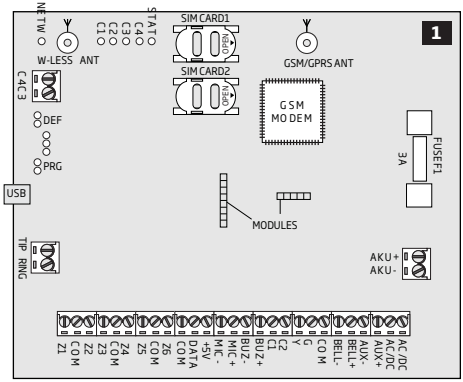
2. TECHNICAL SPECIFICATIONS

2.1. Electrical and Mechanical Characteristics

Electrical and Mechanical Characteristics	
Power supply	16-24V 50 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current consumption in idle state w/o external devices connected	Up to 80mA
Recommended backup battery voltage, capacity	12V; 1,3-7Ah
Recommended backup battery type	Lead-Acid
Backup battery charge current	Up to 500mA
Backup battery charge duration	Up to 30 hours for 7Ah battery
Gsm modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
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
On-board PGM output circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum commuting on-board PGM output values	4 x 30V; 500mA
BELL: Siren output when activated	Connected to COM
BELL: Maximum siren output current	1A
BELL: Maximum cable length for siren connection	Up to 100m (328.08ft)
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
AUX: Maximum accumulative current of auxiliary equipment	1,1A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100m (328.08ft)
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC
BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	8
DATA: Maximum cable length for 1-Wire communication	Up to 30m (98.43ft)
DATA: Cable type for 1-Wire communication	Unshielded
Supported iButton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	16
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100m (328.08ft)
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2m (6.56ft)
MIC: Cable type for microphone connection	Unshielded
Wireless band	ISM868 /ISM 915
Wireless communication range	Up to 30m (98.43ft) in premises; up to 150m (492.13ft) in open areas
Maximum supported number of wireless devices	32
Event log size	500 events
Maximum supported number of zones	76
Maximum supported number of PGM outputs	76
Cable type for zone and PGM output connection	Unshielded
Generated PSTN line values	Voltage: 48V; current: 25mA; impedance: 270Ω
Communications	SMS, Voice calls, GPRS network CSD, PSTN, Ethernet via ELAN3-ALARM
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS, SIA IP
Dimensions	140x100x18mm (5.51x3.94x0.71in)
Operating temperature range	-20...+55°C (-4... +131°F)
Humidity	0-90% RH @ 0... +40°C (0-90% RH @ +32... +104°F) (non-condensing)

2.2. Main Unit, LED Indicator and Connector Functionality

Main Unit Functionality	
GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD1	Primary SIM card slot / holder
SIM CARD2	Secondary SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
W-LESS ANT	Wireless antenna SMA type connector
GSM/GPRS ANT	GSM/GPRS antenna SMA type connector
MODULES*	Slots for EA1, EA2 or EPGM8 module



LED Functionality	
NETW	GSM network signal strength
C1	PGM output C1 status - ON/OFF
C2	PGM output C2 status - ON/OFF
C3	PGM output C3 status - ON/OFF
C4	PGM output C4 status - ON/OFF
STAT	Micro-controller status

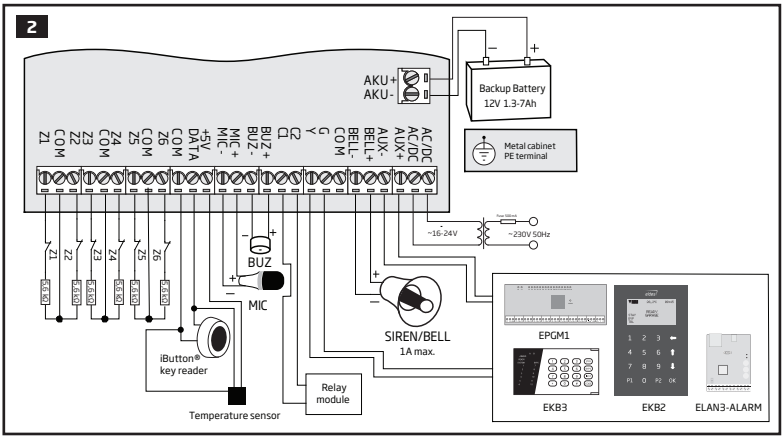
NETW indication	GSM signal strength
OFF	No GSM signal
Flashing every 3 sec.	Poor
Flashing every 1 sec.	Medium
Flashing several times per sec.	Good
Steady ON	Excellent

Connector Functionality	
TIP*	PSTN (landline) terminal
RING*	PSTN (landline) terminal
DATA	1-Wire interface for iButton key and temperature sensor connection
+5V	Temperature sensor power supply terminal (+5V)
MIC-	Microphone negative terminal
MIC+	Microphone positive terminal
BUZ-	Buzzer negative terminal
BUZ+	Buzzer positive terminal
C1 - C4	PGM output terminals
Z1 - Z6	Security zone terminals
Y	RS485 interface CLOCK terminal (yellow wire)
G	RS485 interface DATA terminal (green wire)
COM	Common return terminal
BELL-	Siren negative terminal
BELL+	Siren positive terminal
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
AC/DC	Main power supply terminals
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

* - Optional, implementable on request in advance

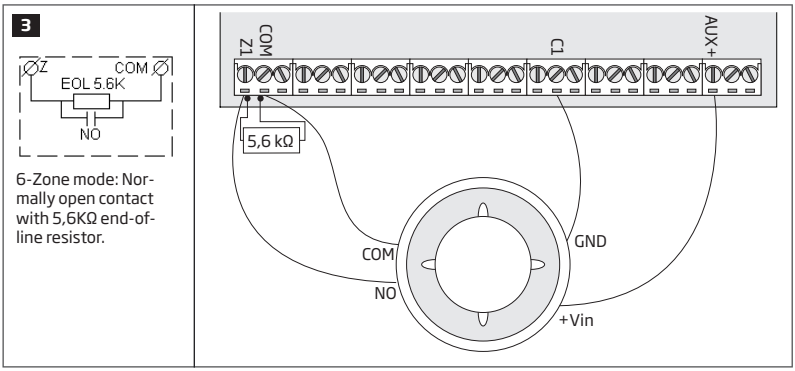
2.3. Wiring Diagrams

2.3.1.General Wiring

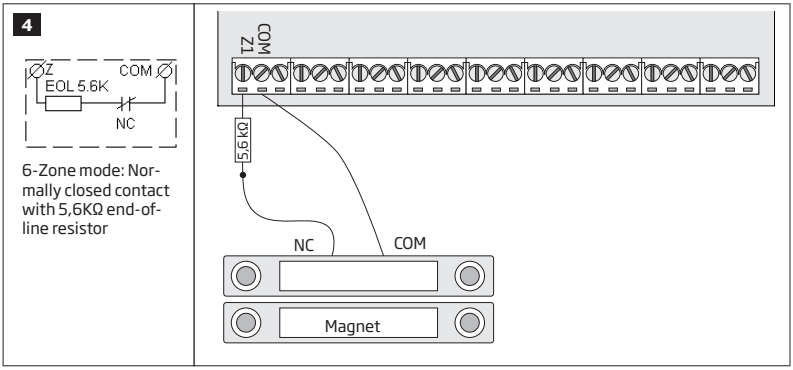


2.3.2. Zone Connection Types

Type 1 Example of 4-wire smoke detector wiring



Type 2 Example of magnetic door contact wiring

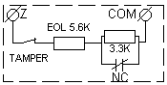


NOTE: Based on the example given, in the event of an alarm, the smoke detector could be reset by turining OFF and ON the PGM output C1. For more details, please refer to **18.4. Turning PGM Outputs ON and OFF.**

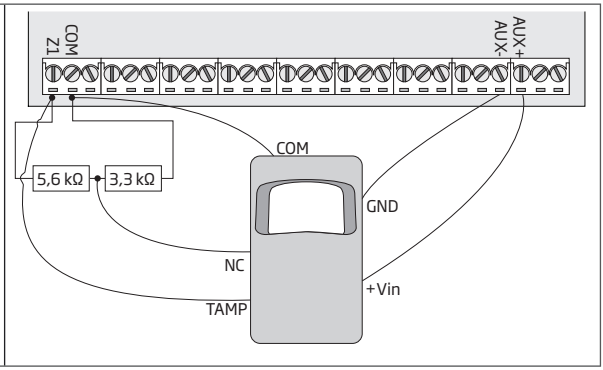
NOTE: The system does NOT support 2-wire smoke detectors.

Type 3 Example of motion detector wiring

5

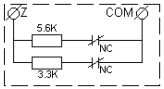


6-Zone mode: Tamper and 5,6KΩ end-of-line resistor and 3,3KΩ end-of-line resistor with normally closed contact.

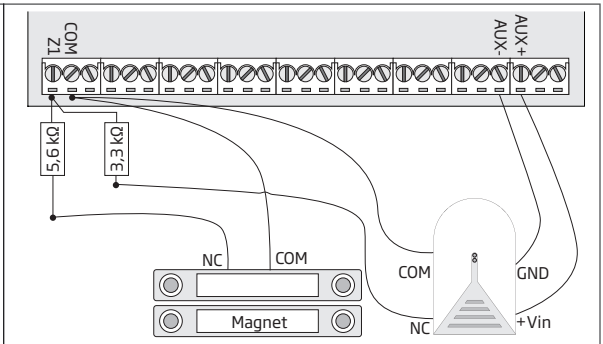


Type 4 Example of magnetic door contact (Z1) and glass break sensor (Z7) wiring

6

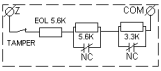


ATZ mode: 5,6KΩ end-of-line resistor and normally closed contact with 3,3KΩ end-of-line resistor and normally closed contact

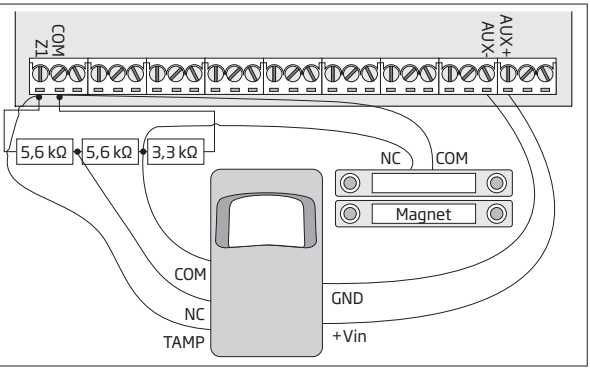


Type 5 Example of motion detector (Z1) and magnetic door contact (Z7) wiring

7

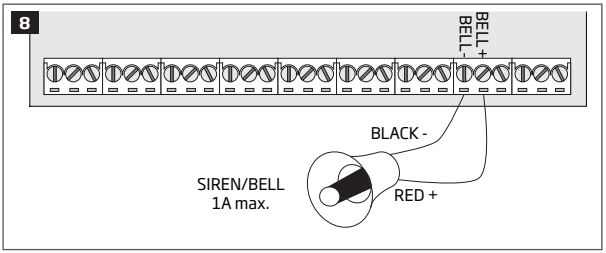


ATZ mode: Tamper, 5,6KΩ end-of-line resistor, 5,6KΩ end-of-line resistor with normally closed contact and 3,3KΩ end-of-line resistor with normally closed contact.



See also **14.3. 6-Zone Mode** and **14.4. ATZ (Advanced Technology Zone) Mode.**

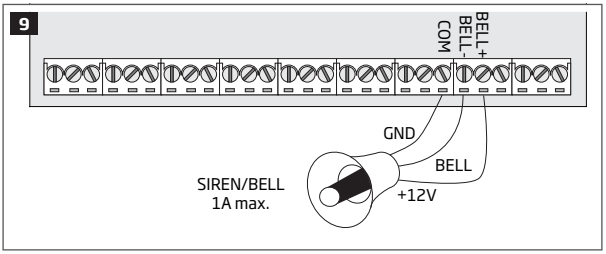
2.3.3. Siren



Piezo siren

1 Connect positive siren wire (red) to **BELL+** terminal.

2 Connect negative siren wire (black) to **BELL-** terminal.

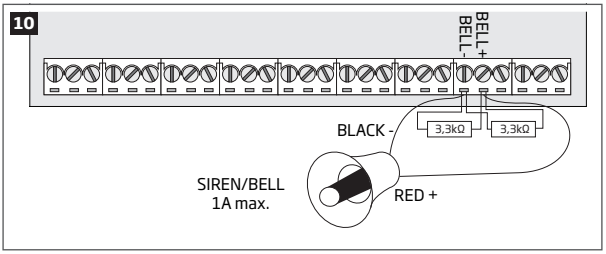


Self-contained siren

1 Connect negative **GND** siren wire to **COM** terminal.

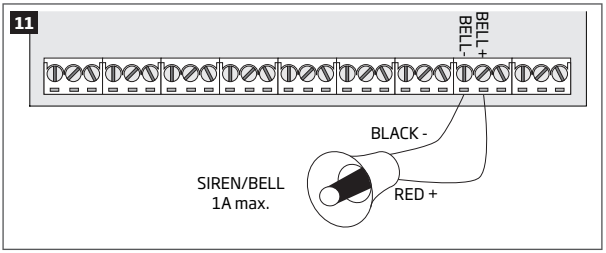
2 Controlling **BELL** siren wire must be connected to **BELL-** terminal.

3 Connect positive **+12V** siren wire to **BELL+** terminal.



Siren status monitoring

By default, the system monitors siren status and indicates system fault on the keypad if the siren is broken/disconnected. However, this feature requires a pair of parallelly connected resistors of 3,3kΩ nominal across **BELL+** and **BELL-** terminals.



No siren status monitoring

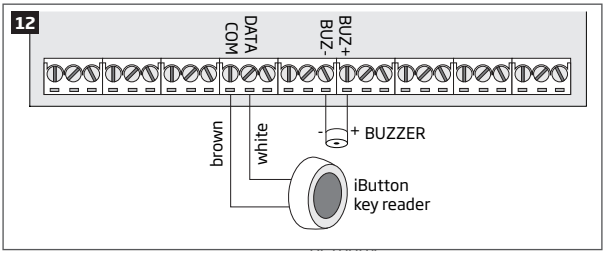
If the siren status monitoring feature is not required, do not connect any resistor in parallel and disable siren fault indication on the keypad (see **29. INDICATION OF SYSTEM FAULTS**).

See also **20. SIREN/BELL**.

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

NOTE: Siren status monitoring feature supervises the resistance across **BELL+** and **BELL-** terminals. The resistance must be ranging from 1kΩ through 3,3kΩ, otherwise the system will indicate system fault. In order to view the siren resistance value, please refer to Diagnostic Management feature available on *ELDES Configuration Tool* software.

2.3.4. iButton Key Reader and Buzzer



Supported iButton key model: Maxim/Dallas DS1990A

The iButton key reader can be installed with buzzer or separately. The buzzer is intended for audio indication of exit/entry delay countdown providing short beeps.

1 Connect iButton key reader brown and white wires to 1-Wire interface: **COM** and **DATA** terminals respectively.
2 Connect buzzer's negative terminal wire to **BUZ-** and positive terminal wire to **BUZ+.**

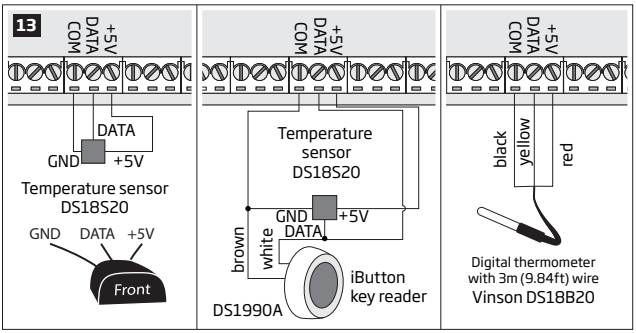
NOTE: The installation of buzzer is not necessary if EKB2/EKB3 keypad is used.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30m (98.43ft) max.

2.3.5. Temperature Sensor and iButton Key Reader

Supported iButton key model: Maxim/Dallas DS1990A

Supported temperature sensor model: Maxim/Dallas DS18S20, DS18B20

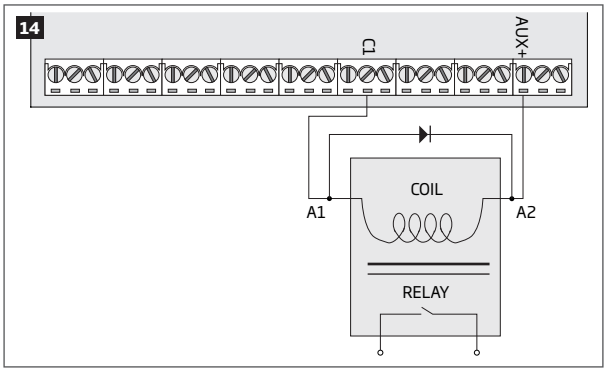


1 Depending on the model, connect temperature sensor **GND**/black wire, **DATA**/yellow wire, **+5V**/red wire terminals to 1-Wire interface: **COM**, **DATA** and **+5V** terminals respectively.
2 When connecting iButton key reader in parallel to temperature sensor, connect iButton key reader terminal wires to **COM** and **DATA** terminals respectively.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30m (98.43ft) max.

2.3.6. Relay Finder 40.61.9.12 with Terminal Socket 95.85.3 to PGM Output

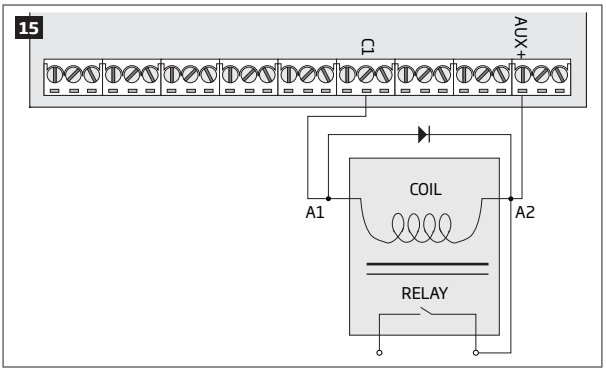
Example of relay wiring for negative PGM output control



1 Wire up relay **A1** terminal to PGM output **Cx** and **A2** terminal to **AUX+**.
2 In addition, connect the switching diode to relay's **A2** and **A1** terminals.

NOTE: We highly recommend using switching diode model 1N4148 or similar.

Example of relay wiring for positive PGM output control

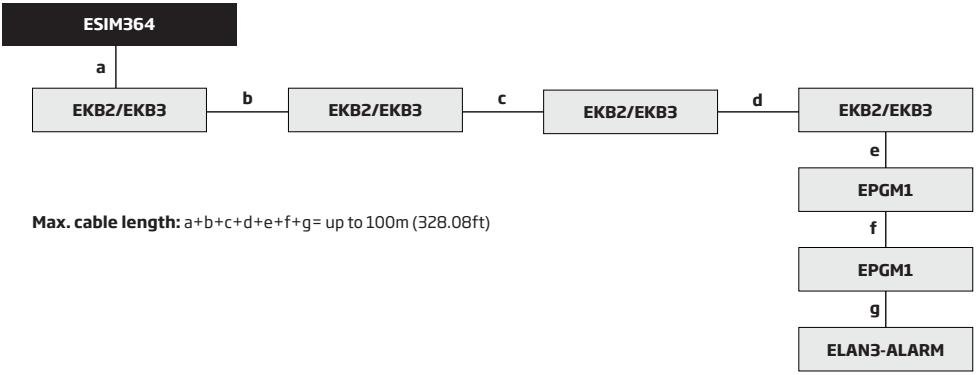


1 Wire up relay **A1** terminal to PGM output's **Cx** terminal and **A2** terminal to **AUX+** and one of the relay's switch contacts: NC or NO.
2 In addition, connect the switching diode to relay's **A2** and **A1** terminals.

NOTE: We highly recommend using switching diode model 1N4148 or similar.

2.3.7. RS485

Serial Wiring Method



Max. cable length: a+b+c+d+e+f+g= up to 100m (328.08ft)

ATTENTION: The cable length must not exceed 100m (328.08ft) in total.

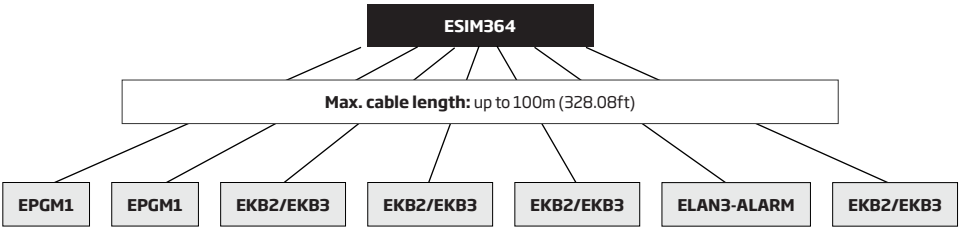
ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module is different.

NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

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

For more details on RS485 interface, please refer to **32.1. RS485 Interface**

Parallel Wiring Method



ATTENTION: The cable between ESIM364 and each RS485 device must be of the same length and can NOT exceed 100m (328.08ft).

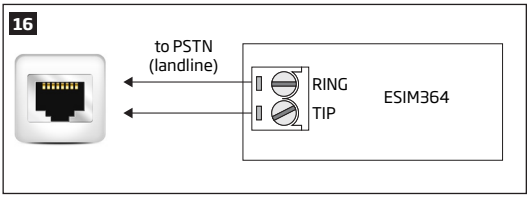
ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module is different.

NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

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

For more details on RS485 interface, please refer to **32.1. RS485 Interface**

2.3.8. RING/TIP



ATTENTION: The **TIP/RING** connectors and PSTN module are NOT included in a standard ESIM364 alarm system unit. These components are optional and can be implemented on request in advance.

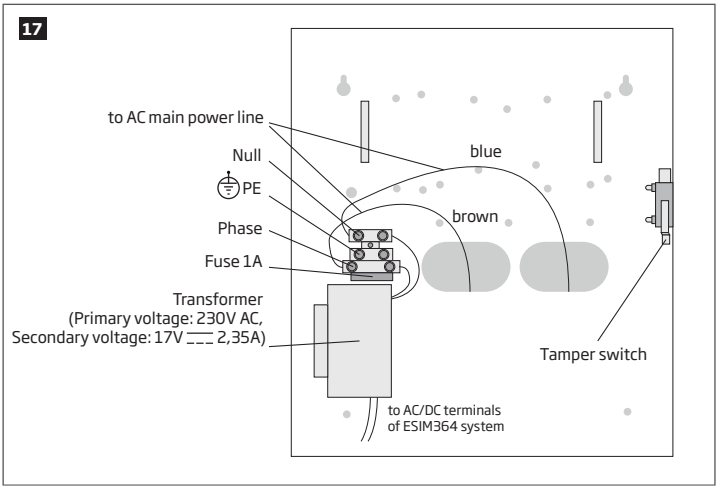
3. INSTALLATION

When professional installation, OEM integration or assembly by a third-party is expected, the installation instructions and assembly requirements approved for equipment approval must be provided to the integrators to clearly identify the specific requirements necessary to maintain RF exposure compliance. The grantee of a transmitter, typically the manufacturer, is responsible for ensuring installers and integrators have a clear understanding of the compliance requirements by including the required instructions and documentation with the product and, if necessary, to provide further support to fulfill grantee responsibilities for ensuring compliance. The integrators must be fully informed of their obligations and verify the resolution of any issues and concerns with each transmitter manufacturer or grantee.

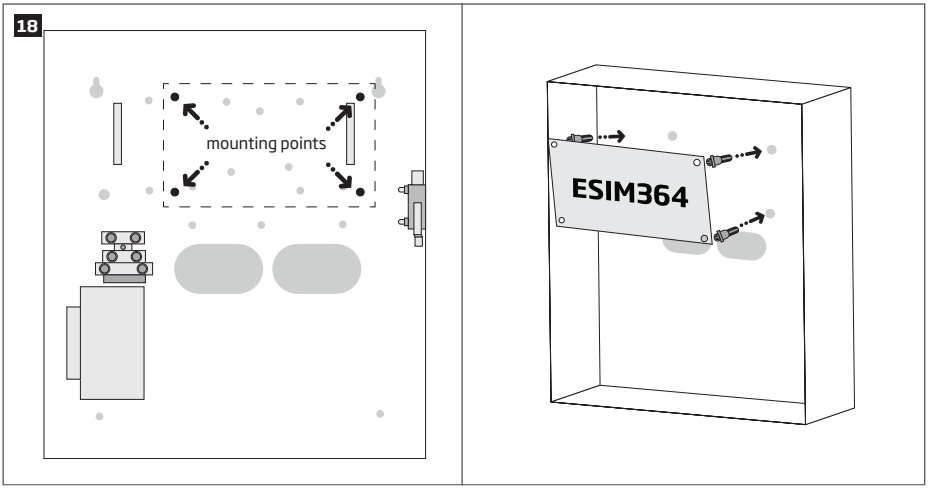
- The system can be installed in a metal or non-flammable cabinet only. For a convenient installation, ME1 metal cabinet is highly recommended. The metal cabinet must always be grounded as well as ESIM364 system's PCB by connecting one of the COM terminals to the PE contact of the metal cabinet.
- For the connection of 230V transformer, use 3x0.75 mm² 1 thread double isolated cable. 230V power supply cables must not be grouped with low voltage cable group.
- For the connection of auxiliary and BELL outputs, use 2x0.75 mm² 1 thread unshielded cable of up to 100m (328.08ft) length.
- For the connection of zone/PGM output connectors, use 0.50 mm² 1 thread unshielded cable of up to 100m (328.08ft) length.

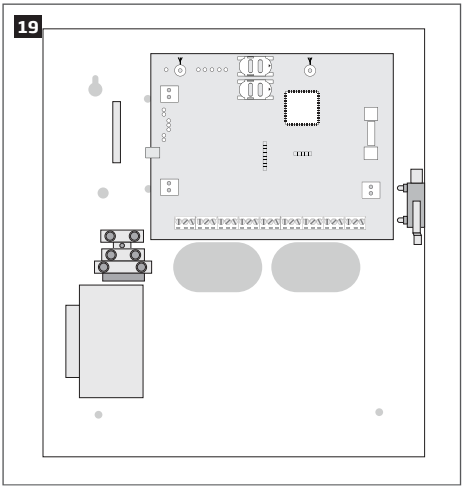
System Installation in ME1 Metal Cabinet

1. ME1 metal cabinet components

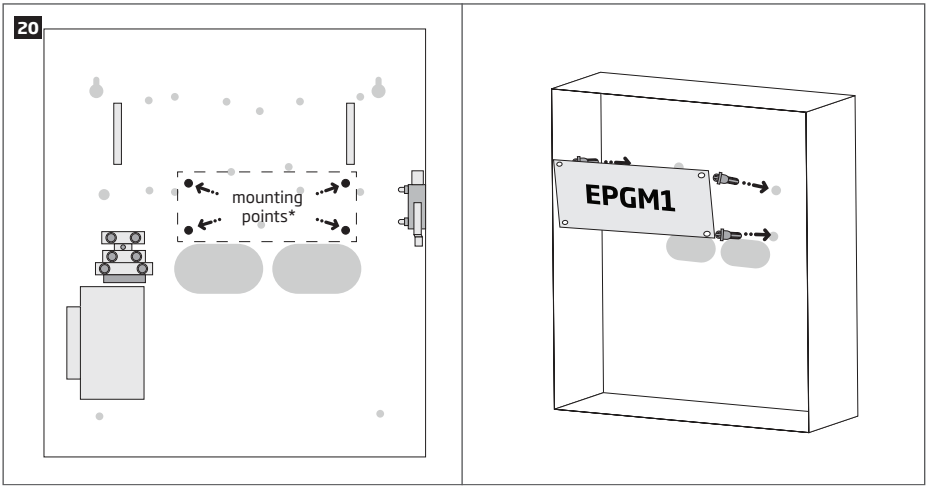


2. Insert the plastic standoffs into the appropriate mounting points and fix the board of ESIM364 on the holders as indicated below.

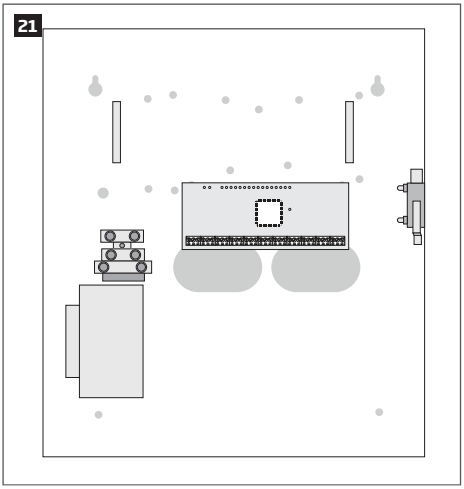


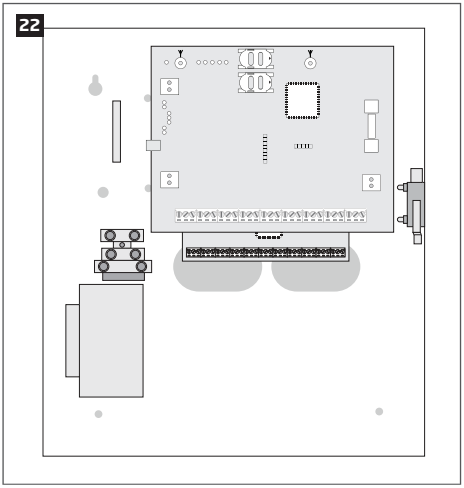


3. If EPGM1 module is to be installed, please install it in the first place and ESIM364 alarm system afterwards. EPGM1 must be mounted on the shorter plastic standoffs, while ESIM364 – on the longer ones. The mounting points of EPGM1 module are indicated below.



* The standard ME1 metal cabinet does NOT contain the mounting points intended for EPGM1 module mounting, therefore it will be necessary to drill out the mounting points by yourself.

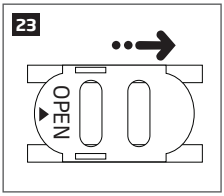




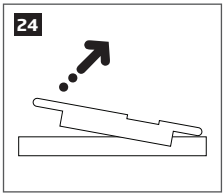
4. Wire up the accessories, such as keypads, zone and PGM output expansion modules, ELAN3-ALARM module, temperature sensors, according to the wiring diagrams. Install the buzzer closer to iButton key reader in order to hear the exit delay countdown (see **2.3 Wiring Diagrams for more details**).

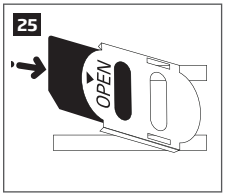
5. Disable the PIN code of the SIM card by inserting it into a mobile phone and following the proper menu steps. Ensure that the additional services, such as **voice mail, call forwarding, report on missed/busy calls ("call catcher")** are disabled on the SIM card. For more details on how to disable these services, please contact your GSM operator.

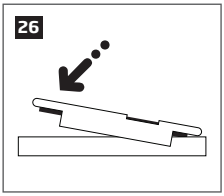
6. Once the PIN code is disabled, place the SIM card into the SIM CARD1 slot of the alarm system. If Dual-SIM feature is to be used, insert another SIM card into the SIM CARD2 slot. For more details, please refer to **31. DUAL-SIM MANAGEMENT.**

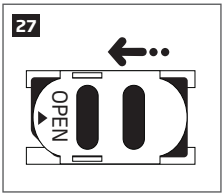


Inserting a SIM card into SIM CARD1 slot is mandatory as it is the main SIM card slot, while using a SIM card in SIM CARD2 slot is optional.

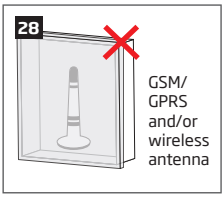






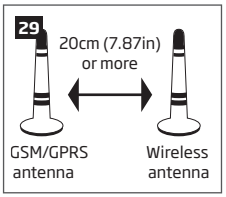


7. Connect the GSM/GPRS and wireless antennas and follow the recommendations for the installation:



Never install in the following locations:

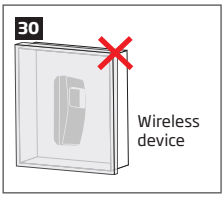
- inside the metal cabinet
- closer than 20cm (7.87in) from the metal surface and/or power lines



Recommended installation:

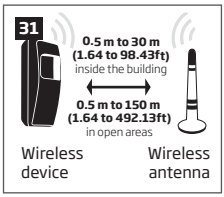
- keep the distance of at least 20cm (7.87in) or more.

8. If one or more wireless devices are to be paired, follow the recommendations for the installation to achieve the strongest wireless signal:



Never install in the following locations:

- inside the metal cabinet
- closer than 20cm (7.87in) from the metal surface and/or power lines



Recommended installation:

- face the front side of the wireless device towards the antenna
- keep the distance: 0,5 to 30m (1.64 to 98.43ft) inside the building, 0,5 to 150m (1.64 to 492.13ft) in open areas

For more details on how to install the wireless devices, please refer to **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual and the latest user manual of the wireless device located at www.eldes.lt/download

9. Power up the system and wait until indicator STAT lights up (see **2.2 Main Unit, LED Indicator and Connector Functionality**).
10. Indicator STAT should be flashing indicating successful micro-controller operation.
11. The illuminated indicator NETW indicates that the system successfully registered to GSM network. To find the strongest GSM signal, place the GSM/GPRS antenna and follow the indications provided by NETW indicator (see **2.2 Main Unit, LED Indicator and Connector Functionality**).
12. Change the default SMS password (see **6. SMS PASSWORD AND INSTALLER CODE** for more details).
13. Set the phone number for User 1 (see **8. USER PHONE NUMBERS** for more details).
14. Set system date and time (see **9. DATE AND TIME** for more details).
15. Once the system is fully configured, it is ready for use. However, if you fail to receive an SMS reply from the system, please check the SMSC (Short Message Service Center) phone number. For more details regarding the SMS centre phone number, please refer to **27.1. SMSC (Short Message Service Center) Phone Number.**
16. If it is required to change the batteries for the wireless devices or carry out other system maintenance tasks, please activate the Service mode. For more detail regarding this mode, please refer to **33. SERVICE MODE.**

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

NOTE: The installation of iButton key reader, EKB2/EKB3/EKB3W keypad, EWK1 wireless keyfob 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.

NOTE: For maximum system reliability we recommend you do NOT use a Pay As You Go SIM card. Otherwise, in the event of insufficient credit balance on the SIM card, the system would fail to make a phone call or send messages.

NOTE: We advise you to choose the same GSM SIM provider for your system as for your mobile phone. This will ensure the fastest, most reliable SMS text message delivery service and phone call connection.

NOTE: Even though alarm system ESIM364 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. GENERAL OPERATIONAL DESCRIPTION

When the system is being armed, it will initiate the exit delay countdown intended for the user to leave the secured area. During the countdown period the buzzer will emit short beeps. By default, exit delay duration is 15 seconds. After the countdown is complete, the system will become armed and lock the configuration by keypad possibility. In case the user does not leave the secured area before the countdown is complete, the system will Stay-arm if at least 1 zone has Stay attribute enabled. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the 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 Force attribute enabled.

After the system is armed and if a zone (depending on type) or tamper is violated, the system will cause an alarm lasting for 1 minute (by default), During the alarm, the siren/bell will provide an alarm sound along with the buzzers of the keypads. By default, the system will also makes a phone call and send an SMS text message containing the violated zone or tamper number to a listed user phone number and indicate the violated zone or tamper number on the keypad. If another zone or tamper is violated or the same one is restored and violated again during the alarm, the system will act as mentioned previously, but will not extend the alarm time.

After the user enters the secured area, the system will initiate the entry delay countdown intended for system disarming. During the countdown period, the buzzer will emit a steady beep. By default, entry delay duration is 15 seconds. After the user successfully performs the disarming process, the system will unlock the keypads. If the user does not disarm the system in time, the alarm system will cause an instant alarm.

NOTE: The alarm will be caused even if a tamper is violated while the system is disarmed.

For more details, please refer to **12. ARMING AND DISARMING**.

5. CONFIGURATION METHODS

!!! In this installation manual the underscore character "_" represents one space character. Every underscore character must be replaced by a single space character. There must be no spaces or other unnecessary characters at the beginning and at the end of the SMS text message.

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool* software.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3**

5.1. SMS Text Messages

SMS

In order to configure and control the system by SMS text message, send the text command to the ESIM364 system phone number from one of the listed user phone numbers. The structure of SMS text 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 e. g. STATUS. The variables are indicated in lower-case letters, while a valid parameter value range is indicated in brackets.

5.2. EKB2 LCD Keypad

EKB2

The system configuration and control by EKB2 keypad is carried out 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 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 touching the ↓ key. In this installation manual, the menu path is based on the EKB2 menu tree by starting at home screen view (see **32.1.1.2. Master and User Menu Tree** and **32.1.1.3. Installer Menu Tree**). The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

Activate Configuration mode

EKB2

Menu path:
OK → iiii → OK
Value: *iiii* - 4-digit installer code.

Deactivate Configuration mode

EKB2

Return to home screen view

EN50131-1 GRADE 3

Activate Configuration mode

EKB2

Menu path:
OK → mmmmmm → OK → CONIFGURATION → OK → iiiiii → OK
Value: *mmmmmm* - 6-digit master code; *iiiiii* - 6-digit installer code.

EN50131-1 GRADE 3

Deactivate Configuration mode

EKB2

Return to home screen view

NOTE: By default, menu section CONFIGURATION is secured with installer code. The default installer code is 1470.

NOTE: Default master code is 1111.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the menu section CONFIGURATION is opened. The inactive EKB2 keypads will display ✕ icon.

NOTE: The keypad will automatically exit the menu section CONFIGURATION and return to home screen view if 1 minute after the last key-touch expires.

5.3. EKB3/EKB3W LED Keypad

EKB3/ EKB3W

The system configuration and control by EKB3/EKB3W keypad is carried out by activating the Configuration mode using the installer code (by default – installer code is 1470) and entering a valid configuration command using the number keys [0]... [9], [#] key for confirmation and [*] key to clear the characters that have been entered. Alternatively, the user can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cleared. When typing in the characters, the indication of each pressed key is provided by short beep of keypad buzzer and red indicators when the number keys [0]... [9] are being pressed. Some commands require [STAY], [BYPS], [INST] and [CODE] keys as well. The structure of a standard configuration command is a combination of digits. The commands, which do not require the Configuration mode being activated, are noted. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: If you have accidentally typed in an unnecessary character, please press [*] key or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cleared.

NOTE for EKB3W: Even if Back-light Timeout has expired, the character will be considered as type in once the appropriate EKB3W key is pressed. For more details, please refer to **19.5.3. Wireless Communication, Sleep Mode and Back-light Timeout**.

Activate/deactivate Configuration mode

EKB3/ EKB3W

Enter installer code:
[INST] iiii #
Value: *iiii*- 4-digit installer code.
Example: *INST1470#*

EN50131-1 GRADE 3

Activate Configuration mode

EKB3/ EKB3W

Enter installerr and master codes:
[INST] iiiii mmmmmm #
Value: *iiiii* - 6-digit installer code; *mmmmmm* - 6-digit master code.
Example: *INST147000111111#*

EN50131-1 GRADE 3

Deactivate Configuration mode

EKB3/ EKB3W

Enter installerr code:
[INST] iiiiii #
Value: *iiiiii* - 6-digit installer code.
Example: *INST147000#*

The following table provides a list of EKB3/EKB3W indications, which are relevant during Configuration mode.

Indication	Description
Indicator ARMED flashing	Configuration mode activated successfully.
Indicator SYSTEM flashing	Valid parameter is entered and waiting for valid value to be enetered.
1 long beep	Non-existing command or invalid parameter value entered.
3 short beeps	Command entered successfully.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the Configuration mode is activated.

NOTE: Configuration mode will automatically deactivate if 1 minute after the last key-stroke expires.

5.4. ELDES Configuration Tool Software

Config Tool

Software *ELDES Configuration Tool* is intended for ESIM364 alarm system configuration locally via USB port or remotely via GPRS network or Ethernet connection (ELAN3-ALARM device required). This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use *ELDES Configuration Tool* software, please read the user guide provided in the software's HELP section.

5.4.1. Remote Connection

ATTENTION: The system will NOT transmit any data to monitoring station while configuring the system remotely via GPRS network or Ethernet connection. However, during the remote connection session, the data messages are queued up and transmitted to the monitoring station after the configuration session is over.

ATTENTION: When the Configuration mode is activated by EKB3/EKB3W keypad or when menu section CONFIGURATION is opened by the installer using EKB2 keypad, remote system configuration is disabled.

ATTENTION: The keypad (-s) become inactive while the system is being configured remotely.

ELDES Configuration Tool software provides remote system configuration ability via Internet using one of the following methods:

- ELDES proxy server (recommended). The connection can be established on the system via GPRS network or Ethernet using ELAN3-ALARM communicator.
- Running TCP/IP server on *ELDES Configuration Tool* (advanced). The connection can be established on the system via GPRS network or Ethernet using ELAN3-ALARM communicator.
- Direct connection via Ethernet using ELAN3-ALARM communicator.

In order to start using the remote configuration feature, please run the step-by-step wizard and follow the steps provided in the start page of *ELDES Configuration Tool* software. Please, note that based on the selected method, it might be necessary to send an SMS text message to the system's phone number in order to initiate the remote connection. By following the steps you will be instructed on what text must be sent to the system's phone number in such case.

5.4.2. Ending the Remote Connection Session

After the remote system configuration is complete, use one of the following methods to end the configuration process:

- Click **Disconnect** or **Stop** button and close *ELDES Configuration Tool* software.
- The session will automatically expire in 20 minutes. Before the last 5 minutes, the software will offer the user to extend the session for another 20 minutes.
- Alternatively, the connection with the server can be terminated at any time by sending an SMS text message.

Terminate the connection with server

SMS

SMS text message content:
ssss_ENDCONFIG
Value: *ssss* – 4-digit SMS password.
Example: *1111_ENDCONFIG*

Once the session is expired or terminated, the system will reply with an SMS text message confirming the end of the session.

6. SMS PASSWORD AND INSTALLER CODE

For security reasons, the system uses the following type of password and code:

SMS password - 4-digit password used for system arming/disarming and configuration by SMS text messages. By default, SMS password is 0000, which MUST be changed!. SMS password is authorized to carry out the following:

- Access system configuration by SMS text messages.
- Arm/disarm partition.
- Activate/deactivate service mode.
- Set system date and time.
- Add/remove user phone numbers.
- Set SMS password.
- Turn ON/OFF PGM outputs.
- Restart system remotely.

Installer code - 4-digit password used for system configuration by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software. By default, installer code is 1470, which is highly recommended to change. Installer code is authorized to carry out the following:

- Access system configuration by keypad and *ELDES Configuration Tool* software.
- Set installer code.
- Set master code.
- Activate/deactivate service mode.
- Set system date and time.
- Add/remove user phone numbers.
- Set SMS password.
- Restore system configuration to default.
- Clear tamper fault (if enabled).

Set SMS password

SMS

SMS text message content:
wwww_PSW_ssss
Value: *wwww* - 4-digit existing SMS password; *ssss* - 4-digit new SMS password; range - [0001... 9999].
Example: *0000_PSW_1111*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SMS PASSWORD → OK → ssss → OK
Value: *iiii* **-** 4-digit installer code; *ssss* - 4-digit new SMS password; range - [0001... 9999].

EKB3/ EKB3W

Enter parameter 14 & new SMS password:
14 ssss #
Value: *ssss* - 4-digit new SMS password; range - [0001... 9999].
Example: *141111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set installer code

EKB2

Menu path:
OK → 1470 → OK → PRIMARY SETTINGS → OK → INSTALLER CODE → OK → iiii → OK
Value: *iii* - 4-digit new installer code; range - [0000... 9999].

EKB3/ EKB3W

Enter parameter 16 & new installer code:
16 iiii #
Value: *iii* - 4-digit new installer code; range - [0000... 9999].
Example: *162538#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

7. SYSTEM LANGUAGE

The system comes equipped with a single language for communication with the user by SMS text messages and EKB2 keypad menu display. The system language depends on ESIM364 firmware, which is based on the user's location.

List of currently available system languages (firmwares):

- Czech
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish

NOTE: To obtain a firmware that features a different SMS and EKB2 menu language, please contact your local dealer.

8.USER PHONE NUMBERS

The system supports up to 10 user phone numbers identified as User 1 through 10. When the phone number is set, the user will be able to arm/disarm the system by SMS text messages and free of charge phone calls (see **12.1. Free of Charge Phone Call** and **12.2. SMS Text Message**) as well as to configure the system by SMS text messages. User phone numbers are also used to receive alarm phone calls via GSM connection and SMS text messages from the system (see **17. ALARM INDICATIONS AND NOTIFICATIONS FOR USER)**.

By default, the system accepts incoming calls and SMS text messages from any phone number. Once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number (see **8.2. System Control from any Phone Number**).

To set User 1 phone number is mandatory, while the other 9 are optional. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for UK: *+44170911XXXX1*. This format can be used when setting up the phone number by SMS text message and *ELDES Configuration Tool software*.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: *0044170911XXXX1*. This format can be used when setting up the phone number by SMS text message, EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool software*.
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for UK: *0170911XXXX1*. This format can be used when setting up the phone number by SMS text message, EKB2/ EKB3/EKB3W keypad and *ELDES Configuration Tool software*.

Add user phone number

SMS

SMS text message content:
ssss_NRup:ttteeellnnuumm
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [1... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1111_NR1:+44170911XXXX1*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PHONE NUMBER → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits user phone number.

EKB3/ EKB3W

Enter parameter 17, user phone number slot & phone number:
17 up ttteeellnnuumm #
Value: *up* – user phone number slot, range – [01... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *170100441709 11XXXX1#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View user phone number

SMS

SMS text message content:
ssss_HELPNR
Value: *ssss* – 4-digit SMS password.
Example: *1111_HELPNR*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PHONE NUMBER
Value: *iiii* – 4-digit installer code;

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user phone number

SMS

SMS text message content:
ssss_NRup:DEL
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [2... 10].
Example: *1111_NR2:DEL*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 2... 10 → OK → PHONE NUMBER → OK → OK
Value: *iiii* – 4-digit installer code;

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: NEVER add a phone number of the device's SIM card as a user phone number!

ATTENTION: Once User 1 phone number is set, it will be restricted to modify it only.

NOTE: Multiple user phone numbers can be set by a single SMS text message,
Example: *1111_NR1:+44170911XXXX1_ NR2:+44170911XXXX2_NR6:0170911XXXX3_NR10:+44170911XXXX4*

NOTE: Multiple user phone numbers can be deleted by a single SMS text message, **Example:** *1111_NR2:DEL_NR3:DEL_NR6:DEL_NR9:DEL_ NR:10:DEL*

8.1. User Phone Number Names

When the system is armed or disarmed by free of charge phone call or SMS text message, the system sends a confirmation by SMS text message to user phone number that the system arming/disarming was initiated from. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user phone number.

Manage user phone number name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

8.2. System Control from any Phone Number

By default, once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number. To permit/deny system arming/disarming by phone call and SMS text message that contain a valid SMS password, configuration by SMS text message that contain a valid SMS password from any phone number, please refer to the following configuration methods.

Enable system control from any phone number

SMS

SMS text message content:
ssss_STR:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_STR:ON*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code;

EKB3/ EKB3W

Enter parameter 12 & parameter status value:
12 1 #
Example: *121#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Due to security reasons it is HIGHLY UNRECOMMENDED to enable this feature.

Disable system control from any phone number

SMS

SMS text message content:
ssss_STR:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_STR:OFF*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code;

EKB3/ EKB3W

Enter parameter 12 & parameter status value:
12 0 #
Example: *120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

9. DATE AND TIME

The system comes equipped with internal real-time clock (RTC) that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly. By default, after shutting down and starting up the system, the date and time must be set again.

Set date and time

SMS

SMS text message content:
ssss_yyyy.mt.dd_hr:mn
Value: *ssss* - 4-digit SMS password; *yyyy* - year; *mt* - month, range - [01... 12]; *dd* - day, range - [01... 31]; *hr* - hours, range - [00... 23]; *mn* - minutes, range - [00... 59].
Example: *1111_2014.03.16_14:33*

EKB2

Menu path:
a) OK → uumm → OK → DATE/TIME SETTINGS → OK → yyyy-mt-dd hr:mn → OK
b) OK → iiii → OK → PRIMARY SETTINGS → OK → DATE/TIME SETTINGS → OK → yyyy-mt-dd hr:mn → OK
Value: *uumm* - 4-digit user/master code; *yyyy* - year; *mt* - month, range - [01... 12]; *dd* - day, range - [01... 31]; *hr* - hours, range - [00... 23]; *mn* - minutes, range - [00... 59]; *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 66, date & time:
66 yyyy mt dd hr mn#
Value: *yyyy* - year; *mt* - month, range - [01... 12]; *dd* - day, range - [01... 31]; *hr* - hours, range - [00... 23]; *mn* - minutes, range - [00... 59].
Example: *66201405291235#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When the system is connected to the monitoring station via GPRS network connection (see **30. MONITORING STATION**) and/or when Smart Security feature is in use (see **36. ELDES CLOUD SERVICES**), the date and time will be automatically synchronized with the monitoring station or Smart Security server upon the system startup.

9.1. Automatic Date and Time Synchronization

This feature enables the system to set the date and time automatically without the user being involved in this process. The system supports the following methods of automatic date and time synchronization that are used automatically on system start-up and periodically (by default - every 30 days):

- **Via GSM network** - Once enabled, the system automatically sends a date/time request to the GSM operator. This method is the most accurate synchronization method. Some GSM operators might not support it.
- **By SMS text message** - Once enabled, the system automatically sends the SMS text message to its own phone number and retrieves the date and time from the SMS text message reply, as the included date and time is set by the SMSC (SMS center). This method is not as accurate as the synchronization via GSM network, but always effective.

By default, synchronization via GSM network is disabled. To enable/disable automatic date and time synchronization via GSM network, please refer to the following configuration methods.

Enable/disable synchronization via GSM network

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, synchronization by SMS text message is disabled. To enable/disable automatic date and time synchronization by SMS text message, please enter/remove device phone number using one of the following configuration methods.

Enter/remove device phone number for synchronization by SMS text message

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

10. MASTER AND USER CODES

NOTE for EKB3/EKB3W: The Configuration mode must be deactivated, while managing user and master codes.

The system supports up to 30 numeric codes, identified as Master code and User code 2 through 30, allowing to carry out system arming/disarming as well as minor system configuration and control by the keypad.

Master code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View event log,
- View and clear alarm log,
- Set/delete user codes.
- Turn ON/OFF PGM outputs.
- Assign an existing user code as Duress code.
- Assign an existing user code as SGS code.

User code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View and clear alarm log.

By default, only Master code is listed as 1111 and assigned to Partition 1, 2, 3 and 4. For more details regarding User/Master code partition, please refer to **23.4. User/Master Code Partition.**

Set master code

EKB2

Menu path:
a) OK → vvvv → OK → CODES → OK → MASTER CODE → OK → CODE → OK → mmmm → OK
b) OK → iiii → OK → PRIMARY SETTINGS → OK → MASTER CODE → mmmm → OK
Value: *vvvv* - 4-digit existing master code, range - [0000... 9999]; *iiii* - 4-digit installer code; *mmmm* - 4-digit new master code, range - [0000... 9999].

EKB3/ EKB3W

a) Press [CODE], [0], enter existing master code & new master code:
[CODE] [0] vvvv 01 mmmm #
Value: *vvvv* - 4-digit existing master code; *mmmm* - 4-digit new master code; range - [0000... 9999].
Example: CODE01111012222#

b) Enter parameter 63, existing master code & new master code:
63 vvvv mmmm #
Value: *vvvv* - 4-digit existing master code; *mmmm* - 4-digit new master code, range - [0000... 9999].
Example: 6311112222#

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set user code

EKB2

Menu path:
User code 2... 16: OK → mmmm → OK → CODES → OK → USER CODE (2-16) → OK → USER CODE 2... 16 → OK → CODE → OK → uuuu → OK
User code 17... 30: OK → mmmm → OK → CODES → OK → USER CODE (17-30) → OK → USER CODE 17... 30 → OK → CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code, range – [0000... 9999].

EKB3/ EKB3W

Press [CODE], [0], enter master code, user code slot & user code:
[CODE] [0] mmmm us uuuuu #
Value: *mmmm* - 4-digit master code; *us* - user code slot, range - [02... 30]; *uuuu* - 4-digit user code, range - [0000... 9999].
Example: *CODE01111092556#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user code

EKB2

Menu path:
OK → mmmm → OK → CODES → OK → REMOVE CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code.

EKB3/ EKB3W

Press [CODE], [0], enter master code & user code slot:
[CODE] [0] mmmm us #
Value: *mmmm* - 4-digit master code; *us* - user code slot, range - [02... 30].
Example: *CODE0111109#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system does not allow to set a duplicate code.

The user codes ranging from User code 2 through 10 can be set as SGS (Security Guard Service) code, which is used as a checkpoint by a security service guard upon his/her visit in the secured location. When used, a data message, containing a certain event code, will be delivered to the monitoring station. However, NO system arming or disarming will be carried out after entering the SGS code.

Set SGS code

EKB2

Menu path:
OK → mmmm → OK → CODES → OK → SGS CODE → OK → N/A | USER CODE 2... 10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – SGS code not in use.

EKB3/ EKB3W

Press [CODE], [4], enter user code slot & enter master code:
[CODE] [4] us mmmm #
Value: *us* - user code slot, range - [02... 10]; *mmmm* - 4-digit master code.
Example: *CODE4041111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The Duress code is used when system arming or disarming is demanded by force. When used, the system will arm/disarm as well as it will silently transmit an alert to the monitoring station. Only one of the user codes ranging from User code 2 through 10 can be set as Duress code.

Set Duress code

EKB2

Menu path:
OK → mmmm → OK → CODES → OK → DURESS CODE → OK → N/A | USER CODE 2... 10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – Duress code not in use.

EKB3/ EKB3W

Press [CODE], [3], enter user code slot & master code:
[CODE] [3] us mmmm #
Value: *us* - user code slot, range - [02... 10]; *mmmm* - 4-digit master code.
Example: *CODE3081111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

10.1. Master and User Code Names

When the system is armed or disarmed by entering a master or user code using a keypad, the system sends a confirmation by SMS text message to user phone number, sharing the same partition (-s) as the keypad and user/master code. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user/master code.

Manage user/master code name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

11. iBUTTON KEYS

An iButton key is a unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. ESIM364 system supports up to 16 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.

11.1. Adding and Removing iButton Keys

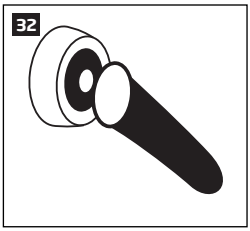
NOTE: iButton Key 1 can be added without Allow Adding New iButton Keys mode being enabled.

To add an iButton key to the system, do the following:

a) Disarm the system in all partitions (see **12. ARMING AND DISARMING**).

b) Enable Allow Adding New iButton Keys mode.

c) Touch the key to the iButton key reader when the system is disarmed.



d) The successfully added iButton key will be indicated by short beeps emitted by the system's buzzer.

e) Add as many iButton keys as necessary – touch one key after another to the reader – until the number of 16 keys is reached.

Enable Allow Adding New iButton Keys mode

SMS

SMS text message content:
ssss_IBPROG:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_IBPROG:ON*

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 18 & parameter status value:
18 0 #
Example: *180#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When adding of iButton keys is complete, please disable Allow Adding New iButton Keys mode.

Disable Allow Adding New iButton Keys mode

SMS

SMS text message content:
ssss_IBPROG:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_IBPROG:ON*

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 18 & parameter status value:
18 1 #
Example: *181#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To view the ID of the added iButton keys, please refer to the following configuration methods.

View iButton key ID

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1...16 → OK → ID
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If the iButton key is lost or stolen, due to security reasons it is highly recommended to remove it from the system.

Remove individual iButton key from the system

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1...16 → OK → REMOVE → OK
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Remove all iButton keys from the system

SMS

SMS text message content:
ssss_RESETIB
Value: *ssss* – 4-digit SMS password.
Example: *1111_RESETIB*

11.2. iButton Key Names

When the system is armed or disarmed by iButton key, the system sends a confirmation by SMS text message to listed user phone number, sharing the same partition (-s) as the key. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the iButton key.

Manage iButton key name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

12. ARMING AND DISARMING

The system features the following methods to carry out arming and disarming process:

- Free of charge phone call.
- SMS text message.
- EKB2/EKB3/EKB3W keypad and user/master code.
- iButton key.
- EWK1/EWK2/EWK2A wireless keyfob.
- Arm-Disarm by Zone.
- EGR100 middle-ware.
- ELDES Cloud Services platform

When attempting to arm the system (by any method, except EKB2/EKB3/EKB3W keypad and user/master code, iButton key, EWK1/EWK2/EWK2A keyfob, EGR100 middle-ware) in case of violated zone/tamper presence, the system will reply with SMS text message containing violated zone/tamper number. Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system. For more details on how to arm the system despite the violated zone presence, please refer to **14.6. Zone Attributes** and **14.7. Bypassing and Activating Zones**.

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message. For more details on SMS text message regarding system arming/disarming and how to manage it, please refer to **12.9. Disabling and Enabling Arm/Disarm Notifications**.

By default, it is allowed to arm the system while the following system faults are present (see **29. INDICATION OF SYSTEM FAULTS**):

- Mains power is lost.
- Low battery.
- Battery dead or missing.
- Battery failed.
- Siren failed.
- Date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Wireless antenna failed.
- Keypad lost.

NOTE: When the system is configured to operate in accordance with EN 50131-1 Grade 3 requirements, the aforementioned system faults, including tamper alarm, will prevent the system from arming when present.

In case of violated zone/tamper presence when attempting to arm the system by free of charge phone call, SMS text message and Arm-Disarm by Zone method, the system will reply with SMS text message containing violated zone/tamper number. Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system. For more details on how to arm the system regardless of the violated zone or tamper presence, please refer to **14.6. Zone Attributes, 14.7. Bypassing and Activating Zones** and **16.TAMPERS respectively**.

The system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number. For more details regarding arming/disarming the system from a non-listed phone number, please refer to **8.2. System Control from any Phone Number**.

NOTE: The system remembers the last status (armed/disarmed) of all partitions even after complete shut down.

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

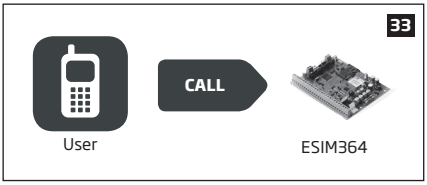
12.1. Free of Charge Phone Call

To arm, disarm the system and turn OFF the alarm, dial the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). The phone call is free charge as the system rejects it and carries out arming/disarming procedure afterwards. When arming – the system rejects the phone call after 2 rings, when disarming – the system rejects the phone call immediately. If there is more than one listed user dialing to the system at the same time, the system will accept the incoming call from the user who was the first to dial while other user (-s) will be ignored.

When system's phone number is dialed for arming, the system will proceed as follows:

- Non-partitioned system:
  - If ready (no violated zone/tamper), the system will arm.
  - If unready (violated zone/tamper is present), the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.
- Partitioned system:
  - If all partitions are disarmed ready, the system will arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
  - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by dialing the system's phone number. For example, if User 1 is assigned to Partition 1, 2 and 3, the user will be able to arm/disarm Partition 1, 2 and 3 by a single phone call to the system from User 1 phone number. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition**.



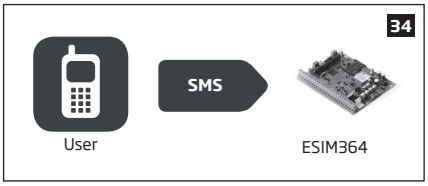
12.2. SMS Text Message

SMS

To arm the system by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management).

Arm the system

SMS text message content:
ssss_ARMp or ssss_ARMp,p,p,p
Value: *ssss* - 4-digit SMS password; *p* - partition number, range - [1... 4].
Example: *1111_ARM1*



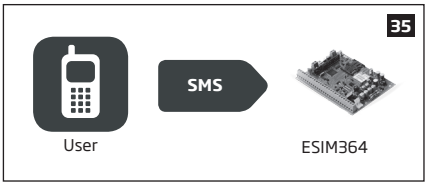
When the SMS text message for arming is sent to the system's phone number, the system will proceed as follows:

- Non-partitioned system:
  - If ready (no violated zone/tamper), the system will arm.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.
- Partitioned system:
  - If all partitions are disarmed ready (no violated zone/tamper), the system will arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
  - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

To disarm the system and turn OFF the alarm by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers:

Disarm the system and turn OFF the alarm

SMS text message content:
ssss_DISARMp or ssss_DISARMp,p,p,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4].
Example: *1111_DISARM1,2,4*



When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by sending the SMS text message to the system's phone number. For example, if User 3 is assigned to Partition 2 and 3, the user will be able to arm/disarm Partition 2 and/or 3 by sending an SMS text message from User 3 phone number. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition**.

12.3. EKB2 Keypad and User/Master Code

✓ icon displayed next to the partition name in the home screen view of EKB2 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If ✗ icon is displayed instead, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**), while the tampers can be disabled (see **16. TAMPERS**). icon appears in the home screen view if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

When a user/master code is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by EKB2 keypad using partition selection menu. However, if a user/master code is assigned to Partition 1, 2 and 4, while EKB2 keypad is assigned to Partition 2, the user will be able to arm/disarm Partition 1, 2 and 4, but the keypad will only display Partition 2 name and the related information in home screen view. For more details on how to set keypad partition and user/master code partition, please refer to **23.3. Keypad Partition and Keypad Partition Switch** and **23.4. User/ Master Code Partition** respectively.

12.3.1. Arming the System

To arm the system by EKB2 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **10. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

- **Non-partitioned system** - When a valid user code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps, the keypad will switch to home screen view and display the countdown timer.

Arm the system

Enter user/master code:
uumm → OK
Value: *uumm* – 4-digit user/master code.

- **Partitioned system - arming a single partition** – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If ← key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name that is being armed.

Arm the system

Enter user/master code and select partition:
uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Value: *uumm* – 4-digit user/master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name

- **Partitioned system - arming multiple partitions simultaneously** – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **ARM ALL** menu item is selected the system will proceed as follows:
  - if all partitions are disarmed-ready (no violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display multiple **ARMING part-name** messages for 3 seconds reflecting each partition the user/master code is assigned to, followed by partition selection menu.
  - if one or more partitions are disarmed-unready (contains violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message (-s) reflecting ready

partition (-s), while the unready partition (-s) will be skipped indicated by **part-name NOT READY** message (-s) followed by partition selection menu. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.

- if a combination of armed and disarmed-ready partitions exist, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message (-s) seconds reflecting ready partition (-s), while the pre-armed partition (-s) will be skipped. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.

When the keypad back-light timeout expires, the home screen view will follow. If ← key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timers next to the partition names the keypad is assigned to.

Arm all partitions simultaneously

Enter user/master code:
uumm → OK → ARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → ARM ALL → OK
Value: *uumm* - 4-digit user/master code; *p* - partition number, range - [1... 4], *part-name* - up to 15 characters partition name

When successfully armed:

- the countdown timers will disappear.
- in addition, the keypad may display 🔒 icon next to the partition name that has been armed (by default - disabled).

Enable/disable Show ARMED status in keypad

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: If the user fails to enter a correct user/master code 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user/master code. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message

12.3.2. Canceling System Arming

To cancel the arming process:

- **Non-partitioned system** - Enter the user/master code again during exit delay countdown.
- **Partitioned system** - Select the partition again, that is currently being armed, from the partition selection menu during exit delay countdown. The keypad will display **part-name ARMING TERMINATED** message for 2 seconds followed by partition selection menu.

12.3.3. Disarming the System and Turning OFF the Alarm

To disarm and turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

- **Non-partitioned system** - When a valid user or master code is entered, the keypad will switch to home screen view.

Disarm the system and turn OFF the alarm

Enter user/master code:
uumm → OK
Value: *uumm* - 4-digit user/master code.

- **Partitioned system - disarming a single partition** - When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be disarmed is selected, the keypad will display **part-name DISARMED** message for 2 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ← key may be touched in order to instantly return to home screen view.

Disarm the system and turn OFF the alarm

Enter user/master code and select partition:
uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Value: *uumm* - 4-digit user/master code; *p* - partition number, range - [1... 4], *part-name* - up to 15 characters partition name

- **Partitioned system; disarming multiple partitions simultaneously** - When a valid user or master code is entered, the keypad will display the partition selection menu. Once **DISARM ALL** menu item is selected, the keypad will display multiple **part-name DISARMED** messages for 2 seconds reflecting each partition the user/master code is assigned to and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ← key may be touched in order to instantly return to home screen view.

Disarm all partitions and turn OFF the alarm simultaneously

Enter user/master code:
uumm → OK → DISARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → DISARM ALL → OK
Value: uumm - 4-digit user/master code; p - partition number, range - [1... 4], part-name - up to 15 characters partition name

When successfully disarmed, the keypad may display 🔓 icon next to the partition name that has been disarmed (by default - disabled).

Enable/disable Show ARMED status in keypad

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: If the user fails to enter a correct user/master code 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user/master code. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

12.4. EKB3 Keypad and User/Master Code

ATTENTION: EKB3 keypad can operate either in 2-partition or in 4-partition mode. The description of the following procedure is based on 4-partition mode operation on EKB3 keypad. The arming/disarming procedure in 2-partition mode using EKB3 keypad would be carried out identically to EKB3W wireless keypad. For more details on 2-partition mode, please refer to **12.5. EKB3W Keypad and User/Master Code.**

Illuminated indicator READY on EKB3 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If the indicator READY is not illuminated, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**), while the tampers can be disabled (see **16. TAMPERS**). Indicator SYSTEM will illuminate or flash if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

The system will arm/disarm the partition corresponding to the one that user/master code and the keypad are assigned to. For example, if User code 4 is assigned to Partition 2, 3 and 4, while EKB3 keypad is assigned to Partition 2, the user will be able to arm/disarm only Partition 2 by entering User code 4. For more details on how to set keypad partition and user/master code partition, please refer to **23.3. Keypad Partition and Keypad Partition Switch** and **23.4. User/ Master Code Partition** respectively.

12.4.1. Arming the System

To arm the system by EKB3 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **10. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

- **Non-partitioned system** – When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - arming a single partition** – To arm a different partition than the keypad is assigned to, use keypad partition switch feature (by default - disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before the arming process.

Switch keypad partition

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

Once the partition is switched and a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - arming all 4 partitions simultaneously** – If a user/master code assigned to all 4 partitions exists, user can arm all partitions simultaneously. When this feature is used, the system will proceed as follows:
  - if all partitions are disarmed-ready (no violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and indicator ARMED along with number [1], [2], [3] and [4] keys will light ON. When the system is successfully armed, the keypad's buzzer will silent down.
  - if one or more partitions are disarmed-unready (keypad number [1]... [4] key flashing, indicating the partition that contains violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a non-violated partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The ready partition (-s) will be armed and the unready one (-s) will be skipped.
  - if a combination of armed and disarmed ready partitions is present, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a disarmed partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The disarmed-ready partitions will be armed and the pre-armed ones will be skipped.

Arm all 4 partitions simultaneously

Hold the [0] key, release it after 3 short beeps and enter user/ master code:
0 uumm
Value: *uumm* – 4-digit user/master code.
Example: *0 2222*

Alternatively, the user can arm multiple partitions one by one (see **Partitioned system - arming a single partition** above).

NOTE: Before arming all 4 partitions simultaneously, the user/master code must be assigned to all 4 partitions and the keypad partition switch feature enabled (see **23.3. Keypad Partition and Keypad Partition Switch**).

12.4.2. Canceling System Arming

To cancel the arming process, enter the user/master code again during exit delay countdown.

12.4.3. Disarming the System and Turning OFF the Alarm

To disarm and turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

- **Non-partitioned system** – When a valid user/ master code is entered, indicator ARMED and the number [1]... [4] key, indicating the partition that has been disarmed, will light OFF.

Disarm the system and turn OFF the alarm

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - disarming a single partition** – To disarm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before the disarming process.

Switch keypad partition

Hold the [1]... [4] key and release it after 3 short beeps:
Value: [1]... [4] key – parition number 1... 4 respectively.

Once the partition is switched and a valid user/master code is entered, indicator ARMED and the number [1]... [4] key, indicating the partition that has been disarmed, will light OFF.

Disarm the system and turn OFF the alarm

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - disarming all 4 partitions simultaneously** – If a user/master code assigned to all 4 partitions exists, user can disarm and turn OFF the alarm in all partitions simultaneously. When this feature is used, the system will proceed as follows:
  - if all partitions are armed and a valid user/master code is entered, indicator ARMED along with the number [1], [2], [3] and [4] keys will light OFF.
  - if a combination of armed and disarmed ready partitions is present, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a disarmed partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The disarmed-ready partitions will be armed and the pre-armed ones will be skipped.
  - if one or more partitions are disarmed-unready (keypad number [1]... [4] key flashing, indicating the partition that contains violated zone/tamper), the system will deny simultaneous partition disarming until the partition's zone/tamper violation is removed.

Disarm and turn OFF the alarm in all 4 partitions simultaneously

Hold the [0] key, release it after 3 short beeps and enter user/ master code:
0 uumm
Value: *uumm* – 4-digit user/master code.
Example: *0 2222*

Alternatively, the user can disarm and turn OFF the alarm in multiple partitions one by one (see **Partitioned system - disarming a single partition** above).

NOTE: Before disarming all 4 partitions simultaneously, the user/master code must be assigned to all 4 partitions and the keypad partition switch feature enabled (see **23.3. Keypad Partition and Keypad Partition Switch**).

12.5. EKB3W Keypad and User/Master Code

ATTENTION: The user will be able arm/disarm only the first two system partitions using EKB3W keypad. Partition 3 and Partition 4 are NOT supported by EKB3W keypad.

Illuminated indicator READY on EKB3W keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If the indicator READY is not illuminated, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**), while the tampers can be disabled (see **16. TAMPERS**). Indicator SYSTEM will illuminate or flash if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

The system will arm/disarm the partition corresponding to the one that user/master code and the keypad are assigned to. For example, if User code 4 is assigned to Partition 2, while EKB3W keypad is assigned to Partition 1, the user will be able to arm/disarm only Partition 2 by entering User code 4. For more details on how to set keypad partition and user/master code partition, please refer to **23.3. Keypad Partition and Keypad Partition Switch** and **23.4. User/ Master Code Partition** respectively.

12.5.1. Arming the System

- **Non-partitioned system** – When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - arming a single partition** – To arm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before the arming process.

Switch keypad partition

Hold the [1]... [2] key and release it after 3 short beeps:
Value: [1]... [2] key – parition number 1... 2 respectively.

Once the partition is switched and a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

To arm multiple partitions, please arm the partitions one by one by following the aforementioned procedure.

12.5.2. Canceling System Arming

To cancel the arming process, enter the user/master code again during exit delay countdown.

12.5.3. Disarming the System and Turning OFF the Alarm

To disarm and turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

- **Non-partitioned system** – When a valid user/ master code is entered, indicator ARMED will light OFF.

Disarm the system and turn OFF the alarm

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

- **Partitioned system - disarming a single partition** – To disarm and turn OFF the alarm in a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before the disarming process.

Switch keypad partition

Hold the [1]... [2] key and release it after 3 short beeps:
Value: [1]... [2] key – parition number 1... 2 respectively.

Once the partition is switched and a valid user/master code is entered, indicator ARMED will light OFF.

Disarm the system and turn OFF the alarm

Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

To disarm and turn OFF the alarm in multiple partitions, please disarm the partitions one by one by following the aforementioned procedure.

12.6. iButton Key

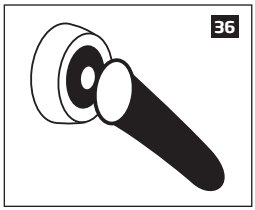
To arm or disarm the system and turn OFF the alarm, touch the iButton key reader by any of 16 available iButton keys (see **11. iBUTTON KEYS** for iButton key management). When the iButton is touched to the iButton key reader for arming, the system will proceed as follows:

Non-partitioned system:

- If ready (no violated zone/tamper), the system will initiate exit delay and arm.
- If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**), while the tampers can be disabled (see **16. TAMPERS**).

Partitioned system:

- If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and arm them.
- If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).
- If a combination of armed and disarmed ready partitions is present, the system will initiate exit delay, arm the disarmed ready partitions and skip the armed ones.



When an iButton key is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by touching the iButton key to the reader. For example, if iButton 5 is assigned to Partition 1 and 4, the user will be able to arm/disarm Partition 1 and 4 by touching iButton 5 to the reader. For more details on how to set iButton key partition, please refer to **23.5. iButton Key Partition**.

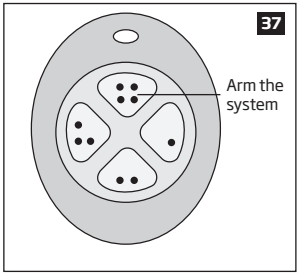
12.7. EWK1/EWK2 Wireless Keyfob

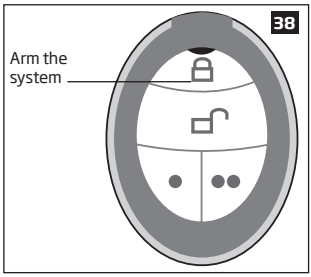
EWK1/ EWK2

To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 – ;EWK 2 -). When EWK1/ EWK2 button is pressed for arming, the system will proceed as follows:

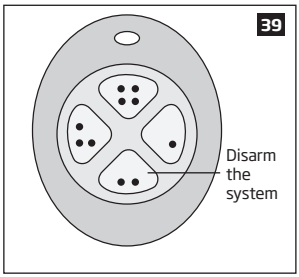
Non-partitioned/partitioned system:

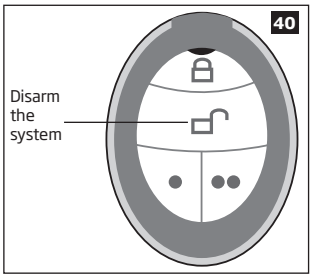
- If ready (no violated zone/tamper), the system will arm.
- If unready, the system will not arm. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).





To disarm the system, press 1 of 4 keyfob buttons set to disarm the system (by default, EWK1 - ; EWK2 -).





To verify if the system has been successfully armed, do not release the *Arm the system* keyfob button and wait for the 3 short keyfob buzzer's beeps/indicator's flashes indicating the successfully carried out command. The long beep/flash indicates the unsuccessful command.

The system will arm/disarm the partition corresponding to the one that EWK1/EWK2 wireless keyfob is assigned to (see **23.6. EWK1/EWK2/EWK2A Wireless Keyfob Partition**). For example, if EWK1/EWK2 wireless keyfob is assigned to Partition 3, the user will be able to arm/ disarm only Partition 3. To arm a different partition than the EWK1/EWK2 wireless keyfob is assigned to, pair another EWK1/EWK2 keyfob with the system and assign it to a different partition.

For more details on how to manage EWK1/EWK2 keyfob buttons, please refer to *ELDES Configuration Tool* software's HELP section.

12.8. Arm-Disarm by Zone

ARM/ DISARM ZONE

The Arm-Disarm by Zone feature allows to use a zone for arming and disarming the alarm system. The process is performed by applying a low-level pulse for more than 3 seconds to the specified zone. It means that violating and restoring the zone leads to system arming and by repeating this action the system becomes disarmed. The system will arm/disarm the partition (-s) that the zone is assigned to. Up to 4 on-board zones can be set to arm/disarm up to 4 system partitions by this method.

Set zone for Arm-Disarm by Zone method

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → ZONE 1... 4 → OK → nn
Value: *iiii* – 4-digit installer code; *nn* – on-board zone number, range – [01... 12].

EKB3/ EKB3W

Enter parameter 34, on-board zone slot & zone number:
34 z nn #
Value: *z* – on-board zone slot for Arm-Disarm by Zone method; range - [1... 4]; *nn* – on-board zone number, range – [01... 12].
Example: *34023#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Arm-Disarm by Zone method

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → ZONE 1... 4 → OK → 0
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 34, on-board zone slot & parameter status value:
34 z 00 #
Value: *z* - on-board zone slot for Arm-Disarm by Zone method; range - [1... 4].
Example: *34200#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

12.9. Disabling and Enabling Arm/Disarm Notifications

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message to:

- user phone number, sharing the same partition as EKB2/EKB3/EKB3W keypad and user/master code, iButton key, EWK1/EWK2 wireless keyfob or zone, set up for Arm/Disarm by Zone method.
- user phone number that the system arming/disarming by free of charge phone call was initiated from.
- user phone number that the system arming/disarming by SMS text message was initiated from.

The confirmation SMS text message is sent to the user phone number regarding each partition separately and contains system status and partition name as well as it may contain a user name assigned to user phone number, user/master code or iButton key. For more details on names, please refer to **8.1. User Phone Number Names, 10.1. User/Master Code Names** and **11.2. iButton Key Names.**

To disable/enable this notification for individual user phone number, please refer to the following configuration methods.

Disable arm/disarm notification

EKB2

Menu path:
System armed:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → SYS ARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → SYS ARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

System disarmed:
User phone number: ... → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → SYS DISARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → SYS DISARMED EVENT → OK → SMS REPORT → OK → DISABLE→ OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
System armed event
User phone number: 25 01 up 0 #
SMS text message to all users simultaneously: 21 01 up 0 #
SMS delivery report: 55 01 up 0 #

System disarmed event
User phone number: 25 02 up 0 #
SMS text message to all users simultaneously: 21 02 up 0 #
SMS delivery report: 55 02 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2502040#*

	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Enable arm/disarm notification	**EKB2**	**Menu path:** **System armed**: User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK SMS text message to all users simultaneously: ... → SYS ARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK SMS delivery report: ... → SYS ARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK **System disarmed:** User phone number: ... → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK SMS text message to all users simultaneously: ... → SYS DISARMED EVENT → OK → SMS TO ALL → OK → ENBABLE → OK SMS delivery report: ... → SYS DISARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK **Value:** *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 25/21/55, event number, user phone number slot & parameter status value:** **System armed event** User phone number 25 01 up 1 # SMS text message to all users simultaneously: 21 01 up 1 # SMS delivery report: 55 01 up1 # **System disarmed event** User phone number: 25 02 up 1 # SMS text message to all users simultaneously: 21 02 up 1 # SMS delivery report: 55 02 up 1 # **Value:** *up* - user phone number slot, range - [01... 10]. **Example:** *2502061#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: The system will always deliver an SMS notification to the user after arming/disarming the system by SMS text message method even if the arm/ disarm SMS notification is disabled.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery* report parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

13. EXIT AND ENTRY DELAY

When arming, the system initiates the exit delay countdown (by default - 15 seconds) intended for the user to leave the secured area. The exit delay is indicated by short beeps emitted by EKB2/EKB3/EKB3W keypad buzzer and buzzer, connected to the alarm system. When arming:

- a non-partitioned system, a countdown timer will be displayed in the home screen view of EKB2 during exit delay.
- a partitioned system, EKB2 keypad will display **ARMING part-name** message on the screen for 2 seconds and switch to partition selection menu during exit delay.

Exit delay is provided when arming the system by the following methods:

- EKB2/EKB3/EKB3W keypad and user/master code.
- iButton key.
- Arm/Disarm by Zone.

To arm the system without exit delay, use one of the following system arming methods:

- Free of charge phone call.
- SMS text message.
- EWK1/EWK2/EWK2A wireless keyfob
- EGR100 middle-ware.

Set exit delay

SMS

SMS text message content:
ssss_EXITDELAY:p,ext or ssss_EXITDELAY:p,ext;p,ext;p,ext;p,ext
Value: *ssss* - 4-digit SMS password; *p* - partition number, range - [1... 4], *ext* - exit delay duration, range - [0... 600] seconds.
Example: *1111_EXITDELAY:1,20;3,43*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EXIT DELAY → OK → PARTITION 1... 4 → OK → ext → OK
Value: *iiii* - 4-digit installer code;, *ext* - exit delay duration, range - [0... 600] seconds.

EKB3/ EKB3W

Enter parameter 72, partition number & exit delay duration:
72 pp ext #
Value: *pp* - partition number, range - [01... 04], *ext* - exit delay duration, range - [0... 600] seconds.
Example: *7203259#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Alternatively, you can set exit delay value to 0 in order to arm the system without exit delay by any available method.

NOTE: EKB3/EKB3W keypad buzzer will only beep if the keypad is operating in the partition where exit delay countdown is in progress.

Once the exit delay has expired, the system initiates the entry delay countdown (by default - 15 seconds) if a Delay type zone is violated. The countdown is indicated by short beeps emitted by keypad buzzer and by steady beep emitted by system's buzzer. The indication is intended to advise the user that the system should be disarmed. Once the user presses/touches any key on the keypad during this delay, the buOer of the keypad will be silenced. If the system is disarmed before the entry delay expires, no alarm will be caused.

Set entry delay for Delay zone

SMS

SMS text message content:
ssss_ENTRYDELAY:nn,eeeee or ssss_ENTRYDELAY:nn,eeeee;nn,eeeee;nn,eeeee;nn,eeeee
Value: *ssss* - 4-digit SMS password; *nn* - zone number, range - [1... 76], *eeeee* - entry delay duration, range - [0... 65535] seconds.
Example: *1111_ENTRYDELAY:1,25;54,14;12,20*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → ENTRY DELAY → OK → eeeee → OK
Wireless zone: ... WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → ENTRY DELAY → OK → eeeee → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → ENTRY DELAY → OK → eeeee → OK
EPGM1 zone: .. → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → ENTRY DELAY → OK → eeeee → OK
Value: *iiii* - 4-digit installer code; *eeeee* - entry delay duration, range - [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 54, partition number and entry delay duration:
54 nn eeeee #
Value: *nn* - zone number, range - [01... 76], *eeeee* - entry delay duration, range - [0... 65535] seconds
Example: *5403259#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Due to battery power saving reasons, EKB3W keypad buzzer will not sound during exit and entry delay if the violated Delay type zone is not of the associated EKB3W keypad.

For more details on zone types, please refer to **14.5. Zone Type Definitions**.

14. ZONES

Detection devices such as motion detectors and door contacts are connected to the alarm system's zone terminals. Once connected, the associated zone's parameters must be configured.

ESIM364 comes equipped with 6 on-board zones allowing to connect up to 6 detection devices. For more details regarding zone expansion, please refer to **14.2. Zone Expansion**.

ESIM364 zones are classified by 5 categories:

Zone category	Description	Max. number of zones per device	Max. number of zones in total
On-board zones	Built-in wired zones of ESIM364 alarm system.	6/12*	6/12*
Keypad zones	Hardwired zones of EKB2/EKB3/EKB3W keypad.	1	4
EPGM1 zones	Zones of EPGM1 - hardwired zone and PGM output expansion module.	16	32
Wireless zones	Non-physical zones automatically created by connected wireless devices.	4**	64***
Virtual zones	Non-physical zones intended for Panic button feature (alarm activaton upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using *ELDES Configuration Tool* software.	64****	64****

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

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

14.1. Zone Numbering

The zone numbers ranging from Z1 through Z12 are permanently reserved for on-board zones even when ATZ mode is disabled. The Z13-Z76 zone numbers are automatically assigned in the chronological order to the created virtual zones and the devices connected to the system: keypads, wireless devices, EPGM1 modules.

14.2. Zone Expansion

For additional detection device connection, the number of zones can be expanded by:

- enabling the ATZ (Advanced Technology zone) mode (see **14.4. ATZ (Advanced Technology Zone) Mode**).
- connecting EPGM1 hardwired zone and PGM output expansion module (for more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download).
- connecting keypads (see **32.1.1. EKB2 - LCD Keypad**, **32.1.2. EKB3 - LED Keypad** and **19.4. EKB3W - Wireless LED Keypad**).
- pairing wireless devices (see **19. WIRELESS DEVICES**).
- creating virtual zones (see *ELDES Configuration Tool* software's Help section).

The maximum supported number of zones is 76.

14.3. 6-Zone Mode

By default, ESIM364 alarm system runs in the 6-Zone mode under zone connection Type 1 allowing to connect up to 6 detection devices of NO (normally-open) or NC (normally-closed) type to the on-board zone terminals as indicated in the wiring diagram of Type 1 or Type 2 respectively. Once a Type 3 zone connection type is set, the detection device wiring must be done according to the wiring diagram of the associated type.

Zone connection types for the 6-Zone mode:

- **Type 1** - Parallel wiring of NO (normally-open) detection device with 5,6kΩ EOL (end-of-line) resistor.
- **Type 2** - Serial wiring of NC (normally-closed) detection device with 5,6kΩ EOL resistor.
- **Type 3** - Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and NC (normally-closed) detection device with 3,3kΩ EOL resistor.

For zone wiring diagrams of the 6-Zone mode, please refer to **2.3.2. Zone Connection Types**.

Set zone connection type for 6-Zone mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ZONE TYPE:6-ZONE M → OK → TYPE 1... 3 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 39 & number of zone connection type:
39 1 # – Type 1
39 2 # – Type 2
39 3 # – Type 3
Example: *392#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system supports a mixed combination of Type 1 and Type 2 zone connection types simultaneously regardless of the type (Type 1 or Type 2) selected in the system's configuration. This applies to on-board zones, keypad zones and EPGM1 zones. **Example:** *On-board zone Z1 and keypad zone is wired based on Type 1, while on-board zone Z3 and EPGM1 zone is wired based on Type 2.*

NOTE: Type 3 is NOT supported by keypad zones.

NOTE: ATZ mode is NOT supported by keypad zones and EPGM1 zones. If ATZ mode is enabled, EPGM1 zones must be wired in accordance with the last selected 6-Zone mode zone connection type before the ATZ mode has been enabled. The ATZ mode setting does NOT affect the zone connection type of the keypad zones.

14.4. ATZ (Advanced Technology Zone) Mode

The ATZ mode is a software-based feature that doubles the number of on-board zones and enables two detection devices to be installed per 1 zone terminal. Once this mode is enabled, the zone connection Type 4 is set automatically. The detection devices must be wired to the on-board zone terminals as indicated in the wiring diagram of the associated zone connection type.

Available zone connection types for the ATZ mode:

- **Type 4** – Parallel wiring of 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL (end-of-line) resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.
- **Type 5** – Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.

For zone wiring diagrams of the ATZ mode, please refer to **2.3.2. Zone Connection Types**.

Enable ATZ mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ATZ MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 28 & parameter status value:
28 1 #
Example: *281#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable ATZ mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ATZ MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 28 & parameter status value:
28 0 #
Example: *280#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set zone connection type for ATZ mode

EKB2

Menu path:
OK → CONFIGURATION → OK → iiii → OK → ZONES → OK → ZONE TYPE:ATZ MODE → OK → TYPE 4... 5 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 38 & number of zone connection type:
38 1 # - Type 4
38 2 # - Type 5
Example: *381#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Once enabled, the ATZ mode DOES NOT affect EPGM1 zones, nor keypad zones and applies to on-board zones only.

14.5. Zone Type Definitions

- **Interior Follower** – The zone can be violated during exit and entry delay without causing an alarm. If the zone is violated before the entry delay has begun, it will cause an instant alarm followed by single notification delivery even if the zone has been violated multiple times or another Interior Follower-type zone has been violated while alarm period (by default - 1 minute) is in progress. Typically, this zone is used for indoor protection devices, such as motion detectors, installed close to the exit/entry doors.
- **Instant** – The alarm is instantly caused if this zone is violated when the system is armed or during entry delay. This zone type is usually used for doors, windows, shock sensors or other zones.
- **24-Hour** – When the system is either armed or disarmed, the zone will cause instant alarm if violated. Normally, this type of zone is used for securing the areas that require constant supervisory.
- **Delay** – This zone type can be violated during exit and entry delay without causing an alarm. If the zone is violated when the system is armed, it will initiate entry delay countdown intended for the user to disarm the system. If the zone is left violated after the exit delay expires, it will cause an instant alarm. Typically, this zone type is used for door contacts installed at designated exit/entry doors.
- **Fire** – If this zone type is violated when the system is either armed or disarmed, the alarm will be instantly caused and the siren/bell will emit pulsating sound. Typically, this zone type is used for flame and smoke detectors.
- **Panic/Silent** – This zone operates the same as 24-Hour zone type, but the system will not activate the siren/bell and keypad buzzer if violated. Normally, this zone type used for panic alarm buttons.

Set zone type for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24- HOUR | DELAY | FIRE | PANIC/ SILENT → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 53, zone number & zone type number:
53 nn 1 # - Interior Follower
53 nn 2 # - Instant
53 nn 3 # -24-Hour
53 nn 4 # - Delay
53 nn 5 # - Fire
53 nn 6 # - Panic/Silent
Value: *nn* - zone number, range - [01... 76]
Example: *53125#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system will NOT activate siren/bell and keypad buzzer only when Panic/Silent zone type is violated.

14.6. Zone Attributes

- **Stay** - If this attribute is enabled, the zone, regardless of type, will not cause an alarm if violated when the system is Stay armed. For more details on arming the system in the Stay mode, please refer to **15. STAY MODE**.
- **Force** - This attribute determines whether the system can be armed or not while a zone is violated. If a zone with the Force attribute enabled remains violated until the exit delay expires, it will be ignored. Once the system is armed and the zone is restored, the violation will not be ignored and the zone will operate according to the determined type. For more details on zone types, please refer to **14.5. Zone Type Definitions**.
- **Shared** - This attribute determines whether a zone, assigned to multiple partitions, will cause an alarm or not in the associated armed partition if violated. If a zone with the Shared attribute enabled is violated when at least one of the associated partitions is disarmed, the alarm will not be caused. Once the system is armed in all of the associated partitions, the zone with Shared attribute enabled will operate according to the determined type. Typically, this attribute is used for shared areas, such as corridors.
- **Delay, ms** - This attribute determines the zone sensitivity level by delay time (By default - 800 milliseconds). If a zone is left triggered until the delay time expires, the zone is considered violated. This attribute does not apply to wireless zones, keypad zones and virtual zones.
- **Cross-Zone/Intelli-Zone** is a method used to prevent false alarms. The system will not cause an alarm unless two associated zones are violated within a specified time period, known as Alarm Confirmation Timeout. By associating a certain zone to itself, the system would cause an alarm only if the zone has been violated repeatedly within the Alarm Confirmation Timeout. This feature operates with all zone categories including virtual zones.
- **Delay becomes Instant in Stay mode** - This attribute determines whether or not any Delay type zone will operate as Instant type zone when the system is armed in the Stay mode. When the system is fully armed, the Delay type zone will operate normally. For more details on Delay and Instant zone types, please refer to **14.5. Zone Type Definitions**.
- **Chime** - This feature is used to emit 3 short beeps from the keypad buzzer whenever any Delay type zone is violated while the system is disarmed. Typically, the feature is used for designated exit/entry doors to indicate the opening of the doors.
- **Bell** - This attribute operates identically as Chime and applies to EKB3W keypad only.

NOTE: Due to battery power saving reasons, EKB3W wireless keypad buzzer will not sound if the Bell attribute is not enabled and the vio-lated Delay type zone is not of the associated EKB3W wireless keypad. For more details on EKB3W wireless keypad, please refer to **19.5. EKB3W - Wireless LED Keypad.**

Enable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → ENABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → ENABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEPAD ZONE → OK → STAY → OK → ENABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 1 #
Value: *nn* - zone number, range - [01... 76].
Example: *56041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → DISABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → DISABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STAY → OK → DISABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 0 #
Value: *nn* - zone number, range - [01... 76].
Example: *56190#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → ENABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → ENABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → ENABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → FORCE → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 1 #
Value: *nn* - zone number, range - [01... 76].
Example: *82061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → DISABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → DISABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → DISABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → FORCE → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 0 #
Value: *nn* - zone number, range - [01... 76].
Example: *82110#*

	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Enable/disable Shared attribute for individual zone	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Set Delay, ms atrribute	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Enable/disable Delay becomes Instant in Stay mode attribute	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Disable Chime attribute	EKB2	**Menu path:** OK →iiii → OK → ZONES → OK → CHIME → OK → DISABLE → OK **Value:** *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 32 & parameter status value:** 32 0 # **Example:** *320#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Enable Chime attribute	EKB2	**Menu path:** OK →iiii → OK → ZONES → OK → CHIME → OK → ENABLE → OK **Value**: *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 32 & parameter status value:** 32 1 # **Example:** *321#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, Cross-Zone/Intelli-Zone is not set. To associate two zones and/or set the Alarm Confirmation Timeout, please refer to the following configuration method.

Associate a zone for Cross-Zone/Intelli-Zone	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Set Alarm Confirmation Timeout	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: This feature is NOT recommended in case it is necessary to bypass the associated zone, otherwise the zone that requires alarm confirmation will never cause an alarm when violated.

14.7. Bypassing and Activating Zones

NOTE for EKB3/EKB3W: The Configuration mode must be deactivated, while bypassing and activating a bypassed zone.

Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. When a zone is bypassed, EKB3/EKB3W keypad indicator BYPS will light ON and EKB2 keypad will display [⇆] icon in the home screen view.

Bypass individual violated zone

EKB2

Menu path:
OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 5 → OK → Z1-zone-name... Z76-zone-name → OK → BYPASS → OK
Value: *uumm* – 4-digit user/master code; *zone-name* – up to 24 characters zone name.

EKB3/ EKB3W

Press the [BYPS[key, enter zone number & user/master code:
BYPS nn uumm #
Value: *nn* – zone number, range – [01... 76]; *uumm* – 4-digit user/master code.
Example: *BYPS091111#*

Bypass all violated zones

EKB2

Menu path:
OK → uumm → OK →BYPASS → OK → BYP VIOLATED ZONES → OK
Value: *uumm* – 4-digit user/master code.

The zone will remain bypassed until the system is disarmed. Once the system is disarmed, the corresponding zone state will be indicated on the keypads (see **32.1.1. EKB2 - LCD Keypad, 32.1.2. EKB3 - LED Keypad** and **19.5. EKB3W - Wireless LED Keypad**) and Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**). Alternatively, the user can activate the bypassed zone by the following configuration methods.

Activate bypassed zone

EKB2

Menu path:
OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 5 → OK → Z1-zone-name... Z76-zone-name → OK → UNBYPASS → OK
Value: *uumm* – 4-digit user/master code; *zone-name* – up to 24 characters zone name.

EKB3/ EKB3W

Press the [BYPS] key, enter zone number & user/master code:
BYPS nn uumm #
Value: *nn* – zone number, range – [01... 76]; *uumm* – 4-digit user/master code.
Example: *BYPS251111#*

NOTE: Zones can only be bypassed and activated when the system is not armed.

14.8. Zone Names

Each zone has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined zone terminal, for **Example:** Kitchen doors opened. The zone names are used in SMS text messages that are sent to the user during alarm. the By default, the zone names are: *Z1 - Zone1, Z2 - Zone2, Z3 - Zone3, Z4 - Zone4 etc.*

Set zone name

SMS

SMS text message content:
ssss_Znn:zone-name
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76]; *zone-name* – up to 24 characters zone name.
Example: *1111_Z3:Door sensor triggered*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View zone names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → NAME
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → NAME
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → NAME
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → NAME
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in zone names

NOTE: Multiple zone names can be set by a single SMS text message, **Example:** *1111_Z1:Kitchen doors opened;Z3:Movement in basement;Z4:Bedroom window opened*

14.9. Disabling and Enabling Zones

By default, all zones, except keypad and virtual zones, are enabled. To permanently disable/enable an individual zone, please refer to the following configuration methods.

Disable zone

SMS

SMS text message content:
ssss_Znn:OFF
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76].
Example: *1111_Z13:OFF*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → DISABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → DISABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STATUS → DISABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 0 #
Value: *nn* – zone number, range – [01... 76].
Example: *52360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable zone

SMS

SMS text message content:
ssss_Znn:ON
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76].
Example: *1111_Z6:ON*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → ENABLE → OK
Wireless zone: ... → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → ENABLE → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STATUS → ENABLE → OK
EPGM1 zone: ... → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 1 #
Value: *nn* – zone number, range – [01... 76].
Example: *52151#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

14.10. Viewing Zone State

The zone state (violated/restored) is indicated in real-time by all available configuration methods. However, the most convenient way to view the zone state is using the graphical interface of *ELDES Configuration Tool* software as follows:

- Red - zone is violated.
- Green - zone is restored.
- Grey - zone is disabled.

To view the zone state, please refer to the following configuration methods.

View zone state

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Menu path:
OK → uumm → OK → VIOLATED ZONES → OK → ZONE 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W

Please, refer to illuminated zone indicators ranging from 1 through 12 on the keypad. The flashing indicator SYSTEM stands for violated high-numbered zones (Z13-Z76). For more details on violated high-numbered zone indication, please refer to **29. INDICATION OF SYSTEM FAULTS**.

15. STAY MODE

Stay mode allows the user to arm and disarm the alarm system without leaving the secured area. If the zones with Stay attribute enabled are violated when the system is Stay armed, no alarm will be caused. Typically, this feature is used when arming the system at home before going to bed.

The system can be Stay armed under the following conditions:

- If a Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exists, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay. For more details on these methods, please refer to **13. EXIT AND ENTRY DELAY.**
- The system will instantly arm in Stay mode when using one of the following methods.

Arm the system in Stay mode

EKB2

Menu path:
Non-partitioned system: P2 → uumm → OK
Partitioned system: P2 → uumm → OK → [p] part-name → OK
Value: *uumm* – 4-digit user/master code; *p* – partition number, range – [1... 4]; *part-name* – up to 15 characters partition name.

EKB3/ EKB3W

Press the [STAY] key & enter user/master:
STAY uumm
Value: *uumm* – 4-digit user/master code.
Example: *STAY1111*

When one or more system partitions are successfully armed in Stay mode, EKB2 keypad will display icon in the home screen view.

NOTE for EKB3/EKB3W: The Configuration mode must be deactivated, when Stay-arming the system.

NOTE: The system can be armed in Stay mode, only if there is at least one zone with Stay attribute enabled.

NOTE: Stay mode is not supported by virtual zones.

For more details on how to enable Stay attribute for zone, please refer to **14.6. Zone Attributes**.

16. TAMPERS

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren/bell and the keypad buzzer and send the SMS text message to the listed user phone number. The system will cause tamper alarm under the following conditions:

- If the enclosure of a detection device, siren/bell, metal cabinet or keypad is opened, the physical tamper switch will be triggered. By default, indicated *as Tamper x* in the SMS text message (x = tamper number). Alternatively, the tamper switch can be connected to a zone resulting in zone alarm when tampered (see **15. ZONES**).
- If the wireless signal is lost due to low signal level or low battery power on a certain wireless device (see **19.3. Wireless Signal Status Monitoring**).

By default, all tampers and tamper alarm notification by SMS text message is enabled. To disable/enable a certain tamper and/or tamper alarm notification, please refer to the following configuration methods

Disable/enable tamper

Config Tool — This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View violated tampers

SMS — The system will automatically send an SMS text message, containing a violated tamper name, to user phone number.

EKB2 — **EKB2 Menu path:**
OK → uumm → OK → VIOLATED TAMPERS → OK → TAMPER 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W — The illuminated indicator SYSTEM stands for system fault presence including violated tamper. For more details on violated tamper indication, please refer to **29. INDICATION OF SYSTEM FAULTS**.

Disable tamper alarm notification

EKB2 — **Menu path:**
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → TAMPER ALARM → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → TAMPER ALARM → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W — **Enter parameter 25/21/55, event number, user phone number slot & parameter status value:**
User phone number: 25 13 up 0 #
SMS text message to all users simultaneously: 21 13 up 0 #
SMS delivery report: 55 13 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2513030#*

Config Tool — This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable tamper alarm notification

EKB2 — **Menu path:**
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → TAMPER ALARM → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → TAMPER ALARM → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 13 up 1 #
SMS text message to all users simultaneously: 21 13 up 1 #
SMS delivery report: 55 13 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2513041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how to view violated tamper, please refer to 1**7. ALARM INDICATIONS AND NOTIFICATIONS FOR USER**.

ATTENTION: Once a certain tamper is disabled, the system will NOT deliver any text message regarding the physical tamper violation nor wireless signal loss or restore.

ATTENTION: The system will NOT deliver any text message regarding wireless signal loss or restore while the physical tamper violation is in progress.

ATTENTION: The system will NOT cause any tamper alarm regarding the physical tamper violation nor wireless signal loss if the associated zone is disabled.

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3**.

16.1. Tamper Names

Each tamper has a name that can be customized by the user. The tamper names are used in SMS text messages that are sent to the user during the tamper alarm. By default, the tamper names are: *Tamper 1, Tamper 2, Tamper 3, Tamper 4 etc*. To set a different tamper name, please refer to the following configuration methods.

Manage tamper name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

17. ALARM INDICATIONS AND NOTIFICATIONS FOR USER

When a zone, depending on zone type (see **14.5. Zone Type Definitions**), or tamper is violated, the system will cause an alarm. By default, the alarm duration is 1 minute (see **20. SIREN/BELL** regarding the alarm duration). During the alarm, the system will follow this pattern:

1. The system activates the siren/bell and the keypad buzzer.

a) The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.

b) The keypad buzzer will emit short beeps.

c) EKB2 keypad will display !!! icon next to the alarmed partition in the home screen view followed by icon indicating the presence of the alarm events in the alarm log (see **28. EVENT AND ALARM LOG**). In case a Fire-type zone is violated in any system partition, icon will appear in the home screen view.

d) EKB3 keypad operating in 4-partition mode will flash the [1]... [4] key corresponding to the alarmed partition number.

e) If one or more zones are violated, EKB3/EKB3W will light ON the corresponding violated zone indicator (-s) ranging from 1 through 12. Indicator SYSTEM will flash if one or more high-numbered zones are violated. If one or tampers are violated, indicator SYSTEM will light ON. For more details on viewing violated high-numbered zone and tamper numbers by EKB3/EKB3W keypad, please refer to **29. INDICATION OF SYSTEM FAULTS**.

2. The system attempts to send an SMS text message, containing the violated zone/tamper name (see **14.8. Zone Names** on how to set a zone name), to the first listed user phone number, sharing the same partition as the violated zone/tamper. The system will send SMS text messages regarding each violated zone/tamper separately.

a) If the user phone number is unavailable and the system fails to receive the SMS delivery report during 45 seconds, it will attempt to send the SMS text message to the next listed user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

b) By default, the system will continue sending the SMS text message to the next listed user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

3. By default, the system attempts to ring the first user phone number via GSM, sharing the same partition as the violated zone/tamper. The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the system will shut down the siren/bell and play the audio file that can be listened to on the user's mobile phone. This feature will be available only if an audio file is recorded and assigned to the violated zone (see **17.2. Audio Files**).

b) When the audio record has played, the user will be able to listen on the mobile phone for approx. 30 seconds to what is happening in the area, surrounding the alarm system. This feature will be available only if a microphone is connected to the system (see **25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION**).

c) The system will dial the next listed user phone number, assigned to the same partition, if the previous user was unavailable due to the following reasons:
- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided "busy" signal.
- user did not answer the call after several rings, predetermined by the GSM operator.

d) The system will continue dialing the next listed user phone numbers in the priority order until one is available. The system will dial the user phone number 5 times if the first user phone number was out of GSM signal coverage/switched OFF, otherwise the system will dial only once. If the system ends up with all unsuccessful attempts to contact any listed user phone number, will stop dialing and will not return to the first user phone number.

e) The system will not dial the next listed user phone number if the previous one was available, but rejected the phone call.

4. If enabled, the system attempts to ring the first phone number via PSTN (see **30.2.3. PSTN**). The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the system will automatically drop the call.

b) The system will dial the next listed phone number if the previous one was unavailable due to the following reasons:
- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided "busy" signal.
- user did not answer the call after several rings, predetermined by the GSM operator.

c) The system will continue dialing the next listed phone numbers in the priority order until one is available. The system will dial the phone number 5 times (by default) if the first phone number was unavailable. If the system ends up with all unsuccessful to contact any listed phone number, it will return to the first phone number.

To silent the siren/bell as well as to cease system phone calls and SMS text message sending to the user phone numbers, please disarm the system (see **12. ARMING AND DISARMING**).

ATTENTION: The wireless siren EWS2/EWS3 will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed (see **23.1. Zone Partition**).

View violated zones

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Menu path:
OK → uumm → OK → VIOLATED ZONES → OK → ZONE 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W

Please, refer to illuminated zone indicators ranging from 1 through 12 on the keypad. The flashing indicator SYSTEM stands for violated high-numbered zones (Z13-Z76). For more details on violated high-numbered zone indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View violated tampers

SMS

The system will automatically send an SMS text message, containing a violated tamper name, to user phone number.

EKB2

Menu path:
OK → uumm → OK → VIOLATED TAMPERS → OK → TAMPER 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W

The illuminated indicator SYSTEM stands for system fault presence including violated tamper. For more details on violated tamper indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

For more details details on how to disable/enable SMS text messages and phone calls to listed user phone number in case of alarm, please refer to **17.1. Enabling and Disabling Alarm Notifications**

ATTENTION: Phone calls via GSM network to the listed user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. MONITORING STATION**).

NOTE: If one or more zones/tampers are violated during the alarm, the system will attempt to send as many SMS text message and dial the user phone number as many times as the zone/tamper was violated. However, this does NOT apply to Interior Follower-type zones.

NOTE: If the system has delivered an SMS text message and/or dialed the user phone number after disarming the system, it means that the SMS text message and/or phone call was queued up in the memory before the system was disarmed. The capacity of the queue is 24 events maximum.

NOTE: In some case, the system might be UNABLE to dial the next listed user phone number in case the phone number has been migrated from a different GSM operator.

17.1. Enabling and Disabling Alarm Notifications

By, default the system will ring the listed user phone numbers via GSM in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable call in case of alarm

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 30, user phone number slot & parameter status value:
30 us 1 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *30081#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable call in case of alarm

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 30, user phone number slot & parameter status value:
30 us 0 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *30090#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By, default the system will send SMS text message to listed user phone numbers in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable SMS text message in case of alarm

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → GENERAL ALARM → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → GENERAL ALARM → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 03 up 0 #
SMS text message to all users simultaneously: 21 03 up 0 #
SMS delivery report: 55 03 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2503060#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable SMS text message in case of alarm

EKB2

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → GENERAL ALARM → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → GENERAL ALARM → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 03 up 1 #
SMS text message to all users simultaneously: 21 03 up 1 #
SMS delivery report: 55 03 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2503101#*

Config Tool — This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By, default the system will not ring the listed phone number via PSTN in case of alarm. To manage this feature, please refer to **30.2.3. PSTN)**

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

By default, tamper alarm notification by SMS text message is enabled. For more details on how to disable/enable tamper alarm notification, please refer to **16. TAMPERS**.

ATTENTION: Regardless of the Call in Case of Alarm parameter status, the system will NOT ring the listed user phone number via GSM network if the system is connected to the monitoring station (see **30. MONITORING STATION**).

17.2. Audio Files

The system comes equipped with a feature allowing to record up to 16 audio files of up to 6 seconds length using the microphone of the PC. The recorded file can be assigned to any system zone, except virtual zone, and be played when the alarm is caused by zone with an audio file assigned. This feature will be available only if the system is able to dial user phone number in the event of an alarm and the user answers the call. The supported audio file format is as follows:

- Max. number of audio files: up to 16
- Max. audio length: up to 6 seconds
- File format: .wav
- Specifications: 8,000 kHz; 8 Bit; Mono

Record and manage audio files — Config Tool — This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Assign audio file to individual zone — Config Tool — This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Single audio file can be assigned to multiple zones.

18. PROGRAMMABLE (PGM) OUTPUTS

A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system, the scheduled weekday and time has come or if the user has initiated the PGM output state change manually. Normally, PGM outputs can be used to open/close garage doors, activate lights, heating, watering and much more. When a PGM output turns ON, the system triggers any device or relay connected to it.

ESIM364 comes equipped with four open-collector PGM outputs allowing to connect up to four devices or relays. For more details on PGM output expanding, please refer to **18.2. PGM Output Expansion**.

ESIM364 PGM outputs are classified by 4 categories:

PGM output category	Description	Max. number of PGM outputs per device	Max. number of PGM outputs in total
On-board PGM Outputs	Built-in wired PGM outputs of ESIM364 alarm system.	4	4
EPGM8 PGM Outputs	PGM outputs of EPGM8 - hardwired PGM output expansion module.	8	8
EPGM1 PGM Outputs	PGM outputs of EPGM1 - hardwired zone & PGM output expansion module.	2	4
Wireless PGM Outputs	Non-physical PGM outputs automatically created by connected wireless devices.	2*	64**

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

For PGM output wiring diagram, please refer to **2.3.6. Relay Finder® 40.61.9.12 with Terminal Socket 95.85.3**.

18.1. PGM Output Numbering

The PGM output numbers ranging from C1 through C12 are permanently reserved for on-board PGM outputs even if EPGM8 module mode is disabled. The C13-C76 PGM output number are automatically assigned in the chronological order to the devices connected to the system: EPGM1 modules and wireless devices.

18.2. PGM Output Expansion

For additional electrical appliance connection, the number of PGM outputs can be expanded by:

- connecting EPGM8 hardwired PGM output expansion module. (for more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download).
- connecting EPGM1 hardwired zone and PGM output expansion module (for more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download).
- pairing the wireless devices (see **19. WIRELESS DEVICES**).

The maximum supported PGM output number is 76.

18.2.1. EPGM8 Mode

EPGM8 is an expansion module, which expands the system with 8 additional hardwired PGM outputs. For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

Once the EPGM8 module is installed, the EPGM8 mode must be enabled.

Enable EPGM8 mode

EKB2

Menu path:
OK → iiii → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 33 & parameter status value:
33 1 #
Example: *331#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EPGM8 mode

EKB2

Menu path:
OK → iiii → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 33 & parameter status value:
33 0 #
Example: *330#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

18.3. PGM Output Names

Each PGM output has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined PGM output, for **Example:** Lights. The name can be used instead of PGM output number when controlling the PGM output by SMS text message. By default, the PGM output names are: *C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.*

Set PGM output name

SMS

SMS text message content:
ssss_Coo:out-name
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_C2:Lights*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View PGM output names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS*

EKB2

Menu path:
On-board PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → NAME
Wireless PGM output: ... → WIRELESS OUTPUTS 1... 4 → OK → WIRELESS OUTPUT 13... 76 → OK → NAME
Value: *mmmm* – 4-digit master code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Space, colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in PGM output names.

18.4. Turning PGM Outputs ON and OFF

By default, all PGM outputs are turned OFF. To instantly turn ON/OFF an individual PGM output and set its state to ON/OFF when the system starts-up, please refer to the following configuration methods.

Turn ON PGM output/ Set PGM output start-up state as ON

SMS

SMS text message content:
ssss_Coo:ON or ssss_out-name:ON
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_Lights:ON*

EKB2

Menu path:
On-board PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → ENABLE → OK
Wireless PGM output: ... → WIRELESS OUTPUTS 1... 4 → OK → WIRELESS OUTPUT 13... 76 → OK → STATUS → OK → ENABLE → OK
Value: *mmmm* - 4-digit master code.

EKB3/ EKB3W

Enter parameter 61, PGM output number & parameter status value:
61 oo 1 #
Value: *oo* - PGM output number, range - [01... 76].
Example: *61031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EWK1/ EWK2/ EWK2A

This operation may be carried out from the wireless keyfob if pre-configured using the PC running *ELDES Configuration Tool* software.

Turn OFF PGM output/ Set PGM output start-up state as OFF

SMS

SMS text message content:
ssss_Coo:OFF or ssss_out-name:OFF
Value: *ssss* - 4-digit SMS password; *oo* - PGM output number, range - [1... 76]; *out-name* - up to 16 characters PGM output name.
Example: *1111_C2:OFF*

EKB2

Menu path:
On-board PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → DISABLE → OK
Wireless PGM output: ... → WIRELESS OUTPUTS 1... 4 → OK → WIRELESS OUTPUT 13... 76 → OK → STATUS → OK → DISABLE → OK
Value: *mmmm* - 4-digit master code.

EKB3/ EKB3W

Enter parameter 61, PGM output number & parameter status value:
61 oo 0 #
Value: *oo* - PGM output number, range - [01... 76].
Example: *61020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EWK1/ EWK2/ EWK2A

This operation may be carried out from the wireless keyfob if pre-configured using the PC running *ELDES Configuration Tool* software.

To instantly turn ON an individual PGM output for a determined time period and automatically turn it OFF when the time period expires, please refer to the following configuration method.

Turn ON PGM output for time period

SMS

SMS text message content:
ssss_Coo:ON:hr.mm.sc or ssss_out-name:ON:hr.mn.sc
Value: *ssss* - 4-digit SMS password; *oo* - PGM output number, range - [1... 76]; *out-name* - up to 16 characters PGM output name; *hr* - hours, range - [00... 23]; *mn* - minutes, range - [00... 59]; *sc* - seconds, range - [00... 59].
Example: *1111_C4:ON:10.15.35*

To instantly turn OFF an individual PGM output for a determined time period and automatically turn it ON when the time period expires, please refer to the following configuration method.

Turn OFF PGM output for time period

SMS

SMS text message content:
ssss_Coo:OFF:00.00.sc or ssss_out-name:OFF:hr.mn.sc
Value: *ssss* – 4-digit SMS password;*oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *sc* – seconds, range – [00... 59].
Example: *1111_Lights:OFF:00.00.23*

When the PGM output is turned ON or OFF, the system will send a confirmation by SMS text message to the user phone number that the SMS text message was sent from.

NOTE: PGM output can be turned ON for a determined time period only when it is in OFF state

NOTE: PGM output can be turned OFF for a determined time period only when it is in ON state

NOTE: Multiple PGM outputs can be turned ON/OFF by a single SMS text message, **Example:** *1111_C1:ON C2:OFF Pump:ON C4:ON:00.20.25*

18.5. PGM Output Control by Event and Scheduler

The PGM outputs can automatically operate when a specific event occurs in the system and/or when the scheduled weekday and time comes.

PGM Output Actions

The automatic action of the determined PGM output can be set as follows:

- **Turn ON** – Determines whether the PGM output is to be turned ON.
- **Turn OFF** – Determines whether the PGM output is to be turned OFF.
- **Pulse** – Determines whether the PGM output is to be turned ON or OFF for a set period of time in seconds based on the PGM output startup state set up.

System Events

The aforementioned PGM output action can be automatically carried out under the following events that have occurred in the system:

- **System armed** – System is armed in a determined partition ranging from Partition 1 through 4 or any partition.
- **System disarmed** – System is disarmed in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm begins** – Alarm begins in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm stops** – Alarm stops in a determined partition ranging from Partition 1 through 4 or any partition.
- **Temperature falls** – Temperature falls below the set MIN value of a determined temperature sensor 1-8.
- **Temperature rises** – Temperature rises above the set MAX value of a determined temperature sensor 1-8.
- **Zone violated** – A determined zone ranging from Z1 through Z76 is violated.
- **Zone restored** – A determined zone ranging from Z1 through Z76 is restored.
- **Scheduler starts** – Operates based on Start Time of a selected scheduler 1-16.
- **Scheduler ends** – Operates based on End Time of a selected scheduler 1-16.

The user can also set a custom text, which will be sent by SMS text message to user phone number when the automatic PGM output action is carried out.

Schedulers

The system supports up to 16 schedulers that allow the PGM outputs to operate according to the day of the week and time. When the scheduler, which includes the set weekday and time, is selected, the PGM output will operate according to it. Each scheduler includes the following parameters:

- **Always** – The scheduler is not in use.
- **At specified time** – Determines whether weekday and time settings are enabled:
  - **Start Time** – Determines the point in time when the PGM output action can be initiated for Scheduler starts event.
  - **End Time** – Determines the point in time when the PGM output action can be initiated for Scheduler ends event
  - **On weekdays** – Determines days in week when the PGM output action is valid.

Additional Conditions

Additional condition narrows down the chances for a determined automatic PGM output operation to be carried out. If this feature is en-

abled, the PGM output will become dependent on one more system event that must be occurred prior or must occur after the aforementioned system event. The PGM output will not operate until the chain of system events meets the set values:

- **System armed** - System is armed in a determined partition ranging from 1 to 4 or any partition.
- **System disarmed** - System is disarmed in a determined partition ranging from 1 to 4 or any partition.
- **Zone violated** - A determined zone ranging from Z1 to 76 is violated.
- **Zone restored** - A determined zone ranging from Z1 to Z76 is restored.

Example: *PGM output C1 is set to be turned ON when zone Z6 is violated. The additional condition feature is enabled and set to allow this action to be carried out only if system's Partition 2 is disarmed. It means that the PGM output C1 will be turned ON when zone Z6 is violated, but only if system's Partition 2 is disarmed.*

Manage PGM output control by event & scheduler

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: If the date and time are not set, the system will NOT be able to automatically control the PGM outputs. For more details on how to set date and time, please refer to **9. DATE AND TIME**.

NOTE: When both - a system event is determined and a scheduler is selected, the PGM output will operate only if the determined event has occurred in the system during the scheduled time period.

NOTE: When PGM output action is selected as pulse, the PGM output will turn ON or turn OFF for a set period of time based on the PGM output state set up (ON or OFF) for system startup.

18.6. Wireless PGM Output Type Definitions

- **Output** - Operates as normal PGM output that can be controlled by the user or automatically by event and scheduler. Normally, this type is used for any device or relay.
- **Siren** - Operates as siren output that automatically activates during alarm. Typically, this type is used for bell/siren connected to EW2 wireless device.

Set output type for individual wireless PGM output

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19. WIRELESS DEVICES

ESIM364 system has a built-in wireless module for system extension capabilities. The wireless module easily allows the user to pair up to 32 ELDES-made wireless devices with the system. This includes the following:

- EWP2 – wireless PIR sensor (motion detector).
- EWD2 - wireless magnetic door contact/shock sensor/flood sensor.
- EWS3 – wireless indoor siren..
- EWS2 – wireless outdoor siren.
- EWK1 and EWK2/EWK2A – wireless keyfob.
- EKB3W – wireless keypad.
- EW2 – wireless zone and PGM output expansion module.
- EWF1/EWF1CO - wireless smoke/CO detector.
- EWR2 - wireless signal repeater.

For more details on technical specifications and installation of the wireless devices, please refer to **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual and the latest user manual of the wireless device located at www.eldes.lt/download

The wireless devices can operate at a range of up to 30m (98.43ft) from the alarm system unit while inside the building and at up to 150m (492.13ft) range in open areas. The wireless connection is two-way and operates in one of four available channels in ISM868 (EU version) / ISM915 (US version) non-licensed band.

The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period, known as Test Time. When the wireless device is switched ON, it will initiate the Test Time transmission to the system within its wireless connection range. In order to optimize battery power saving of the wireless device, the Test Time periods vary by itself while the device is switched ON, but still unpaired. When the alarm system is switched OFF or if the wireless device is unpaired or removed the Test Time period of the wireless device is as follows (non-customizable):

- EKB3W, EW2, EWP2, EWS2, EWS3, EWF1/EWF1CO:
  - First 360 attempts after the device startup (reset) - every 10 seconds.
  - The rest of attempts - every 1 minute.
- EWD2:
  - First 360 attempts after the device startup (reset) - every 10 seconds.
  - The rest of attempts - every 2 minutes.

Once the wireless device is paired, it will attempt to exchange data with ESIM364 system. Due to battery saving reasons, all ELDES wireless devices operate in sleep mode. The data exchange will occur instantly if the wireless device is triggered (zone alarm or tamper alarm) or periodically when the wireless device wakes up to transmit the supervision signal, based on Test Time value, to the system as well as to accept the queued up command (if any) from the system. By increasing the Test Time period, EWS2/EWS3 siren response time will decrease.
Example: *The alarm occurred at 09:15:25 and the system queued up the command for EWS3 siren to start sounding. By default, Test Time value of EWS3 siren is 7 seconds, therefore EWS2 siren will sound at 09:15:32.*

By default, the Test Time period is as follows (customizable):

- EKB3W: every 60 seconds.
- EW2, EWP2, EWF1/EWF1CO, EWD2: every 30 seconds.
- EWS2, EWS3: every 7 seconds.

To set a different Test Time value, please refer to the following configuration method.

Set custom Test Time

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Test Time affects the wireless device pairing process due to the alarm system listening for the incoming data from the wireless device. The system pairs with the wireless device only when the first data packet is received.

NOTE for EKB3W: In comparison with other ELDES wireless devices, EKB3W keypad features some exceptions regarding the wireless communication. For more details on EKB3W keypad wireless communication and back-light timeout, please refer to **19.5.3. Wireless Communication, Sleep Mode and Back-light Timeout.**

19.1. Pairing, Removing and Replacing Wireless Device

Wireless device management can be easily and conveniently carried out using the graphical interface of *ELDES Configuration Tool* software. If you intend to manage the wireless devices by SMS text massage, an 8-character wireless device ID code will be required in order to pair the device with the system or to remove it from the system. The wireless ID code is printed on a label, which can be located on the inner or outer side of the enclosure or on the printed circuit board (PCB) of the wireless device.

To pair a wireless device, please refer to the following configuration methods.

Pair wireless device with the system	**SMS**	**SMS text message content:** ssss_SET:wless-id **Value:** *ssss* – 4-digit SMS password; *wless-id* – 8-character wireless device ID code. **Example:** *1111_SET:535185D*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE FOR EWK1/EWK2/EWK2A: When pairng EWK1/EWK2/EWK2A wireless keyfob, it is necessary to press several times any button on the device.

Once a wireless device is paired, it occupies one of 32 available wireless device slots and the system adds single or multiple wireless zones and wireless PGM outputs depending on the wireless device model.

To remove a wireless device, please refer to the following configuration methods.

Remove wireless device from the system	**SMS**	**SMS text message content:** ssss_DEL:wless-id **Value:** *ssss* – 4-digit SMS password; *wless-id* – 8-character wireless device ID code. **Example:** *1111_DEL:535185D*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Once a wireless device is removed from the system, please restore its default parameters and remove the batteries from it.

To replace an existing wireless device with a new same model device, please refer to the following configuration method.

Replace wireless device	**SMS**	**SMS text message content:** ssss_REP:wless-id<oldwl-id **Value:** *ssss* – 4-digit SMS password; *wless-id* – 8-character wireless device ID code of the new device; *oldwl-id* – 8-character wireless device ID code of the old device. **Example:** *1111_REP:535185D<41286652*

When a wireless device is successfully replaced with a new one, the configuration of the old wireless device remains.

ATTENTION: In order to correctly remove the wireless device from the system, the user must remove the device using SMS text message or *ELDES Configuration Tool* software and restore the parameters of the wireless device to default afterwards. If only one of these actions is carried out, the wireless device and the system will attempt to exchange data to keep the wireless connection alive. This leads to fast battery power drain on the battery-powered wireless device.

NOTE: If you are unable to pair a wireless device, please restore the wireless device's parameters to default and try again. For more details on how to restore the default parameters, please refer to the user manual provided along with the wireless device or visit www.eldes.lt/download to download the latest user manual.

19.2. Wireless Device Information

Once a wireless device is paired, the user can view the following information of a determined wireless device:

- Battery level (expressed in percentage).
- Wireless signal strength (expressed in percentage).
- Error rate (number of failed data transmission attempts in 10-minute period) - indicated only in EKB2 keypad menu.
- Firmware version.
- Test Time period (expressed in milliseconds) of a wireless device - indicated only in SMS text message reply.

To view the wireless device information, please refer to the following configuration methods.

View wireless device information

SMS

SMS text message content:
ssss_RFINFO:wless-id or ssss_RFINFO:Znn
Value: *wless-id* – 8-character wireless device ID code; *nn* – wireless zone number, range – [13... 76].
Example: *1111_RFINFO:535185D*

EKB2

Menu path:
Battery level: OK → iiii → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → BATTERY
Wireless signal: ... → wless-dev wless-id → OK → SIGNAL
Error rate: ... → wless-dev wless-id → OK → ERROR RATE
Firmware version: ... → wless-dev wless-id → OK → FW RELEASE
Value: *iiii* – 4-digit installer code; *wless-dev* – wireless device model; *wless-id* – 8-character wireless device ID code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The system supports up to 32 wireless devices. To view the number of unoccupied wireless device slots in the system, please refer to the following configuration methods

View unoccupied wireless device slots

SMS

SMS text message content:
ssss_STATUS_FREE
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS_FREE*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19.3. Wireless Signal Status Monitoring

If the wireless signal is lost due to poor signal strength or low battery power on a certain wireless device and does not restore within 1-hour period (by default; customizable), the system will cause an alarm. This event is identified as Wireless Signal Loss. By default, indicated as *No wireless signal from wless-dev wless-id Tamper x* in the SMS text message (*wless-dev* = wireless device model; *wless-id* = 8-character wireless device ID code; *x* = tamper number). The user will also be notified by SMS text message as soon as the wireless signal is restored.

The default 1-hour period for wireless signal loss detection is a EN 50131-1 Grade 2 requirement. However, a custom wireless signal loss timeout can be set up that must be at least 3 times longer than the longest Test Time period of a wireless device currently paired with the system. In addition, *ELDES Configuration Tool* software indicates a timer of the last Test Time signal delivered by a paired and unpaired wireless device. The software will also warn you if the delivery of the Test Time signal is delayed for a time period 3 times longer than the Test Time period of a paired wireless device. In case the Test Time signal delivery of an unpaired wireless device is delayed for more than 1,5 minute, a warning will follow and the icon of such wireless device will be removed from the software's interface in 10 seconds.

To set a custom wireless signal loss timeout and manage the wireless signal loss/restore notifications, please refer to the following configuration method.

Set custom wireless signal loss timeout

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable wireless signal loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → DISABLE → OK
Value: iiii - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 18 up 0 #
SMS text message to all users simultaneously: 21 18 up 0 #
SMS delivery report: 55 18 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2518030#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable wireless signal loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 18 up 1 #
SMS text message to all users simultaneously: 21 18 up 1 #
SMS delivery report: 55 18 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2518031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Once a certain tamper is disabled, the system will NOT deliver any SMS text message regarding the physical tamper violation nor wireless signal loss or restore. For more details on how to manage the tampers, please refer to **16. TAMPERS**.

ATTENTION: The system will NOT deliver any text message regarding wireless signal loss or restore while the physical tamper violation is in progress.

19.4. Disabling and Enabling Siren if Wireless Signal is Lost

If a wireless device loses its wireless signal for 1 hour (by default) or longer, the system will send notification by SMS text message to user phone number and activate the siren/bell. By default, the siren will not be activated when wireless signal is lost. To enable/disable this feature, please refer to the following configuration methods.

Enable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 76 & parameter status value:
76 1 #
Example: *761#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 76 & parameter status value:
76 0 #
Example: *760#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19.5. EKB3W - Wireless LED Keypad

Main features:

- Alarm system arming and disarming (see **12.5. EKB3W Keypad and User/Master Code**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- Visual indication by LED indicators (see **19.5.1. LED Functionality**).
- Audio indication by built-in buzzer.
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

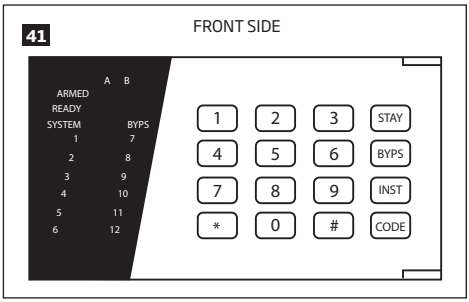
For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

19.5.1. LED Functionality

ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready – no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zone (-s)
BYPS	Steady ON - zone bypass mode
1-12	Steady ON - violated zone Z1-Z12

19.5.2. Keys Functionality

[BYPS]	Bypass violated zone
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[1]... [2]	Keypad partition switch
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/ deactivation command



19.5.3. Wireless Communication, Sleep Mode and Back-light Timeout

Once the wireless device is paired, it will attempt to exchange data with ESIM364 system. The communication process follows this pattern:

1. Due to battery power saving reasons, most of the time EKB3W keypad operates in sleep mode and periodically wakes up (by default - every 60 seconds) to transmit the supervision signal, identified as Test Time, to the ESIM364 system. However, when the keypad wakes up, it will NOT activate its buzzer and/or the LED indicators.
2. When any EKB3W key is pressed, the keypad LED indicators and the back-light will activate for a set up period of time (by default - 10 seconds), identified as Back-light Timeout. During the Back-light Timeout, the Test Time will automatically switch to 2 seconds period allowing to indicate system alarms, faults and arm/disarm process on the EKB3W keypad if it is assigned to the same partition as the one that is violated or being armed/disarmed (see **23. PARTITIONS)**.
3. The Back-light timeout will expire after 10 seconds (by default) of EKB3W idling. When the Back-light Timeout expires, the keypad will light OFF the LED indicators and the back-light and return to sleep mode. Meanwhile:

   a) if a zone or tamper, which is of the associated EKB3W keypad, is violated, EKB3W will instantly wake up and initiate the Back-light Timeout. Meanwhile the keypad buzzer will emit short beeps and the LED indicators will light ON indicating the violated zone or tamper number.

   b) if a zone or tamper, which is not of the associated EKB3W keypad, is violated, EKB3W keypad will NOT wake up and will NOT initiate the Back-light Timeout as well as the buzzer will NOT emit short beeps and the LED indicators will NOT light ON.

To set a different Back-light Timeout value, please refer to the following configuration method:

Set Back-light Timeout → **Config Tool** This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details and how to set a different Test Time value, please refer to *ELDES Configuration Tool* software.

NOTE: By default, the keypad zone and tamper is enabled, therefore a resistor supplied with the EKB3W keypad must be connected to the keypad zone terminal and the tamper switch must be properly pressed in when inserting the keypad into the holder. By disabling the keypad zone, the keypad tamper will disable as well (see **14.9. Enabling and Disabling Zones** and **16. TAMPERS**).

NOTE: To wake up the keypad it is highly recommended to press the [*] key in order not to enter any unnecessary character.

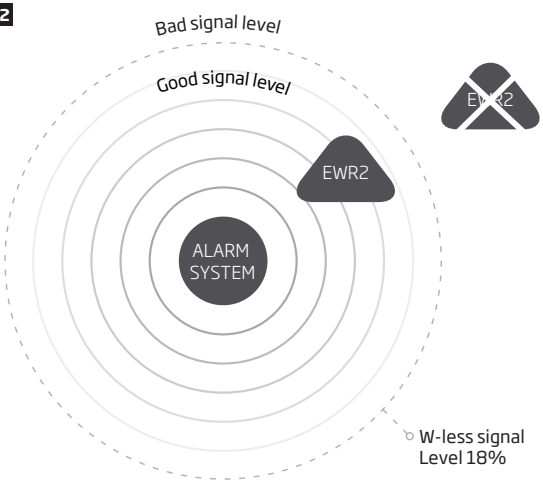
19.6. EWR2 - Wireless Signal Repeater

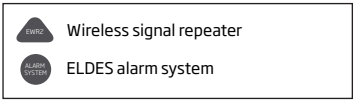
Main features:

- Expands the wireless signal range (up to 30m (98.43ft) in premises; up to 150m (492.13ft) in open areas)
- LED indicator for data transmission indication.
- External and internal antenna.
- Backup battery

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

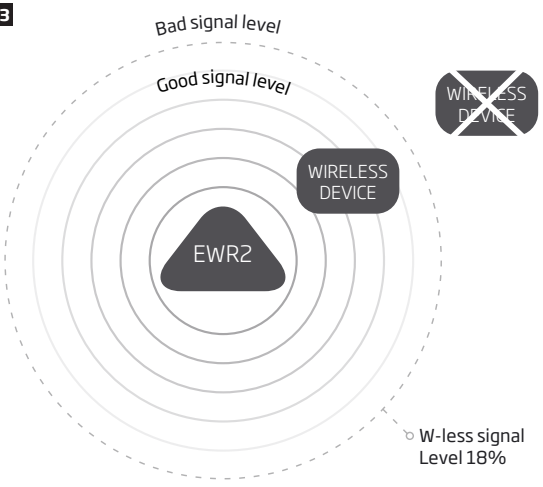
42

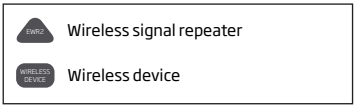




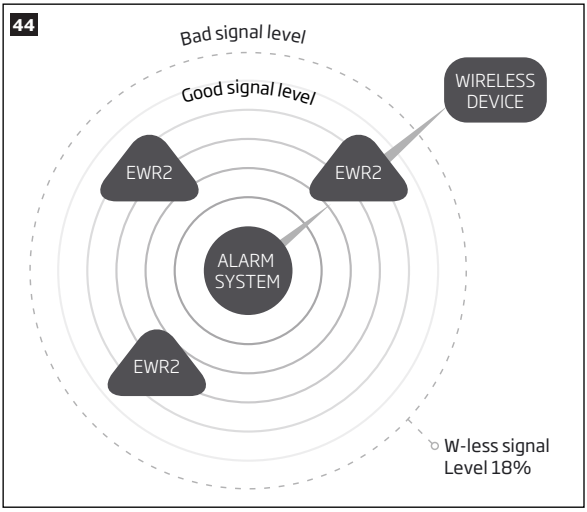
EWR2 begins expanding the signal range for wireless devices if the certain conditions are met. In order for EWR2 to function properly, the wireless signal level between EWR2 and ELDES alarm system must be at least 18%.

43





In order for EWR2 to start expanding the signal range of a wireless device, the wireless signal level between EWR2 and a wireless device must be at least 18%.



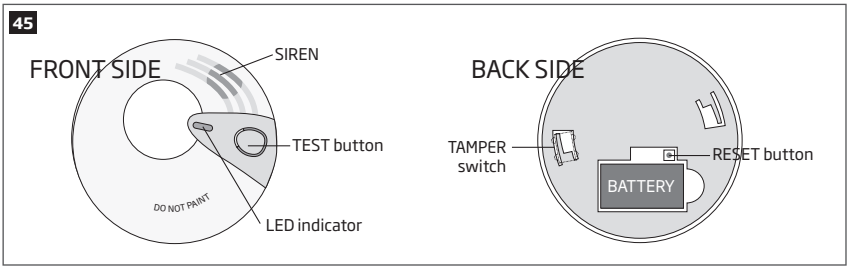
If more then one repeater is connected to Eldes alarm system at a time, the one that recieves the strongest signal from a wireless device, will be used to expand it's signal range.

19.7. EWF1/EWF1CO - Wireless Smoke/CO Detector

Main features:

- Photoelectric sensor for slow smouldering fires
- TEST button
- Non-radioactive technology for environmental friendly
- High and stable sensitivity
- Quick fix mounting plate for easy installation
- LED operation indicator
- Built-in speaker for audio alarm indication
- Auto-reset when smoke/CO clears

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download



19.7.1. Interconnection

The interconnection feature automatically links all wireless smoke/CO detectors that are paired with the alarm system. When any EWF1/EWF1CO detects smoke or carbon monoxide (CO), it will sound the built-in siren and send the signal to the alarm system resulting in an instant alarm followed by built-in siren sound caused by the rest of EWF1/EWF1CO wireless smoke/CO detectors. EWF1/EWF1CO device that detected smoke/CO will auto-reset when the smoke/CO clears, while the rest of EWF1/EWF1CO smoke/CO detectors will continue to sound in accordance with the set time period (by default - 30 seconds).

By default, the interconnection feature is enabled and the siren alarm duration is 30 seconds. To manage these parameters, please refer to the following configuraiton methods.

Disable interconnection

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 50 & parameter status value:
50 0 #
Example: *500#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable interconnection

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
50 1 #
Example: *501#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set EWF1/EWF1CO siren alarm duration

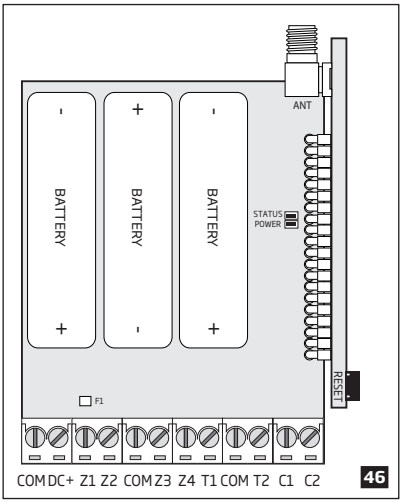
Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The maximum supported EWF1/EWF1CO siren alarm duration is 255 seconds (4 mins. 15 secs.) even if the system's alarm duration value is longer.

NOTE: System's alarm duration has a higher priority against the EWF1/EWF1CO siren alarm duration, therefore EWF1/EWF1CO will sound as long as the system's alarm duration set up, unless the set up value for EWF1/EWF1CO siren alarm duration is shorter.

19.8. EW2 - Wireless Zone and PGM Output Expansion Module



Main features:

- 4 zone terminals.
- 2 open-collector outputs.
- Battery or externally-powered.
- Compatible with any third-party wired sensor or siren.

EW2 is a wireless device intended to expand ELDES alarm system capabilities by providing wireless connection access to any third-party wired devices. EW2 comes equipped with 4 zone terminals designed for wired digital sensor connection, such as magnetic door contact, motion detector etc. In addition, the 2 open-collector outputs on board allow to connect any wired siren as well as to connect and control any electrical appliance, such as gates, lights, watering etc. The device can operate by powering it either using an external power supply or 3 x 1,5V AA type alkaline batteries on board. Once the external power supply is disconnected, EW2 will automatically switch to battery power.

The maximum number of EW2 devices that can be paired with the system depends on the number of the existing zones in system's configuration. In case no keypad zones, no EPGM1 zones, no virtual zones and no other wireless zones exist, the system will support up to 16 EW2 devices.

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/ download

20. WIRED SIREN/BELL

When the system is in alarm state, the siren/bell will sound until the set time (by default - 1 minute) expires or until the system is disarmed. To set the alarm duration, please refer to the following configuration methods.

Set alarm duration

SMS

SMS text message content:
ssss_SIREN:t
Value: *ssss* - 4-digit SMS password; *t* - alarm duration, range - [0... 5] minutes.
Example: *1111_SIREN:4*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION → OK → tt → OK
Value: *iiii* - 4-digit installer code; *tt* - alarm duration, range - [1... 10] minutes.

EKB3/ EKB3W

Enter parameter 10 & alarm duration:
10 tt #
Value: *tt* - alarm duration, range - [00... 10] minutes.
Example: *1007#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View alarm duration

SMS

SMS text message content:
ssss_SIREN
Value: *ssss* - 4-digit SMS password
Example: *1111_SIREN*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For siren/bell wiring diagram, please refer to **2.3.3. Siren**.

NOTE: The maximum supported alarm duration is 127 minutes that can be set up using *ELDES Configuration Tool* software only. 0 value disables the siren/bell.

NOTE: Due to battery power saving reasons, the wireless siren will sound for up to 6 minutes max. regardless of the set up alarm duration value when it is longer than 6 minutes

20.1. BELL Output Status Monitoring

The system constantly supervises the BELL output. If the siren/bell is disconnected/cut-off, the system may send the notification by SMS text message (by default- disabled) to the listed user phone number and indicate system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**). Once the bell/siren is connected/fixed, the system may notify the listed user by SMS text message (by default - disabled) and the keypad will no longer indicate system fault. Please, note that in order to use this feature, the resistors must be connected to BELL output (see **2.3.3. Siren**).

By default, the notification by SMS text message regarding the BELL output status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable Siren Fail/ Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → ENABLE → OK
MS delivery report: ... → SIREN FAIL/REST EV → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 08 up 1 #
SMS text message to all users simultaneously: 21 08 up 1 #
SMS delivery report: 55 08 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2508021#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Siren Fail/ Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → SIREN FAIL/REST EV → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 08 up 0 #
SMS text message to all users simultaneously: 21 08 up 0 #
SMS delivery report: 55 08 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2508040#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

20.2. Bell Squawk

If enabled, the siren/bell indicates the completed system arming and disarming process. After the system is successfully armed, the siren/bell will emit 2 short beeps and 1 long beep after the system is disarmed. To enable/disable the Bell Squawk feature, please refer to the following configuration methods.

Enable Bell Squawk

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

	EKB3/ EKB3W	**Enter parameter 29 & parameter status value:** 291 # **Example:** *291#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.
Disable Bell Squawk	EKB2	**Menu path:** OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → DISABLE → OK **Value:** *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 29 & parameter statusvalue:** 290 # **Example:** *290#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.3. Bell Squawk in Stay Mode

If enabled, the Bell Squawk will be available when arming/disarming the system in Stay mode (see **15. STAY MODE**). To enable/disable this feature, please refer to the following configuration methods

Enable Bell Squawk in Stay Mode	EKB2	**Menu path:** OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK STAY → OK → ENABLE → OK **Value:** *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 95 & parameter status value:** 951 # **Value:** *951#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool software.*
Disable Bell Squawk in Stay Mode	EKB2	**Menu path:** OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK STAY → OK → DISABLE → OK **Value:** *iiii* - 4-digit installer code.
	EKB3/ EKB3W	**Enter parameter 95 & parameter status value:** 950 # **Value:** *950#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

20.4. Indication by EWS2 - Wireless Outdoor Siren Indicators

When enabled, the built-in LED indicators of EWS2 wireless outdoor siren will flash during the alarm. To enable/disable this feature, please refer to the following configuration methods.

Enable EWS2 LED indication

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
881 #
Example: *881#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EWS2 LED indication

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
880 #
Example: *880#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.5. Indication by EWS3 - Wireless Indoor Siren Indicators

When enabled, the built-in LED indicators of EWS3 wireless indoor siren will flash during the alarm. In the event of burglary, 24-hour or tamper alarm, EWS3 will flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator. To enable/ disable these features, please refer to the following configuration methods.

Enable EWS3 LED indication

EKB2

Menu path:
Burglary/24-hour/tamper alarm LED: OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWS3 ALARM LED → OK → ENABLE → OK
Fire alarm ... → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 94/93 & parameter status value:
Burglary/24-hour/tamper alarm LED: 941 #
Fire alarm LED: 931 #
Example: *931#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

Disable EWS3 LED indication

EKB2

Menu path:
Burglary/24-hour/tamper alarm LED: OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWS3 ALARM → OK → DISABLE → OK
Fire alarm LED: ... → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 94/93 & parameter status value:
Burglary/24-hour/tamper alarm LED: 940 #
Fire alarm LED: 930 #
Example: *940#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

21. BACKUP BATTERY, MAINS POWER STATUS MONITORING AND MEMORY

21.1. Backup Battery Status Monitoring

The system may comes equipped with a backup battery maintaining power supply of the system when the mains power is temporally lost. The implemented feature allows the system to perform a self-test on the backup battery and notify the user by SMS text message as well as to indicate system fault by the keypad (see **29. INDICATION OF SYSTEM FAULTS**) if:

- battery has failed and requires replacement - battery resistance is 2Ω or higher; self-tested every 24 hours.
- battery is dead or missing - battery is not present or battery voltage is below 5V; self-tested every 1 minute.
- battery power is running low - battery voltage is 10.5V or lower; constantly self-tested.

By default, all notifications regarding the backup battery status are enabled. To disable/enable a determined backup battery notification, please refer to the following configuration methods.

Disable Battery Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → BATTERY FAILED → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → BATTERY FAILED → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 05 up 0 #
SMS text message to all users simultaneously: 21 05 up 0 #
SMS delivery report: 55 05 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2105010#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Battery Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → BATTERY FAILED → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → BATTERY FAILED → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 05 up 1 #
SMS text message to all users simultaneously: 21 05 up 1 #
SMS delivery report: 55 05 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2505031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Battery Dead or Missing notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → BATTERY DEAD/MISS → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 06 up 0 #
SMS text message to all users simultaneously: 21 06 up 0 #
SMS delivery report: 55 06 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *5506070#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Battery Dead or Missing notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → BATTERY DEAD/MISS → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 06 up 1 #
SMS text message to all users simultaneously: 21 06 up 1 #
SMS delivery report: 55 06 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *5506101#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Low Battery notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → LOW BATTERY → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → LOW BATTERY → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 07 up 0 #
SMS text message to all users simultaneously: 21 07 up 0 #
SMS delivery report: 55 07 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2107100#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Low Battery notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → LOW BATTERY → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → LOW BATTERY → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 07 up 1 #
SMS text message to all users simultaneously: 21 07 up 1 #
SMS delivery report: 55 07 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2107021#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text massage transmission, please refer to **27. SYSTEM NOTIFICATIONS**.

NOTE: In order to view the backup battery voltage, resistance,, please refer to Diagnostic Management feature available on *ELDES Configuration Tool* software.

21.2. Mains Power Status Monitoring

If the household electricity is unstable in the system installation area, the system may temporally lose its power supply and continue operating on the backup battery power. The system supervises the mains power and notifies the user by SMS text message as well as indicates system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**) when the mains power is lost. When the mains power restores, the system will notify the user by SMS text message and the keypad will no longer indicate system fault.

By default, system notification by SMS text message regarding mains power status is enabled. To disable/enable this notification, please refer to the following configuration methods.

Disable mains power loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → GSM USER 1... 10 → OK → DISBLE → OK
SMS text message to all users simultaneously: ... → MAIN POWER L/R → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → MAIN POWER L/R → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 04 us 0 #
SMS text message to all users simultaneously: 21 04 us 0 #
SMS delivery report: 55 04 us 0 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *2504050#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable mains power loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → MAIN POWER L/R → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → MAIN POWER L/R → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 04 up 1 #
SMS text message to all users simultaneously: 21 04 up 1 #
SMS delivery report: 55 04 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2514091#*

Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, mains power loss and restore delay are 30 and 120 seconds respectively. To set a different mains power loss and restore delay duration, please refer to the following configuration methods.

Set mains power loss delay

EKB2	**Menu path:** OK → iii → OK → PRIMARY SETT INGS → OK → MAIN POWER STATUS → OK → LOSS DELAY → OK → IIIII → OK **Value:** *iiii* – 4-digit installer code; *IIIII* – mains power loss delay duration, range - [0... 65535] seconds.
EKB3/ EKB3W	**Enter parameter 70 & loss delay duration:** 70 IIIII # **Value:** *IIIII* – mains power loss delay duration, range - [0... 65535] seconds. **Example:** *7043#*
Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set mains power restore delay

EKB2	**Menu path:** OK → iiii → OK → PRIMARY SETT INGS → OK → MAIN POWER STATUS → OK → RESTORE DELAY → OK → rrrrr → OK **Value:** *iiii* – 4-digit installer code; *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds.
EKB3/ EKB3W	**Enter parameter 71 & restore delay duration:** 71 rrrrr # **Value:** *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds. **Example:** *71150#*
Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

NOTE: In order to view mains power status and value, please refer to Diagnostic Management feature available on *ELDES Configuration Tool* software.

21.3. Memory

The configuration settings and event log records are stored in a built-in EEPROM memory, therefore even if the system is fully shut down, the configuration and event log remain. For more details regarding the event log, please refer to **28. EVENT AND ALARM LOG**.

22. GSM CONNECTION AND ANTENNA STATUS MONITORING

22.1. GSM Connection Status Monitoring

The system supervises the GSM connection every 10 minutes. When the GSM connection loss is detected, the system indicator NETW will light OFF and the system will attempt to restore the GSM connection. In case the system fails to restore the GSM connection within a 3-minute period (by default), the keypad will indicate the system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) and the system will continue the attempt to restore the GSM connection. In addition, the system may notify the listed user by SMS text message (by default - disabled) and turn ON a determined PGM output to indicate the GSM connection loss fault (by default - disabled)..

Once the GSM signal restores, the system may notify the listed user by SMS text message (by default - disabled), the keypad will no longer indicate system fault and the determined PGM output will turn OFF (if set up).

By default, the notifications by SMS text message regarding GSM signal loss is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable GSM Connection Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → GSM CONNECT FAILED → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → GSM CONNECT FAILED → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 11 up 1 #
SMS text message to all users simultaneously: 21 11 up 1 #
SMS delivery report: 55 11 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *21114091#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable GSM Connection Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → GSM CONNECT FAILED → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 11 up 0 #
SMS text message to all users simultaneously: 21 11 up 0 #
SMS delivery report: 55 11 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *21114020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, the PGM output for GSM signal loss indication is not set. To set the PGM output and delay duration for GSM signal loss indication, please refer to the following configuration method.

Manage GSM signal loss indication by PGM output

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text massage transmission, please refer to **27. SYSTEM NOTIFICATIONS**.

22.2. GSM Antenna Status Monitoring

The system constantly monitors the GSM/GPRS antenna status. If the GSM/GPRS antenna is disconnected/cut-off, the system may send notification by SMS text message (by default - disabled) to the listed user and the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**). Once the antenna is connected/fixed, the system may notify the user by SMS text message (by default - disabled) and the keypad will no longer indicate system fault.

By default, the notification by SMS text message regarding the GSM/GPRS antenna status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: ... → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: ... → GSM ANT FAIL/REST → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 12 us 1 #
SMS text message to all users simultaneously: 21 11 us 1 #
SMS delivery report: 55 11 us 1 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *2512031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: ... → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: ... → GSM ANT FAIL/REST → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 12 us 0 #
SMS text message to all users simultaneously: 21 11 us 0 #
SMS delivery report: 55 11 us 0 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *2512030#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

23. PARTITIONS

ESIM364 system comes equipped with a partitioning feature that can divide the alarm system into four independently controlled areas identified as Partition 1 through 4, which are all supervised by one alarm system unit. Partitioning can be used in installations where shared alarm system is more practical, such as a house and a garage or within a single multi-storey building. When partitioned, each system element, like zone, user phone number, keypad, user/master code, iButton key and wireless keyfob can be assigned to single or multiple partitions. The user will then be able to arm/disarm the system partition (-s) that the zones and arm/disarm method, except EKB2 keypad, are assigned to.

The following table reflects the values used for system element assignment to partitions by EKB2/EKB3/EKB3W keypad. A sum of values is used to assign the element to multiple partitions.

Partition	Value
Partition 1	1
Partition 2	2
Partition 3	4
Partition 4	8

Example1: The user wants to assign a certain iButton key to Partition 4 only. According to the table value 8 reflects Partition 4. He would then have to enter value 8.

Example2: The user wants to assign a certain user code to Partition 2 and 3. According to the table value 2 reflects Partition 2, while value 4 reflects Partition 3, therefore 2 + 4 = 6. He would then have to enter value 6.

Example3: The user wants to assign a certain zone to Partition 1, 3 and 4. According to the table value 1 reflects Partition 1, while values 4 and 8 reflect Partitions 3 and 4 respectively, therefore 1 + 4 + 8 = 13. He would then have to enter value 13.

23.1. Zone Partition

Zone partition determines which system partition (-s) the zone will operate in.

Set zone partition

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → PARTITION → OK → pv → OK
Wireless zone: ... → WIRELESS ZONE 13... 76 → OK → PARTITION → OK → pv → OK
Keypad zone: ... → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → PARTITION → OK → pv → OK
EPGM1 zone: .. → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → PARTITION → OK → pv → OK
Value: *iiii* - 4-digit installer code; *pv* - partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 57, zone number & partition value:
57 nn pv #
Value: *nn* - zone number, range - [01... 76]; *pv* - partition value (see **23. PARTITIONS**).
Example: *57032#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Wireless siren EWS2/EWS3 siren will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed.

23.2. User Phone Number Partition

User phone number partition determines which system partition (-s) can be armed/disarmed from a certain user phone number by dialing system's phone number or sending an SMS text message.

Set user phone number partition

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PARTITION → pv → OK
Value: *iiii* - 4-digit installer code; *pv* - partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 59, user phone number slot & partition value:
59 us pv #
Value: *us* - user phone number slot, range - [01... 10]; *pv* - partition value (see **23. PARTITIONS**).
Example: *591013#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.3. Keypad Partition and Keypad Partition Switch

Keypad partition determines which system partition the keypad will operate in. To identify which partition the keypad is operating in:

- EKB2 – Refer to partition name (by default – PART1) indicated in home screen view.
- EKB3W/EKB3 (2-partition mode) – Refer to the location of the illuminated indicator READY on the keypad. The indicator will be illuminated under section A or B, which represent Partition 1 and Partition 2 respectively.

EKB3 keypad can operate in the following modes:

- **2-partition mode** – This parameter determines whether EKB3 keypad can operate only in one of the first two system partitions allowing to arm/disarm them and switch the keypad partition using [1]... [2] keys. This mode is set up by default.

- **4-partition mode** – This parameter determines whether EKB3 keypad can operate in one of the four system partitions allowing to arm/disarm them, indicate arm/disarm status, partition state (alarmed/not alarmed) on [1]... [4] keys (see **32.1.2. EKB3 - LED Keypad**) and switch the keypad partition using [1]... [4] keys.

The keypad must be assigned to the same partition as the user/master code (see **23.4. User/Master Code Partition**) in order to arm/disarm the system by the keypad. For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User/Master Code**, **12.4. EKB3 Keypad and User/Master Code** and **12.5. EKB3W Keypad and User/Master Code.**

Set EKB3 partition mode as 2-partition or 4-partition

Config Tool – This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

Set keypad partition

EKB2

Menu path:
EKB2 partition: OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → [k] EKB2 → OK → PARTITION 1... 4 → OK → DISABLE | ENABLE → OK
EKB3 partition: ... → KEYPAD PARTITION → OK → [k] EKB3 → OK → PARTITION 1... 4 → OK
EKB3W partition: ... → KEYPAD PARTITION → OK → EKB3W PARTITION → OK → EKB3W wless-id → OK → PARTITION 1... 2 → OK
Value: *iiii* – 4-digit installer code; *k* – keypad slot, range – [1... 4]; *wless-id* – 8-character wireless device ID code.

EKB3/ EKB3W

Enter parameter 51, keypad slot & partition number:
EKB3 partition: 51 kk p #
EKB3W partition: 51 kw r #
Value: *kk* – EKB3 keypad slot, range – [01... 04]; *kw* – EB3W keypad slot, range – [05... 08]; *p* – EKB3 partition number, range – [1... 4]; *r* – EKB3W partition number, range – [1... 2].
Example: *51062#*

Config Tool – This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: 4-partition mode must be enabled in order to assign EKB3 keypad to Partition 3 or Partition 4.

NOTE: EKB2 keypad can be assigned to multiple partitions, while EKB3 keypad can only be assigned only to single partition.

NOTE: EKB3W keypad assignment is restricted to Partition 1 and Partition 2.

NOTE: The slots for EKB3W keypads are automatically assigned to the paired keypad in the chronological order, hence the earliest paired keypad would acquire slot 5, while the latest paired keypad would acquire slot 8.

Keypad partition switch allows to quickly change the EKB3/EKB3W keypad partition. When the keypad partition is changed and when 1 minute after the last key-stroke expires, the system will return to the assigned keypad partition. Typically, this feature is used for viewing arm/ disarm status and alarms of a different partition or when arming/disarming a different system partition by EKB3/EKB3W keypad than the keypad is assigned to.

By default, keypad partition switch is disabled. To enable/disable this feature, please refer to the following configuration methods.

Enable keypad partition switch

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 77 & parameter status value:
77 1#
Example: *771#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable keypad partition switch

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 77 & parameter status value:
77 0 #
Example: *770#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Keypad partition switch can only be used when the system is partitioned.

23.4. User/Master Code Partition

User/master code partition determines which system partition (-s) can be armed/disarm using a certain user/master code. User/master code must be assigned to the same partition as the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) in order to arm/disarm the system by EKB2/EKB3/EKB3W keypad . For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User/Master Code**, **12.4. EKB3 Keypad and User/Master Code** and **12.5. EKB3W Keypad and User/Master Code**.

Set user/master code partition

EKB2

Menu path:
Master code: OK → mmmm → OK → CODES → OK → MASTER CODE → OK → PARTITION → OK → pv → OK
User code 2... 17: ... → CODES → OK → USER CODE (2-17) → OK → USER CODE 2... 17 → OK → PARTITION → OK → pv → OK
User code 18... 30: ... → CODES → OK → USER CODE (18-30) → OK → USER CODE 18... 30 → OK → PARTITION → OK → pv → OK
Value: *mmmm* – 4-digit master code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Press [CODE], [5], enter 01/user code slot, partition value & master code:
Master code: [CODE] [5] 01 pv mmmm #
User code: [CODE] [5] us pv mmmm #
Value: *us* - user code slot, range - [02... 30]; *pv* – partition value (see **23. PARTITIONS**); *mmmm* - 4-digit master code.
Example: *CODE50481111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE for EKB3/EKB3W: The Configuration mode must be deactivated, while managing user and master code partition.

23.5. iButton Key Partition

iButton key partition determines which system partition (-s) can be armed/disarmed using a certain key. iButton key must be assigned to the partition (-s) that the user desires to arm. For more details on system arming/disarming by iButton key, please refer to **12.6. iButton Key**.

Set iButton key partition

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1... 16 → OK → PARTITION → OK → pv → OK

Value: *iiii* – 4-digit installer code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 60, iButton key slot & partition value:
60 is pv #

Value: *is* – iButton key slot, range – [01... 16]; *pv* – partition value (see **23. PARTITIONS**).
Example: *600511#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.6. EWK1/EWK2/EWK2A Wireless Keyfob Partition

EWK1/EWK2/EWK2A wireless keyfob partition determines which system partition can be armed/disarmed using a certain EWK1/EWK2 wireless keyfob. For more details on system arming/disarming by EWK1/EWK2 wireless keyfob, please refer to **12.7. EWK1/EWK2 Wireless Keyfob**.

Set EWK1/EWK2/ EWK2A partition

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: EWK1/EWK2/EWK2A wireless keyfob can only be assigned to one partition.

24. TEMPERATURE SENSORS

The system may be equipped with up to 8 temperature sensors intended for temperature measurement in the surrounding areas. This feature allows to monitor the temperature of up to 8 different areas in real-time and receive a notification by SMS text message to the listed user phone number when the set temperature boundaries are exceeded. The temperature is measured at 0,5 degree centigrade (°C) accuracy and automatically rounded to the higher value when 0,5 or above, e. g. temperature ranging from 23,5°C through 24,4°C will be treated as 24 °C.

24.1. Adding, Removing and Replacing Temperature Sensors

To add a temperature sensor to the system, do the following:

a) Shutdown the system.

b) Wire up the temperature sensor to the 1-Wire interface terminals (see **2.3.5. Temperature Sensor and iButton Key Reader for temperature sensor wiring diagram**).

c) Power up the system.

d) Run *ELDES Configuration Tool* software to check if the temperature sensor has been recognized by the system.

e) If more than one temperature sensor is required, shut down the system again and wire another sensor in parallel to the previous one. By default, the first added temperature sensor will be identified as primary and the second one – as secondary temperature sensor (see **24.2. Primary and Secondary Temperature Sensors**).

f) Repeat the procedure as mentioned in steps from a) to d).

g) Add as many temperature sensors as necessary – wire up one after another in parallel – until the number of 8 sensors is reached.

To view the real-time temperature values measured by each temperature sensor, please refer to the following configuration methods.

View real-time temperature values of individual temperature sensor

SMS

SMS text message content:
ssss_ITEMP:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_ITEMP:4*

EKB2

Menu path:
OK → uumm → OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View real-time temperature values of all temperature sensors

SMS

SMS text message content:
ssss_ITEMP:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_ITEMP:?*

EKB2

Menu path:
OK → uumm → OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If a temperature sensor is faulty, it is recommended to remove it or replace it by a functional sensor. In order to assign the temperature sensor slot of the damaged temperature sensor to the new temperature sensor, please follow the procedure:

a) Run *ELDES Configuration Tool* software.

b) Select the number of the faulty temperature sensor that is to be replaced.

c) Click the **Replace** button.

d) Disconnect the faulty temperature sensor, replace it with a new one by following the on-screen instructions provided by *ELDES Configuration Tool* software.

Remove/replace individual temperature sensor

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When multiple temperature sensors are connected, please touch and hold the sensor with your fingers and watch the temperature value change to identify the number of the temperature sensor slot.

24.2. Primary and Secondary Temperature Sensors

By default, the first added temperature sensor is automatically set as primary, while the second one is set as secondary temperature sensor. The real-time temperature values of the primary and secondary temperature sensors are included in the Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**) as well as the temperature measured by the primary temperature sensor is indicated in the home screen view of EKB2 keypad.

To set a different temperature sensor as primary or secondary, please refer to the following configuration methods.

Set primary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:PRIM:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:PRIM:4*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → PRIMARY TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 89 & temperature sensor slot:
89 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *8903#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set secondary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:SEC:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:SEC:3*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → SECOND. TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 90 & temperature sensor slot:
90 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *9005#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To view the slot number of primary and secondary temperature sensors, please refer to the following configuration methods.

View primary and secondary temperature sensor slot number

SMS

SMS text message content:
ssss_TEMPI:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_TEMPI:?*

EKB2

Menu path:
Primary: OK → uumm → OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: ... → TEMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View primary and secondary temperature sensor real-time temperature values

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Menu path:
Primary: OK → uumm → OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: ... → TEMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Primary and secondary temperature sensors can be set by a single SMS text message, **Example:** *1111_TEMPI:PRIM:4,SEC:3*

24.3. Setting Up MIN and MAX Temperature Boundaries. Temperature Info SMS

The system supports an SMS text message identified as the Temperature Info SMS, which is automatically delivered to the listed user phone number if the specified minimum (MIN) or maximum (MAX) temperature boundary of any temperature sensor is exceeded by at least 1°C.

To set the MIN and MAX temperature boundaries for a certain temperature sensor, please refer to the configuration methods.

Set MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMPts:MIN:mnn,MAX:mxx
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] °C.
Example: *1111_TEMP2:MIN:-5,MAX:28*

EKB2

Menu path:
MIN: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN → OK → mnn → OK
MAX: ... → TEMPERATURE SENS 1... 8 → OK → TEMP. MAX → OK → mxx → OK
Value: *iiii* – 4-digit installer code; *mnn* – MIN boundary, range – [-55... 125] °C; *mxx* - MAX boundary, range – [-55... 125] °C.
Keys P1 or P2 are used to enter minus character, e.g. -20.

EKB3/ EKB3W

Enter parameter 19 & temperature value:
19 ts mnn mxx #
Value: *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] °C. 00 value stands for minus character, e. g. 0020 = -20
Example: *1906001530#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMPts
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP4*

EKB2

Menu path:
MIN: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN
MAX: ... → TEMPERATURE SENS 1... 8 → OK → TEMP. MAX
Value: *iiii* – 4-digit installer code

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

NOTE: MIN and MAX boundaries can also be set separately by multiple SMS text messages, **Example:** *1111_TEMP1:MIN:6 and 1111_TEMP1:MAX:40*

24.4. Temperature Sensor Names

The temperature sensor name is included in the Temperature Info SMS when delivered to the listed user phone number. This feature allows easier identification of the temperature sensor and normally it is used when monitoring temperature changes in different areas.

Set temperature sensor name

SMS

SMS text message content:
ssss_TEMPts:NAME:temp-sens-name
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range - [1... 8]; *temp-sens-name* - 4 to 24 characters temperature sensor name.
Example: *1111_TEMP3:NAME:Warehouse*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View temperature sensor name

SMS

SMS text message content:
ssss_TEMPts
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range - [1... 8].
Example: *1111_TEMP3*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → NAME
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete temperature sensor name

SMS

SMS text message content:
ssss_TEMPts:NAME:
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range - [1... 8].
Example: *1111_TEMP2:NAME:*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION

ESIM364 comes equipped with a microphone that allows the user to listen on his mobile phone to what is happening in the secured area. By installing the audio module EA2, the user will be able to have a 2-way voice communication (see **32.3.2. EA2 - Audio Output Module with Amplifier**). Remote listening and 2-way voice communication can operate under the following conditions:

- The system makes a phone call via GSM to a listed user phone number in case of alarm and the user answers the call.
- The user initiates remote listening by sending the SMS text message, the system makes a phone call via GSM to the user phone number that the SMS text message was sent from and the user answers the call.

Initiate remote listening

SMS

SMS text message content:
ssss_MIC
Value: *ssss* - 4-digit SMS password.
Example: *1111_MIC*

Set microphone gain

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *iiii* - 4-digit installer code; *mg* - microphone gain, range - [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set speaker level

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → SPEAKER LEVEL → OK → sl → OK
Value: *iiii* - 4-digit installer code; *sl* - speaker level, range - [0... 85].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Phone calls to the listed user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. MONITORING STATION).**

26. SYSTEM INFORMATION. INFO SMS

The system supports an informational SMS text message identified as the Info SMS, which can be delivered upon request. Once requested, the system will reply with Info SMS that provides the following:

- System date & time.
- System status: partition armed (ON)/disarmed (OFF).
- GSM signal strength.
- Mains power status.
- Temperature of the area surrounding primary and secondary temperature sensors (if any).
- State of zones (OK/alarm).
- Name and status (ON/OFF) of PGM outputs.

Request for system information

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

26.1. Periodic Info SMS

By default, the system sends Info SMS to User 1 phone number periodically once a day at 11:00 (frequency – 1 day; time – 11). The minimum period is every 1 hour (frequency – 0 days; time – 1). Typically, this feature is used to verify the power supply and online status of the system.

To set a different frequency and time or disable periodic Info SMS, please refer to the following configuration methods.

Set periodic Info SMS frequency and time

SMS

SMS text message content:
ssss_INFO:fff:it
Value: *ssss* – 4-digit SMS password; *fff* – frequency, range – [00... 99] days; *it* – time, range – [01... 23].
Example: *1111_INFO:3.15*

EKB2

Menu path:
Frequency: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → fff → OK
Time: .. → INFO SMS SCHEDULER → OK → TIME → it → OK
Value: *iiii* – 4-digit installer code; *fff* – frequency, range – [00... 125] days; *it* – time, range – [01... 23].

EKB3/ EKB3W

Enter parameter 11, time & frequency:
11it fff #
Value: *it* – time, range – [01... 23]; *fff* – frequency, range – [00... 125] days.
Example: *110412#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable periodic Info SMS

SMS

SMS text message content:
ssss_INFO:00:00
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO:00.00*

EKB2

Menu path:
Frequency: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → 0 → OK
Time: .. → INFO SMS SCHEDULER → OK → TIME → 0 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 11 & parameter status value:
11 00 00 #
Example: *110000#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Unlike Info SMS upon request, periodic Info SMS text message does not included zone states, PGM output names and status.

27. SYSTEM NOTIFICATIONS

By default in case of a certain event, the system attempts to send an SMS text message to the first listed user phone number only. If the user phone number is unavailable and the system fails to receive the SMS delivery report during 45 seconds, it will attempt to send the SMS text message to the next listed user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

The system will continue sending the SMS text message to the next listed user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

To change the SMS text message delivery algorithm, user can enable/disable the following parameters for certain events:

- **Send SMS text message to all users simultaneously** - This parameter determines whether to ignore the SMS delivery report or not. Once enabled, the system will attempt to send the SMS text message to every listed user phone number that is enabled to receive a certain event from the system by SMS text message. In addition, this parameter overrides the SMS delivery report parameter regardless of the SMS delivery report parameter's status (enabled/disabled).
- **SMS delivery report** - This parameter determines whether to request for SMS delivery report or not. Once disabled, the system will not verify the status of the SMS text message delivery and will attempt to deliver the SMS text message only to the first listed user phone number regardless if the next listed user phone number (-s) is enabled to receive a certain event by SMS text message or not.

When using Dual-SIM feature, the Secondary SIM card is involved in the communication process. For more details, please refer to **31. DUAL SIM MANAGEMENT.**

The following table provides the description of system notifications by SMS text message sent to the user phone number.

Seq. No.	Event	Description
1	System armed	SMS text message sent to the user regarding armed system.
2	System disarmed	SMS text message sent to the user about disarmed system.
3	General alarm	SMS text message sent to the user in case of system alarm occurrence.
4	Mains power loss/ restore	SMS text message sent to the user in case the mains power is lost or restored
5	Battery failed	SMS text message sent to the user in case the backup battery resistance is 2Ω or higher (battery requires replacement).
6	Battery dead or missing	SMS text message sent to the user in case the backup battery is not present or the battery voltage runs below 5V.
7	Low battery	SMS text message sent to the user in case the backup battery voltage is 10.5V or lower.
8	Siren fail/restore	SMS text message sent to the user in case the siren is disconnected/broken or connected/fixed.
9	Date/time not set	SMS text message sent to the user in case system date & time is not set.
10	GSM connection failed	SMS text message sent to the user in case the GSM connection is lost.
11	GSM/GPRS antenna fail/restore	SMS text message sent to the user in case the GSM/GPRS antenna is disconnected/broken or connected/broken.
12	Tamper alarm	SMS text message sent to the user in case of tamper violation. Indicated as *Tamper x*.
13	Keypad failed	SMS text message sent to the user in case the keypad is disconnected/broken.
14	Temperature info	SMS text message sent to the user in case of temperature deviation by the set values.
15	System started	SMS text message sent to the user on system startup.
16	Periodical info	Info SMS text message sent to the user periodically by the set values.
17	Wireless signal loss/ restore	SMS text message sent to the user in case the wireless signal is lost or restored.. Indicated as *No wireless signal from wless-dev wless-id Tamper x and Wireless signal restored. From wless-dev wless-id Tamper x respectively.*
18	Unable to arm	SMS text message sent to the user in case the system denies arming due to existing violated zone (-s)/tamper (-s).

To enable/disable a certain system notification, please refer to the following configuration methods.

Disable system notification

EKB2

Menu path:

System armed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → SYS ARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → SYS ARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

System disarmed:

User phone number: ... → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → SYS DISARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → SYS DISARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

General alarm:

User phone number: ... → GENERAL ALARM EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → GENERAL ALARM EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → GENERAL ALARM EV → OK → SMS REPORT → OK → DISABLE → OK

Mains power loss/restore:

User phone number: ... → MAIN POWER L/R EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → MAIN POWER L/R EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → MAIN POWER L/R EV → OK → SMS REPORT → OK → DISABLE → OK

Battery failed:

User phone number: ... → BATTERY FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → BATTERY FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → BATTERY FAILED → OK → SMS REPORT → OK → DISABLE → OK

Battery dead or missing:

User phone number: ... → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → BATTERY DEAD/MISS → OK → SMS REPORT → OK → DISABLE → OK

Low battery:

User phone number: ... → LOW BATTERY EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → LOW BATTERY EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → LOW BATTERY EVENT → OK → SMS REPORT → OK → DISABLE → OK

Siren fail/restore:

User phone number: ... → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → SIREN FAIL/REST EV → OK → SMS REPORT → OK → DISABLE → OK

Date/time not set:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → DATE/TIME NOT SET → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → DATE/TIME NOT SET → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → DATE/TIME NOT SET → OK → SMS REPORT → OK → DISABLE → OK

GSM connection failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → OK → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → GSM CONNECT FAILED → OK → SMS REPORT → OK → DISABLE → OK

GSM/GPRS antenna fail/restore:

User phone number: ... → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → GSM ANT FAIL/REST → OK → SMS REPORT → OK → DISABLE → OK

Tamper alarm:

User phone number: ... → TAMPER ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → TAMPER ALARM → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → TAMPER ALARM → OK → SMS REPORT → OK → DISABLE → OK

Keypad failed:

User phone number: ... → KEYPAD FAILED→ OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → KEYPAD FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → KEYPAD FAILED → OK → SMS REPORT → OK → DISABLE → OK

Temperature info:

User phone number: ... → TEMP INFO EVENT→ OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → TEMP INFO EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → TEMP INFO EVENT → OK → SMS REPORT → OK → DISABLE → OK

System started:

User phone number: ... → SYSTEM STARTED EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → SYSTEM STARTED EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → SYSTEM STARTED EV → OK → SMS REPORT → OK → DISABLE → OK

Periodical info:

User phone number: ... → PERIOD INFO SMS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → PERIOD INFO SMS EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → PERIOD INFO SMS EV → OK → SMS REPORT → OK → DISABLE → OK

Wireless signal loss/restore:

User phone number: ... → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → DISABLE → OK

Unable to arm:

User phone number: ... → FAIL TO ARM SMS → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: ... → FAIL TO ARM SMS → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: ... → FAIL TO ARM SMS → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/
EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

System armed event
User phone number: 25 01 up 0 #
SMS text message to all users simultaneously: 21 01 up 0 #
SMS delivery report: 55 01 up 0 #

System disarmed event
User phone number: 25 02 up 0 #
SMS text message to all users simultaneously: 21 02 up 0 #
SMS delivery report: 55 02 up 0 #

General alarm
User phone number: 25 03 up 0 #
SMS text message to all users simultaneously: 21 03 up 0 #
SMS delivery report: 55 03 up 0 #

Main power loss/restore
User phone number: 25 04 up 0 #
SMS text message to all users simultaneously: 21 04 up 0 #
SMS delivery report: 55 04 up 0 #

Battery failed
User phone number: 25 05 up 0 #
SMS text message to all users simultaneously: 21 05 up 0 #
SMS delivery report: 55 05 up 0 #

Battery dead or missing
User phone number: 25 06 up 0 #
SMS text message to all users simultaneously: 21 06 up 0 #
SMS delivery report: 55 06 up 0 #

Low battery
User phone number: 25 07 up 0 #
SMS text message to all users simultaneously: 21 07 up 0 #
SMS delivery report: 55 07 up 0 #

Siren fail/restore
User phone number: 25 08 up 0 #
SMS text message to all users simultaneously: 21 08 up 0 #
SMS delivery report: 55 08 up 0 #

Date/time not set
User phone number: 25 10 up 0 #
SMS text message to all users simultaneously: 21 10 up 0 #
SMS delivery report: 55 10 up 0 #

GSM connection failed
User phone number: 25 11 up 0 #
SMS text message to all users simultaneously: 21 11 up 0 #
SMS delivery report: 55 11 up 0 #

GSM/GPRS antenna fail/restore
User phone number: 25 12 up 0 #
SMS text message to all users simultaneously: 21 12 up 0 #
SMS delivery report: 55 12 up 0 #

Tamper alarm
User phone number: 25 13 up 0 #
SMS text message to all users simultaneously: 21 13 up 0 #
SMS delivery report: 55 13 us 0 #

Keypad failed
User phone number: 25 14 up 0 #
SMS text message to all users simultaneously: 21 14 up 0 #
SMS delivery report: 55 14 up 0 #

Temperature info
User phone number: 25 15 up 0 #
SMS text message to all users simultaneously: 21 15 up 0 #
SMS delivery report: 55 15 up 0 #

System started
User phone number: 25 16 up 0 #
SMS text message to all users simultaneously: 21 16 up 0 #
SMS delivery report: 55 16 up 0 #

Periodical info
User phone number: 25 17 up 0 #
SMS text message to all users simultaneously: 21 17 up 0 #
SMS delivery report: 55 17 up 0 #

Wireless signal loss/restore
User phone number: 25 18 up 0 #
SMS text message to all users simultaneously: 21 18 up 0 #
SMS delivery report: 55 18 up 0 #

Unable to arm
User phone number: 25 19 up 0 #
SMS text message to all users simultaneously: 21 19 up 0 #
SMS delivery report: 55 19 up 0 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2514020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable system notification

EKB2

Menu path:

System armed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → SYS ARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → SYS ARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK

System disarmed:

User phone number: ... → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → SYS DISARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → SYS DISARMED EVENT → OK → SMS REPORT → OK → ENABLE→ OK

General alarm:

User phone number: ... → GENERAL ALARM EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → GENERAL ALARM EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → GENERAL ALARM EV → OK → SMS REPORT → OK → ENABLE → OK

Mains power loss/restore:

User phone number: ... → MAIN POWER L/R EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → MAIN POWER L/R EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → MAIN POWER L/R EV → OK → SMS REPORT → OK → ENABLE→ OK

Battery failed:

User phone number: ... → BATTERY FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → BATTERY FAILED → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → BATTERY FAILED → OK → SMS REPORT → OK → ENABLE → OK

Battery dead or missing:

User phone number: ... → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → BATTERY DEAD/MISS → OK → SMS REPORT → OK → ENABLE → OK

Low battery:

User phone number: ... → LOW BATTERY EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → LOW BATTERY EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → LOW BATTERY EVENT → OK → SMS REPORT → OK → ENABLE → OK

Siren fail/restore:

User phone number: ... → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → SIREN FAIL/REST EV → OK → SMS REPORT → OK → ENABLE → OK

Date/time not set

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → DATE/TIME NOT SET → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → DATE/TIME NOT SET → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → DATE/TIME NOT SET → OK → SMS REPORT → OK → ENABLE → OK

GSM connection failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DENABLE → OK

SMS delivery report: ... → GSM CONNECT FAILED → OK → SMS REPORT → OK → ENABLE → OK

GSM/GPRS antenna fail/restore:

User phone number: ... → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → GSM ANT FAIL/REST → OK → SMS REPORT → OK → ENABLE → OK

Tamper alarm:

User phone number: ... → TAMPER ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → TAMPER ALARM → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → TAMPER ALARM → OK → SMS REPORT → OK → ENABLE → OK

Keypad failed:

User phone number: ... → KEYPAD FAILED→ OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → KEYPAD FAILED → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → KEYPAD FAILED → OK → SMS REPORT → OK → ENABLE → OK

Temperature info:

User phone number: ... → TEMP INFO EVENT→ OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → TEMP INFO EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → TEMP INFO EVENT → OK → SMS REPORT → OK → ENABLE → OK

System started:

User phone number: ... → SYSTEM STARTED EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: .. → SYSTEM STARTED EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → SYSTEM STARTED EV → OK → SMS REPORT → OK → ENABLE → OK

Periodical info:

User phone number: ... → PERIOD INFO SMS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → PERIOD INFO SMS EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → PERIOD INFO SMS EV → OK → SMS REPORT → OK → ENABLE → OK

Wireless signal loss/restore:

User phone number: ... → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → ENABLE → OK

Unable to arm:

User phone number: ... → FAIL TO ARM SMS → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: ... → FAIL TO ARM SMS → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: ... → FAIL TO ARM SMS → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

System armed event
User phone number: 25 01 up 1 #
SMS text message to all users simultaneously: 21 01 up 1 #
SMS delivery report: 55 01 up 1 #

System disarmed event
User phone number: 25 02 up 1 #
SMS text message to all users simultaneously: 21 02 up 1 #
SMS delivery report: 55 02 up 1 #

General alarm
User phone number: 25 03 up 1 #
SMS text message to all users simultaneously: 21 03 up 1 #
SMS delivery report: 55 03 up 1 #

Main power loss/restore
User phone number: 25 04 up 1 #
SMS text message to all users simultaneously: 21 04 up 1 #
SMS delivery report: 55 04 up 1 #

Battery failed
User phone number: 25 05 up 1 #
SMS text message to all users simultaneously: 21 05 up 1 #
SMS delivery report: 55 05 up 1 #

Battery dead or missing
User phone number: 25 06 up 1 #
SMS text message to all users simultaneously: 21 06 up 1 #
SMS delivery report: 55 06 up 1 #

Low battery
User phone number: 25 07 up 1 #
SMS text message to all users simultaneously: 21 07 up 1 #
SMS delivery report: 55 07 up 1 #

Siren fail/restore
User phone number: 25 08 up 1 #
SMS text message to all users simultaneously: 21 08 up 1 #
SMS delivery report: 55 08 up 1 #

Date/time not set
User phone number: 25 10 up 1 #
SMS text message to all users simultaneously: 21 10 up 1 #
SMS delivery report: 55 10 up 1 #

GSM connection failed
User phone number: 25 11 up 1 #
SMS text message to all users simultaneously: 21 11 up 1 #
SMS delivery report: 55 11 up 1 #

GSM/GPRS antenna fail/restore
User phone number: 25 12 up 1 #
SMS text message to all users simultaneously: 21 12 up 1 #
SMS delivery report: 55 12 up 1 #

Tamper alarm
User phone number: 25 13 up 1 #
SMS text message to all users simultaneously: 21 13 up 1 #
SMS delivery report: 55 13 up 1 #

Keypad failed
User phone number: 25 14 up 1 #
SMS text message to all users simultaneously: 21 14 up 1 #
SMS delivery report: 55 14 up 1 #

Temperature info
User phone number: 25 15 up 1 #
SMS text message to all users simultaneously: 21 15 up 1 #
SMS delivery report: 55 15 up 1 #

System started
User phone number: 25 16 up 1 #
SMS text message to all users simultaneously: 21 16 up 1 #
SMS delivery report: 55 16 up 1 #

Periodical info
User phone number: 25 17 up 1 #
SMS text message to all users simultaneously: 21 17 up 1 #
SMS delivery report: 55 17 up 1 #

Wireless signal loss/restore
User phone number: 25 18 up 1 #
SMS text message to all users simultaneously: 21 18 up 1 #
SMS delivery report: 55 18 up 1 #

Unable to arm
User phone number: 25 19 up 1 #
SMS text message to all users simultaneously: 21 19 up 1 #
SMS delivery report: 55 19 up 1 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2517041#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

27.1. SMSC (Short Message Service Center) Phone Number

An SMS center (SMSC) is a GSM network element, which routes SMS text messages to the destination user and stores the SMS text message if the recipient is unavailable. Typically, the phone number of the SMS center is already stored in the SIM card provided by the GSM operator. If the user fails to receive replies from the system, the SMS center phone number, provided by the GSM operator, must be set manually.

Set SMSC phone number

SMS

SMS text message content:
ssss_SMS_+ttteeellnnuumm

Value: *ssss* - 4-digit SMS password; *ttteeellnnuumm* – up to 15 digits SMSC phone number.
Example: *1111_SMS_+44170311XXXX1*

ATTENTION: Before setting the SMSC phone number, please check the credit balance of the system's SIM card. The system will fail to reply if the credit balance is insufficient.

28. EVENT AND ALARM LOG

28.1. Event Log

The event log allows to chronologically register up to 500 timestamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Wireless device management.
- Temperature deviation by MIN and MAX boundaries.
- System faults.

The event log is of LIFO (last in, first out) type that allows the system to automatically replace the oldest records with the the latest ones.

View event log

EKB2

Menu path:
OK → mmmm → OK → VIEW EVENT LOG → OK
Value: *mmmm* - 4-digit master code.

To export the event log to .log file or clear it, please refer to the following configuration method.

Export/clear event log

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, event log is enabled. To disable/enable this feature, please refer to the following configuration methods.

Disable event log

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 36 and parameter status value:
36 0 #
Example: *360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable event log

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 36 and parameter status value:
36 1 #
Example: *361#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

28.2. Alarm Log

The alarm log provides a list of last 16 alarm events generated after last arming period. The alarm log can be viewed via EKB2 and includes only the alarms of the partition that the user/master code is assigned to. Each alarm record includes alarm type, partition number and zone number. When highlighted, the date and time of the alarm occurrence can be viewed at the bottom of EKB2 screen. In case of alarm, icon will appear in home screen view of EKB2. The alarm log auto-clears when the next system arming follows or after viewing it via the keypad.

View alarm log

EKB2

Menu path:
OK → uumm → OK → ALARM LOG → OK
Value: *uumm* - 4-digit user/master code.

Syntax of alarm log record: *[alarm-type P:p Z:nn]*

Value: *alarm-type* - BURGLARY/FIRE/24H/SILENT/TAMPER/WS LOST, *p* - partition number, range - [1... 4], *nn* - zone/tamper number, range - [1... 76].

#1 example of alarm log record: *BURGLARY P:1 Z:1*

Value: *BURGLARY* - Instant, Int. Follower or Delay-type zone alarm; *P:1* - Partition 1; *Z:1* - zone Z1.

#2 example of alarm log record: *TAMPER P:2 Z:13*

Value: *TAMPER* - tamper alarm; *P:2* - Partition 2; *Z:13* - tamper 13.

#3 example of alarm log record: *FIRE P:4 Z:9*

Value: *FIRE* - Fire-type zone alarm; *P:4* - Partition 4; *Z:9* - zone Z9.

#4 example of alarm log record: *WS LOST P:2 Z:14*

Value: *WS LOST* - wireless signal loss alarm; *P:2* - Partition 2; *Z:14* - tamper 14.

29. INDICATION OF SYSTEM FAULTS

The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault by the keypad as well as by SMS text message notification to the listed user phone number. By default the indication for all system faults is indicated on the keypad. To disable/enable the indication of a certain system fault, please refer to the following configuration method.

Disable/enable individual system fault indication on keypad

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: After enabling/disabling a certain system fault indication, it is necessary to restart the system locally by powering down and powering up the system the system or remotely (see **34. REMOTE SYSTEM RESTART**).

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user wil not be able to arm the system until all existing system faults are solved.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

EKB2

icon displayed in home screen view indicates presence of system faults. In order to view the currently present system faults, please enter a valid user/master code to access menu section **FAULTS**. The description on each system fault is provided in the table below.

View system faults

Menu path:
OK → uumm → OK → FAULTS → OK

Value: *uumm* - 4-digit user/master code.

Name	Description
MAIN POWER LOSS	Mains power is lost
LOW BATTERY	Low backup battery power - backup battery voltage is 10.5V or lower
BATTERY DEAD/MISS	Backup battery is not present or the battery voltage runs below 5V
BATTERY FAILED	Backup battery requires replacement - backup battery resistance is 2Ω or higher
SIREN FAILED	Siren is disconnected/broken
VIOLATED TAMPER	One or more tampers are violated
DATE/TIME NOT SET	Date/time not set
GSM CONNECT FAILED	GSM connection is lost
GSM ANTENNA FAILED	GSM/GPRS antenna is disconnected/broken
WLESS ANTENNA FAIL	Wireless antenna is disconnected/broken
KEYPAD LOST	Keypad is disconnected/broken

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

SYSTEM LED	Description
Steady ON	One or more tampers are violated; other system faults (see below)
Flashing	One or more high-numbered zones (Z13-Z76) are violated

In order to find out more on the particular system fault, please enter command A provided below. 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	Mains power is lost
2	Low backup battery power - backup battery voltage is 10.5V or lower
3	Backup battery is not present or the battery voltage runs below 5V
4	Backup battery requires replacement - backup battery resistance is 2Ω or higher
5	Siren is disconnected/broken
7	One or more tampers are violated
8	Date/time not set
9	One or more high-numbered zones (Z13-Z76) are violated
10	GSM connection is lost
11	GSM/GPRS antenna is disconnected/broken
12	Wireless antenna is disconnected/broken

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

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

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

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

The number of violated high-numbered 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 steady ON. According to the table below LED #8 is equal to number 18, therefore 18 + 3 = 21.

Result: Violated high-numbered zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (steady ON)
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

30. MONITORING STATION

The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the monitoring station when the MS (Monitoring Station) mode is enabled.

When using the MS mode, the data messages transmitted to the monitoring station (see **30.1. Data Messages - Events**) will gain the highest priority for the delivery, therefore based on the communication method (see **30.2. Communication**), a constant and stable connection with the monitoring station must be ensured. In case of connection failure, the system will attempt to restore the connection and if the monitoring is unavailable for a lengthy period of time, the system might consume a large amount of voice calls/data resulting in additional charges applied by the GSM operator according to the cell phone service plan.

Enable MS mode

SMS

SMS text message content:
ssss_SCNSET:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:ON*

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → MS MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 23 & parameter status value:
23 1 #
Example: *231#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable MS mode

SMS

SMS text message content:
ssss_SCNSET:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:OFF*

EKB2

Menu path:
OK →iiii → OK → MS SETTINGS → OK → MS MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 23 & parameter status value:
23 0 #
Example: *230#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Account is a 4-digit number (By default - 9999) required to identify the alarm system unit by the monitoring station. Account 2 and Account 3 are used only when GPRS network method is selected and when necessary to set up to 3 server IP addresses (see **30.2.1. GPRS Network and ELAN3-ALARM**)

Set account

EKB2

Menu path:
Main Account: OK → iiii → OK → MS SETTINGS → OK → ACCOUNT → OK → cccc → OK
Account 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → ACCOUNT ID IP2 → OK → cccc → OK
Account 3: ... → ACCOUNT ID IP3 → OK → cccc → OK
Value: *iiii* – 4-digit installer code; *cccc* – 4-digit account number.

EKB3/ EKB3W

Enter parameter 27 & account number:
Main Account: 27 cccc #
Account 2: 96 12 cccc #
Account 3: 96 13 cccc #
Value: *cccc* – 4-digit account number.
Example: *278853#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening/2-way voice communication is in progress. However, during the remote configuration session, firmware update process or remote listening/2-way voice communication process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening/2-way voice communication process is over.

ATTENTION: Phone calls via GSM network to the listed user phone number in case of alarm are disabled by force when MS mode is enabled.

NOTE: Additional charges may apply for voice calls/data traffic based on your cell phone service plan when using the MS mode.

30.1. Data Messages - Events

The configuration of data messages is based on Ademco Contact ID protocol. The data messages can either be transmitted to the monitoring station alone or with duplication by SMS text message to listed user phone number. For more details on system notifications by SMS text message, please refer to **27. SYSTEM NOTIFICATIONS**.

Seq. No.	Contact ID® Code	Event	Description
1	1110	Fire alarm	Transmitted in case a zone of Fire type is violated.
2	3110	Fire restore	Transmitted in case a zone of Fire type is restored.
3	1121	Disarmed by user (Duress code)	Transmitted in case the system is disarmed by Duress code.
4	3121	Armed by user (Duress code)	Transmitted in case the system is armed by Duress code.
5	1130	Burglary alarm	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is violated.
6	3130	Burglary restore	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is restored.
7	1133	24-Hour zone alarm	Transmitted in case of zone of 24-Hour type is violated.
8	3133	24-Hour zone restore	Transmitted in case of zone of 24-Hour type is restored.
9	1144	Tamper alarm	Transmitted in case the tamper is violated.
10	3144	Tamper restore	Transmitted in case the tamper is restored.
11	1146	Panic/Silent zone alarm	Transmitted in case of zone of Panic/Silent type is violated.
12	3146	Panic/Silent zone restore	Transmitted in case of zone of Panic/Silent type is restored.
13	1158	Temperature risen	Transmitted in case of the temperature has increased above the MAX set value.
14	1159	Temperature fallen	Transmitted in case of temperature has decreased below the MIN set value.
15	1301	Mains power loss	Transmitted in case the main power supply is lost.
16	3301	Mains power restore	Transmitted in case the main power supply is restored.
17	1302	Low battery	Transmitted in case the backup battery voltage is 10.5V or lower / the wireless sensor battery level runs below 5%.
18	1308	System shutdown	When the system is running on backup battery power, it transmits the data message before the backup battery power is fully depleted.
19	1309	Battery failed	Transmitted in case the backup battery resistance is 2Ω or higher.
20	1311	Battery dead or missing	Transmitted in case the backup battery is not present or the battery voltage runs below 5V.
21	3311	Battery connection restore	Transmitted in case the backup battery connecton is fixed.
22	1321	Siren fail	Transmitted in case the siren is disconnected/broken.
23	3321	Siren restore	Transmitted in case the siren is connected/fixed.
24	1330	Keypad fail	Transmitted in case the keypad is disconnected/broken.
25	3330	Keypad restore	Transmitted in case the keypad is connected/fixed
26	1354	GPRS connection loss	Transmitted in case the GPRS connection is lost.
27	1358	GSM connection failed	Transmitted in case the GSM connection is lost.
28	1359	GSM/GPRS antenna fail	Transmitted in case the GSM/GPRS antenna is disconnected/broken
29	3359	GSM/GPRS antenna restore	Transmitted in case the GSM/GPRS antenna is connected/fixed.
30	1381	Wireless signal loss	Transmitted in case the connection with any wireless device is lost.
31	3381	Wireless signal restore	Transmitted in case the connection with any wireless device is restored.
32	1401	Disarmed by user	Transmitted in case the system is disarmed.

33	3401	Armed by user	Transmitted in case the system is armed.
34	1456	Disarmed in Stay mode	Transmitted in case the system is disarmed in Stay mode.
35	3463	SGS code entered	Transmitted in case the SGS code is entered.
36	1570	Zone bypassed	Transmitted in case a violated zone is bypassed.
37	3570	Bypassed zone activated	Transmitted in case a bypassed zone is activated.
38	3602	Test event/Kronos ping	Transmitted for system online status verification purposes.
39	3626	Date/time not set	Transmitted in case system date & time is not set.
40	1900	System started	Transmitted on system startup.

The following table refers to user codes included in arm/disarm data messages.

Type	Code
User Phone Number 1	0
User Phone Number 2	1
User Phone Number 3	2
User Phone Number 4	3
User Phone Number 5	4
User Phone Number 6	5
User Phone Number 7	6
User Phone Number 8	7
User Phone Number 9	8
User Phone Number 10	9
iButton 1	10
iButton 2	11
iButton 3	12
iButton 4	13
iButton 5	14
iButton 6	15
iButton 7	16
iButton 8	17
iButton 9	18
iButton 10	19
iButton 11	20
iButton 12	21
iButton 13	22
iButton 14	23
iButton 15	24
iButton 16	25
Master Code	26
User Code 2	27
User Code 3	28
User Code 4	29
User Code 5	30
User Code 6	31

Type	Code
User Code 7	32
User Code 8	33
User Code 9	34
User Code 10	35
User Code 11	36
User Code 12	37
User Code 13	38
User Code 14	39
User Code 15	40
User Code 16	41
User Code 17	42
User Code 18	43
User Code 19	44
User Code 20	45
User Code 21	46
User Code 22	47
User Code 23	48
User Code 24	49
User Code 25	50
User Code 26	51
User Code 27	52
User Code 28	53
User Code 29	54
User Code 30	55
Remote Code (EGR100)	56
KeyFob 1	87
KeyFob 2	88
KeyFob 3	89
KeyFob 4	90
KeyFob 5	91
Arm/Disarm by Zone Z1-Z76	163-239

Disable data message

EKB2

Menu path:
Burglary alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BURGLR ALM/REST EV → OK → DISABLE → OK
Mains power loss/restore: ... → MAIN POWER L/R EV → OK → DISABLE → OK
Armed/disarmed by user: ... → ARM/DISARM EVENT → OK → DISABLE → OK
Battery failed: ... → BATTERY FAILED → OK → DISABLE → OK
Battery dead or missing/battery connection restore: ... → BATTERY DEAD/MISS → OK → DISABLE → OK
Test event: ... → TEST EVENT → OK → DISABLE → OK
Tamper alarm/restore: ... → TAMPER ALM/REST EV → OK → DISABLE → OK
Panic/Silent zone alarm/restore: ... → PA/SIL ALM/REST EV → OK → DISABLE → OK
System started: ... → SYSTEM STARTED EV → OK → DISABLE → OK
Fire alarm/restore: ... → FIRE ALM/REST EV → OK → DISABLE → OK
24-Hour zone alarm/restore: ... → 24H ALM/REST EVENT→ OK → DISABLE → OK
Low battery: ... → LOW BATTE RY EVENT → OK → DISABLE → OK
Temperature risen: ... → TEMP HIGH EVENT → OK → DISABLE → OK
Temperature fallen: ... → TEMP LOW EVENT → OK → DISABLE → OK
Wireless signal loss/restore: ... → WLESS SIGN L/R EV → OK → DISABLE → OK
Disarmed by user (Duress code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DISARM DURESS EV → OK → DISABLE → OK
Armed/disarmed by user (SGS code): ... → ARM/DARM SGS EVENT → OK → DISABLE → OK
Armed/disarmed in Stay mode: ... → ARM/DARM STAY EV → OK → DISABLE → OK
Siren fail/restore: ... → SIREN FAIL/REST EV → OK → DISABLE → OK
Date/time not set: ... → DATE/ TIME NOT SET → OK → DISABLE → OK
GSM connection failed: ... → GSM CONNECT FAILED → OK → DISABLE → OK
GSM/GPRS antenna fail/restore: ... → GSM ANT FAIL/REST → OK → DISABLE → OK
System shutdown: ... → SYSTEM SHUTDOWN EV → OK → DISABLE → OK
Keypad fail/restore: ... → KEYPAD FAIL/REST → OK → DISABLE → OK
GPRS connection failed: ... → GPRS CONNECT FAIL → OK → DISABLE → OK
Zone bypassed/activated: ... → ZONE BYPASS→ OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 24, event number & parameter status value:
24 01 0 # - Burglary alarm/restore
24 02 0 # - Mains power loss/restore
24 03 0 # - Armed/disarmed by user
24 04 0 # - Test event
24 05 0 # - Battery failed
24 06 0 # -Battery dead or missing/battery connection restore
24 07 0 # - Tamper alarm/restore
24 08 0 # - Panic/Silent zone alarm/restore
24 09 0 # - Kronos ping
24 10 0 # - System started
24 13 0 # - 24-Hour zone alarm/restore
24 14 0 # - Fire zone alarm/restore
24 15 0 # - Low battery
24 16 0 # -Temperature risen
24 17 0 # - Temperature fallen
24 18 0 # - Wireless signal loss/restore
24 19 0 # - Disarmed by user (Duress code)
24 20 0 # - Armed/disarmed by user (SGS code)
24 21 0 # - Armed/disarmed in Stay mode
24 22 0 # - Siren fail/restore
24 24 0 # -Date/time not set
24 25 0 # - GSM connection failed
24 26 0 # - GSM/GPRS antenna fail/restore
24 27 0 # - System shutdown
24 28 0 # - Keypad fail/restore
24 29 0 # - GPRS connection failed
24 30 0 # - Zone bypassed/activated
Example: *24080#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable data message

EKB2

Menu path:

Burglary alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BURGLR ALM/REST EV → OK → ENABLE → OK

Mains power loss/restore: ... → MAIN POWER L/R EV → OK →ENABLE → OK

Armed/disarmed by user: ... → ARM/DISARM EVENT → OK → ENABLE → OK

Battery failed: ... → BATTERY FAILED → OK → ENABLE → OK

Battery dead or missing/battery connection restore: ... → BATTERY DEAD/MISS → OK → ENABLE → OK

Test event: ... → TEST EVENT → OK → ENABLE → OK

Tamper alarm/restore: ... → TAMPER ALM/REST EV → OK → ENABLE → OK

Panic/Silent zone alarm/restore: ... → PA/SIL ALM/REST EV → OK → ENABLE → OK

System started: ... → SYSTEM STARTED EV → OK → ENABLE → OK

Fire alarm/restore: ... → FIRE ALM/REST EV → OK → ENABLE → OK

24-Hour zone alarm/restore: ... → 24H ALM/REST EVENT→ OK → ENABLE → OK

Low battery: ... → LOW BATTE RY EVENT → OK → ENABLE → OK

Temperature risen: ... → TEMP HIGH EVENT → OK → ENABLE → OK

Temperature fallen: ... → TEMP LOW EVENT → OK → ENABLE → OK

Wireless signal loss/restore: ... → WLESS SIGN L/R EV → OK → ENABLE → OK

Disarmed by user (Duress code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DISARM DURESS EV → OK → ENABLE → OK

Armed/disarmed by user (SGS code): ... → ARM/DARM SGS EVENT → OK → ENABLE → OK

Armed/disarmed in Stay mode: ... → ARM/DARM STAY EV → OK → ENABLE → OK

Siren fail/restore: ... → SIREN FAIL/REST EV → OK → ENABLE → OK

Date/time not set: ... → DATE/ TIME NOT SET → OK → ENABLE → OK

GSM connection failed: ... → GSM CONNECT FAILED → OK → ENABLE → OK

GSM/GPRS antenna fail/restore: ... → GSM ANT FAIL/REST → OK → ENABLE → OK

System shutdown: ... → SYSTEM SHUTDOWN EV → OK → ENABLE → OK

Keypad fail/restore: ... → KEYPAD FAIL/REST → OK → ENABLE → OK

GPRS connection failed: ... → GPRS CONNECT FAIL → OK → ENABLE → OK

Zone bypassed/activated: ... → ZONE BYPASS → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 24, event number & parameter status value:

24011# - Burglary alarm/restore
24021# - Mains power loss/restore
24031# - Armed/disarmed by user
24041# - Test event
24051# - Battery failed
24061# - Battery dead or missing/battery connection restore
24071# - Tamper alarm/restore
24081# - Panic/Silent zone alarm/restore
24091# - Kronos ping
24101# - System started
24131# - 24-Hour zone alarm/restore
24141# - Fire zone alarm/restore
24151# - Low battery
24161# - Temperature risen
24171# - Temperature fallen
24181# - Wireless signal loss/restore
24191# - Disarmed by user (Duress code)
24201# - Armed/disarmed by user (SGS code)
24211# - Armed/disarmed in Stay mode
24221# - Siren fail/restore
24241# -Date/time not set
24251# - GSM connection failed
24261# - GSM/GPRS antenna fail/restore
24271# - System shutdown
24281# - Keypad fail/restore
24291# - GPRS connection failed
24301# - Zone bypassed/activated

Example: *24031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2. Communication

The system supports the following communication methods and protocols:

- GPRS network – EGR100, Kronos, SIA IP protocol (ANSI/SIA DC-09-2007; configurable as encrypted and non-encrypted).
- Voice calls (GSM audio channel) – Ademco Contact ID protocol.
- CSD (Cricuit Switched Data).
- PSTN (landline) – Ademco Contact ID protocol.
- SMS – Cortex SMS format.
- ELAN3-ALARM – EGR100, Kronos, SIA IP protocol (ANSI/SIA DC-09-2007; configurable as encrypted and non-encrypted).

Any communication method can be set as primary or backup connection. The user can set up to 5 backup connections in any sequence order.

Initially, the system communicates via primary connection with the monitoring station. By default, if the initial attempt to transmit data is unsuccessful, the system will make additional attempts until the data is successfully delivered. If all attempts are unsuccessful, the system will follow this pattern:

a) The system switches to the backup connection that follows in the sequence (presumably - Backup 1).

b) The system then attempts to transmit data by the backup connection.

c) If the initial attempt is unsuccessful, the system will make additional attempts until the data is successfully delivered.

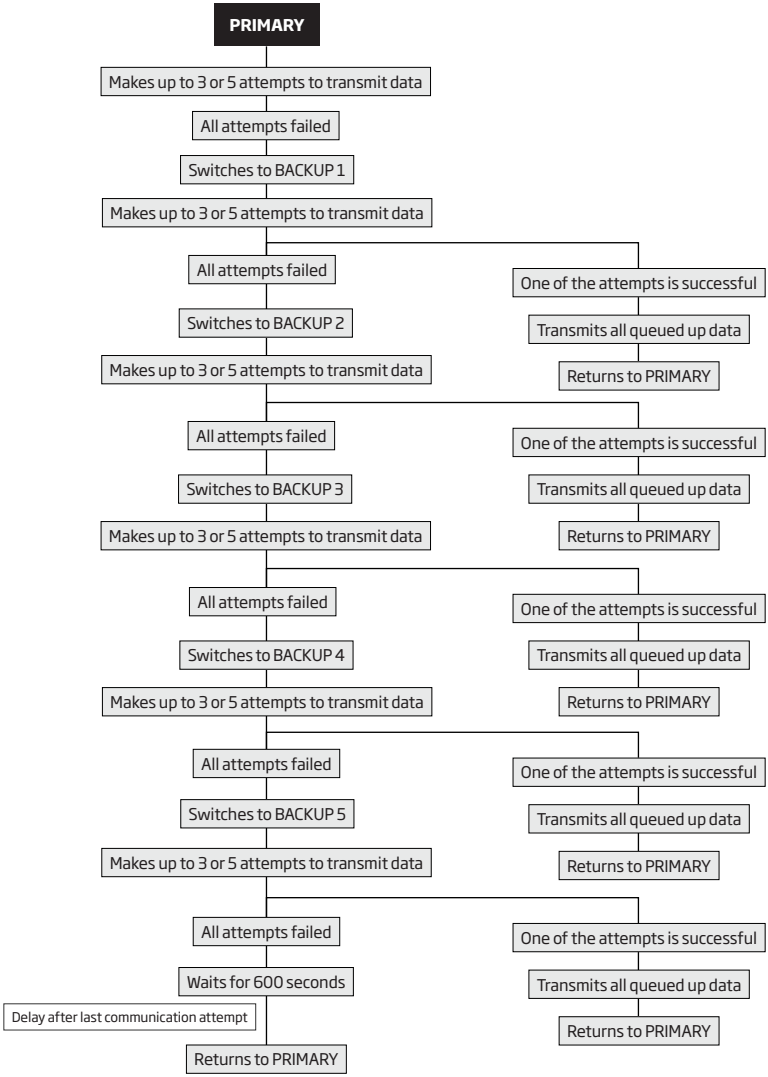
d) If the system ends up with all unsuccessful attempts, it will switch to the next backup connection in the sequence (presumably - Back-up 2) and will continue to operate as described in the previous steps. The connection is considered unsuccessful under the following conditions:
   - GPRS network/ELAN3-ALARM – The system has not received the ACK data message from the monitoring station within 40 seconds.
   - Voice calls:
     - The system has not received the "handshake" signal from the monitoring station within 40 seconds.
     - The system has not received the "kissoff" signal from the monitoring station within 5 attempts each lasting 1 second.
   - CSD – The system has not received the ACK data message from the monitoring station within 35 seconds.
   - PSTN:
     - The system has not received the "handshake" signal from the monitoring station within 40 seconds.
     - The system has not received the "kissoff" signal from the monitoring station within 5 attempts each lasting 1 second.
   - SMS – The system has not received the SMS delivery report from the SMSC (Short Message Service Center) within 45 seconds.

e) If one of the attempts is successful, the system will transmit all queued up data messages by this connection.

f) The system then returns to the primary connection and attempts to transmit the next data messages by primary connection.

g) If the system ends up with all unsuccessful attempts by all connections, it will wait until the *Delay after last communication attempt* time (By default – 600 seconds) expires and will return to the primary connection afterwards.

h) If a new data message, except Test Event (ping), is generated during *Delay* after last communication attempt time, the system will immediately attempt to transmit it to the monitoring station, regardless of *Delay* after last communication attempt being in progress.



NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method.

NOTE: When using Dual-SIM feature, the Secondary SIM card is involved in the communication process. For more details, please refer to **31. DUAL SIM MANAGEMENT.**

Set primary connection

EKB2

Menu path:
GPRS network - Server 1... 3: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → IP1... IP3 → OK
Voice calls: ... → PRIMARY CONNECTION → OK → VOICE CALLS → OK
CSD: ... → PRIMARY CONNECTION → OK → CSD → OK
PSTN: ... → PRIMARY CONNECTION → OK → PSTN → OK
SMS: ... → PRIMARY CONNECTION → OK → SMS → OK
ELAN3-ALARM: ... → PRIMARY CONNECTION → OK → ELAN3-ALARM → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 48 & communication method number:
480 # - GPRS network - Server 1
481 # - Voice calls
483 # - CSD
484 # - PSTN
485 # - SMS
486 # - ELAN3-ALARM
487 # - GPRS network - Server 2
488 # - GPRS network - Server 3
Example: *484#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set backup connection 1... 5

EKB2

Menu path:
GPRS network - Server 1... 3: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → IP1... IP3 → OK
Voice calls: ... → BACKUP CONNECTION1... 5 → OK → VOICE CALLS → OK
CSD: ... → BACKUP CONNECTION1... 5 → OK → CSD → OK
PSTN: ... → BACKUP CONNECTION1... 5 → OK → PSTN → OK
SMS: ... → BACKUP CONNECTION1... 5 → OK → SMS → OK
ELAN3-ALARM: ... → BACKUP CONNECTION1... 5 → OK → ELAN3-ALARM → OK
connection not in use: ... → BACKUP CONNECTION1... 5 → OK → N/A → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 83, backup connection slot number & communication method number:
83 bb 0 # - GPRS network - Server 1
83 bb 1 # - Voice calls
83 bb 3 # - CSD
83 bb 4 # - PSTN
83 bb 5 # - SMS
83 bb 6 # - ELAN3-ALARM
83 bb 7 # - GPRS network - Server 2
83 bb 8 # - GPRS network - Server 3
Value: *bb* - backup connection slot, range - [01... 05].
Example: *83024#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If all attempts by all set connections are unsuccessful, the system will wait until the delay time (By default - 600 seconds) expires and will attempt to transmit data to the monitoring station again starting with the primary connection.

Set delay after last communication attempt

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → DELAY LAST ATTEMPT → OK → aaapp → OK
Value: *iiii* - 4-digit installer code; *aaapp* - duration of delay after last attempt, range - [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 69 & duration of delay after last attempt:
69 aaapp #
Value: *aaapp* - duration of delay after last attempt, range - [0... 65535] seconds.
Example: *69200#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables delay after last communication attempt.

NOTE: The system is fully compatible with Kronos NET/Kronos LT monitoring station software for communication via GPRS network. When using a different monitoring station software, EGR100 middleware is required. EGR100 is freeware and can be downloaded at www.eldes.lt/en/download

30.2.1. GPRS Network and ELAN3-ALARM

The system supports up to 3 server IP addresses (applies to GPRS network method only) for data transmission to the monitoring station via IP-based networks by GPRS network or Ethernet connection using ELAN3-ALARM device. The supported data formats are the following:

- EGR100
- Kronos
- SIA IP

To set up the system for data transmission via GPRS network or Ethernet using ELAN3-ALARM, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Main Account number (see **30. MONITORING STATION**). If GPRS network is selected, you may set the Account for up to 3 servers individually.
3. Set Server 1 IP address, which is a public IP address of the machine running EGR100, Kronos or SIA IP-based monitoring station software. If GPRS network method is selected, you can set up to 3 server IP addresses in total.
4. Set Server 1 port, which is a port of the machine running EGR100, Kronos or SIA IP-based monitoring station software. If GPRS network is selected, you may set the port for up to 3 servers individually.
5. Select TCP or UDP protocol for Server 1. UDP is highly recommended for EGR100 and SIA IP data format. If GPRS network is selected, you may select the protocol for up to 3 servers individually.
6. Select data format for Server 1: EGR100, Kronos or SIA IP. If GPRS network is selected, you may select the data format for up to 3 servers individually.
7. In case EGR100 is selected, set 4-digit Unit ID numbers. Unit ID number can be identical to Account number. If GPRS network is selected, you may set the Unit ID for up to 3 servers individually.
8. When using GPRS network connection, it is necessary to set up APN, user name and password provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.
9. In case GPRS network method is selected and more than one server IP address is set up, you may wish to enable parallel data transmission to all IP addresses simultaneously. By default, this feature is disabled, therefore the system will switch to the next IP address (if set up and selected in the connection priority sequence) in the event of failed connection with the previous server.

For detailed step-by-step instructions on how to establish the communication between ESIM364 alarm system and EGR100 middleware, please refer to the middleware's HELP file.

NOTE: ELAN3-ALARM method supports data transmission to Server IP 1 address ONLY. Data transmission to multiple server IP addresses is NOT supported by this method.

Set server IP address

SMS

SMS text message content:
Server 1: ssss_SETGPRS:IP:add.add.add.add
Value: *ssss* - 4-digit SMS password; *add.add.add.add* - server IP address.
Example: *1111_SETGPRS:IP:65.82.119.5*

EKB2

Menu path:
Server 1: OK → iiii → OK → GPRS SETTINGS → OK → SERVER IP → OK → add.add. add.add → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → SERVER2 IP → OK → add.add. add. add → OK
Server 3: ... → SERVER3 IP → OK → add.add. add.add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – server IP address.

EKB3/ EKB3W

Enter parameter 40 & server IP address/parameter 96, parameter number & server IP address:
Server 1: 40 add add add add #
Server 2: 96 02 add add add add #
Server 3: 96 03 add add add add #
Value: *add add add add* – server IP address.
Example: *40065082119005#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set server port

SMS

SMS text message content:
Server 1: ssss_SETGPRS:PORT:pprrt
Value: *ssss* – 4-digit SMS password; *pprrt* – server port number, range – [1... 65535].
Example: *1111_SETGPRS:PORT:5521*

EKB2

Menu path:
Server 1: OK → iiii → OK → GPRS SETTINGS → OK → SERVER PORT → OK → pprrt → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → SERVER2 PORT → OK → pprrt → OK
Server 3: ... → SERVER3 PORT → OK → pprrt → OK
Value: *iiii* – 4-digit installer code; *pprrt* – server port number, range – [1... 65535].

EKB3/ EKB3W

Enter parameter 44 & server port number/parameter 96, parameter number & port number:
Server 1: 44 pprrt #
Server 2: 96 04 pprrt #
Server 3: 96 05 pprrt #
Value: *pprrt* – server port number, range – [1... 65535].
Example: *443365#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS1 server IP address

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → DNS1 → OK → add. add.add. add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – DNS1 server IP address.

EKB3/ EKB3W

Enter parameter 41 & DNS1 server IP address:
41 add add add add #
Value: *add add add add* – DNS1 server IP address.
Example: *41065082119001#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS2 server IP address

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → DNS2 → OK → add. add.add. add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – DNS2 server IP address.

EKB3/ EKB3W

Enter parameter 42 & DNS2 server IP address:
42 add add add add #
Value: *add add add add* – DNS2 server IP address.
Example: *41065082119002#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set protocol

SMS

SMS text message content:
Server 1: ssss_SETGPRS:PROTOCOL:ptc
Value: *ssss* – 4-digit SMS password; *ptc* – protocol, range – [TCP... UDP].
Example: *1111_SETGPRS:PROTOCOL:UDP*

EKB2

Menu path:
Server 1: OK → iiii → OK → GPRS SETTINGS → OK → PROTOCOL → OK → TCP | UDP → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → PROTOCOL2→ OK → TCP | UDP → OK
Server 3: ... → PROTOCOL3 → OK → TCP | UDP → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 43 & protocol number/parameter 96, parameter number & protocol number:
Server 1: 43 0 # - TCP | 43 1 # - UDP
Server 2: 96 06 0 # - TCP | 96 06 1 # - UDP
Server 3: 96 07 0 # - TCP | 96 07 1 # - UDP
Example: *431#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set data format as Kronos, EGR100 or SIA IP

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Manage SIA IP data format parameters

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: It is necessary to restart the system locally by powering down and powering up the system the system or remotely (see **34. REMOTE SYSTEM RESTART**) after changing the IP address or switching from TCP to UDP.

NOTE: Kronos NET/Kronos LT software communicates via TCP protocol, while EGR100 middle-ware v1.2 and up supports both – TCP and UDP protocols. However, TCP protocol is NOT recommend to use with EGR100.

By default, if the initial attempt to transmit data to the monitoring station via GPRS network or Ethernet method is unsuccessful, the system will make up to 2 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
Server 1: OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → IP ATTEMPTS → OK → att → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → IP2 ATTEMPTS → OK → att → OK
Server 3: ... → IP3 ATTEMPTS → OK → att → OK
Value: *iiii* – 4-digit installer code; *att* – number of attempts, range – [1... 255].

EKB3/ EKB3W

Enter parameter 68 & number of attempts/parameter 96, parameter number & number of attempts:
Server 1: 68 att #
Server 2: 96 08 att #
Server 3: 96 09 att #
Value: *att* – number of attempts, range – [01... 255].
Example: *6809#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To report the online status, the system periodically transmits (By default – every 180 seconds) Test Event data message (ping) to the monitoring station via GPRS network or Ethernet.

Set test period

EKB2

Menu path:
Server 1: OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → TEST PERIOD → OK → tteessttpp → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → TEST PERIOD2 → OK → tteessttpp → OK
Server 3: ... → TEST PERIOD3 → OK → tteessttpp → OK
Value: *iiii* – 4-digit installer code; *tteessttpp* – test period, range – [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 46 & number of attempts/parameter 96, parameter number & number of attempts:
Server 1: 46 tteessttpp #
Server 2: 96 10 tteessttpp #
Server 3: 96 11 tteessttpp #
Value: *tteessttpp* – test period, range – [0... 65535] seconds.
Example: *46120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables test period. However, disabling the test period is HIGHLY UNRECOMMENDED.

Unit ID is a 4-digit number (By default – 0000) required to identify the alarm system unit by EGR100 middle-ware. It is MANDATORY to change the default Unit ID before using EGR100.

Set unit ID

EKB2

Menu path:
Server 1: OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → UNIT ID → OK → unid → OK
Server 2: OK → iiii → OK → PARAL.DS.SETTINGS → OK → UNIT ID IP2 → OK → unid → OK
Server 3: ... → UNIT ID IP3 → OK → unid → OK
Value: *iiii* – 4-digit installer code; *unid* – 4-digit unit ID number.

EKB3/ EKB3W

Enter parameter 47 & unit ID number/parameter 96, parameter number & unit ID number:
Server 1: 47 unid #
Server 2: 96 14 unid #
Server 3: 96 15 unid #
Value: *unid* – 4-digit unit ID number.
Example: *472245#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For communication via GPRS network, the GPRS parameters provided by the GSM operator are necessary to be set up. To set those parameters, please refer to the following configuration methods.

Set APN

SMS

SMS text message content:
ssss_SETGPRS:APN:acc-point-name
Value: *ssss* – 4-digit SMS password; *acc-point-name* – up to 31 character APN (Access Point Name) provided by the GSM operator.
Example: *1111_SETGPRS:APN:internet*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set user name

SMS

SMS text message content:
ssss_SETGPRS:USER:usr-name
Value: *ssss* – 4-digit SMS password; *usr-name* – up to 31 character user name provided by the GSM operator.
Example: *1111_USER:mobileusr*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set password

SMS

SMS text message content:
ssss_SETGPRS:PSW:password
Value: *ssss* – 4-digit SMS password; *password* – up to 31 character password provided by the GSM operator.
Example: *1111_SETGPRS:PSW:mobilepsw*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View IP and GPRS network settings

SMS

SMS text message content:
ssss_SETGPRS?
Example: *1111_SETGPRS?*

EKB2

Menu path:
Server IP: OK → iiii → OK → GPRS SETTNGS → OK → IP SETTINGS → OK → SERVER IP
Server port: OK → iiii → OK → GPRS SETTNGS → OK → PORT
DNS1: OK → iiii → OK → GPRS SETTNGS → OK → DNS1
DNS2: OK → iiii → OK → GPRS SETTNGS → OK → DNS2
Protocol: OK → iiii → OK → GPRS SETTNGS → OK → PROTOCOL
APN: OK → iiii → OK → GPRS SETTINGS → OK → APN
User name: OK → iiii → OK → GPRS SETTINGS → OK → USERS
Password: OK → iiii → OK → GPRS SETTINGS → OK → PASSWORD
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable parallel data transmission

EKB2

Menu path:
OK → iiii → OK → PARAL.DS.SETTINGS → OK → PARAL.DS.MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter command 96, parameter number & parameter status value:
96 01 1 #
Example: *96011#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable parallel data transmission

EKB2

Menu path:
OK → iiii → OK → PARAL.DS.SETTINGS → OK → PARAL.DS.MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter command 96, parameter number & parameter status value:
96 01 0 #
Example: *96010#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2.2. Voice Calls and SMS

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by Voice Calls or SMS communication method using Ademco Contact ID or Cortex SMS data format respectively. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for UK: *+44170911XXXX1*. This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: *0044170911XXXX1*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad.
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for UK: *0170911XXXX1*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

To set up the system for data transmission via Voice Calls or SMS, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Main Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 3.

Set monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.

EKB3/ EKB3W

Enter parameter 26, phone number slot & phone number:
26 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 03]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *26010044170911XXXX1#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → OK
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via Voice Calls or SMS method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will continue to communicate with the monitoring station by switching to the next phone number that follows in the sequence and making up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W

Enter parameter 37 & number of attempts:
37 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *3706#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Due to the individual configuration of each monitoring station, the system may fail to deliver the data message via Voice Calls communication method. In such cases it is recommended to adjust the microphone gain until the optimal value, leading to successful data message delivery, is discovered.

Set microphone gain

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *iiii* – 4-digit installer code; mg – microphone gain, range – [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2.3. PSTN

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by PSTN communication method using Ademco Contact ID data format. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: *0044170911XXXX1*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for UK: *0170911XXXX1*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

To set up the system for data transmission via PSTN, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Main Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 3.

Set monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → TEL. NUMBER 1... 3 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.

EKB3/ EKB3W

Enter parameter 58, phone number slot & phone number:
58 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 03]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *580200441709 11XXXX1#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → TEL. NUMBER 1... 3 → OK → OK
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via PSTN method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will switch to the next phone number that follows in the sequence and will make up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W

Enter parameter 91 & number of attempts:
91 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *9108#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Alternatively, the phone number entries can be treated as phone numbers for receiving calls in case of alarm. For more details on how this method operates, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS FOR USER.**

To enable/disable this feature, please refer to the following configuration method.

Enable/disable Treat PSTN Call as User Call

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

30.2.4. CSD

The system supports up to 5 monitoring station phone numbers for communication with the alarm system by CSD communication method. Tel. Number 1 is mandatory, the other four can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone number must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for UK: *+44170911XXXX1*. This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone number must be entered starting with 00 and an international country code in the following ž format: 00[international code][area code][local number], example for UK: *0044170911XXXX1*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad.

To set up the system for data transmission via CSD, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Main Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 5.

Set monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; ttteeellnnuumm – up to 15 digits monitoring station phone number.

EKB3/ EKB3W

Enter parameter 85, number of entry & phone number:
85 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 05]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *85010044170911XXXX1#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → OK
Value: *iiii* – 4-digit installer code.

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's phone number via CSD method is unsuccessful, the system will make up to 4 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W

Enter parameter 84 & number of attempts:
84 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *8403#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

31. DUAL SIM MANAGEMENT

The Dual-SIM feature allows the system to operate with one of the two inserted SIM cards identified as Primary SIM and Secondary SIM respectively. The Primary SIM card works as the main default card, while the Secondary SIM card is intended for backup purposes or addition to the Primary SIM card - SMS text message sending/calling to the listed user phone number and/or communication with the monitoring station.

The Dual-SIM feature can operate in one of the following modes:

- **Disabled** - The Secondary SIM card will not be functional and the system operates with Primary SIM card only (by default - enabled).
- **Automatic** - The system switches between the SIM cards in case of a GSM connection or one of the SIM cards failure.
- **Manual** - Provides a fully customizable set up of switching between the SIM cards. FOR ADVANCED USERS ONLY!

Manage Dual -SIM feature

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Regardless of the selected mode, only one of the two SIM cards can operate at the same time.

31.1. Disabled Mode

Disabled mode is the default system mode that does not involve the Secondary SIM in the communication process. When this mode is in use, the system will ignore the Secondary SIM card even if inserted in the SIM card slot.

For more details on how the system communicates with the user and the monitoring station in Disabled mode, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS FOR USER** and **30.2. Communication respectively**.

31.2. Automatic Mode

Automatic mode involves both SIM cards in the communication process. In this mode there is no Primary or Secondary SIM card hierarchy, since both cards are equal and the SIM card that is currently in use maintains the GSM connection at all time, unless a failure occurs and the other card would replace the previous one.

When one of the SIM card fails, the system attempts to re-establish a connection with it by starting an initial reconnection for a set number of attempts (by default - 3 attempts). If all attempts fail, the system will switch to the other SIM card. If the other SIM card is responsive and a GSM connection is successfully established, the system will remain operating with that SIM card until it fails. However, if the other SIM card is unresponsive or it is not present in the SIM card slot, the system will return to the previous SIM card and attempt to establish a GSM connection with it. If the system fails to carry out this action, after a single attempt it will switch to the other SIM card. This cycle continues until one of the SIM cards responds and a GSM connection is successfully established. When the SIM card fails, the system will once again attempt to restore the GSM connection for a set number of attempts (by default - 3 attempts). If all attempts fail, the cycle will continue as described previously.

In Automatic mode the priority is to transmit data to the monitoring station, but if an event, which requires the system to send an SMS text message occurs , the system will send the SMS text message via the SIM card that is currently in use. This can only be carried out under the following conditions:

- among the attempts to transmit data to the monitoring station (depending on communication method).
- while switching the monitoring station connections.
- while switching between the SIM cards.

NOTE: ELDES Cloud Services will remain operational in Automatic mode, when used.

31.3. Manual Mode

Manual mode allows to use both - Primary and Secondary SIM cards and fully customize the algorithm of the communication. The system can be set up to send SMS text messages/call to the listed user phone number and/or communicate with the monitoring station as follows:

- **Primary SIM** - Determines that the SMS text messages/calls/data will be transmitted via the Primary SIM card.
- **Secondary SIM** - Determines that the SMS text messages/calls/data will be transmitted via the Secondary SIM card.
- **Currently in use SIM** - Determines that the SMS text messages/calls/data will be transmitted via the SIM card that the system is currently switched to - either Primary or the Secondary SIM card.
- **Return to Primary SIM Enabled** - Determines that the Primary SIM card will be the main SIM card of the system. If it is set up to use the Secondary SIM in the communication process, the system will do so, but after completing the task via the Secondary SIM card, the system will always return to the Primary SIM card
- **Try to find operator for a maximum of x times** - Determines the maximum number of attempts the system should attempt to re-establish a GSM connection on the current SIM card in case of unsuccessful initial attempt (by default - 3 attempts).

In Manual mode the priority is to transmit data to the monitoring station, but if an event, which requires the system to send an SMS text message via one of the SIM cards, occurs , the system will switch to the requested SIM card and send the SMS text message. This can only be carried out under the following conditions:

- among the attempts to transmit data to the monitoring station (depending on communication method).
- while switching the monitoring station connections.
- while switching between the SIM cards.

Example: System settings are the following:

Dual SIM Management:

- **Manual Mode** selected
- **Return to Primary SIM** – Disabled.
- **Send SMS / Call via** – Secondary SIM.

MS Settings – Communication:

- **Primary** – Voice Calls via Secondary SIM.
- **Backup1** – CSD via Primary SIM.
- **Backup2** – GPRS Network via Primary SIM.

Let's say, the system is configured to send an SMS text message to user phone number in case of a Fire Zone Alarm and to transmit data to the monitoring station when the system is ARMED. The system is currently switched to the Primary SIM card. The system will follow this pattern:

a) The user arms the system followed by system switching to the Secondary SIM and attempting to transmit data to the monitoring station via the Primary connection, which is Voice Calls communication method, but fails.

b) The system then switches to the Primary SIM and attempts to transmit data via Backup1 connection, which is CSD communication method, but fails again.

c) During the event described in step b), a Fire Zone Alarm occurs. The system will switch to the Secondary SIM and attempt to send the SMS text message to the user regarding this event.

d) The system continues with the data transmission to the monitoring station by switching back to Primary SIM and attempting to transmit data via Backup2 connection, which is GPRS Network communication method, and succeeds.

e) In case of occurrence of a new event, the alarm system will switch back to the Primary connection (Voice Calls) and to the Secondary SIM card and will attempt to transmit the data to the monitoring station.

NOTE: If the Return to Primary SIM parameter is enabled, the system would return to the Primary SIM after each data transmission.

NOTE: ELDES Cloud Services will remain operational in Manual mode, when used.

32. WIRED DEVICES

32.1. RS485 Interface

The system comes equipped with RS485 interface used for the communication with the following devices:

- EKB2 - LCD keypad. Up to 4 units supported..
- EKB3 - LED keypad. Up to 4 units supported..
- EPGM1 - hardwired zone and PGM output expansion module. Up to 2 units.
- ELAN3-ALARM - Ethernet communicator. 1 unit supported.

The terminals of RS485 interface are Y (yellow wire) and G (green wire) terminals, which are data bus. The devices, connected to RS485 interface, must be powered from the AUX+ and AUX- terminals or by an external power supply.

For more details on RS485 device wiring, please refer to **3.2.7. RS485**.

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

32.1.1. EKB2 - LCD Keypad

Main features:

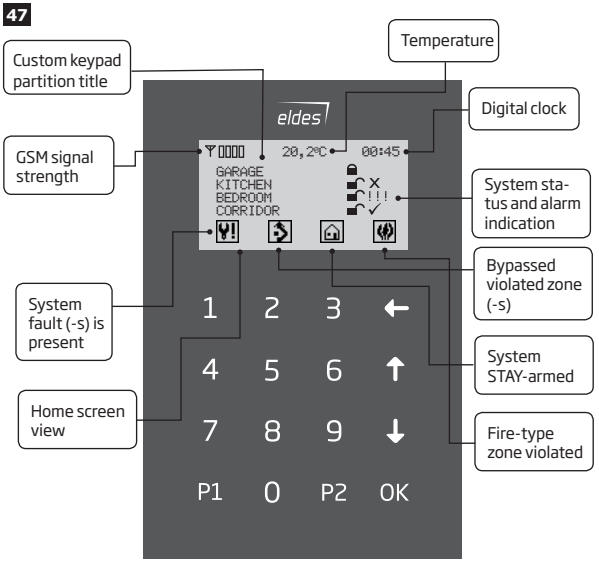
- Alarm system arming and disarming (see **12.3. EKB2 Keypad and User/Master Code**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- System information display (see **32.1.1.1. Icons and Messages**).
- Audio indication by built-in buzzer.
- Wireless device information display (see **19.2. Wireless Device Information and Signal Status Monitoring**).
- Temperature display (see **32.1.1.1. Icons and Messages**).
- Time display (see **32.1.1.1. Icons and Messages**).

For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

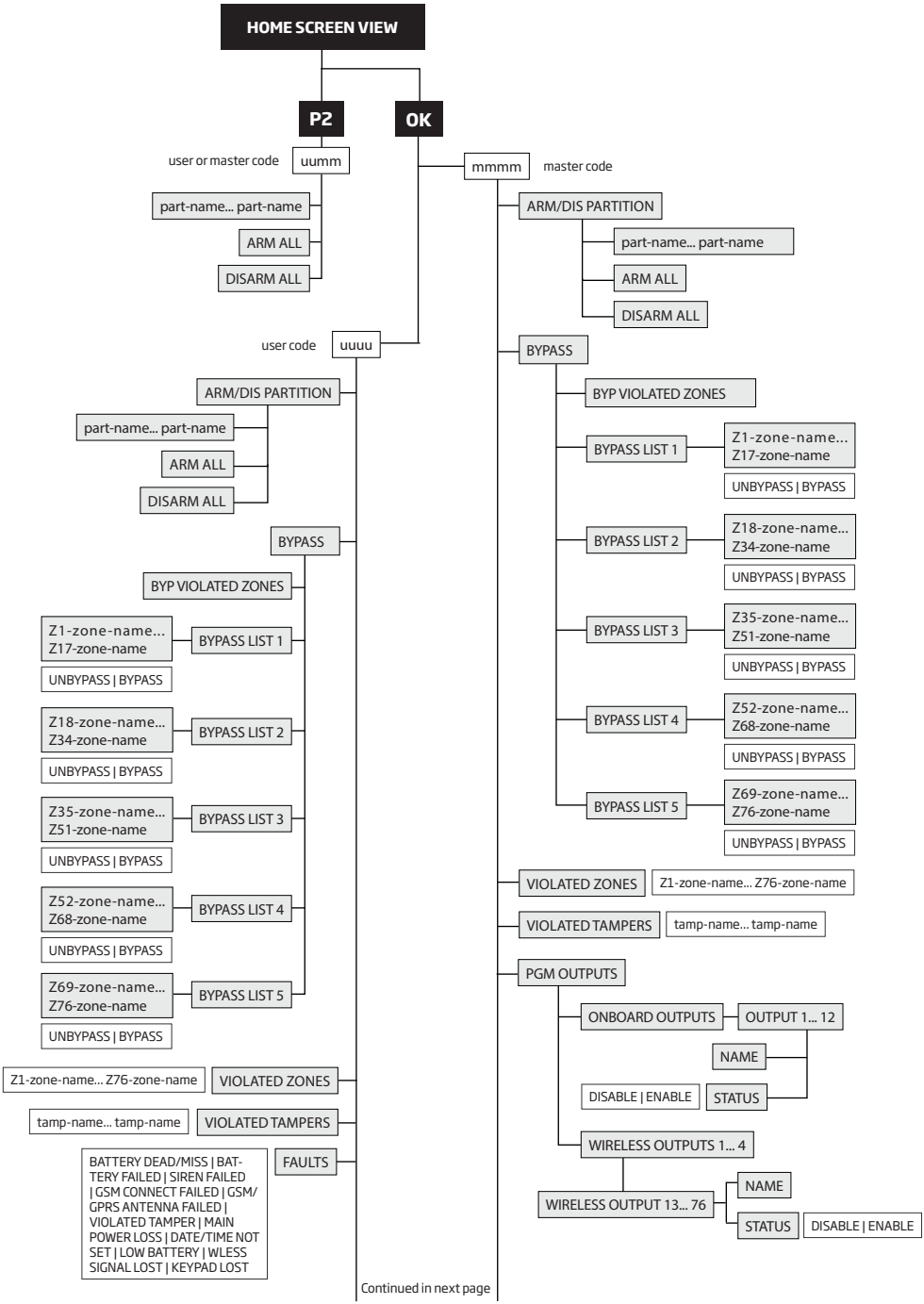
32.1.1.1. Icons and Messages

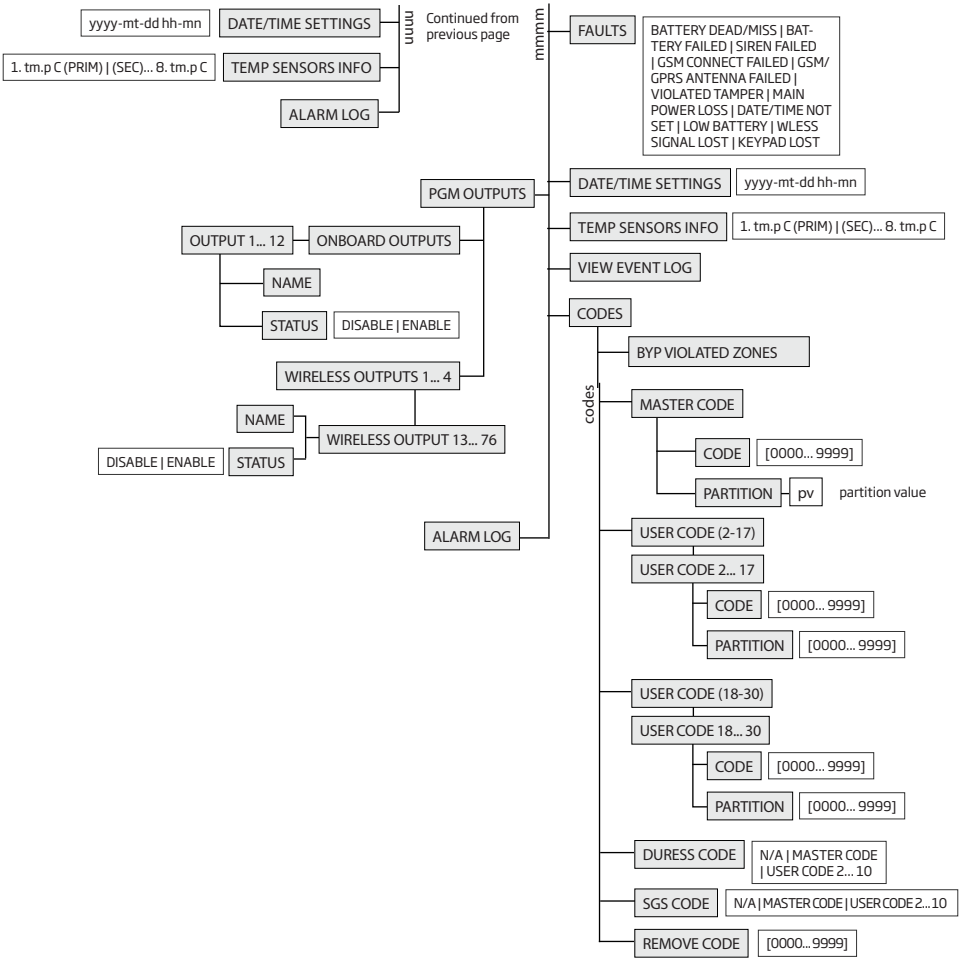
Icon / Message	Description
(by default - disabled)	Partition is armed and menu is locked
(by default - disabled)	Partition is disarmed and menu is unlocked
	Configuration mode activated
!!!	Zone or tamper alarm in partition
✓	Partition is ready to be armed.
X	Partition is not ready to be armed – one or more zones / tampers violated.
	One or more system faults present
	One or more violated zones bypassed
	One or more partitions STAY-armed
	One or more Fire-type zones violated
	Alarms in alarm log present
SERVICE MODE	Service mode activated

47

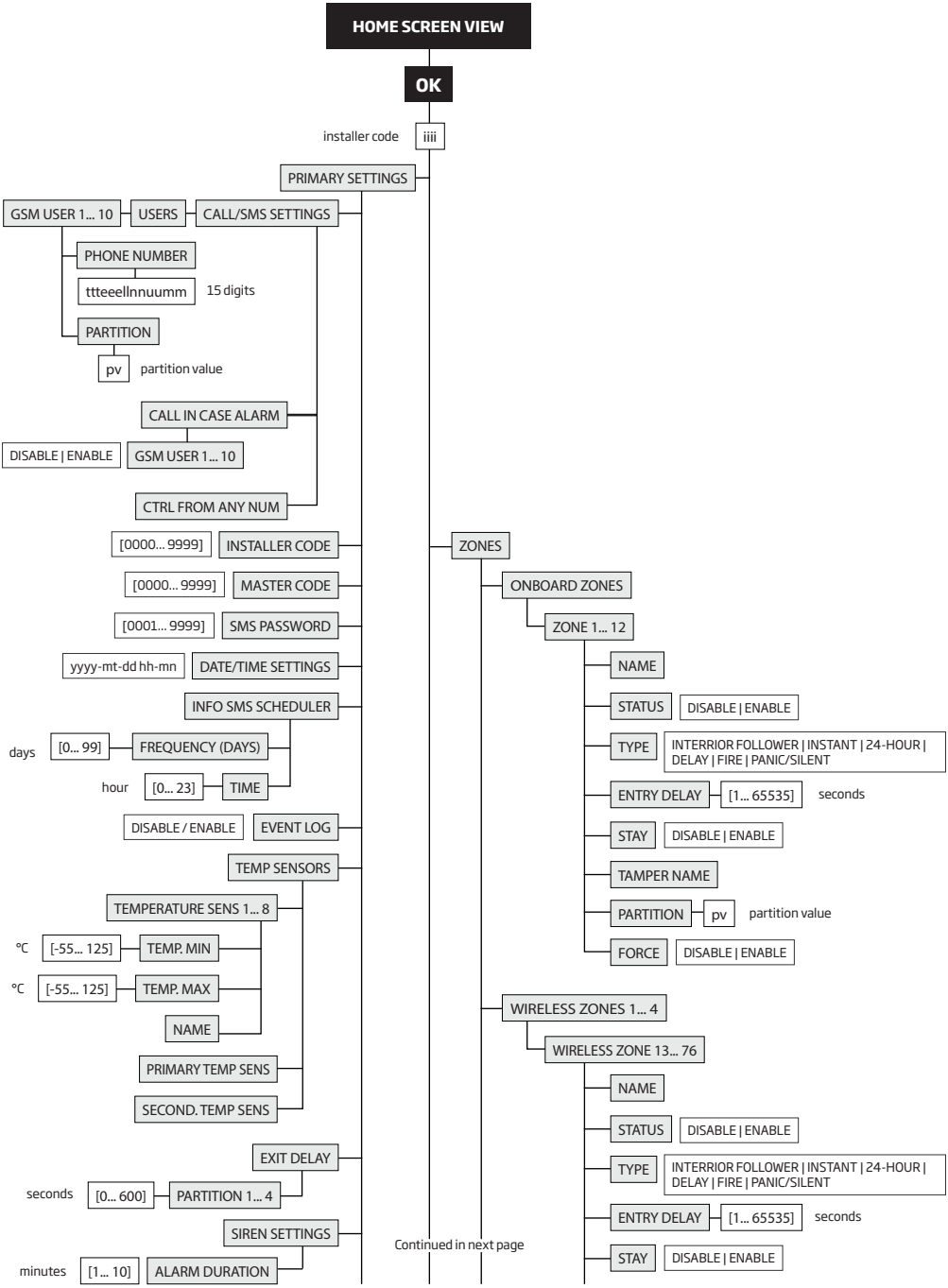


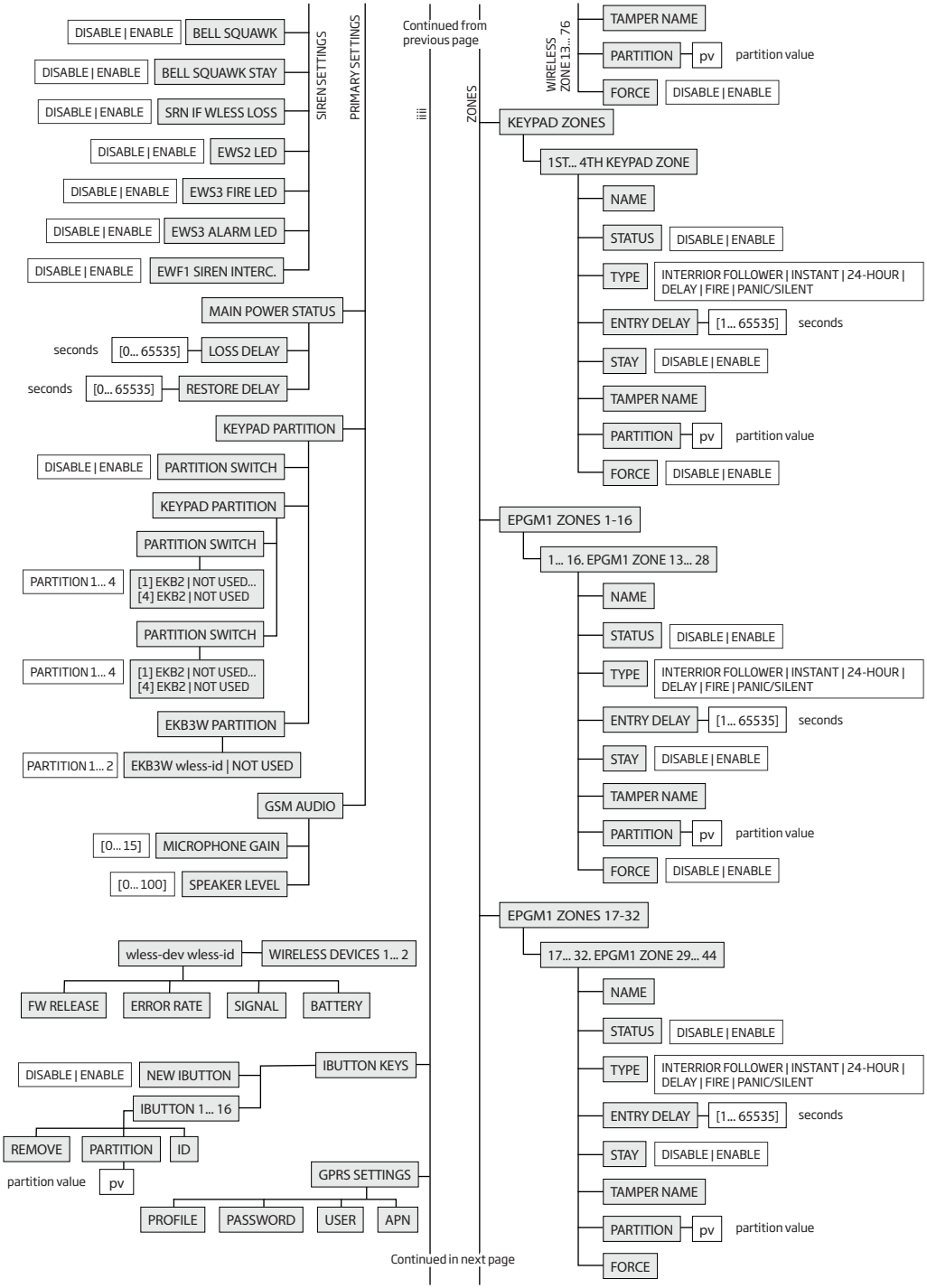
32.1.1.2. Master and User Menu Tree

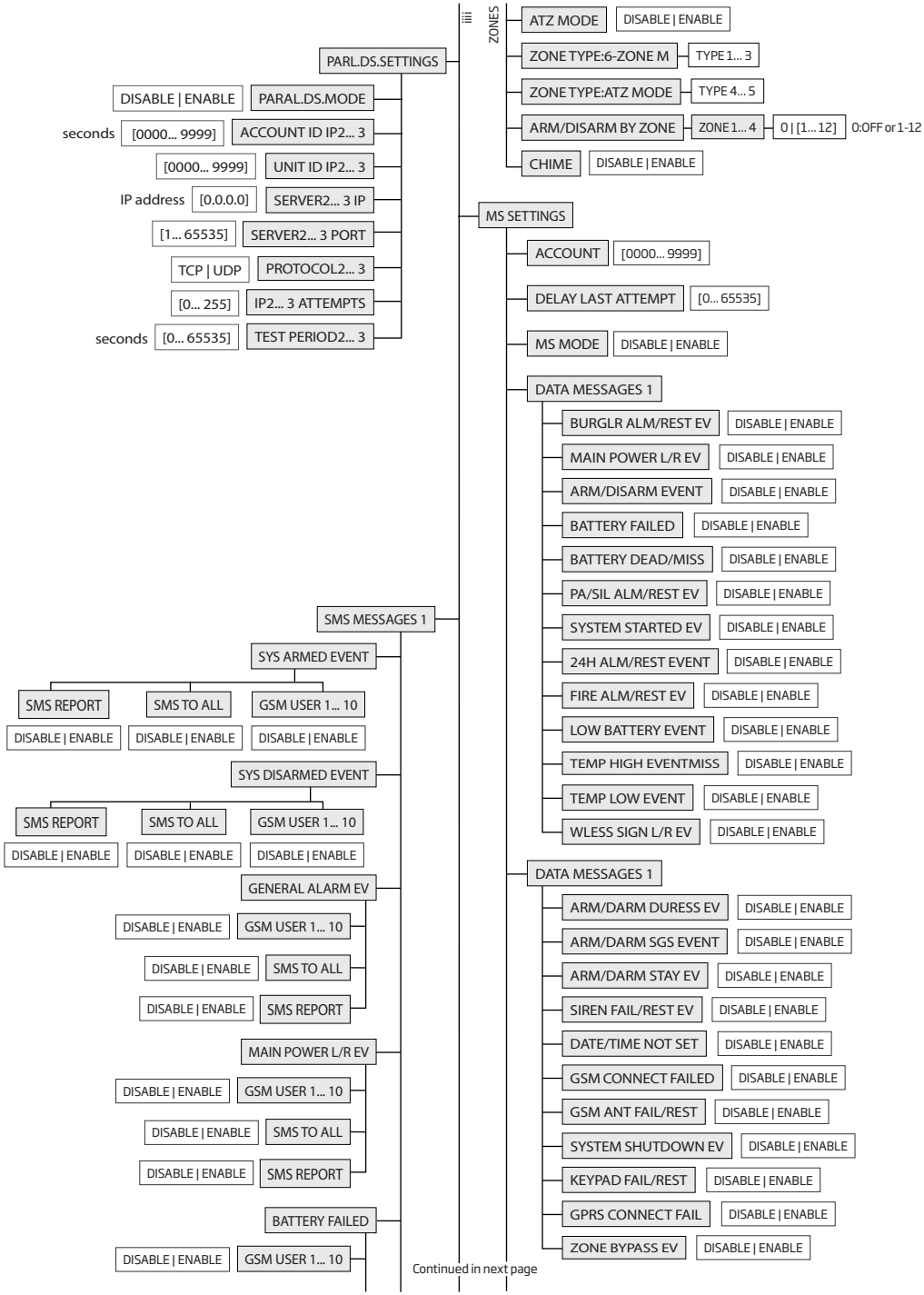


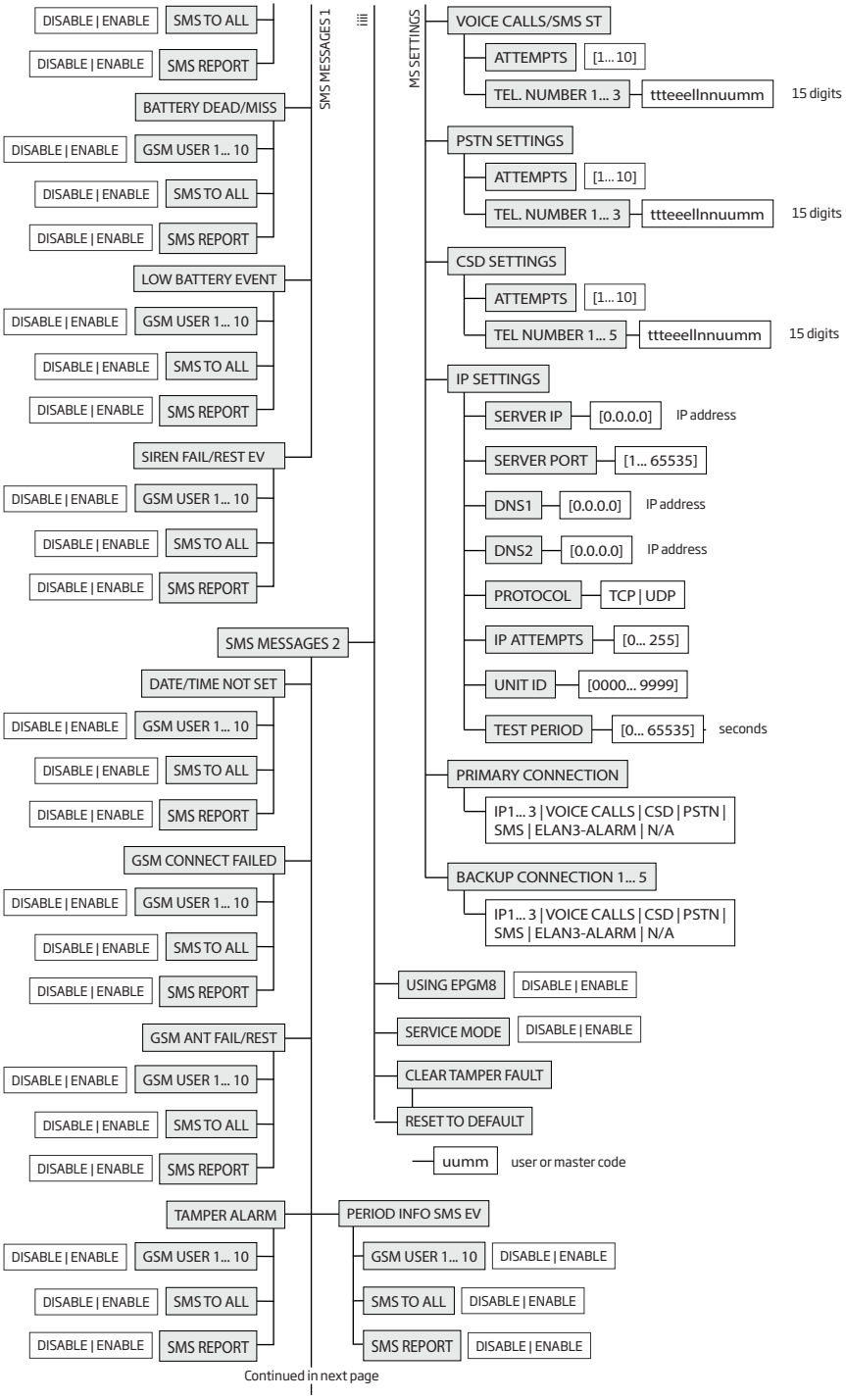

yyyy-mt-dd hh-mn
DATE/TIME SETTINGS
1. tm.p C (PRIM) | (SEC)... 8. tm.p C
TEMP SENSORS INFO
ALARM LOG
mmm
Continued from previous page
mmmm
FAULTS
BATTERY DEAD/MISS | BATTERY FAILED | SIREN FAILED | GSM CONNECT FAILED | GSM/GPRS ANTENNA FAILED | VIOLATED TAMPER | MAIN POWER LOSS | DATE/TIME NOT SET | LOW BATTERY | WLESS SIGNAL LOST | KEYPAD LOST
DATE/TIME SETTINGS
yyyy-mt-dd hh-mn
TEMP SENSORS INFO
1. tm.p C (PRIM) | (SEC)... 8. tm.p C
VIEW EVENT LOG
CODES
PGM OUTPUTS
OUTPUT 1... 12
ONBOARD OUTPUTS
NAME
STATUS
DISABLE | ENABLE
WIRELESS OUTPUTS 1... 4
NAME
STATUS
WIRELESS OUTPUT 13... 76
DISABLE | ENABLE
ALARM LOG
codes
BYP VIOLATED ZONES
MASTER CODE
CODE
[0000... 9999]
PARTITION
pv
partition value
USER CODE (2-17)
USER CODE 2... 17
CODE
[0000... 9999]
PARTITION
[0000... 9999]
USER CODE (18-30)
USER CODE 18... 30
CODE
[0000... 9999]
PARTITION
[0000... 9999]
DURESS CODE
N/A | MASTER CODE | USER CODE 2... 10
SGS CODE
N/A | MASTER CODE | USER CODE 2... 10
REMOVE CODE
[0000... 9999]

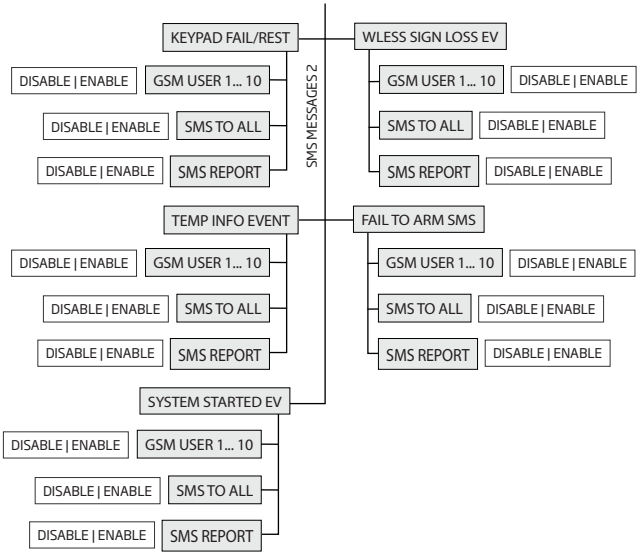
32.1.1.3. Installer Menu Tree




PRIMARY SETTINGS
SIREN SETTINGS
DISABLE | ENABLE
BELL SQUAWK
DISABLE | ENABLE
BELL SQUAWK STAY
DISABLE | ENABLE
SRN IF WLESS LOSS
DISABLE | ENABLE
EWS2 LED
DISABLE | ENABLE
EWS3 FIRE LED
DISABLE | ENABLE
EWS3 ALARM LED
DISABLE | ENABLE
EWF1 SIREN INTERC.
MAIN POWER STATUS
seconds
[0... 65535]
LOSS DELAY
seconds
[0... 65535]
RESTORE DELAY
KEYPAD PARTITION
DISABLE | ENABLE
PARTITION SWITCH
KEYPAD PARTITION
PARTITION SWITCH
PARTITION 1... 4
[1] EKB2 | NOT USED...
[4] EKB2 | NOT USED
PARTITION SWITCH
PARTITION 1... 4
[1] EKB2 | NOT USED...
[4] EKB2 | NOT USED
EKB3W PARTITION
PARTITION 1... 2
EKB3W wless-id | NOT USED
GSM AUDIO
[0... 15]
MICROPHONE GAIN
[0... 100]
SPEAKER LEVEL
wless-dev wless-id
WIRELESS DEVICES 1... 2
FW RELEASE
ERROR RATE
SIGNAL
BATTERY
DISABLE | ENABLE
NEW IBUTTON
IBUTTON KEYS
IBUTTON 1... 16
REMOVE
PARTITION
ID
partition value
pv
GPRS SETTINGS
PROFILE
PASSWORD
USER
APN
Continued from previous page
Continued in next page
ZONES
WIRELESS ZONE 13... 76
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
KEYPAD ZONES
1ST... 4TH KEYPAD ZONE
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
EPGM1 ZONES 1-16
1... 16. EPGM1 ZONE 13... 28
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
EPGM1 ZONES 17-32
17... 32. EPGM1 ZONE 29... 44
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE


ZONES
ATZ MODE
DISABLE | ENABLE
ZONE TYPE:6-ZONE M
TYPE 1... 3
ZONE TYPE:ATZ MODE
TYPE 4... 5
ARM/DISARM BY ZONE
ZONE 1... 4
0 | [1... 12]
0:OFF or 1-12
CHIME
DISABLE | ENABLE
PARL.DS.SETTINGS
DISABLE | ENABLE
PARAL.DS.MODE
seconds
[0000... 9999]
ACCOUNT ID IP2... 3
[0000... 9999]
UNIT ID IP2... 3
IP address
[0.0.0.0]
SERVER2... 3 IP
[1... 65535]
SERVER2... 3 PORT
TCP | UDP
PROTOCOL2... 3
[0... 255]
IP2... 3 ATTEMPTS
seconds
[0... 65535]
TEST PERIOD2... 3
MS SETTINGS
ACCOUNT
[0000... 9999]
DELAY LAST ATTEMPT
[0... 65535]
MS MODE
DISABLE | ENABLE
DATA MESSAGES 1
BURGLR ALM/REST EV
DISABLE | ENABLE
MAIN POWER L/R EV
DISABLE | ENABLE
ARM/DISARM EVENT
DISABLE | ENABLE
BATTERY FAILED
DISABLE | ENABLE
BATTERY DEAD/MISS
DISABLE | ENABLE
PA/SIL ALM/REST EV
DISABLE | ENABLE
SYSTEM STARTED EV
DISABLE | ENABLE
24H ALM/REST EVENT
DISABLE | ENABLE
FIRE ALM/REST EV
DISABLE | ENABLE
LOW BATTERY EVENT
DISABLE | ENABLE
TEMP HIGH EVENTMISS
DISABLE | ENABLE
TEMP LOW EVENT
DISABLE | ENABLE
WLESS SIGN L/R EV
DISABLE | ENABLE
DATA MESSAGES 1
ARM/DARM DURESS EV
DISABLE | ENABLE
ARM/DARM SGS EVENT
DISABLE | ENABLE
ARM/DARM STAY EV
DISABLE | ENABLE
SIREN FAIL/REST EV
DISABLE | ENABLE
DATE/TIME NOT SET
DISABLE | ENABLE
GSM CONNECT FAILED
DISABLE | ENABLE
GSM ANT FAIL/REST
DISABLE | ENABLE
SYSTEM SHUTDOWN EV
DISABLE | ENABLE
KEYPAD FAIL/REST
DISABLE | ENABLE
GPRS CONNECT FAIL
DISABLE | ENABLE
ZONE BYPASS EV
DISABLE | ENABLE
SMS MESSAGES 1
SYS ARMED EVENT
SMS REPORT
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SYS DISARMED EVENT
SMS REPORT
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
GENERAL ALARM EV
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
MAIN POWER L/R EV
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
BATTERY FAILED
DISABLE | ENABLE
GSM USER 1... 10
Continued in next page


SMS MESSAGES 1
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
BATTERY DEAD/MISS
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
LOW BATTERY EVENT
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
SIREN FAIL/REST EV
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
SMS MESSAGES 2
DATE/TIME NOT SET
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
GSM CONNECT FAILED
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
GSM ANT FAIL/REST
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
TAMPER ALARM
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
PERIOD INFO SMS EV
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
Continued in next page
MS SETTINGS
VOICE CALLS/SMS ST
ATTEMPTS
[1... 10]
TEL. NUMBER 1... 3
ttteeellnnuumm
15 digits
PSTN SETTINGS
ATTEMPTS
[1... 10]
TEL. NUMBER 1... 3
ttteeellnnuumm
15 digits
CSD SETTINGS
ATTEMPTS
[1... 10]
TEL NUMBER 1... 5
ttteeellnnuumm
15 digits
IP SETTINGS
SERVER IP
[0.0.0.0]
IP address
SERVER PORT
[1... 65535]
DNS1
[0.0.0.0]
IP address
DNS2
[0.0.0.0]
IP address
PROTOCOL
TCP | UDP
IP ATTEMPTS
[0... 255]
UNIT ID
[0000... 9999]
TEST PERIOD
[0... 65535]
seconds
PRIMARY CONNECTION
IP1... 3 | VOICE CALLS | CSD | PSTN | SMS | ELAN3-ALARM | N/A
BACKUP CONNECTION 1... 5
IP1... 3 | VOICE CALLS | CSD | PSTN | SMS | ELAN3-ALARM | N/A
USING EPGM8
DISABLE | ENABLE
SERVICE MODE
DISABLE | ENABLE
CLEAR TAMPER FAULT
RESET TO DEFAULT
uumm
user or master code


SMS MESSAGES 2
KEYPAD FAIL/REST
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
WLESS SIGN LOSS EV
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
TEMP INFO EVENT
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
FAIL TO ARM SMS
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
SYSTEM STARTED EV
DISABLE | ENABLE
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT

32.1.2. EKB3 - LED Keypad

Main features:

- Alarm system arming and disarming (see **12.4. EKB3 Keypad and User/Master Code**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- Visual indication by LED indicators (see **32.1.2.1. LED Functionality**).
- Audio indication by built-in buzzer..
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

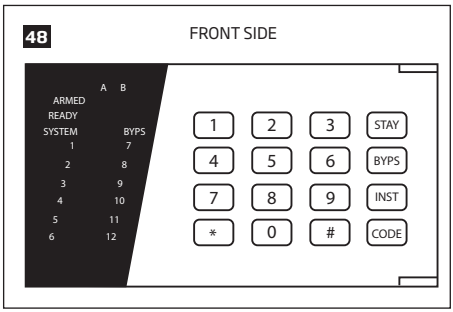
For more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download

32.1.2.1. LED Functionality

ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready – no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zone (-s)
BYPS	Steady ON - zone bypass mode
1-12	Steady ON - violated zone Z1-Z12

32.1.2.2. Keys Functionality

[BYPS]	Bypass violated zone
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[1] ... [4]	Keypad partition switch / steady ON - armed partition indication / flashing - violated partition indication
[0]	Simultaneous 4-partition arming
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/deactivation command



32.2. 1-Wire Interface

1-Wire interface is used for the system to communicate with an iButton key reader and up to 8 temperature sensors. 1-Wire interface COM and DATA terminals are ground and data respectively. When connecting single or multiple temperature sensors, the +5V terminal must be used along.

For more details on 1-Wire device wiring, please refer to **2.3.4. iButton Key Reader and Buzzer** and **2.3.5. Temperature Sensor and iButton Key Reader.**

32.3. Modules Interface

The system might be equipped with modules interface slots thus enabling to use one of the following devices at a time:

- EPGM8 - hardwired PGM output expansion module (for more details on technical specifications and installation, please refer to the latest user manual of the device located at www.eldes.lt/download)
- EA1 - audio output module (see **32.2.1. EA1 - Audio Output Module**)
- EA2 - audio output module with amplifier (see **32.2.2. EA2 - Audio Output Module with Amplifier**)

32.3.1. EA1 - Audio Output Module

EA1 audio output module enables a duplex audio connection for ESIM364 alarm system.

Main features:

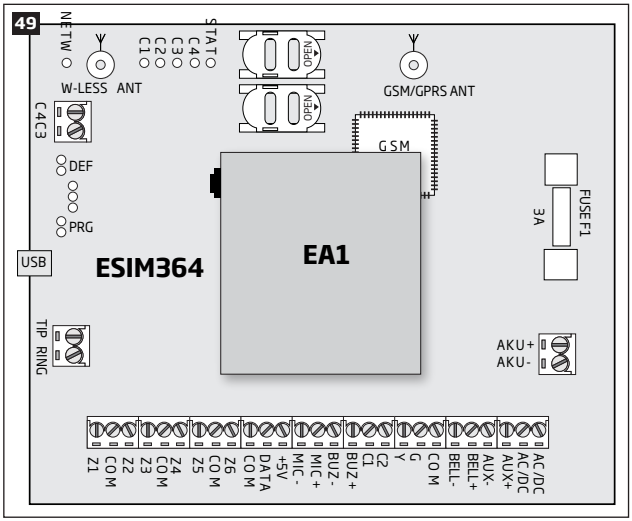
- Two-way voice conversation during a phone call;
- Possibility to connect headphones or desktop speakers.

32.3.1.1. Technical Specifications

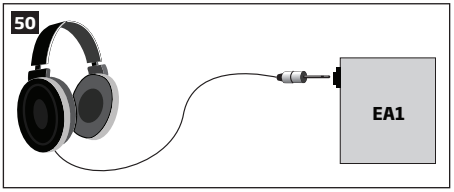
- 3,5 mm female jack
- Dimensions: 35x33x12mm (1.38x1.30x0.47in)

32.3.1.2. Installation

1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Insert EA1 pins into appropriate ESIM364 alarm system slots.



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



4. Power up ESIM364 alarm system.
5. EA1 is ready for use with ESIM364 alarm system.

32.3.2. EA2 - Audio Output Module with Amplifier

EA2 audio output module enables a duplex audio connection for ESIM364 alarm system.

Main features:

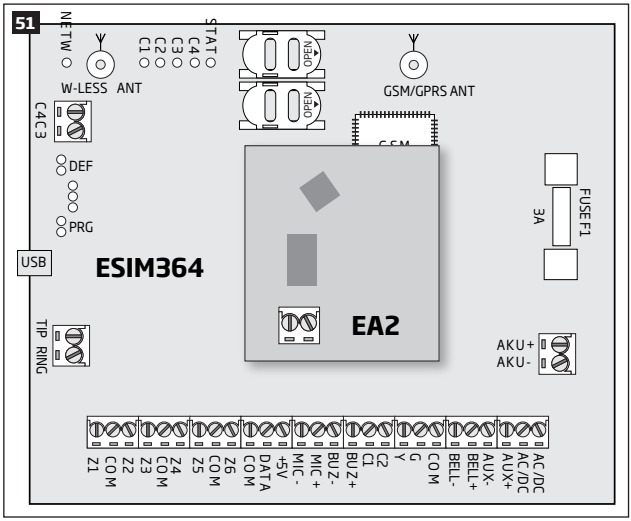
- Two-way voice conversation during a phone call;
- Possibility to connect a speaker.

32.3.2.1. Technical Specifications

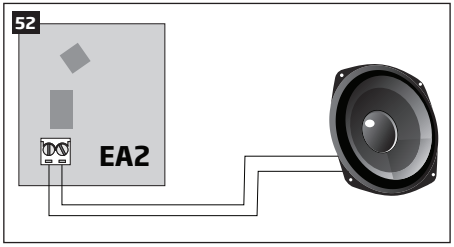
- 1W 8Ω audio amplifier
- Dimensions: 41x40x24mm (1.61x1.57x0.95in)

32.3.2.2. Installation

1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Insert EA2 pins into appropriate ESIM364 alarm system slots.



3. Connect a speaker to EA2 **Speaker** terminals.



4. Power up ESIM364 alarm system.
5. EA2 is ready for use with ESIM364 alarm system.

33. SERVICE MODE

The system comes equipped with Service mode allowing to carry out system maintenance tasks, such as detection device replacement, tamper switch installation, wireless device battery replacement without causing zone or tamper alarm when Service mode is activated. To activate/deactivate Service mode, please refer to the following configuration methods:

Activate Service mode

SMS

SMS text message content:
ssss_SERVICEMODE:ON
Value: *ssss* - 4-digit SMS password.
Example: *1111_SERVICEMODE:ON*

EKB2

Menu path:
OK → iiii → OK → SERVICE MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 67 & parameter status value:
671 #
Example: *671#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

Deactivate Service mode

SMS

SMS text message content:
ssss_SERVICEMODE:OFF
Value: *ssss* - 4-digit SMS password.
Example: *1111_SERVICEMODE::OFF*

EKB2

Menu path:
OK → iiii → OK → SERVICE MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 67 & parameter status value:
670 #
Example: *670#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

NOTE: Alternatively, the Service mode automatically deactivates when 1-hour timeout period expires or after arming the system.

34. REMOTE SYSTEM RESTART

In some critical situations, a system restart may be required. To remotely carry out system restart, please refer to the following configuration method.

Restart the system

SMS

SMS text message content:
ssss_RESET
Value: *ssss* – 4-digit SMS password.
Example: *1111_RESET*

35. EN 50131-1 GRADE 3

EN50131-1 GRADE 3

ESIM364 system complies with EN 50131-1 Grade 3 security standard requirements and comes equipped with the following features:

- 6-digit SMS password, user/master and installer codes.
- Prompt for master and installer codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.
- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

By default, the EN 50131-1 Grade 3 features are disabled. To enable them, please refer to the following configuration methods:

Set 6-digit format for SMS password, user/master and installer codes

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Prompt for master and installer codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Deny system arming if any system fault exists

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Clear tamper fault

EKB2

Menu path:
OK → mmmmmm → OK → CONFIGURATION → OK → iiiiii → OK → CLEAR TAMPER FAULT → OK
Value: *mmmmmm* - 6-digit master code; *iiiiii* - 6-digit installer code.

EKB3/ EKB3W

Enter parameter 22:
22 #
Example: *22#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

NOTE: Before clearing a tamper fault using EKB3/EKB3W, it is necessary to activate the Configuration mode (see 5.3. EKB3/EKB3W LED Keypad).

36. ELDES CLOUD SERVICES

ELDES Cloud Services is a cloud-based platform providing a user-friendly graphical interface intended for system status monitoring and control:

- Arm/disarm the system
- View system faults and alerts
- Monitor GSM signal strength, backup battery level and temperature
- Control electrical appliance connected to the PGM outputs

The connection with the platform can be established either via GPRS network or Ethernet using ELAN3-ALARM device and can be accessed via web browser and smart-phone application developed for Android and iOS-based devices (iPhone, iPad).

In order to start using ELDES Cloud Services platform, please enable it using the following configuration methods.

Enable ELDES Cloud Services

SMS

SMS text message content:
ssss_SMART:ON
Value: *ssss* - 4-digit SMS password.
Example: *1111_SMART:ON*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Once enabled, visit https://security.eldes.lt and create your personal account. Then log in to your ELDES Cloud Services account and add a device by following the step-by-step instructions provided in ELDES Cloud Services website. When adding the device to your account, you will be prompted for Cloud Services ID, which can be obtained using *ELDES Configuration Tool* software or by sending the following SMS text message to the system's phone number.

Request for ELDES Cloud Services ID

SMS

SMS text message content:
ssss_SMART_ID
Value: *ssss* - 4-digit SMS password.
Example: *1111_SMART_ID*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To disable ELDES Cloud Services, please refer to the following configuration methods.

Disble ELDES Cloud Services

SMS

SMS text message content:
ssss_SMART:OFF
Value: *ssss* - 4-digit SMS password.
Example: *1111_SMART:OFF*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: In case you DO NOT wish to use ELDES Cloud Services and your device is not associated with any ELDES Cloud Services account, please DO NOT leave ELDES Cloud Services enabled. Otherwise additional charges may apply for data traffic based on your cell phone service plan.

NOTE: Additional charges may apply for data traffic based on your cell phone service plan when using ELDES Cloud Services platform.

NOTE: ELDES Cloud Services platform will remain operational even when using Automatic or Manual dual-SIM modes.

37. TECHNICAL SUPPORT

37.1. Troubleshooting

Indication	Possible reason
Indicator STAT is off	· No main power supply · Wiring done improperly · Blown fuse
Indicator NETW is off or flashing	· Missing SIM card · PIN code is enabled · SIM card is inactive · Disconnected antenna · GSM network signal too weak · GSM network unavailable · Microcontroller is not started due to electrical mains noise or static discharge
System does not send any SMS text messages and/or does not ring	· SIM card credit balance depleted · Incorrect SMS centre phone number · No GSM network signal · User number is not added (or control from anu phone number is disabled) · SIM card changed before disconnecting main power supply or backup battery
Received SMS text message "Wrong syntax"	· Incorrect SMS text message structure · Extra space symbol could be left in SMS text message
Missing temperature indication in Info SMS text message/EKB2 keypad	· Temperature sensor not connected · Temperature sensor broken · Connection wires too long
24H and/or *Fire* zones do not work	· Specified zone must be enabled by SMS, *ELDES Configuration Tool*, EKB2, EKB3 or EKB3W
No sound during remote listening	· Microphone not connected · Improper microphone connection

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 local distributor. More up to date information about your device and other products can be found at the manufacturer's website www.eldes.lt

37.2. 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.

37.3. Updating the Firmware via USB Cable Locally

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 updated.

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

37.4. Updating Firmware via GPRS Connection Remotely

ATTENTION: The system will NOT transmit any data to monitoring station while updating the firmware remotely via GPRS network. All data messages will be lost and will NOT be transmitted to the monitoring station after the firmware upgrade process is over.

Before updating the firmware remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM CARD1 slot of ESIM364 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to ESIM364.
- Default SMS password is changed to a new 4-digit password (see **6. SMS PASSWORD AND INSTALLER CODE**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).
- APN, user name and password are set up (see **30.2.1. GPRS Network and ELAN3-ALARM**).

Initiate FOTA

ESIM364 alarm system supports FOTA (firmware-over-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. The firmware file must be located in a folder titled **Firmware**. In order to initiate the upgrade process please , send the following SMS message.

SMS

SMS text message content:
ssss_FOTA:ftp-server-ip,port,firmware-file-name.bin,user-name,password
Value: *ssss* - 4-digit SMS password; *ftp-server-io* - public IP address of FTP server where EPIR firmware file is stored; *port* - port number of FTP server (usually - 21); *firmware-file-name.bin* - name of the firmware file, allowed max. length - up to 31 character; *user-name* - user name of FTP server login, allowed max. length - up to 31 character; *password* - password of FTP server login, allowed max. length - up to 31 character.
Example: *1111_FOTA:84.15.143.111,21,esim364fw.bin,eldesuser,eldespassword*

ATTENTION: Firmware filename MUST be renamed in lowercase format before using it.

ATTENTION: Comma and underscore character is NOT allowed to use in user name, password and firmware file name.

ATTENTION: "ELDES UAB" does not run a FTP server and does not host the firmware files online. Please, contact your local distributor to request the latest firmware file.

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

37.5. Frequently Asked Questions

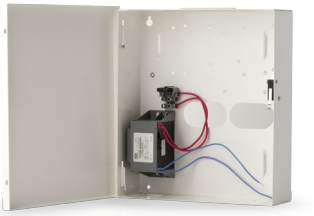
Question	Answer
1. Can ESIM364 operate as standalone device without SIM card inserted?	Yes, ESIM364 device can fully operate without any SIM card inserted. In this case you will not be able to configure and control the device by SMS and calls nor to receive any SMS reports and calls.
2. I am unable to arm the alarm system when one of the zones (some zones) is violated. 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 enable a Force attribute or use the Bypass feature in order to arm the alarm system despite the violated zone (-s) being present. Please, refer to **14.5. Zone Type Definitions** and **14.7. Bypassing and Activating Zones**.
3. When ESIM364 fully powers down my configuration 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.
4. I have a smoke detector connected to ESIM364 system. How do I reset the smoke detector when the "Fire" zone is violated?	If the smoke detector is connected to one of the ESIM364 PGM outputs you can reset it by turning the PGM output OFF and then back ON. This can be performed by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool* software. Please, refer to **18.4. Turning PGM Outputs ON and OFF**.
5. What happens if I switch backup battery pole terminals places?	Switching backup battery pole terminals places is forbidden. Otherwise this will lead to blown fuse and ESIM364 alarm system will have to be repaired.
6. 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 EKB2, EKB3, EKB3W keypads or *ELDES Configuration Tool* software. For mor details, please refer to **16. TAMPERS** or to the software's HELP section. However, due to security reasons it is not recommended to disable this feature.
7. 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.

Question	Answer
8. Does the number of EPGM1 zones duplicate when ATZ mode is activated in the system?	No, the number of EPGM1 zones does not duplicate in ATZ mode as EPGM1 module does not support ATZ mode. Only ESIM364 zones duplicate in ATZ mode.
9. I connect the wired siren to ESIM364 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.
10. 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?	Please, update *ELDES Configuration Tool* software by visiting www.eldes.lt/en/download and downloading the latest version.
11. The buzzer remains active when I disarm the alarm system using the keypad. Why?	The buzzer is intended for iButton indication only and it is not related to disarming process by keypad.
12. One of wireless devices connected to ESIM364 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 ESIM364 system. 2. Interference of other electronic equipment. 3. Physical interference (building walls, floors etc.) 4. Metal material interference.
13. 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 **2.3.2 Zone Connection Types** for more details.
14. 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?	By default, this notification is enabled. The system checks the backup battery resistance once a day and sends an SMS report to User 1 on backup battery replacement if more than 2Ω resistance is detected. For more details, please refer to **21. BACKUP BATTERY, Mains power STATUS MONITORING AND MEMORY.**
15. When I check system SIM card credit balance I see a lot of SMS delivery confirmation reports. How do I disable SMS delivery confirmation ESIM364 system?	Every time an SMS text 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 text message to all listed users simultaneously, but does not require any SMS delivery report.
16. I have set zone names and/or PGM output names containing some Cyrillic and/or non-English characters. The zone names and PGM output names do not fully fit in the SMS message. What's wrong?	According to GSM standards 1 SMS text message may consist of up to 160 Latin alphabet/English characters maximum. 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 text message than the Latin ones. It is recommended not to use any non-Latin/ non-English characters in zone names and PGM output names.
17. The configuration of added wireless keyfob EWK1 to ESIM364 system is not visible in *ELDES Configuration Tool*. What's wrong?	*ELDES Configuration Tool* version is too old. Please, update it.
18. 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.
19. 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, EKB3W or SMS text message.
20. I receive an error message when attempting to configure the device or update the firmware remotely. Whats wrong?	It appears that the device is unable to establish a communication with configuration / FTP server. Please, check the GPRS settings in ESIM364 configuration (APN, user name, password), the location of the firmware ..bin file (must be located in the FTP server folder titled **Firmware**) and the mobile internet feature presence on the SIM card used with ESIM364. If this does not solve the problem, please contact your GSM operator (and ISP - for remote configuration problems) in order to request a list of blocked TCP ports.
21. I waited for at least 5 minutes, but did not receive any SMS message confirming that remote configuration via GPRS connection has stopped. What's wrong?	1. Send the *ssss_endconfig* SMS text message. 2. In *ELDES Configuration Tool* software press Disconnect button and repeat the procedure as described in **5.4.1. Remote Connection.**
22. The SMS password is changed and I have User 1 phone number added. However, whenever I send a text message, such as *ssss INFO* the system always replies with „Wrong password". What's wrong?	Most likely you have wrong character encoding set up in your SMS text messaging settings on your smart-phone. Please, ensure that you have GSM Alphabet selected, NOT Unicode or any other type of character encoding.

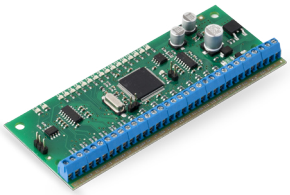
38. RELATED PRODUCTS

EKB2 - LCD keypad

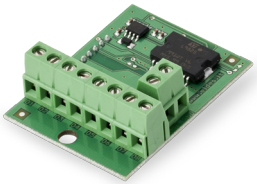
EKB3 - LED keypad



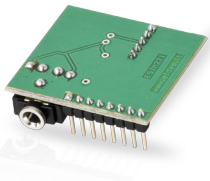
ME1 - metal cabinet



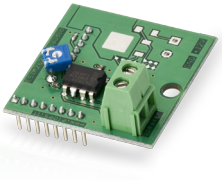
EPGM1 - hardwired zone and PGM output expansion module



EPGM8 - hardwired PGM output expansion module



EA1 - audio output module



EA2 - audio output module with amplifier

DS1990A-F5 - iButton key

DS18S20 - temperature sensor

ED1T - plastic enclosure with iButton key reader and temperature sensor

EWS2 - wireless external siren

EWK1 - wireless keyfob

EWF1/EWF1CO - wireless smoke/CO detector

EKB3W - wireless LED keypad

EWK2 - wireless keyfob

EWD2 - wireless door contact/shock sensor/flood sensor

EWS3 - wireless indoor siren

EWR2 - wireless signal repeater

EW2 - wireless zone and PGM output expansion module

EWK2A - wireless keyfob

EWP2 - wireless motion detector

Vinson DS18B20 - digital thermometer
with 3m (9.84ft) wire

Made in the European Union
www.eldes.lt