

Alarm Control Panel CBP32

(ver. 1.20, 07.2020)

Installation and operation manual

INTRODUCTION	2
OPERATING OPTIONS WITH CBP32 CONTROL PANEL	2
1. <i>Arming and disarming the system using a remote</i>	3
2. <i>Arming & disarming using GSM phone</i>	3
3. <i>Emergency arming & disarming alarm from CBP32 panel buttons</i>	3
<i>Arming the system with bypassing selected alarm zones.</i>	4
CBP32 SELECTED FUNCTIONS DESCRIPTION	4
ALARM ZONES MONITOR	4
EMERGENCY POWER BACKUP	4
ANTI-SABOTAGE PROTECTION OF THE PANEL CABINET	4
OPERATION WITH WIRED ALARM DETECTORS	5
OPERATION WITH REMOTE CONTROL TRANSMITTER (REMOTE)	5
OPERATION WITH EXTERNAL WIRELESS SIREN	5
INTERNAL GSM MODULE FUNCTIONS	5
CBP32 PANEL CONFIGURATION AND FIRMWARE UPDATE USING PC	5
MAIN MENU AND PROGRAMMING THE CBP32	6
ALARM MEMORY	6
FAILURES	6
SYSTEM STATUS	6
SERVICE SETTINGS	6
1. <i>Event Memory</i>	6
2. <i>Password Change</i>	7
3. <i>Zone Settings</i>	7
4. <i>Outputs Settings</i>	8
5. <i>System Users - adding, removing and editing a user</i>	9
6. <i>Times Setting</i>	11
7. <i>GSM Functions</i>	11
8. <i>Auxiliary functions settings.</i>	14
9. <i>System arming signalling modes.</i>	15
SETTINGS RESET	16
RESETTING PASSWORD OF USER 1.	16
RESTORING CBP32 TO FACTORY SETTINGS (DEFAULT SETTINGS).	16
ALARM SYSTEM INSTALLATION	16
POWER SUPPLY: SELECTION OF TRANSFORMER AND BATTERY	18
SEQUENCE OF POWER SUPPLY CONNECTION	18
WIRED DETECTORS INSTALLATION	18
EXAMPLE OF ALARM SYSTEM WITH CBP32 CONTROL PANEL	19
WIRED DEVICES CONNECTION DIAGRAMS WITH CBP32 CONTROL PANEL	20
SPECIFICATION	21
MANUFACTURER'S LIMITED WARRANTY	22
FREQUENTLY ASKED QUESTIONS	23

INTRODUCTION

Elmes Electronic CBP32 is a programmable alarm control panel with integrated mobile phone module, designed for use in anti-theft, intrusion detection, access control and remote control installations. It operates with Elmes Electronic made wireless detectors, RP501 transmitter-receiver set, remote control transmitters and any wired detectors. The panel supports up to 16 system users, up to 6 wired detectors and up to 32 wireless detectors. It features eight programmable all-purpose control outputs out of which two are high current and six are OC type outputs. The panel can be programmed with the use of buttons and LCD display placed on board of the panel. In addition, the control panel can be programmed, configured and firmware updated with the use of personal computer (PC). CBP32 control panel is AC mains transformer powered with 17-18VAC secondary output and 12V battery as backup power.

General features of CBP32 control panel:

CAUTION! *This control panel has been designed to be as effective as possible. However, there are circumstances that alarm system may fail to operate as expected for variety of reasons. Users and installers are warned that radio signals from wireless detectors and sensors may not reach the CBP32 panel under all circumstances. Metal objects placed on radio transmission paths, deliberate jamming or other radio signal interference can seriously reduce operating range.*

- integrated mobile GSM module for SMS & CLIP(*) arming, disarming and notification,
- operation with security monitoring centre in internet GPRS communication mode, data format Ademco Contact ID in SIA DC-09 frame with AES-128 encryption or without encryption,
- 32 wireless and two wired parametric alarm zones with user defined names,
- six parametric inputs for connecting wired detectors,
- identification of up to 16 users,
- panel programming with buttons and LCD on board or, with personal computer (USB),
- arming and disarming of the panel with hand held remote or GSM mobile phone,
- wide range of alarm zone types,
- functional modes of partial arming of the control panel (day and night modes),
- panic and robbery alarm function (call for help) activated by a remote,
- memory of the last 256 events with event type and the time of its occurrence.
- acoustic signalling (beeps) of "chime" type zone violation,
- monitoring of wireless detectors and external devices presence,
- operation with Elmes Electronic WSS wireless external siren & strobe,
- two parametric outputs S1 and S2 (**), rated up to 700mA at 12VDC, with electronic overload current protection and anti-sabotage wires cut or short circuit protection,
- control outputs O1÷ O6 (**) are open collector type (OC) and rated up to 100 mA,
- outputs S2 and O1÷ O6 are programmable and all-purpose type,
- outputs feature programmable set on timing in the range from 1 up to 999 seconds,
- radio jamming sabotage protection signalling in zone 30,
- RF signal and interference level monitor in form of bar graph line displayed on panel's LCD,
- optional panel configuration and firmware update with personal computer (PC),
- powering of the panel with 17-18VAC alternating current,
- control panel backup power with 12V battery of 1.2 ÷ 17Ah capacity.

(*) CLIP - *Calling Line Identification Presentation* – a GSM feature meaning that user can arm/disarm control panel just by making a call to its phone number. Also, the panel can notify user of alarm by calling the user/operator phone number.

(**) symbols used on the panel board.

OPERATING OPTIONS WITH CBP32 CONTROL PANEL

Operating alarm system with CBP32 control panel mean system arming and disarming with periodical check up of its functioning state. Arming and disarming is made by remotes or phones registered in the system. The use of GSM phone allows notification of failures and state of the system, remote blocking of alarm zones and controlling outputs of the panel, in addition to arming and disarming of the system. State of the system, i.e. its armed mode, disarmed or failed to operate properly is SMS notified on SMS request send by the user.

System failure is notified by SMS to the user, beeps by the build in beeper and flashing of the Failure LED on the panel board. Checking the cause of the failure may be done by SMS or, on the panel board by long pressing OK button.

Browsing the control panel menu is made by using the following buttons:

- ▲◀▶▼ - menu navigation cursors,
- OK - menu entry and setting acceptance,
- C - CANCEL button for cancelling setting and exit.

Alarm system arming and disarming

Arming and disarming may be made by the use of hand held transmitter (called later "remote") or GSM phone registered in the system. It is also possible to it with the use of buttons on the control panel board. In the case of GSM phone, arming and disarming is made by sending an appropriate text message (SMS) or call (CLIP) to the phone number of the panel. Every disarming of the system results in immediate stop of alarming (setting OFF alarm sirens).

1. Arming and disarming the system using a remote

The CBP32 panel can operate with Elmes Electronic made remotes in two ways (see pt. 5.7):

1.1 Remote arms and disarms the system.

Control panel may be armed/disarmed with the use of one, two or four button remote. With the use of one button remote alarm system can be armed and disarmed alternately. With two buttons remote, the second button may also arm the system in night mode. Four buttons remote features buttons for all optional modes of system arming (see pt. 5.7).

No matter which remote model, the use of standard system arming button triggers one signal pulse on one or more outputs: S1, S2, O1 or built-in siren (see pt. 9 on page 16) and the countdown of exit delay time starts. The system arms on the delay passage. The use of system disarm button triggers two loud sound signals and the system disarms. If, while in the armed state, intruder alarm occurred then five loud sound signals will be produced.

Arming system in night mode is similar to standard arming (exit delay is also used) with the difference that signal pulse will appear on one of outputs S2, O1 or on buzzer. Arming in day mode is different, it is instant and no exit delay is used.

1.2 Remote activates entry zone delay only.

In this mode pressed remote button activates entry delay in zone type "remote delayed" for pre-defined delay time, signalled by two loud beeps. Now, system should be disarmed using wireless keypad KB1. Violation of "remote delayed" zone while in entry delay countdown without system disarming will set up intruder alarm after passage of the delay.

2. Arming & disarming using GSM phone

The GSP32 control panel may be remotely armed and disarmed by SMS command or CLIP call from any registered phone number listed in the panel memory. Phone numbers for the panel control and monitoring are registered for system users in Service Settings pt. 5.5.

3. Emergency arming & disarming alarm from CBP32 panel buttons

This operating method is not recommended as requires opening the control panel cabinet. Nevertheless, in case of emergency, e.g. no access to system registered phone or lost remote, there are two possible methods of system arming/disarming using the panel buttons:

1. If "day/night" mode is set OFF (see pt. 8.5 menu) - by entering user's password (by default: ▲▲▲▲) followed by OK will arm the system or, disarm the system if it was armed. Exit delay time counts down starts prior to system is armed.

2. If "day/night" mode is set ON (see pt. 8.5 menu) - by entering user's password followed by OK will allow selection of one of four methods of system arming:

"▲ - disarm" - disarming the alarm system – "disarmed" status appears on display.
Anti-sabotage zones "24h" remain armed.

"◀ - arm" - arming the system. On the end of the exit delay (signalled acoustically and optically with displayed time countdown on the LCD panel), all alarm zones except blocked are armed. "Armed" status appears on display.

- “▶ - day” - partial arming in day supervision mode. The zones earlier defined as “day armed” and the “24h” zones are armed (as in pt. 3.1). The “day mode” message appears on display.
- “▼- night” - partial arming in night supervision mode. At the end of exit delay (signalled acoustically and optically) all alarm zones are armed, except for blocked zones and zones earlier defined as „night disabled” (as in pt. 3.1.). The “night armed” message appears on display.

Arming the system with bypassing selected alarm zones.

If, in the course of arming the system, one of the zones is violated, the reaction of the system depends on whether the zone was earlier defined as “bypass” type (see pt. 3.1.g) or not:

- if the zone function is defined as “bypass” (Y) – the system generates 3 beeps on arming using remote or panel buttons and waits 8 seconds for user’s decision whether to arm the system bypassing violated zone. Acceptance with the use of remote or panel OK button arms the system bypassing that zone. If no action is detected (>8s) arming procedure is cancelled. Arming with the use of mobile phone will arm the system and SMS notification will be send informing of the bypassed zone.
- if the zone is not defined as “bypass” type (N) – the system generates 3 beeps on arming using remote and will not arm. When arming using panel buttons displays message “Violated zones” with zone name and system will not arm. In that case, the cause of the zone violation should be cleared and a new arming should be made. While arming by mobile phone, the system will respond by sending SMS with information on violated zones.

See also S.S. pt. 9 – “System arming signalling modes”

CBP32 SELECTED FUNCTIONS DESCRIPTION

Alarm zones monitor

CBP32 control panel allows checking operation of all detectors by displaying all alarm zones simultaneously. To activate this function button “◀” must be pressed and hold down until two 16 bar graph lines scale appear on the LCD panel displaying status of all 32 alarm zones of the CBP32 control panel. Any violated zone produces “*” mark (star) to be momentarily displayed on the LCD at dot position corresponding to zone number in which violation was detected. Sabotage activation displays mark “S”. Function deactivation is made by “◀” button.

Emergency power backup

The control panel is designed to operate with typical 12V sealed lead rechargeable battery used for alarm system application. The battery charging current is user set by jumper “ISET” on the panel board. For 1.2Ah battery capacity the jumper should be set to 130mA current and for typical batteries of higher capacity, e.g. 5Ah, 7Ah or 17Ah, the jumper must be set to 450mA charging current. In order to protect battery against destructive discharge, the panel disconnects the battery automatically, if battery voltage drops below 10,2V level.

In addition, the control panel performs regular battery tests. Detected battery failure, or battery absence are notified to the user/alarm system operator.

Anti-sabotage protection of the panel cabinet

In order to enable anti-sabotage protection of the control panel cabinet TAMPER switch of the cabinet should be connected in series with 1kOhm resistor to any of six wired detector input zones of the panel (see example on diagram 5), then unblock the zone using buttons on the panel board and close cabinet cover. Since now, any opening of the cabinet cover will generate sabotage alarm. If the panel cabinet cover/door must be opened for any reason, the only way to do it without generating sabotage alarm, is to block the sabotage zone by sending appropriate SMS command (pt. 5.6.9).

Operation with wired alarm detectors

CBP32 provides six input zones Z1+Z6 for connecting wired alarm detectors with NC (normally closed) outputs. The wired inputs are shared with panel's wireless inputs 1+6 and may be operated together (see pt. 3.3). The wired detectors are connected to the panel according to diagram 2 (resistors 1k and 3k3 Ohm are supplied with the panel).

NOTICE! Zones Z1+Z6 are blocked by default.

Operation with remote control transmitter (remote)

The use of Elmes made remotes with Elmes CBP32 control panel allows remote arming/disarming of alarm system as well as enables personal panic alarm. Detailed description of using a remote with the panel may be found in pt. 1 of Operating CBP32 Control Panel chapter. Programming (learning) a remote to a user of the control panel is described in pt. 5.3 of menu "Users". Activation of the panic alarm is made in pt. 8.6, while pt. 9.4 and pt. 9.5 of the service settings are used for setting how the control panel will signal the use of a remote.

Operation with external wireless siren

The Elmes CBP32 wireless panel can operate with dedicated external wireless sound and strobe siren Elmes WSS with periodical siren presence check test. The siren is powered by external mains power pack (delivered with the siren) that recharges internal sealed battery being siren's main source of power supply. The following steps are required to set Elmes WSS wireless siren to operate with the CBP32 control panel:

1. Learn the siren to alarm zone line 29 of the CBP32 panel by selecting detector learning mode (see 3.3) and activating the siren to transmit RF signals in one of the three ways, as below:
 - a. Connecting siren's battery while mains power supply is off.
 - b. Connecting or disconnecting mains power while battery is connected.
 - c. Activating siren's housing top cover sabotage switch.
2. Set required alarming time at S1 of the panel that equals to alarming time of the wireless siren (pt. 4.3).
3. Set in pt. 6.4 required time interval (1 to 99 minutes – 20 minutes as standard) for wireless siren presence checking frequency and enable radio link testing (pt. 8.2).
4. Choose the way alarm system signals failure of radio link between wireless siren and the control panel. If the system is expected to set on loud alarm along with failure indication, the function in pt. 8.8 should be set ON. If only failure indication is required then the function should be OFF.
5. If control panel is armed/disarmed by a remote, its use may be signalled by signal pulses on external siren (pt. 9.4 and 9.5).

NOTICE! To avoid loud sabotage alarm during external siren's installation or maintenance temporarily disable (block) alarm zone 29.

Internal GSM module functions

The following functions are available when using CBP32 panel with active SIM card: remote arming and disarming of alarm system by SMS or CLIP call; requesting system status notification; remote disabling (blocking) of alarm zones, SMS notifications send to up to 8 mobile phones on alarms, arming/disarming, AC supply failure and return as well as system failures. The notifications include information of the source of the event. In case of alarm and the control panel makes also a CLIP call to registered phone numbers. CBP32 control panel may also operate with security monitoring centre by sending SMS messages or by GPRS internet communication notifications using SIA DC-09 protocol.

Control panel outputs may be toggled on/off by SMS command and may control variety of devices such as switching on/off lighting, heating, etc. The devices should be controlled via external power relay as shown in diagram 3.

CBP32 panel configuration and firmware update using PC

The CBP32 control panel can be easily configured and firmware updated with the use of Windows® based PC (Personal Computer). To connect the panel to personal computer a USB interface cable

with one mini USB plug is needed (ordered separately). Proper cable installation is red LED signalled on the panel board. For data transmission installation of virtual series COM port drivers at the PC are necessary. In recent Windows® versions the drivers load automatically. The COM port drivers as well as dedicated “CB32 Configurator” software for PC are free for download from the CBP32 panel manufacturer web site: www.elmes.pl.

Before any data is sent to or received from the CBP32 panel, the following steps should be followed:

1. In the options of “CB32 Configurator” new serial COM port must be selected that appears on the list of COM ports, after connecting the USB cable to PC.
2. By holding down button ▲ at power on, the panel is forced to set up communication mode with PC. Flashing “?” sign on the panel’s LCD confirms the mode has been entered.

MAIN MENU AND PROGRAMMING THE CBP32

To access the main menu of the CBP32 panel press and hold down OK button for more than two seconds. Navigate the menu using vertical and horizontal cursor buttons ▲, ◀, ▶, ▼. Confirm option selection by OK button while annulations and exit with C button. Exit menu with C button or, automatically, if no user activity is detected for more than 90 seconds. Main menu consists of four submenus:

Alarm Memory

In this menu details of the latest alarms are displayed: date, time and zone of the alarm(s) source. The use of ▲ ▼ buttons selects earlier or later events respectively, while the use of ◀ ▶ buttons selects between alarm type and alarm source, e.g. “Intruder alarm” ↔ “kitchen”.

Failures

This menu is designed to view the causes of the failures signalled on the control panel by flashing yellow “ALARM” LED. Failures signalled on the control panel include:

- Mains power supply failure (no mains).
- Backup rechargeable battery absence or failure.
- Failure of communication with wireless detectors.
- Detector’s low battery (replacement need).
- GSM module network connection failure.

▲ ▼ buttons are used to scroll through failures, if many.

The “ALARM” LED stops flashing when cause of failure is cleared.

System Status

In this menu there are two submenus available:

1. Displays level of received GSM signal by built-in module in graphic mode. Minimum of four bar level is required for proper functioning. Lower lever requires change of the panel placement.
2. Control panel firmware version is displayed.

Service Settings

Access to Service Settings menu is enabled only if the control panel is disarmed and upon entering a valid password code confirmed by OK button. Factory setting of the password for the user No.1 is „▲▲▲▲”. Exit from the menu and cancelling entries are made by the C button. Users Nos. 1-4 (administrators) have access to all functions whereas other users may access functions 1-2 only. All editable service settings available in this menu are described further.

1. Event Memory

Service settings → Event Memory

This menu allows viewing detailed information on last 256 events that occurred in the system (alarms, failures, arming, disarming, errors, etc.). Event memory cannot be edited, and allows only viewing the event details in the sequence of their occurring date and time. Buttons ▲ ▼ select an earlier or later event while ◀ ▶ buttons select between type of event and its source, e.g. “Arming” ↔ “John”.

2. Password Change

Service settings → Password change

This menu allows changing user's own password. Password of other users can be changed in the "Users" menu (see pt. 5). After accessing this menu "Enter password" prompt appears. Enter new password containing 3 to 6 signs ▲, ◀, ▶, ▼ and then press OK. When the "Repeat password" prompt appears, enter the new password again and press OK. The new password replaces old one. In case of entering an existing or incorrect password "Wrong password" message appears.

3. Zone Settings

This menu contains number of submenus. Entering any submenu with ▲▼ buttons selects zones while ◀▶ buttons select between zone number or zone name, e.g. "Zone no 1" ↔ "Kitchen". After selecting a zone confirmed by OK following submenus are accessed:

3.1. Alarm zone function.

Service Settings → Zone Settings → Zone function

This menu of CBP32 control panel allows assigning special functions to alarm zones. Buttons ▲▼ select one of the functions described below while ◀▶ buttons allow setting the function ON (Y) or OFF (N). OK button accepts the selection while the use of C button cancels changes and exits the menu without saving changes.

- a) "24h" - 24 hour zone, e.g. anti-sabotage zone (permanently armed),
- b) "day armed" - zone armed in day supervision mode selection,
- c) "night disabled" - zone disabled in night supervision mode,
- d) "remote delayed" - entry zone with delay set on by a remote;
- e) "delayed" - standard entry zone with delay;
- f) "chime" - door chime feature generates signal pulses at one of selected outputs, or beeps on panel's internal buzzer on zone violation (see pt. 9.6).
- g) "bypass" - zone that can be left disarmed if violated on system arming.
- h) "silent alarm" - zone violation sets on silent panic alarm (no siren sounds) and panel's outputs type "silent alarm" will set on. If the zone is required to be armed all the time, function "24h" must be on as well.

A standard zone has functions a + c set off and supervises when the system is in "armed" or "night armed" mode and does not supervise when system is "disarmed" or "day armed".

IMPORTANT: Zones can have assigned more than one special function, but some functions exclude others. In that case, only one selection is valid, e.g.:

- if a zone is "active 24h" then functions such as "day armed", "night disabled" have no meaning.

Examples of zones with assigned functions:

- "chime" zone generates two beeps sound signal on every violation of the zone (e.g. notifying store personnel of customer entrance).
- "remote delayed" zone – when remote's button is pressed "entry time" countdown is started and the zone is not active. Its violation will not trigger an instant alarm but only after "entry time" has passed. It allows the user to disarm alarm system with the use of valid password input on wireless keypad KB1.
- "delayed" zone – its violation (by entering the zone) triggers "entry time" countdown, during which the system must be disarmed to prevent from system intruder alarm.
- Basement or a garage zone can be "day armed".
- A „bypass" zone allows arming the alarm while intentionally leaving e.g. window opened protected by CTX detector (see "System Arming").

3.2. Zone name.

Service settings → Zone Settings → Zone name

This menu allows alarm zones used in the system to have user defined up to 16-character name, e.g.: kitchen, living room, office, Mark's Room, etc. Upper and lowercase letters, digits, space and characters "-", "." are accepted.

Buttons ◀▶ select the successive letters position of the name while the ▲▼ buttons browse character table for selection. Accept name with OK button. Use C button to exit the menu.

3.3. Learning wireless detectors to control panel.

Service settings → Zone Settings → Learning detectors

It is recommended to learn wireless detectors starting from zone 7 (*).

After selecting a zone number “OK-remove” prompt appears on display, if detector is already learned to the zone. Pressing OK button deletes detector in the zone. If zone is vacant, “OK-learn” will appear on the LCD. Pressing OK button starts learning detector to the zone. In response to the “Awaiting trans. 1” and “Awaiting trans. 2” prompts, two successive alarm transmissions must be triggered in detector (**). Correct learning will be followed by “OK-correct” message. Errors are signalled by 3 beeps and “Program error” message. The use of C button exits the menu.

(*) Zones 1÷ 6 are intended for wired and/or wireless detectors installation and are disabled (blocked) by default. If wireless detector is to be learned to any of these zones, it must be enabled (unblocked) and its wire input shorted to ground (COM) with 1kOhm resistor (supplied). If a wired detector is to be installed in that zone as well, which is possible, then it may create ambiguity issue when both detectors signal zone violation simultaneously. Therefore, it is not recommended to install in these zones detectors with permanent set on output, e.g. door open magnet detector, but detectors with momentary set on, e.g. PIR movement detector.

(**) IMPORTANT! Wireless detectors cannot be learned to the panel by the use of sabotage TAMPER switch to activate radio transmission. For detailed information on how to learn any Elmes detector to CBP32 control panel please refer to instruction manual of the detector.

Description of wired detector installation in zones 1÷ 6 can be found on page 18.

3.4. Zone disabling.

Service settings → Zone Settings → Zone disabling

Zone number is selected with ▲▼ buttons while buttons ◀▶ disable (block) and enable the zone. Accept selection with OK button. Exit the menu with C button.

3.5. Radio range test.

Service settings → Zone Settings → RF range test

To assess the level of radio reception of signals received from detectors, the most distant detectors in particular, the CBP32 panel is provided with “RF range test” function allowing the received signal level to be displayed on 16 bar graph scale of panel's LCD.

After entering this menu all RF signals in the 433.92MHz radio band will be displayed in form of bar graph. The detectors should be triggered to send alarm transmissions. The longer the distance of the detector from the control panel, or the greater difficulty in radio waves propagation, the lower the level of received signals and the length of the displayed bar graphs. If the number of displayed bars is lower than three it should be assumed it does not guarantee reliable alarm operation. The location of detectors or the control panel should be changed in search for better RF reception or, Elmes Electronic made repeater TRX should be installed to prolong operating range of wireless detectors.

The “RF range test” function allows also assessing levels of all local RF signals in the 433.92MHz band, also those that can interfere and disturb operation of the wireless alarm system. The test should be carried out prior to permanent installation of alarm devices or, in tracing causes of short operation range. To find out any interfering signals, the LCD 16 bar graph scale readouts should be observed without activation of own detectors. Frequent or continuous unknown RF signals received and signalled on the control panel display indicate close presence of other RF devices operating in the same RF band. If level of these signals exceeds three bars displayed in the “RF range test” function and their occurrence is frequent, acceptable signals from detectors may not be received and the alarm system may fail to operate properly.

4. Outputs Settings

This menu contains some submenus. Entering any of them select output number with ▲▼ buttons while the use of OK button opens submenu:

4.1. Output types.

Service Settings → Outputs → Output type

This menu allows allocation of wired outputs of the control panel. Outputs S1 and S2 are high current with up to 700 mA rating, short circuit protected and providing 12VDC on output set on. These outputs may be sabotage protected (see pt. 8.3).

Outputs O1+O6 are low current draw, OC type with up to 100 mA rating. Overload of these outputs, such as direct connection to +12V, may cause their damage.

Output S1 is “alarming” type and its function cannot be changed. It is intended for connecting an external siren. The remaining outputs may have assigned the following functions:

“alarming”	for connection of outdoor/external alarm signalling devices, e.g. external siren or/and strobe;
“AC power failure”	signalling 230VAC power supply failure/cut off
“arming”	output active when system armed mode is armed or night armed and inactive when system is disarmed or in day armed mode;
“failure”	signalling any failure state in system (also 230VAC power failure)
“SMS controlled”	output controlled by SMS. Examples of SMS controlling panel output named PUMP are shown below: „PUMP T” - permanently sets output on; „PUMP N” - sets output off; „PUMP” - sets output on for time specified in pt. 4.3; „PUMP 15” - sets output on for 15 seconds; „PUMP 10:30” - sets output on for 10 minutes and 30 seconds; „PUMP 1:00:00” - sets output for 1 hour. Output maximal set on time is 18 hours, 12 minutes and 15 seconds.
„silent alarm”	output will be set on, if zone type “silent alarm” has been violated (pt. 3.1h), or silent panic alarm is activated (pt. 8.6).

Example: if output O2 is “arming” type and the output connects LED to detector’s supply output (AUX) in series with 1kOhm resistor then it will stay lighted on for as long as the system is armed offering additional signalling or warning option.

Outputs S1, S2 and O1 may also pulse signal system arming and disarming, violation of zone with “chime” function and exit time countdown (see pt. 9).

Output type is defined by accessing the menu, selecting output number with ▲ ▼ buttons, accepting with OK, selecting output type with ▲ ▼ or ◀▶ buttons, accepting with OK button.

4.2. Output name.

Service Settings → Outputs → Output name

This menu allows every output to have any up to 16-character long name e.g. “OVEN”, “Lamp”, etc. Upper and lower case letters, digits and “-./” signs are accepted while “space” sign is not allowed. Instead of sample name “lamp garden” a name “lamp-garden” should be used. Output’s names are used only if controlled by SMS.

In the menu ◀▶ buttons are used selecting character position of the name and ▲ ▼ buttons selecting appropriate character. Defined name is accepted with OK and exit menu with C.

4.3. Outputs set on time.

Service Settings → Outputs → Output time

This menu is used to define individual set on time, ranging from 1 to 999 seconds, of outputs type “alarm”, “silent alarm” and “SMS controlled”. Set on time defined for any other output type is irrelevant. Set on time defined for output S1 also defines set on time for external wireless siren (Elmes Electronic WSS), if installed.

5. System Users - adding, removing and editing a user

This menu contains submenus. Entering any submenu with ▲ ▼ buttons selects system user number while ◀▶ buttons select between displaying user number or user name, e.g. “User 1” ↔ “John Dutch”. Accept user selection with OK and pass on to submenu:

5.1. Setting and editing user password.

Service Settings → System Users → Password

Please follow detailed instructions in “Password Change” menu (S.S. pt. 2).

To delete user's password press OK button when "Enter password" prompt appears. On next prompt "OK-delete password" press OK button again. "Password deleted" message confirms password is deleted.

5.2. User name change.

Service Settings → **System Users** → **Name**

Please follow detailed instructions as in "Zone name" menu (S.S. pt. 3.2)

5.3. Remote transmitter learning and deleting.

Service Settings → **System Users** → **Learning a remote**

In this menu a remote is added to user or deleted. Please follow detailed instructions in "Learning detectors" menu (S.S. pt. 3.3). In order to learn all buttons (2 or 4) of multi channel remote to the control panel, the last button must be used while learning the remote, i.e. second or fourth. Operation mode of the remote can be set on in pt. 5.7 of Service Settings.

5.4. Disabling user.

Service Settings → **System Users** → **Disabling user**

Please follow detailed instructions as in "Zone disabling" menu (S.S. pt. 3.4). After disabling a user, its remote and password are inactive. In order to disable user's control of CBP32 panel by SMS or CLIP, the functions should be set off in pt. 5.6.9 and pt. 5.6.10 of S.S.

5.5. Mobile phone number.

Service Settings → **System Users** → **Phone number**

This menu allows entering user's mobile phone number. The number must be preceded by national dialling code number, without the "+" sign. Example: 33xxxxxxx for France.

5.6. Mobile phone functions.

Service Settings → **System Users** → **Phone functions**

This menu allows selection (Y/N) of notifications, messages, commends and SMS/CLIP functions required to be active operating CBP32 control panel with user's GSM phone:

- 1) **SMS on alarm** - sending SMS on alarm set on;
- 2) **SMS on arming** - sending SMS to control panel phone number: "arm" to arm and "disarm" to disarm alarm system;
- 3) **SMS on powering** - sending SMS on mains power failure and return;
- 4) **SMS on radio link off** - sending SMS on radio link failure;
- 5) **SMS on low battery** - sending SMS on low battery;
- 6) **SMS on other failures** - sending SMS on other failures (e.g. accumulator failure);
- 7) **Alarm CLIP** - making alarm CLIP call;
- 8) **Descriptive SMS** <-> **SMS with ID codes** - selection of SMS content: event description such as "Intruder Alarm" or the use of special codes defined in pt. 7.9, 7.10 and 7.11.7.
- 9) **SMS accept** - SMS commands (as below) acceptance received by CBP32.
ARM, DISARM, NIGHT and DAY- sets appropriate arming mode;
DISABLE zone_name - disables zone: zone_name;
ENABLE zone_name - enable zone: zone_name;
STATUS - in response control panel sends SMS on current armed/disarmed status and failure events;
TIME HH:MM - sets current time in control panel;
TEST - sets up instant test procedure and starts time count to next test under condition that "Test every time interval" is selected in pt. 7.11.2 and "Execute test" function is selected in pt. 5.6.12.
LAMP - sample control command for output named LAMP. Detailed description of controlling outputs by SMS commands can be found in pt. 4.1.
- 10) **CLIP arming** - remotely arming and disarming CBP32 pane by CLIP call (by calling the panel phone number). Panel is disarmed if call is rejected after one ring. If the call is rejected after three rings, the panel is armed.
- 11) **Call back** - calling back function. If the control panel is called by user/operator, it will call back. This and next function may be used in operation with monitoring centre:

- a) if the function is set off, CBP32 panel rejects the call after 3-4 seconds and does not call back to calling number,
 - b) if the function is set on, the control panel rejects the call and calls back.
- 12) **Execute test** - executing SMS or CLIP time interval test by CBP32 panel. The function may be used in operation with monitoring centre. See also pt. 7.6, pt. 7.7 and pt. 7.11 of Alarm Notification by GSM section.

5.7. Remote transmitter type and operation mode.

Service Settings → **System Users** → **Remote type**

This menu allows selection of remote's operation modes. Description: 1CH-one channel remote, 2CH-two channels remote, 4CH-four channels remote.

1CH: arm/disarm - any selected button alternatively arms and disarms control panel. Remaining buttons of, e.g. 4-channels remote, may be used for other purposes.

2CH: arm/disarm, night/disarm - button 1 (green) of 2-channels remote (*) alternately arms and disarms control panel while button 2 (red) arms in night mode and disarms the panel.

2CH: disarm, arm - button 1 (green) of 2-channels remote (*) disarms while button 2 (red) arms the panel.

This mode allows real time clock channel of Elmes STX remote transmitter may be used to arm/disarm CBP32 control panel automatically, at predefined times.

2CH: disarm, night arm - button 1 (green) of 2-channels remote disarms while button 2 (red) arms in night mode.

4CH: disarm, arm, night, day arm - button 1 (green) disarms system, button 2 (red) arms, button 3 (blue) night arms, button 4 (grey) day arms.

Remote sets on delay - remote sets on entry delay in "remote delayed" zones (see pt. 3.1.d).

6. Times Setting

This menu allows setting up different times in alarm system. The ▲▼ and ◀▶ buttons are used to select current date and time, OK button accept selection and C cancelling selections.

6.1. System date/time setting.

Service Settings → **Times Setting** → **System date/time**

This menu allows setting system current date and time. To be set on power supply cease.

6.2. Entry delay time (0..99s)

Service Settings → **Times Setting** → **Entry delay**

This menu allows setting entry time delay needed for entering protected premises and disarming alarm system before intruder alarm is activated (in seconds: 0-99).

6.3. Exit delay time (0..99s)

Service Settings → **Times Setting** → **Exit delay**

This menu allows setting time delay needed to exit premises (in seconds: 0-99) after alarm system arming from remote, phone or panel buttons.

6.4. Wireless siren check up interval (1..99 minutes).

Service Settings → **Times Setting** → **WSS siren check-up interval**

This menu allows setting time interval between checking of Elmes WSS wireless siren presence (in minutes: 1 to 99) - as standard set to 10 minutes.

6.5. CBP32 panel clock adjustment.

Service Settings → **Times Setting** → **Clock adjustment**

This menu allows adjustment of control panel clock fast/slow run within -99 to +99 steps range. Decreasing steps slow the clock while increasing steps speed up clock. One adjustment step equals 0,0864 second faster/slower clock run per day (24h).

7. GSM Functions

This menu allows definition of settings for notifications, remote control and other functions of GSM module in the CBP32 panel.

7.1. SMS centre phone number.

Service Settings → GSM Functions → SMS Centre Number

This menu is used to enter the phone number of GSM operator's SMS centre, preceded by country code dialling without "+" mark in front. This is important if option in pt. 7.11.6 "Use entered SMS centre no" is selected. If option "Use default SMS centre no" is selected, then this field can be left empty. Example: the following phone number should be entered for Plus GSM operator (PL): 48601000310

7.2. Alarm SMS daily limit.

Service Settings → GSM Functions → Alarm SMS daily limit

Feature allowing limitation of daily (24h) SMS notifications send by CBP32 control panel on system alarm, arming and disarming. Limit is to 99 by default and resets daily at 12:00 hours.

7.3. Failure SMS daily limit.

Service Settings → GSM Functions → Failure SMS daily limit

Feature allowing limitation of daily (24h) SMS notifications on system failures send by CBP32 control panel and registered in event memory. Failures are divided into 4 categories. First category includes "Mains power failure", "Accumulator failure" and "System restart", second "Radio link failure", third "Low battery" and fourth "short circuit at S1, S2 or AUX outputs".

SMS notification limit for each category is set to 10 by default and resets daily at 12:00 hours. Change of the limit (10) results in limit change in all categories and CBP32 event memory.

7.4. Calling duration.

Service Settings → GSM Functions → Calling duration

This feature defines duration of CBP32 calling, e.g. CLIP calling notification on alarm. It should be set to the time duration allowing user to reject call before the time lapses, if function "Alarm CLIP once" (S.S. pt. 7.11.5) is set off. See also pt. 5 of FAQ section of manual.

7.5. SMS password.

Service Settings → GSM Functions → SMS password

This menu is used to enter a maximum 6-character password that will precede SMS command text, if option "SMS with password" is selected in pt. 7.11.3.

7.6. Test SMS.

Service Settings → GSM Functions → Test SMS

This menu is used to enter Test SMS content send by GSM module, if test function is set on in pt. 5.6.12 and "Test as SMS" option is selected in pt. 7.11.1.

7.7. Interval / Test time.

Service Settings → GSM Functions → Interval/Test time

This menu is used to enter time interval (if option "Test interval" is selected in pt. 7.11.2) or, test time (if option "Test time" is selected in pt. 7.11.2), if the CBP32 control panel is expected to perform SMS or CLIP test. Maximum value is 24h. This feature is valid only if "Execute test" option is selected in pt. 5.6.12.

7.8. Phone Module ON/OFF.

Service Settings → GSM Functions → GSM Module ON/OFF

This menu is used to toggle on/off control panel GSM module operation. Enter the menu with OK and select GSM Module ON or OFF using ◀▶ buttons.

7.9. SMS ID codes.

Service Settings → GSM Functions → SMS ID codes

This menu is used to enter two character ID codes send in SMS event notifications. Each code contains any two characters except for lower case letters. To set the CBP32 panel to send ID codes instead of standard text notification, e.g. "Intruder alarm: kitchen", option "SMS with ID codes" must be selected in S.S. pt. 5.6.8.

7.10. Definition of monitoring station subscriber account number .

Service Settings → GSM monitoring → Subscriber account number

This menu is used to define subscriber code (max. 8 characters) used by monitoring station operating in e.g. "Ademco Contact ID" to identify SMS notification sender (see pt. 7.11.7).

7.11. Auxiliary GSM settings.

Service Settings → GSM Functions → Aux GSM settings

- 1) Test as CLIP or Test as SMS - interval test as CLIP call (default) or SMS.
- 2) Execute test at time or Execute test after interval - test executed daily at predefined test time (default), or test after predefined time interval.
- 3) SMS with password - if Y SMS send to CBP32 must begin with password (default N).
- 4) Letter case sensitive - N (no) (default). If selected Y (yes), the control panel is SMS letters case sensitive.
- 5) Alarm CLIP once - if this function is set off (default), control panel expects CLIP notification rejection. If the call (see pt. 7.4) is not rejected, the panel disconnects and repeats CLIP call twice. If the function is set on (Y), CLIP calling is made once only, even the call is not rejected. It does not refer to a control CLIP that is made only once as standard.
- 6) Use default SMS centre no or Use entered SMS centre no - selection of the first option (default) allows CBP32 panel to use SMS centre number supplied with SIM card, while selection of the second option causes CBP32 to use centre number entered in pt. 7.1.
- 7) Ademco Contact ID → Subscriber + event code → Subscriber + event code + zone no
The settings is valid only, if "SMS with ID codes" is set on in pt. 5.6.8 and allows selection of one of three SMS notification patterns send to monitoring station:
 - 1) "Ademco Contact ID" pattern. SMS notification has the following form:
CCCCQEEEGZZZ
where "CCCC" stands for subscriber code set in pt. 7.10. Other elements are not defined by the user, e.g. three digits event number "EEE". NOTE: if monitoring station requires digits "18" to appear before "CCCC" then subscriber's code should input as "18CCCC" in pt.7.10.
 - 2) "Subscriber + event code" pattern. SMS notification has the following form:
CCCCEE
where CCCC stands for subscriber code set in pt. 7.10 and "EE" event code set in pt.7.9.
 - 3) "Subscriber + event code + zone no" pattern. SMS notification has the following form:
CCCCEZZ
where CCCC is subscriber, "EE" event code and end "ZZ" is zone or user number.
- 8) Return SMS - on output control SMS receipt send „OK.“ SMS in return.

7.12. Operation with security monitoring centre in GPRS communication mode.

Service Settings → GSM Monitoring → GPRS monitoring

This menu is used to set control panel to operate with internet monitoring center. Starting from ver. 1.50 the panel's firmware allows GPRS communication with monitoring centers using TCP or UDP protocols in compliance with SIA, DC-09 standard. Event notifications are transmitted to monitoring center in Ademco Contact ID format, in SIA protocol frame and AES-128 algorithm encrypted, or not encrypted.

- 1) GPRS center no 1 address first monitoring center address in IP format, e.g. 178.121.45.89, or domain name, e.g. www.domain-adresss.com;
- 2) Center no 1 port number first monitoring center TCP or UDP protocol port number;
- 3) GPRS center no 2 address second monitoring center address;
- 4) Center no 2 port number second monitoring center TCP or UDP protocol port number;
- 5) APN GSM network operator's APN name;
- 6) APN login GSM network operator's APN login;
- 7) APN Password GSM network operator's APN password;
- 8) Test interval GPRS mode communication with monitoring center check test frequency;
- 9) SMS test interval SMS check test to phone 16 frequency in the case of GPRS mode communication with monitoring center test failure. Setting is valid only if option "SMS to phone 16 on GPRS error" is set on. See pt 7.12.15.e;

- 10) **Encryption key** encryption key used to encrypt notifications sent to monitoring center in SIA protocol. May contain hexadecimal characters only (0..9, A..F). Valid only if encryption of SIA protocol is set on. See pt 7.12.15.d;
- 11) **Time zone** local time zone shift with regard to Greenwich time (-12..+12). Used only if SIA protocol encryption is set on. See pt 7.12.15.d;
- 12) **Account number** string of 3..16 hexadecimal characters (0..9, A..F) used for identification by monitoring center. Cannot be left empty.
- 13) **Account prefix** string of maximum 6 hexadecimal characters (0..9, A..F) used for identification by monitoring center. May be left empty.
- 14) **Receiver number** similar to above, used for expanded identification;
- 15) **GPRS function**
 - a. **GPRS monitoring disabled** ↔ **GPRS to station no 1** ↔ **GPRS to station no 1 & 2** ↔ **GPRS to station 1, on error – to 2** notification mode to monitoring centers;
 - b. **Station 1 protocol: TCP** ↔ **Station 1 protocol: UDP** selection of internet communication protocol with monitoring center no 1;
 - c. **Station 2 protocol: TCP** ↔ **Station 2 protocol: UDP** as above for center no 2;
 - d. **Encryption** encrypt with AES-128 algorithm notifications in SIA protocol. After setting this option on entering proper encryption key (pt 7.12.10) as well as time zone (pt 7.12.11) are mandatory, because with encryption set on control panel's clock synchronizes with the clock of the monitoring center that use Greenwich time.
 - e. **SMS to phone 16 on GPRS error** after setting this option on control panel will send event notification SMS to phone 16, if GPRS mode notification has failed. This notification is not encrypted even if encryption is set on.

8. Auxiliary functions settings.

This menu contains auxiliary functions and options for alarm system configuration. Use ▲▼ buttons to browse between functions and ◀▶ buttons to change setting. OK button saves selection. Exit menu any time with C button without saving selections.

8.1. Jamming protection (default N)

Service Settings → **Aux functions** → **Jamming protection**

This function allows radio jamming anti-sabotage protection of wireless alarm system. If selected (Y), it will activate sabotage alarm in zone 30 on all deliberate or incidental jamming in used radio band.

8.2. Radio link test (default N)

Service Settings → **Aux functions** → **Radio link test**

Setting this function to (Y) enables monitoring of the detector presence. Cyclic radio link transmissions sent from detectors (except CTX3H) are received by CBP32 control panel. If, for any reason, radio link transmission from a detector is not received during 24 hours, "radio link failure" sabotage alarm sets on.

8.3. Sabotage protection of S1 output (default N)

Service Settings → **Aux functions** → **Output S1 Test**

This function enables sabotage protection of output S1, if installed alarm siren is not provided with dedicated sabotage connectors. Setting the function on will generate sabotage alarm in zone 32, if siren wires connected to S1 are cut off or shorted to ground (COM). Before the function is set on, it is necessary to check that polarizing resistor is installed between output AUX (+12V) and output S1 so, when the output S1 is off its voltage is at within +05...6V range. Such resistor can be directly connected to the control panel connectors or, to appropriate connectors inside the siren. When output S1 testing is on, the control panel monitors voltage level at S1 connectors and sets sabotage alarm, if wires cut or shorted is detected.

8.4. Sabotage protection of S2 output (default N)

Service Settings → **Aux functions** → **Output S2 Test**

As described above, but for output S2 with sabotage alarm in zone 31.

8.5. Activating partial day & night arming modes (default N)

Service Settings → Aux functions → Day/night mode

Activating the function (Y) will display additional menu on LCD allowing selection of supervision modes confirmed by password and the OK button. There are 4 modes available: 1 - disarmed, 2 - armed, 3 – day, 4 – night (see also: “Arming/disarming alarm system”). With the function set off (N), the menu is not displayed and system can be armed and disarmed from the control panel buttons without partial arming options. However, night mode arming is still possible, if arming by remote (see details in pt. 5.7) or by GSM phone.

8.6. Setting on panic alarm or call for help function.

Service Settings → Aux functions → Panic alarm off / Loud panic alarm / Silent panic alarm

This function allows activation of panic alarm for users equipped with remote control by longer than two seconds pressing the remote's button. Control panel starts alarming and registers the event as panic alarm with name of the user that activated the alarm and sends appropriate SMS notification. Loud panic alarm differs from silent panic alarm by setting on outputs type “silent alarm” while alarm sirens remain off (see pt. 4.1).

Switching activated panic alarm OFF is done by entering a password from keypad or by the use of a remote, if this option is set on for the remote (pt. 5.7).

8.7. Control panel buttons beep (default Y)

Service Settings → Aux functions → Buttons beep

This option allows setting on/off beep signals when control panel buttons are used.

8.8. Alarm on radio link with WSS siren failure (default N)

Service Settings → Aux functions → WSS siren link alarm

Setting this function to yes (Y) allows loud alarm along with LED alarm notification on wireless Elmes WSS siren radio link check-up test failure. As standard the function is set to no (N) and the failure is signalled by flashing Alarm LED only. Failure check menu will display “Radio link error” and name of zone 29 (if specified).

8.9. Limitation of alarms from one alarm zone (default Y)

Service Settings → Aux functions → Alarms limit to 3

This function limits number of alarms in one zone to three and is factory set to on (Y). Alarms count is reset on every arming or disarming of the system. When the limit is selected to off (N) alarm sets on every time violation is detected in the alarm zone.

8.10. Selection of menu language: Polish/English.

Service Settings → Aux functions → Język polski / English language

This function allows selection of the panel's menu language using ◀▶ buttons.

NOTE! Change of menu language can be made also with button ▲ pressed on connecting power supply to the panel.

8.11. Beep when failure detected (default N)

Service Settings → Aux functions → Beeps when failure

Setting this function to yes (Y) allows control panel internal buzzer beeps on detected failures.

9. System arming signalling modes.

Service Settings → Arming signalling modes

This menu allows selection of alarm system arming and disarming signalling mode. Use ▲▼ buttons to toggle between functions and ◀▶ to change setting. OK button saves selection. Exit menu any time with C button without saving selection. The following options are possible:

9.1. Remote: pulses or Remote: pulses + SMS if problem – selecting the first option sets on sound pulses on sirens only (**). Selecting second option allows sound pulses on sirens and SMS notification if any problem occurs (*).

9.2. SMS: SMS or SMS: pulses + SMS if problem – selecting first option a return SMS is send on arming SMS. Selecting second option sets on sound pulses (**), while SMS notification is received only if problem occurs (*).

- 9.3. **CLIP: SMS** or **CLIP: pulses + SMS if problem** – selecting first option a return SMS is received on CLIP arming. Selecting second option sets on sound pulses (**), while SMS notification is received only if problem occurs (*).
- 9.4. **Pulses on WSS** - setting on/off arming sound pulses on wireless Elmes WSS siren.
- 9.5. **Pulses on S1**, **Pulses on S2**, **Pulses on O1**, **Pulses on internal buzzer** – setting on arming signalling sound pulses on S1, S2, O1 and buzzer. Signalling may be set on for all outputs independently.
- 9.6. **Chime and countdown on S1** ↔ **...on S2** ↔ **...on O1** ↔ **...on internal buzzer** – setting on sound pulses on Chime zone violation and arming countdown pulses on one of outputs S1, S2, O1 or internal buzzer.
- 9.7. **No pulses at night** or **Pulses on S2 at night** or **...on O1 at night** or **...on buzzer** – setting on night arming signalling sound pulses on S2, O1 or internal buzzer.

(*) While system arming violation of supervised zone may occur. Depending on whether the zone is “bypass” type (see pt. 3.1.g), the system will arm and SMS notification will be received informing of the bypassed zone/s or, if the zone is not “bypass” type, the system will not arm and SMS notification will be received with information of violated zone/s.

(**) In order to obtain sound pulses functionality, a sound siren must be connected to one of S1, S2 or O1 outputs and sound signalling set on at that output (pt. 9.5). Internal buzzer may also be used for the purpose.

SETTINGS RESET

Resetting password of user 1.

If user is disabled or its password is lost and there is no way to enter Service Settings menu, user 1 can be enabled and have factory password “▲▲▲▲” restored, in the following way:

1. Open panel’s cabinet (sabotage alarm may occur, see page 5).
2. Disconnect AC power and remove battery.
3. Short circuit two points marked RESET (in the upper right corner of LCD).
4. Connect AC power supply and wait till start of firmware.
5. Disconnect AC power supply, disconnect shorted RESET points.
6. Connect battery, connect AC power supply.

User 1 is now enabled and its password is restored to “▲▲▲▲”. All other settings remain unchanged.

Restoring CBP32 to factory settings (default settings).

Factory (default) settings are restored according to procedure described below. The procedure restores factory settings deleting all wireless devices in memory. Records in the event memory are not deleted.

1. Open panel’s cabinet (sabotage alarm may occur, see page 5).
2. Disconnect AC power and remove battery.
3. Short circuit two points marked RESET (in the upper right corner of LCD).
4. Holding down button ► connect AC power supply – display will show “Factory settings”.
5. Release button ► and wait until control panel restores normal operation.
6. Disconnect shorted RESET points.
7. Connect battery, connect AC supply.

ALARM SYSTEM INSTALLATION

The following accessories are needed before CBP32 control panel can be installed:

- Typical alarm system 12V battery with appropriate capacity (see chapter: power supply and battery recommendations).
- AC/AC transformer with secondary output 17...18VAC (see chapter: power supply and battery recommendations).
- Dedicated for alarm system control panel plastic or metal cabinet or, any cabinet suitable for all components of the control panel and power supply. If the cabinet is made of plastic, GSM and wireless detector radio antennas can be inside the cabinet. Anti-sabotage cabinet switch should be connected to the control panel according to diagram 5.

- Active SIM card, if the panel's GSM module will be used.

SIM card for use in CBP32 control panel should have SMS memory and address book cleared with voice mail box set off. Used SIM card may have PIN code protection set off. If used SIM card has PIN code set on then the code must be set to **1234**. This can be done using any mobile phone. **The use of SIM card with other than 1234 PIN code in the CBP32 control panel will cause the card to be blocked!**

Designing and installation of alarm system with the Elmes Electronic CBP32 control panel should start with careful planning of detectors, control panel and outdoor siren placement. To ensure satisfactory protection of secured premises a variety of detectors may be needed. Elmes Electronic PTX50 wireless motion detector and CTX wireless magnet contact detectors should be installed in each protected room with window. Additionally, GBX1 wireless glass break detector could be installed for protection of windows breakage in premises and shops. Depending on needs, up to six wired detectors of any manufacturer can be connected to parametric inputs of the panel. Detailed instruction manuals of devices should be observed while installing wireless or wired detectors to the control panel.

If the control panel is to be installed inside of metal cabinet, detector's radio antenna as well as GSM module antenna must be installed outside the cabinet. If the cabinet is made of plastic the antennas can be inside with minimum distance of few centimetres from each other.

Connections of system components to the CBP32 control panel are shown on diagram 1.

After setting on power supply (observe proper sequence) and, if the GSM module is on, the blue GSM LED should be watched for signaling connection to GSM network, as described below.

Current connection to GSM network status is signaled by flashing blue LED :

flashing every 0,8 s, fading few sec.	log-in in progress
flashing every 3 s	logged in
flashing 3 times per second	logged in, GPRS connection established

The GSM network signal level can be checked in System Status in Main Menu.

Described below steps for configuring alarm system with CBP32 control panel assume the user will use hand transmitter (remote) to arm/disarm the system:

1. Set on current date and time (pt. 6.1).
2. Program a remote to the user (pt. 5.3) and select its functions (pt. 5.6).
3. Set arming signalling mode of the control panel (pt. 9.5).
4. Learn wireless detectors to control panel alarm zones (pt. 3.3) according to procedures described in their manuals.
5. Check operation of wireless detectors. To do so, hold down button ◀ until two 16 bar lines appear on display representing all alarm zones. With the help of other person sequentially activate detectors watching for their star "*" signal displayed on the bar corresponding to alarm zone the detector is programmed to.
6. Check radio signal level of each wireless detector by selecting "Radio range test" (pt. 3.5) submenu in the panel and, with the help of other person, activate detectors while watching RF signal level displayed on bar scale of LCD. Weak signals (1-2 bars displayed) coming from detector require changing the detector's place of installation so, as the number of signal level bars displayed are minimum 3-4. In extreme low signal levels, the use of Elmes Electronic TRX signal repeater may be needed to guarantee proper signal reception by the control panel.

After the initial steps above, further setting up of the alarm system can be done, as below:

- configure external wireless siren WSS, if installed;
- set on anti-sabotage protection of output S1, if a wired siren is connected (pt. 8.3);
- set on wireless detectors radio link with the panel test (pt. 8.2);
- set on the GSM module (pt. 7.8), input phone numbers of system users and configure their functions pt. 5.5 and 5.6);
- define users names (pt. 5.2) and learn remotes to other users (pt. 5.3);
- define alarm zone names (pt. 3.2).

Power supply: selection of transformer and battery

For powering of the control panel AC/AC transformer with secondary output of 17VAC should be used with output power exceeding total system power requirement by at least 20%.

Selecting a backup battery, it should be assumed that the system must be operational for at least of 12 hours inclusive of alarming time of 15 minutes (0,25h) after AC power cut off. To perform calculations it should be assumed that:

- control panel current is ca 30mA,
- battery charge current depends on setting of jumper ISET and for battery capacity of 1,2 Ah it is 130mA while 12Ah and higher it is 450mA,
- average current draw at all AUX power outputs should sum up currents of all wired alarm devices such as wired detectors and sirens.

Calculating required battery capacity for sample alarm system with six wired detectors and siren connected according to diagram 4, assuming 12 hours system autonomy operation and 0,25 hour alarming time, we shall conclude with the following equation:

$$\sum Q = 700\text{mA} * 0,25\text{h} + (30\text{mA} + 6*15\text{mA}) * 12\text{h} = 1615\text{mAh} = 1,615\text{Ah}$$

As typical alarm 1,2Ah battery capacity is insufficient so, 7Ah battery is needed with ISET jumper set to 450mAh charging current.

Now, required summarised output current of AC transformer may be calculated:

$$\sum I = 450\text{mA} + 30\text{mA} + 6 * 15\text{mA} = 570\text{mA}.$$

So, with required 20% of surplus power, a transformer of 700mA output will be sufficient.

Sequence of power supply connection

CAUTION! Danger of electric shock. All connections should be made with 230V mains disconnected.

1. Connect battery to the control power using the black-red wire with connectors. Observe correct polarity. Red wire connects to battery + and black to battery -.

2. Connect transformer secondary output wires to AC input of the control panel. Lastly, connect fuse protected AC 230V mains supply to the transformer.

Power supply disconnection must be made in reverse sequence.

NOTE! The control panel will not initialize with only battery connection. AC power supply connection will result in start of the operating system.

CAUTION! Batteries contain dangerous and poisonous substances. Do not dispose of waste batteries with household waste. Dispose waste batteries according to your local recommendations or, ask for disposal instructions your battery supplier.

Wired detectors installation

Installation of any wired detector is made with three wire line (see diagram 2). To supply detector with +12V power, appropriate detector's power terminal should be connected to any AUX terminal on the control panel side. Any COM terminal on the panel should be used as common ground (-12V) while any Z1+Z6 terminal as alarm and sabotage terminal. Next, in submenu Disabling zones - pt.3.4, the zone to which detector is connected should be enabled and in submenu Alarm zone function – pt.3.1, alarm function/s may be assigned to the zone.

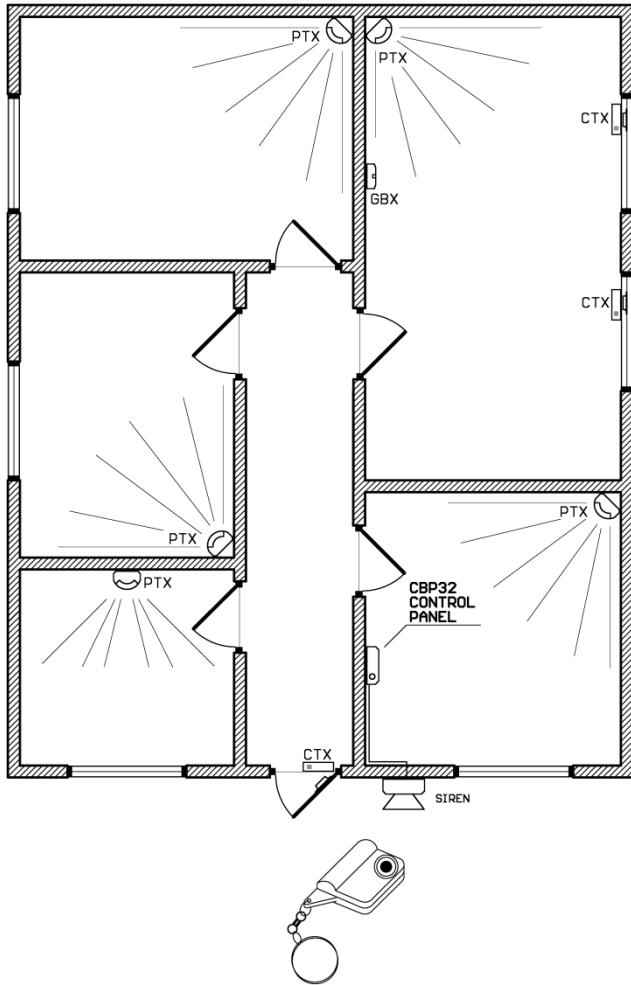
Wired detectors are always connected to CBP32 control panel in configuration with 1k and 3k3 Ohm resistors (supplied), as shown on diagram 2. Such connection configuration allows intruder alarming as well as detection of anti-sabotage box opening, wires cut or short circuit.

Control panel CBP32 operation with RP501 transmitter

The panel may operate with Elmes Electronic RP501 four inputs channel transmitter offering up to four wired detectors (switches, magnets) to be monitored remotely. RP501 transmitter can be learned to four adjacent alarm zones in the CBP32 control panel. Activating input four of the RP501 while learning the transmitter to zone 20 of the panel will assign four RP501 inputs to alarm zones no 17, 18, 19 and 20. When installing RP501 transmitter respective instruction manual must be followed.

Example of alarm system with CBP32 control panel

The following illustration shows example of alarm system installation based on control panel CBP32 with Elmes Electronic made passive infrared detectors PTX50, magnetic detectors CTX, glass break detector GBX and hand held remote transmitter UMB100HT for system arming and disarming. The system may have installed wireless siren WSS or, any wired siren.



Wired devices connection diagrams with CBP32 control panel

Diagram 1. Wired elements of alarm system connection with CBP32 control panel

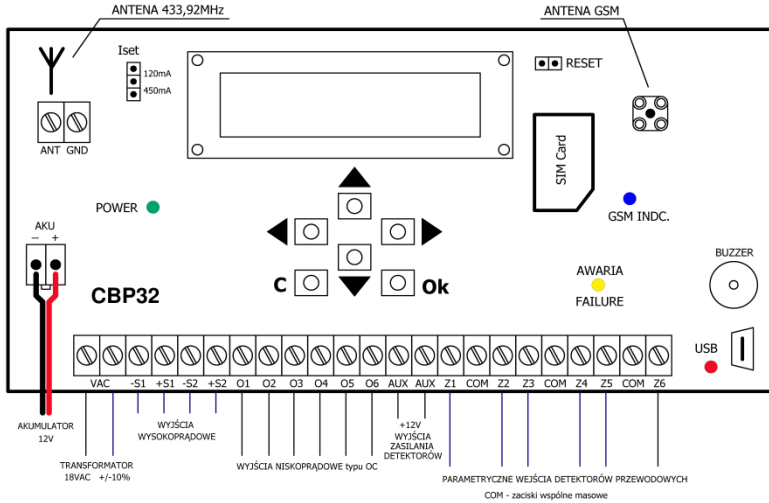


Diagram 2. Connection of wired detectors with CBP32 control panel supporting intruder alarming as well as detection of anti-sabotage box opening, wires cut or short circuit.

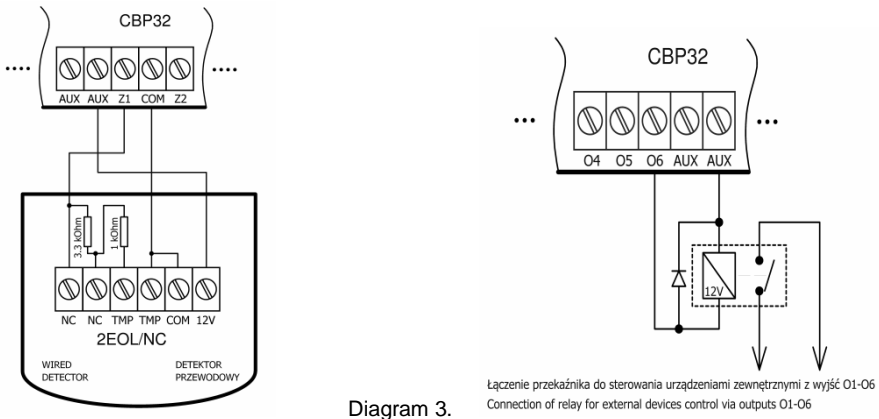


Diagram 3.

Diagram 4.

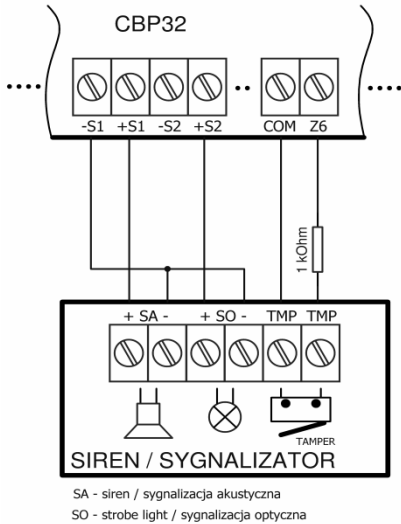
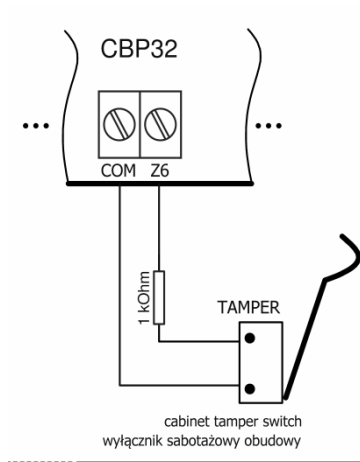


Diagram 5.



This product complies with the following standards:

1. EN-08390-14:1993 Alarm Systems – General requirements.
2. EN-50130-5:2002 Alarm Systems – Environmental requirements.
3. EN-300 220-3 V1.1.1 (2000-09) Electromagnetic Compatibility and Radio Spectrum Matters.



GSM module: GSM 900 / DCS 1800, Registration No. G110306E,

CE0678

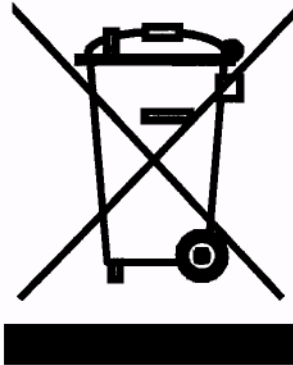
SPECIFICATION

- superheterodyne receiver 433.92 MHz, sensitivity better than -102dBm,
- supports up to 32 Elmes Electronic made wireless detectors,
- supports up to six wired detectors with parametric connections,
- operation with up to 16 users,
- integrated GSM phone module for alarm panel control and notification,
- non-volatile EEPROM memory of last 256 events,
- fuse protected two wired outputs with up to 700mA current draw,
- six OC type outputs with up to 100mA current draw,
- 17..18VAC power supply, control panel current: average 30mA, maximal 70mA,
- backup power cable for connection of 12V battery, charging current 450mA/130mA,
- control panel external dimensions L165/W90/H35 mm,
- indoor use only with temperature range from 0 to +40 °C.

Manufacturer: Elmes Electronic, 54-611 Wroclaw, Poland, ul. Avicenny 2,
phone +48717845961, fax+48717845963, e-mail: elmes@elmes.pl

MANUFACTURER'S LIMITED WARRANTY

The manufacturer of this product warrants the original purchaser that for a period of 24-months as from the date of purchase, the product shall be free of defects in materials and workmanship in normal use. During the warranty period, the manufacturer shall, at its option, repair or replace any defective product upon return of the product to the manufacturer, at no charge for labour and materials. The defective product must be delivered to the point of purchase in a clean condition and at buyer's own expense, along with this guarantee with the date of purchase confirmed below, and a short description of the failure. The cost of dismantling and installing the device is covered by the user. The warranty does not cover batteries and damage arising from improper use or handling, unauthorized adjustments, alterations and repairs.



The use of WEEE symbol indicates that this product may not be treated as household waste. By ensuring this product is disposed of correctly you will protect the environment. For more detailed information about the recycling of this product, please contact your local authority, your household waste disposal service provider, shop or supplier where you purchased the product.

FREQUENTLY ASKED QUESTIONS

1. ALARM led is flashing. What may be the cause?
 - enter panel's Menu (press OK for more than 2 seconds) and check for reason. If it is battery failure then check for battery contacts, possible battery leakage or, set OFF battery failure notification (sub-menu 8.6), if batteries are not installed.
2. ALARM led is lit. What may be the cause?
 - alarm occurred. Enter Menu and check zone number of the alarm and alarm time or, simply enter and leave the menu, the led light sets off.
3. Why occasionally sabotage (tamper) alarm is notified in zone 30?
 - the reason is radio band jamming occurring in the area of panel installation. The jamming may be incidental or deliberate. User may set OFF the radio jamming protection function in sub-menu 8.2 of aux functions however, the entire wireless alarm system is not protected then against deliberate jamming of used radio band and burglary may not be notified.
4. Why sabotage alarm in zone 32 is set on after connecting power supply?
 - the reason is panel's tamper switch not properly functioning. Check if plastic element protecting switch arm is removed. If not remove it and adjust its arm by gentle bending to signal the panel being moved off wall, or place of installation. Use washer to adjust proper distance of switch arm from wall. The other reason of the alarm may be lack of 1kOhm resistor in sabotage protection circuit (input TAMP).
 - sabotage protection of OUT1 is set on (pt. 8.4) and no siren is connected to this output or, wires to the siren are cut off.
5. Despite CLIP call rejection, control panel calls three times with CLIP call notification ?
 - in case of some mobile phone operators reaction to call rejection is "call recipient unavailable, please try later..." lasting up to 20 seconds. Only after then the control panel receives information that the call was rejected. Sometimes it is too late and the panel has already disconnected as the CLIP notification time has lapsed. This, in consequence, launch next connection attempts by the panel. To solve the issue, calling time should be prolonged at pt. 7.4 to 30-35 seconds or, calling recurrence set to OFF at pt. 7.10.5
6. Why the control panel does not respond to wireless detectors signals despite they are programmed to the panel?
 - it may be due to the fact that the detectors were programmed to the panel with the use of TAMPER switch triggering radio transmission. New programming of the detectors to the control panel should be made with radio transmissions triggered according to the procedures described in manuals of the detectors.
7. Control panel does not send SMS notifications? Possible causes:
 - newly used SIM card in CBP32 is not initialised. To initialise a new card install the card in any mobile phone and make a call or send SMS first;
 - no event is assigned to SMS notification. Select events, e.g. arming, alarming, etc., to be notified by SMS in pt. 5.6 of CBP32 manual;
 - daily limit of set SMS notifications has been exceeded. To increase the limit change setting in pt. 7.2 or 7.3 or wait till 12.00 hours for new daily limit count.