Access control modules

ACCO

CONTENTS

1. General

i | *This description does not apply to the access control module which is part of the ACCO NET system.*

The SATEL company offers four types of access control modules: ACCO-KP-PS, ACCO-KP, ACCO-KPWG-PS and ACCO-KPWG. The door controller module is designed for single door control. It can operate as a fully autonomous unit or be part of a larger access control system. The access control is effected by means of electric control of the door status and user identification functions. The users are identified by their proximity card (wherever the word "card" is used in the manual, it means a passive transponder, which may have the form of a card, key fob etc.), DALLAS iButton or access code. The way of user identification depends on the type of identifying devices connected to the module:

- the ACCO-KLCDR-BG / ACCO-KLCDR-BW keypad (the keypads differ by the color of their enclosure: gray in ACCO-KLCDR-BG, white in ACCO-KLCDR-BW) or the ACCO-SCR-BG keypad – the user identification and execution of functions available in the module are possible, based on the proximity card or code. The administrator may define the basis on which access will be granted to the users:
  - proximity card and code;
  - proximity card or code;
  - proximity card;
  - code.

- the CZ-EMM, CZ-EMM2, CZ-EMM3 or CZ-EMM4 proximity card reader – the user identification and execution of functions available in the module are only possible, based on the proximity card.

- CZ-DALLAS DALLAS iButton reader (only ACCO-KPWG-PS and ACCO-KPWG modules) – the user identification and execution of functions available in the module are only possible, based on the DALLAS iButton,

- third-party readers that send data in the WIEGAND format – identification of the user and execution of the functions available in the module is possible based on the data received and read by the module as the proximity card number.

A single module makes it possible to register 1024 users, each of them being assigned a unique identification number. The controller module enables one of 256 weekly access schedules to be assigned to each user. By means of the ANTI-PASSBACK function, it is possible to prevent any attempts of repeated entry or exit by using the same identifier.

The relay output makes it possible to control electric strike, electromagnetic lock, gate controller or other devices which activate the door. Additional inputs and outputs of the module enable it to interface with a security system, protecting the facility from burglary or fire.

The module is fitted with a non-volatile memory, which enables saving more than 24 thousand events. Information related to work time recording can be saved to the events log.

LCD keypad or PC computer with the ACCO-SOFT-LT program installed should be used to program the module settings. The program is delivered free of charge with the device. Apart from the single module configuration function, it permits programming settings of a structure consisting of up to 255 modules. The program enables convenient operation and facilitates supervision over the access control system, offering such tools as the site plan, presence time report or user presence control.

The module can be connected to the RS-485 bus, thus making it possible to build a system including up to 255 modules. Connection of the RS-485 bus to PC computer and

management of the access control system from the computer is possible owing to the USB / RS-485 **ACCO-USB** converter.

The module firmware is updateable.

The switching mode power supply in the ACCO-KP-PS / ACCO-KPWG-PS door controller module is fitted with a battery charging and control system, including discharged battery disconnect feature.

1.1 Electronics board
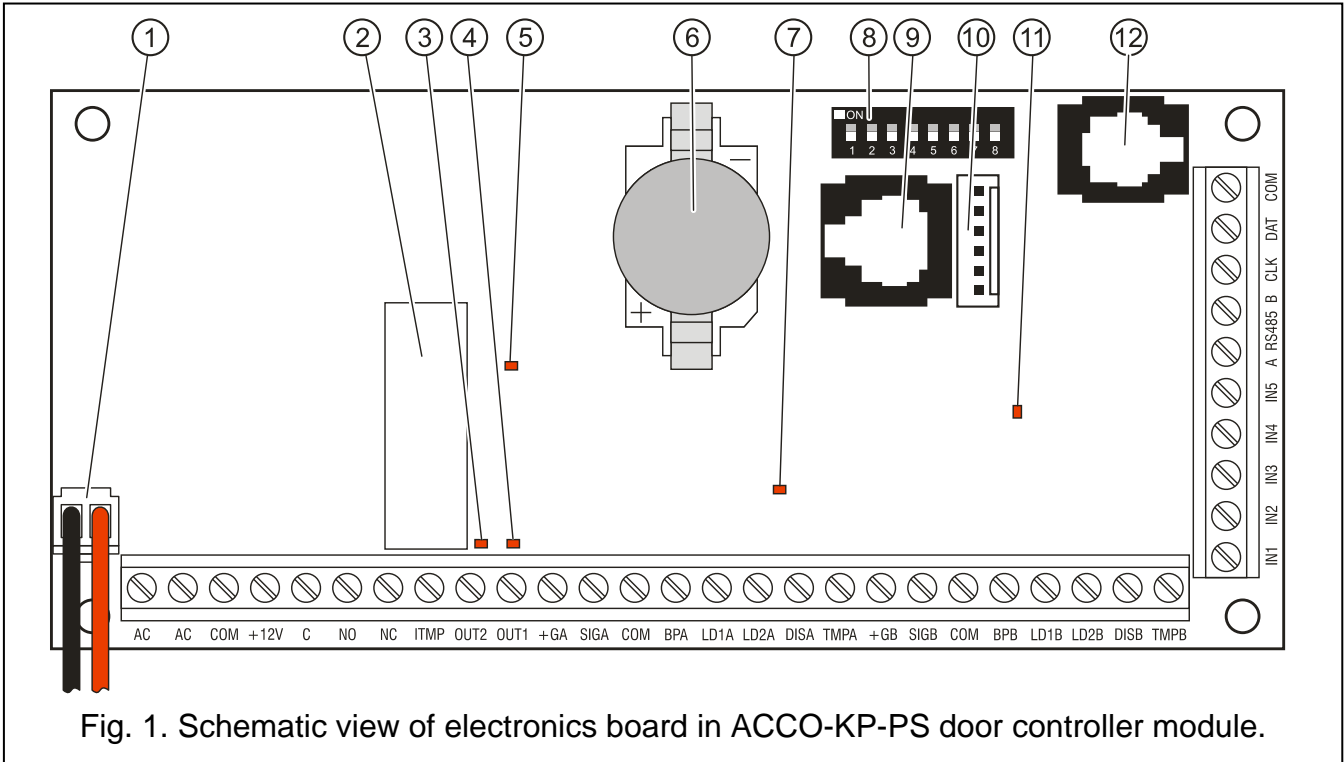
Fig. 1. Schematic view of electronics board in ACCO-KP-PS door controller module.
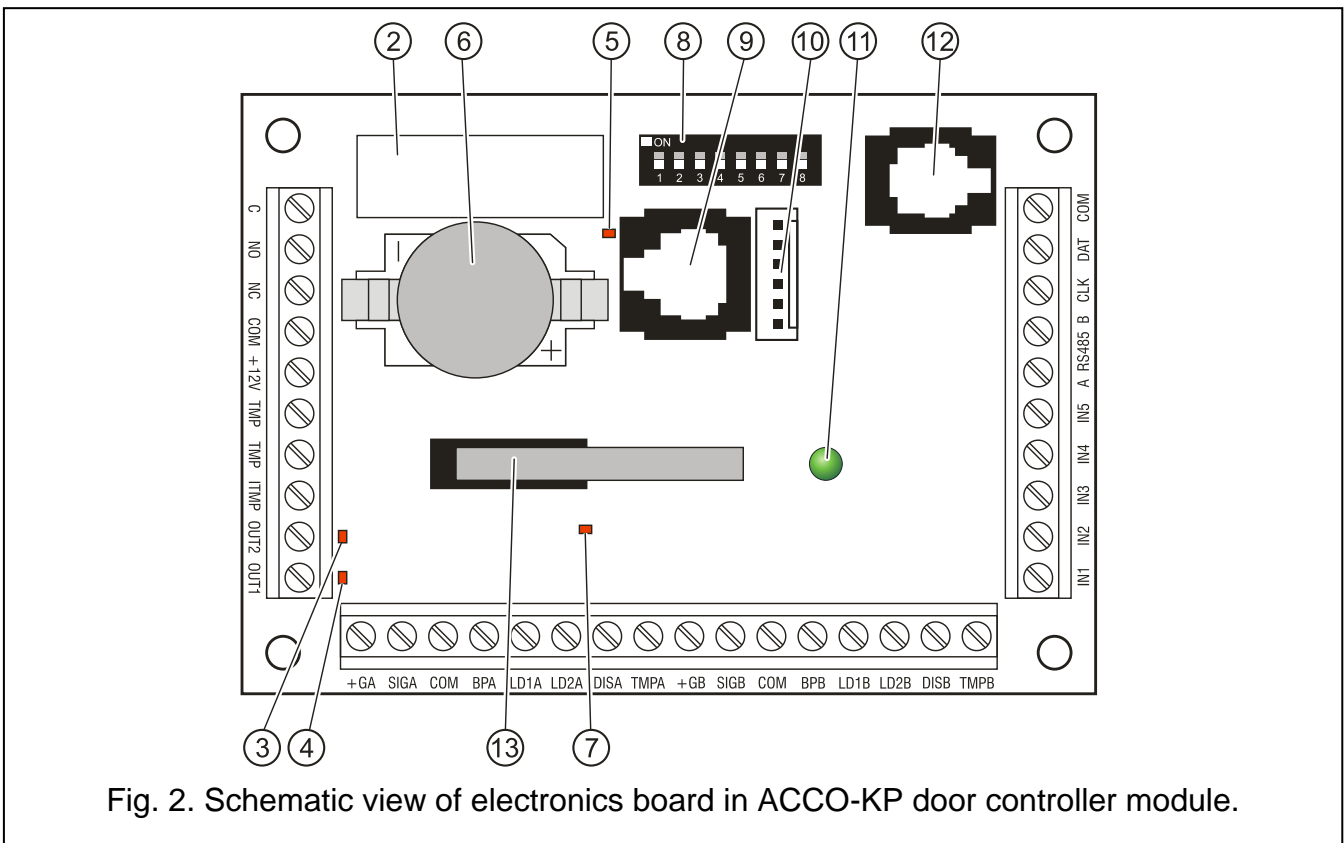
Fig. 2. Schematic view of electronics board in ACCO-KP door controller module.
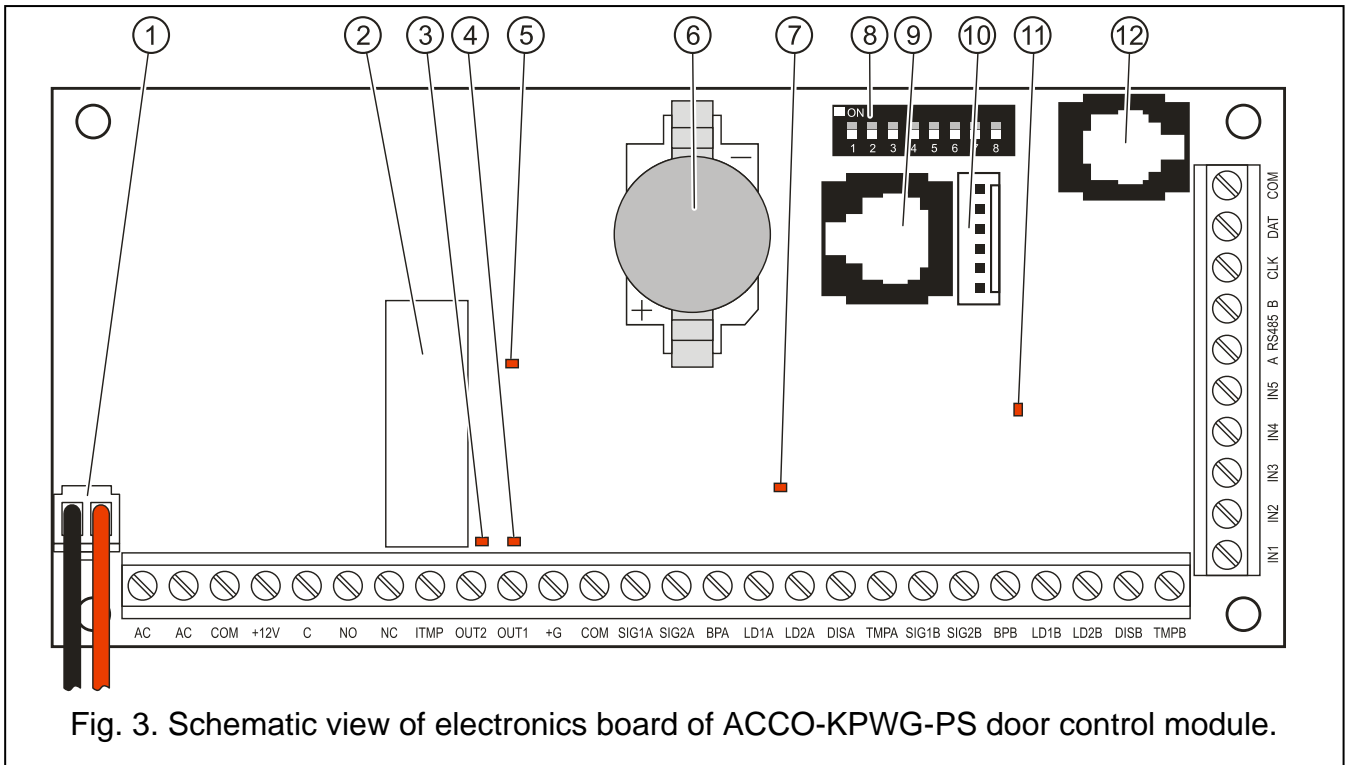
Fig. 3. Schematic view of electronics board of ACCO-KPWG-PS door control module.
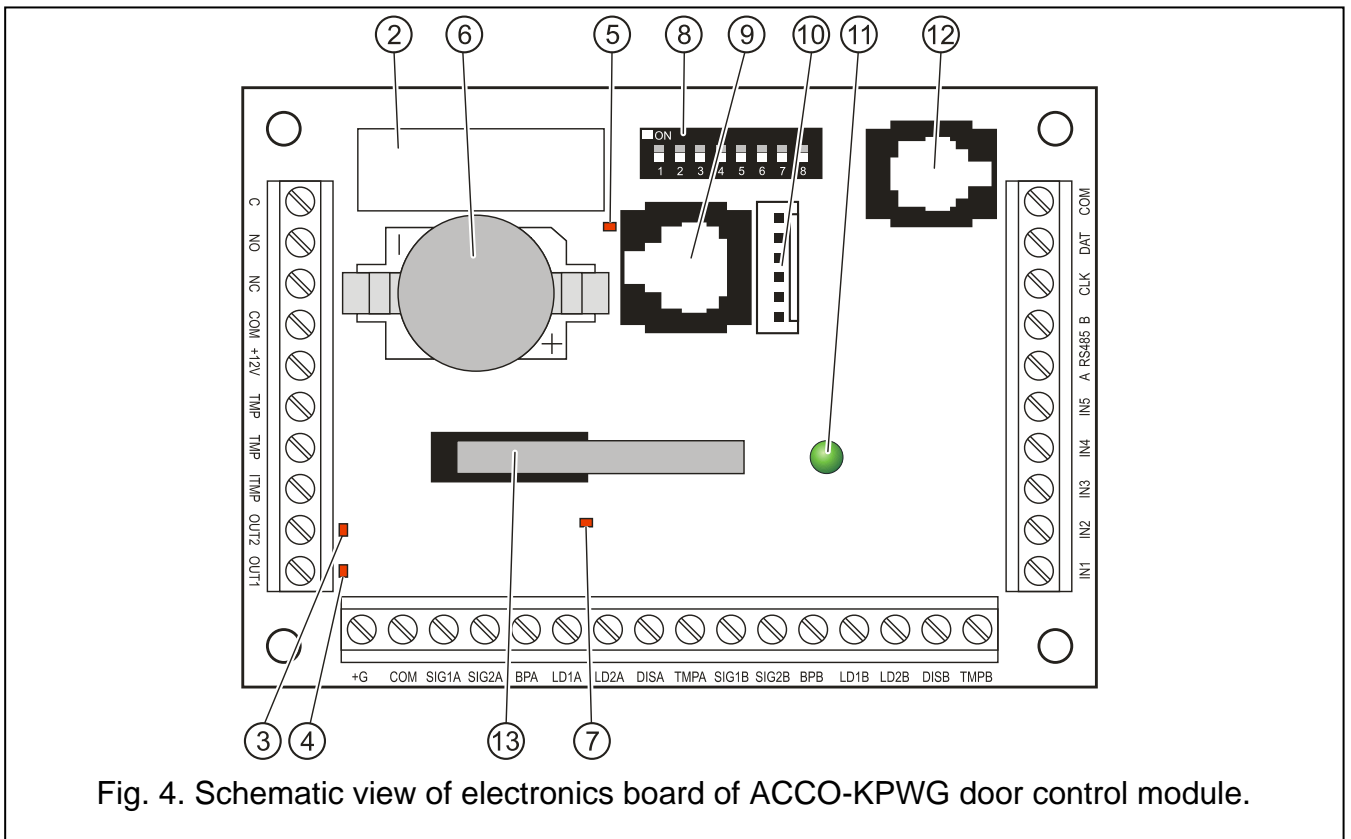
Fig. 4. Schematic view of electronics board of ACCO-KPWG door control module.

Explanations for Fig. 1, 2, 3 and 4:

1 – **battery connecting leads** (ACCO-KP-PS and ACCO-KPWG-PS).

2 – **relay**.

3 – **indicator LED of OUT2 output status** – lit when the output is shorted to common ground.

4 – **indicator LED of OUT1 output status** – lit when the output is shorted to common ground.

5 – **indicator LED for signaling relay operation**.

6 – **CR2032 3 V battery** for real-time clock back-up.

7 – indicator LED of the module microprocessor circuit – lights with changing intensity.

8 – **DIP-switch pack** for setting an individual address of the module. Based on the address, the module is identified by ACCO-SOFT-LT and ACCO Soft programs.

9 – **RS-232 port (TTL standard)** for computer connection (dedicated converter for making the connection is manufactured by SATEL under the name of USB-RS). By means of PC computer with the ACCO-SOFT-LT program installed, it is possible to configure the device and read the events.

10 – socket for future applications.

11 – **indicator LED of module operation** – lit steadily during normal operation; blinking slowly when the LCD keypad connected to the module is running in the service mode; blinking rapidly when the ACCO-SOFT-LT program / ACCO-NT control panel is establishing communication with the controller.

12 – **RJ socket** (4p/4c type) dedicated to connecting the LCD keypad for the time of programming.

13 – **tamper contact** which reacts to opening of the module enclosure (ACCO-KP and ACCO-KPWG).

Description of terminals:

AC	– supply input in ACCO-KP-PS and ACCO-KPWG-PS (18 VAC ±10%).
COM	– common ground.
+12V	– supply output in ACCO-KP-PS and ACCO-KPWG-PS; supply input in ACCO-KP and ACCO-KPWG (12 VDC ±15%).
C	– common terminal of relay output.
NO	– contact normally disconnected from the common terminal of relay output. When active, it is connected to the common terminal.
NC	– contact normally connected to the common terminal of relay output. When active, it is disconnected.
TMP	– terminals of ACCO-KP and ACCO-KPWG module tamper contact (NC). The terminals can be used in two ways:

- connect to the external tamper circuit (e.g. alarm control panel);
- connect one of the terminals to tamper circuit input ITMP, and the other one to common ground COM.

ITMP   – input for connecting tamper circuit.

i   *If the tamper contact is not connected to the ITMP terminal, short the terminal to common ground.*

OUT1…OUT2 – module outputs, OC type.

IN1…IN5 – module inputs.

A RS485 B – terminals to be connected to RS-485 bus.

CLK, **DAT** – terminals to be connected to keypad.

The other terminals are used for connecting the proximity card readers (see section CONNECTING PROXIMITY CARD READERS) and the DALLAS iButton readers (see section CONNECTING DALLAS iBUTTON READERS).

1.2 Inputs

Provided on the module electronics board are 5 inputs which can be programmed as NO or NC and serve the following functions (shown in square brackets are descriptions from LCD keypad):

Door status control [Door control] – control of the door status.

i *The door status control, i.e. connecting a sensor to the input programmed as DOOR STATUS CONTROL is necessary for correct execution of all the functions of access control.*

Unlock button – unlocks the door for the time programmed as ACCESS TIME.

Door unblocking [Unbl. input] – permanently unlocks the door after control signal appears. The door will stay unlocked as long as the control signal is supplied to the input (unless another event occurs which will otherwise change the door status).

Door blocking [Blocking inp.] – permanently locks the door after control signal appears. The door will stay locked as long as the control signal is supplied to the input (unless another event occurs which will otherwise change the door status).

Sluice configuration [Sluice config.] – status control of the other doors, forming a mantrap or airlock. In the mantrap / airlock configuration, both doors cannot be opened simultaneously.

Fire – unblock door [Fire-unblock.] – permanently unlocks the door because of fire. The door status can only be changed when the controller input becomes inactive. It can be done by a user having the SWITCHING authority level.

Alarm – block door [Alarm-block.] – permanently locks the door because of alarm. The door will stay locked until its status is changed by a user having the SWITCHING authority. The time of supplying the signal onto the input has no effect on the door blocking time.

Bell signal [Bell] – activates the BELL SIGNAL type of outputs.

Information inputs 1÷4 [Inform. inp. 1÷4] – generates the pre-defined event. The function can be used e.g. to record working time.

It is necessary to determine the sensitivity for each input, i.e. the minimum time span during which the signal must appear at the input for the module to take the preset action. This time can be programmed within the range from 10 ms to 2.55 s.

Switches, detectors or, for example, alarm or fire protection system can be connected to the inputs. In case of the NO type of inputs, the control is effected by shorting to common ground, and in case of the NC type of inputs – by isolating from common ground.

1.3 Outputs

The module electronics board includes relay output to activate access devices, such as door strikes, magnetic locks, automatic doors or barrier gates, and two OC type outputs. In active state, the OC output is shorted to the common ground (with reversed polarity: isolated from the common ground).

The OC outputs can be configured as (shown in square brackets are descriptions from LCD keypad):

Door status – the output provides information on the current status of the door. It is activated with opening of the door and remains active until the door is closed. The output configured as DOOR STATUS cannot perform other functions.

Open door – the output is activated for the programmed time period after opening the door.

Bell signal – the output becomes active for the programmed time period after signal is supplied to the input programmed as BELL SIGNAL. For the output configured as BELL SIGNAL, the OPEN DOOR function can only be additionally activated.

Forced entry – the output becomes active for a programmed time period after unauthorized opening of the door (the door is locked).

Long open door – the input output becomes active for a programmed time period, if the door remains open after expiry of the DOOR OPEN TIME.

No terminal presence [Lack of term.] – the output becomes active for a programmed time period, if no terminal (LCD keypad, keypad or proximity card reader) has been found during the test. The module controls presence of terminals only when corresponding options are enabled (PRESENCE CONTROL - TERMINAL A, PRESENCE CONTROL - TERMINAL B).

5 invalid attempts – the output becomes active for a programmed time period, after 5 attempts to read an unregistered proximity card, unregistered DALLAS iButton or enter an unknown code have taken place. **The input is activated irrespective of whether the ANTI-SCANNER option is enabled or not.**

AC supply failure [AC loss] – the output becomes active, if the time programmed as AC LOSS REPORT DELAY has elapsed since the AC supply was lost by the ACCO-KP-PS / ACCO-KPWG-PS module, and the supply has not been restored. The output remains active until the AC supply is restored.

Low battery – the output becomes active, if the voltage of battery connected to the ACCO-KP-PS / ACCO-KPWG-PS module drops below 11 V for a period of time longer than 12 minutes (3 battery tests). The output remains active until the battery voltage rises above 11 V for a period of time longer than 12 minutes (3 battery tests).

> *i* *For the output to be able to execute the DOOR STATUS, OPEN DOOR, FORCED ENTRY and LONG OPEN DOOR type of functions, one of the inputs must monitor the door status (DOOR STATUS CONTROL).*

Tamper – the output becomes active if the ITMP input is activated. The function is not available if one of the DOOR STATUS, OPEN DOOR, BELL SIGNAL or ACCESS FROM TERMINAL A / B functions is selected.

Access from terminal A / B – the output becomes active if a user having the required authority level gets access to the door by using the A / B reader.

In case of the outputs activated for a programmed time, you must define the operation time in seconds or minutes within the range of 1-120 seconds or 1-120 minutes.

> *i* *Additional functions of the access control module, which is part of the ACCO NET system, are described in the ACCO Soft program manual.*

A signaling device can be connected to the outputs, or they can be used to control, for example, a security system.

2. Devices interfacing with the module

For the module to be able to execute the access control functions, it is necessary to connect to it some user identification devices, a device activating the controlled door (electric strike, electromagnetic lock, gate controller, turnstile, etc.) and a sensor to monitor the door status. As the user identification devices, the LCD keypads (ACCO-KLCDR-BG / ACCO-KLCDR-BW), keypads (ACCO-SCR-BG) or proximity card readers (CZ-EMM, CZ-EMM2, CZ-EMM3 and CZ-EMM4) can be connected to each type of module. To the ACCO-KPWG-PS and ACCO-KPWG modules you can also connect the DALLAS iButton readers (CZ-DALLAS), as well as third-party readers sending data in the WIEGAND format.

When building an access control system, the ACCO-USB converter must be used. It allows control of the modules connected to the RS-485 bus from a computer. The ACCO-USB converter has been described in a separate manual.

In the case of the ACCO NET system, the access control modules must be connected to the ACCO-NT access control panel. For description of the ACCO-NT control panel, please refer to the manual delivered with the device.

2.1 ACCO-KLCDR-BG / ACCO-KLCDR-BW keypad

- Large, legible LCD display.
- Keypad to enter the access code.
- Built-in proximity card reader.
- Support of cards, key fobs and other 125 kHz passive transponders (UNIQUE, EM4001, EM4002, EM4003, EM4102).
- Indicator LEDs of the door/module status.
- Sounder generating information beeps after reading the card / entering the code (see section: AUDIBLE SIGNALING) and signaling operations performed on the keypad.
- Backlighting of the display and keys.
- Tamper contact reacting to opening of the enclosure.
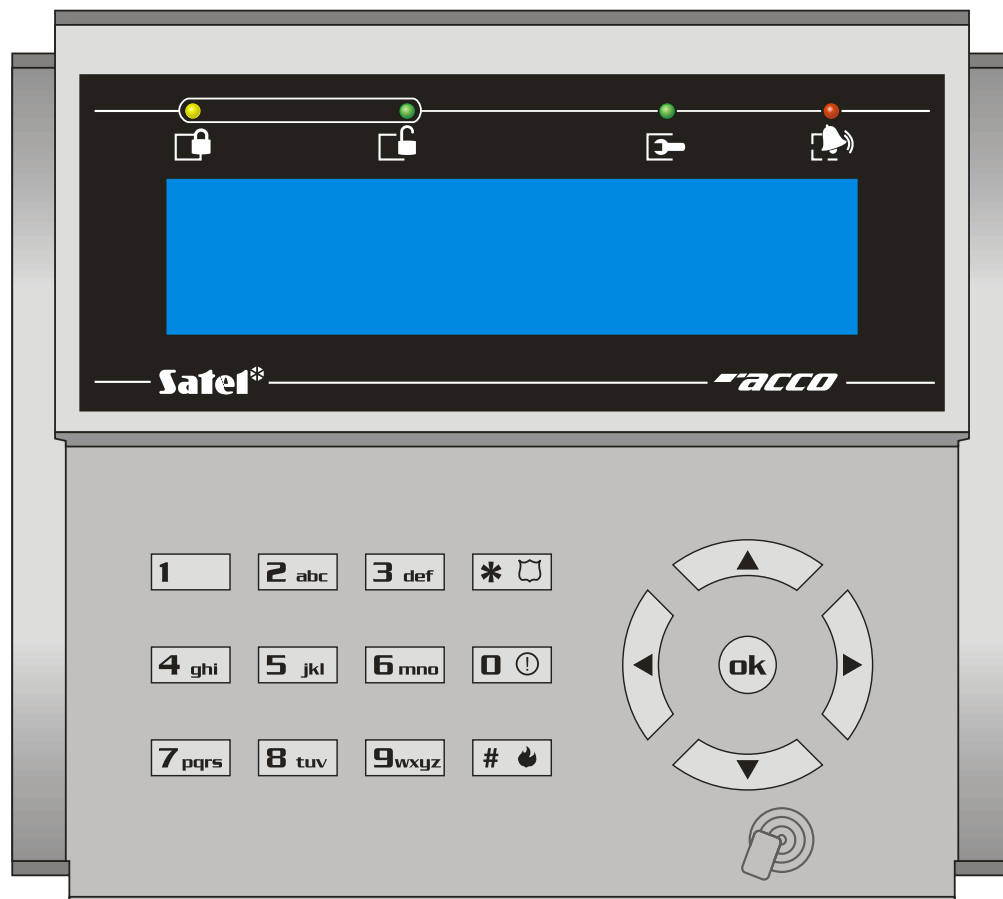
Fig. 5. View of the ACCO-KLCDR-BG keypad (the enclosure of ACCO-KLCDR-BW keypad is white).

Designation of indicator LEDs:

ALARM (red color) – the LED is lit, signaling alarm, when one of the following situations has occurred:

- door opened by force,
- 5 attempts to get access on the basis of an unknown identifier (Anti-scanner function),
- FIRE – UNBLOCK DOOR input activated,
- ALARM – BLOCK DOOR input activated,
- tamper of the door controller module (the ITMP input of module controller is isolated from the common ground),
- tamper of keypad,
- loss of communication with the terminal unit (no terminal presence).

The alarm is signaled for 10 seconds (and accompanied by audible signal). When that time expires, the LED starts blinking, thus signaling alarm memory. After the alarm cause has ceased, the alarm memory signal can be reset by the user having the ADMINISTRATOR authority. This will be done automatically after he uses his identifier. The alarm memory will also be automatically cleared when the alarm cause has ceased to exist, if the controller module is connected to the computer (by means of the RS-232 or RS-485 port) and the ACCO-SOFT-LT program. In the case of the ACCO NET system, alarm memory confirmation in the ACCO Soft program / ACCO Web application will clear the alarm memory indication on the keypad.

DOOR BLOCKED (yellow color)

- LED is lit – the door is blocked (permanently locked) and it cannot be unlock by presenting card / entering code,
- LED is blinking– the door has been blocked (permanently locked) by means of the input programmed as ALARM – BLOCK DOOR (presenting card / entering code will not unlock the door).

DOOR UNBLOCKED (green color)

- LED is lit – the door is unblocked (permanently unlocked) and presenting card / entering code is not required,
- LED is blinking slowly – the door has been unblocked (permanently unlocked) by means of the input programmed as FIRE – UNBLOCK DOOR (presenting card / entering code is not required),
- LED is blinking rapidly – the user has been granted access, the door has been unlocked and the access time countdown is running, i.e. it is possible to open the door.

SERVICE (green color) – the LED is blinking when the module is in the service mode (the function is available to the users with ADMINISTRATOR authority level if the access control module is not part of the ACCO NET system).

2.2 ACCO-SCR-BG keypad with proximity card reader

- The keypad enables entering the code.
- Support of cards, key fobs and other 125 kHz passive transponders (UNIQUE, EM4001, EM4002, EM4003, EM4102).
- Indicator LEDs of the door / module status.
- Sounder generating information beeps after reading the card / entering the code (see section: AUDIBLE SIGNALING) and signaling operations performed on the keypad.

- Backlighting of the keys.
- Tamper contact reacting the enclosure opening/pull-off.
- Bell button.
- Design enabling outdoor installation.

Information conveyed by the keypad through the indicator LEDs 🕭, 🔓 and 🔒 is identical to that in case of the LCD keypad.

Fig. 6. View of the ACCO-SCR-BG keypad.

2.3 CZ-EMM and CZ-EMM2 proximity card readers

- Support of cards, key fobs and other 125 kHz passive transponders (UNIQUE, EM4001, EM4002, EM4003, EM4102).
- Transmission format: EM-MARIN.
- Two-color indicator LED of the door/reader status.
- Built-in sounder generating information beeps after reading the card (see section: AUDIBLE SIGNALING).

The two-color indicator LED in the reader can signal as follows:

steady green light – normal operation of the reader.

blinking green rapidly – access has been granted to the user, the door has been unlocked and the access time countdown is running, so it is possible to open the door.

blinking green slowly – the door is unblocked (permanently unlocked).

blinking red slowly – the door is blocked (permanently locked).

red light, periodically extinguished – the reader has been blocked after 5 attempts to get access by using an unknown identifier (ANTI-SCANNER is activated).

steady red light – the reader cannot be controlled by the module (LCD keypad has been connected, which has disabled operation of the reader).

Fig. 7. CZ-EMM reader.

Fig. 8. CZ-EMM2 reader.

2.4 CZ-EMM3 and CZ-EMM4 proximity card readers
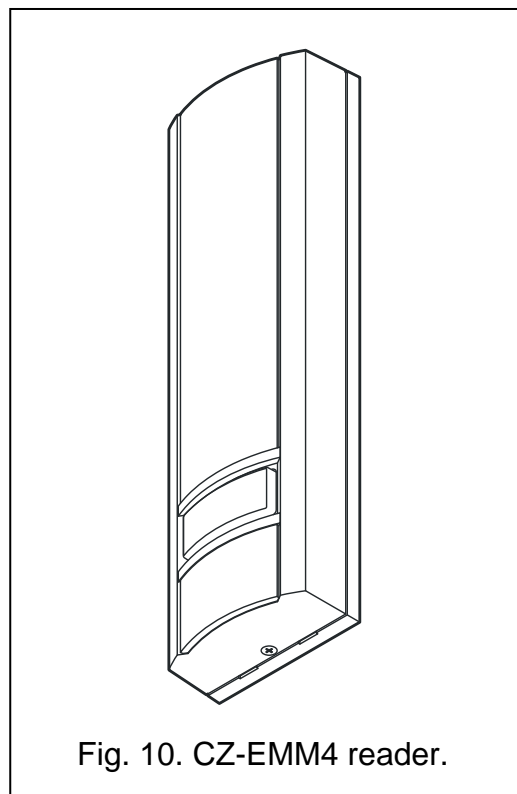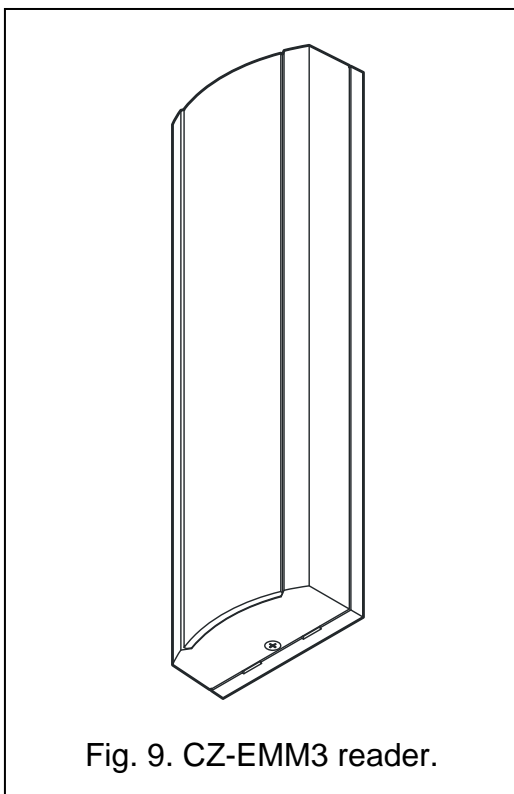
Fig. 9. CZ-EMM3 reader.

Fig. 10. CZ-EMM4 reader.

- Support of cards, key fobs and other 125 kHz passive transponders (UNIQUE, EM4001, EM4002, EM4003, EM4102).
- Transmission format: EM-MARIN or WIEGAND 26.
- Two indicator LEDs of the door/reader status.
- Built-in sounder generating information beeps after reading the card (see section: AUDIBLE SIGNALING).
- Design enabling outdoor installation.
- Bell button in the CZ-EMM4 reader.

i | *In the WIEGAND format, double-tapping the same card on the reader is interpreted as holding the card. Not all readers will support this feature. Please check your readers for this functionality.*

It is recommended that the SATEL's CZ-EMM3 and CZ-EMM4 proximity card readers work in the EM Marin format.

The green LED in the reader signals as follows:

lit – normal operation of the reader.

blinking rapidly – access has been granted to the user, the door has been unlocked and the access time countdown is running, so it is possible to open the door.

blinking slowly – the door is unblocked (permanently unlocked).

The red LED in the reader signals as follows:

lit – the reader cannot be controlled by the module (LCD keypad has been connected, which has disabled operation of the reader).

blinking slowly – the door is blocked (permanently locked).

lit, but periodically extinguished – the reader has been blocked after 5 attempts to get access by using an unknown identifier (ANTI-SCANNER is activated).

2.5 CZ-DALLAS DALLAS iButton reader

- DALLAS iButton support.
- Two-color indicator LED.
- Designed for outdoor installation – directly into the wall or door frame.
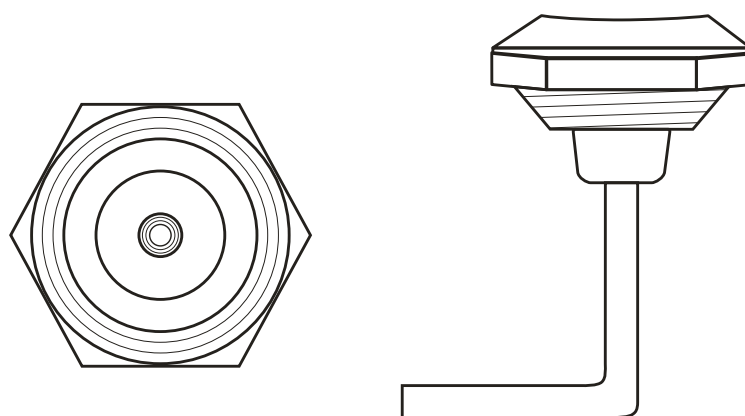
Fig. 11. CZ-DALLAS reader.

The reader bicolor LED indications have the following meaning:

LED lit up green – the reader is working properly.

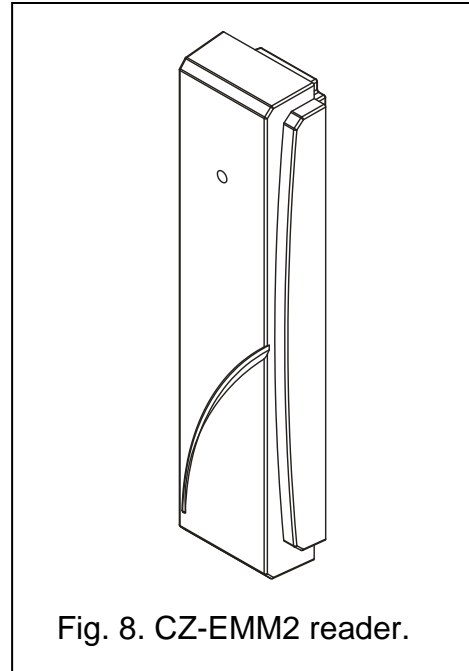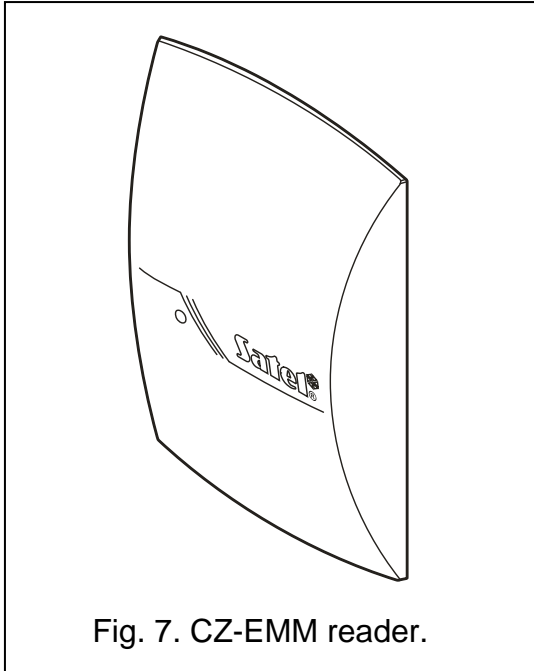**LED flashing fast green** – access has been granted to the user, the door has been unlocked and the access time countdown is running, so it is possible to open the door.

**LED flashing slow green** – the door is unblocked (permanently unlocked).

LED flashing slow red – the door is blocked (permanently locked).

LED lit up red, but periodically extinguished – the reader has been blocked after 5 attempts to get access by using an unknown identifier (ANTI-SCANNER is activated).

LED lit up red – the reader cannot be controlled by the module (LCD keypad has been connected, which has disabled operation of the reader).

2.6 Third-party readers

- WIEGAND transmission format:
  26 bit – parity bit (even) + card number (24 bits) + parity bit (odd); byte order: from MSB to LSB;

  32 bit – card number (32 bits) without parity check; byte order: from MSB to LSB;

  34 bit – parity bit (even) + card number (32 bits) + parity bit (odd); byte order: from MSB to LSB;

  36 bit – parity bit (even) + card number (34 bits) + parity bit (odd); byte order: from MSB to LSB;

  40 bit – card number (40 bits) without parity check; byte order: from MSB to LSB;

  42 bit – parity bit (even) + card number (40 bits) + parity bit (odd); byte order: from MSB to LSB;

  56 bit – card number (56 bits) without parity check; byte order: from LSB to MSB; the controller uses the five most significant bytes received, rejecting the other ones.

i | *In the WIEGAND format, double-tapping the same card (identifier) on the reader is interpreted as holding the card. Not all readers will support this feature. Please check your readers for this functionality.*

3. CZ-USB-1 proximity card reader

- Connection to the computer USB port.
- Ability to add 125 kHz (EM4100) cards and key fobs to the system users.

4. Access control installation

⚠️ | **Disconnect power supply before making any electrical connections.**

Explanations for Fig. 12:

1 – **door controller module**.

2 – **controlled door activator** (electromagnetic lock controlled from the module relay output).

3 – **controlled door sensor** (magnetic detector connected to the module input programmed as DOOR STATUS CONTROL).

4 – **exit terminal** (proximity card reader connected as reader B).

5 – **entry terminal** (proximity card reader connected as reader A).
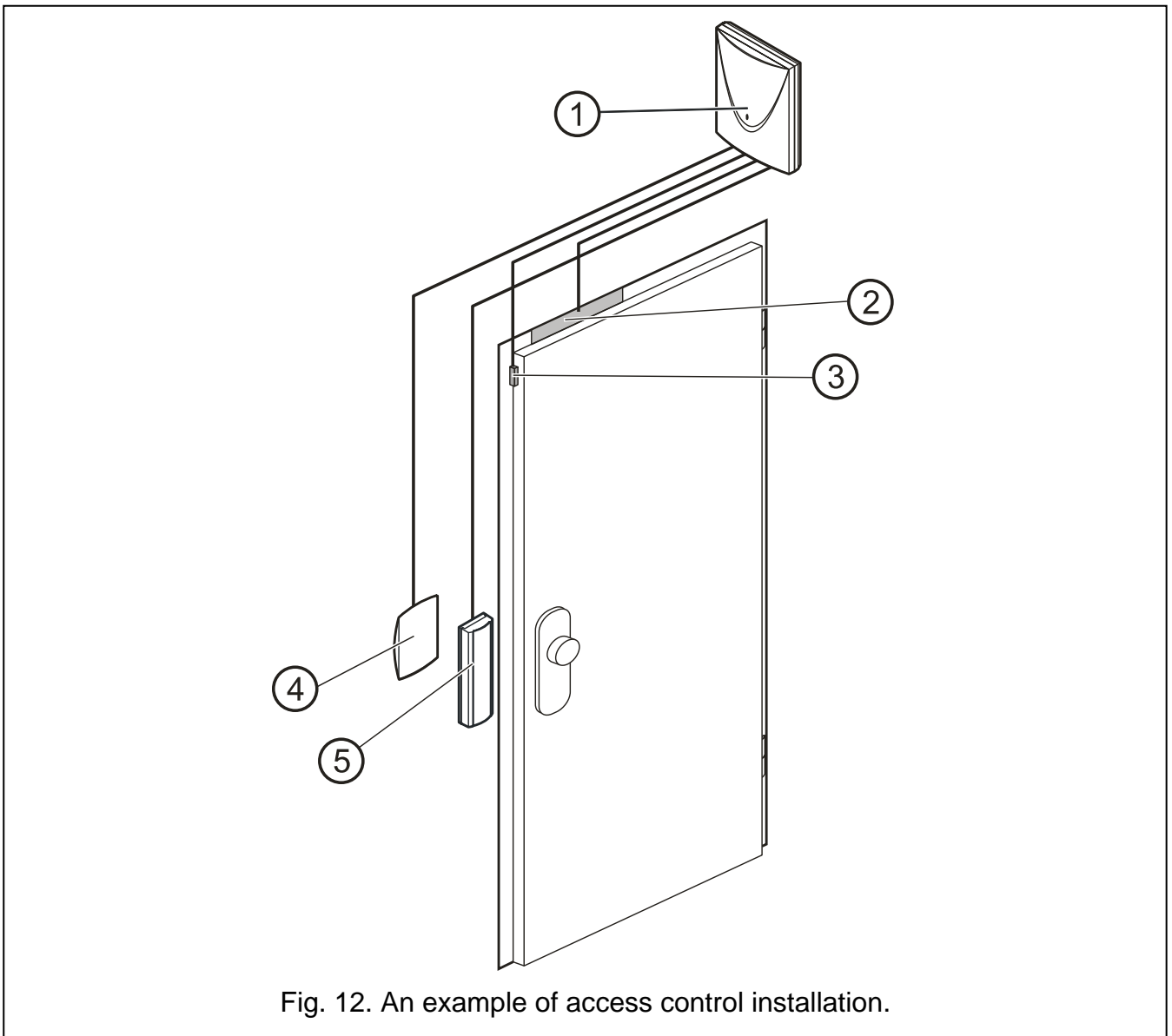
Fig. 12. An example of access control installation.

The door controller module should be installed indoors, in spaces with normal air humidity. The controller module installation place should be protected against access of unauthorized persons. It is recommended that the controller module be installed within the area which is protected (e.g. by security system).

The distance between the terminal units should be not less than 50 cm.

Mounting the terminals (keypads with proximity card reader, readers) on metal surface or in metal enclosure may result in reduction of the reader range or even make the proximity card readout entirely impossible.

For connection of the terminals, activators (electric strike, electromagnetic lock) and sensors of the controlled door, it is recommended that straight-through unscreened cable be used (using the "twisted-pair" type of cable, e.g. UTP, STP, FTP, is not recommendable). Select the cross-section area of the power leads so that the supply voltage drop between the power supply unit and the supplied device not exceed 1 V as compared with the output voltage.

When connecting a proximity card / iButton reader or LCD keypad as the terminal A, you should remember that it will be recognized as the entry terminal. A proximity card / iButton reader or LCD keypad working as the terminal B will be recognized as the exit terminal.

The above description of how to connect a reader or keypad working as terminal A / B does not apply to a reader or keypad to be connected to the module being part of the ACCO NET system.

4.1 Connecting the ACCO-KLCDR-BG / ACCO-KLCDR-BW keypad

You can connect the LCD keypad to the module by means of the terminals on electronics board or the RJ socket. Use four-core cable for making the connection. The distance between the keypad and the module can be up to 300 m.
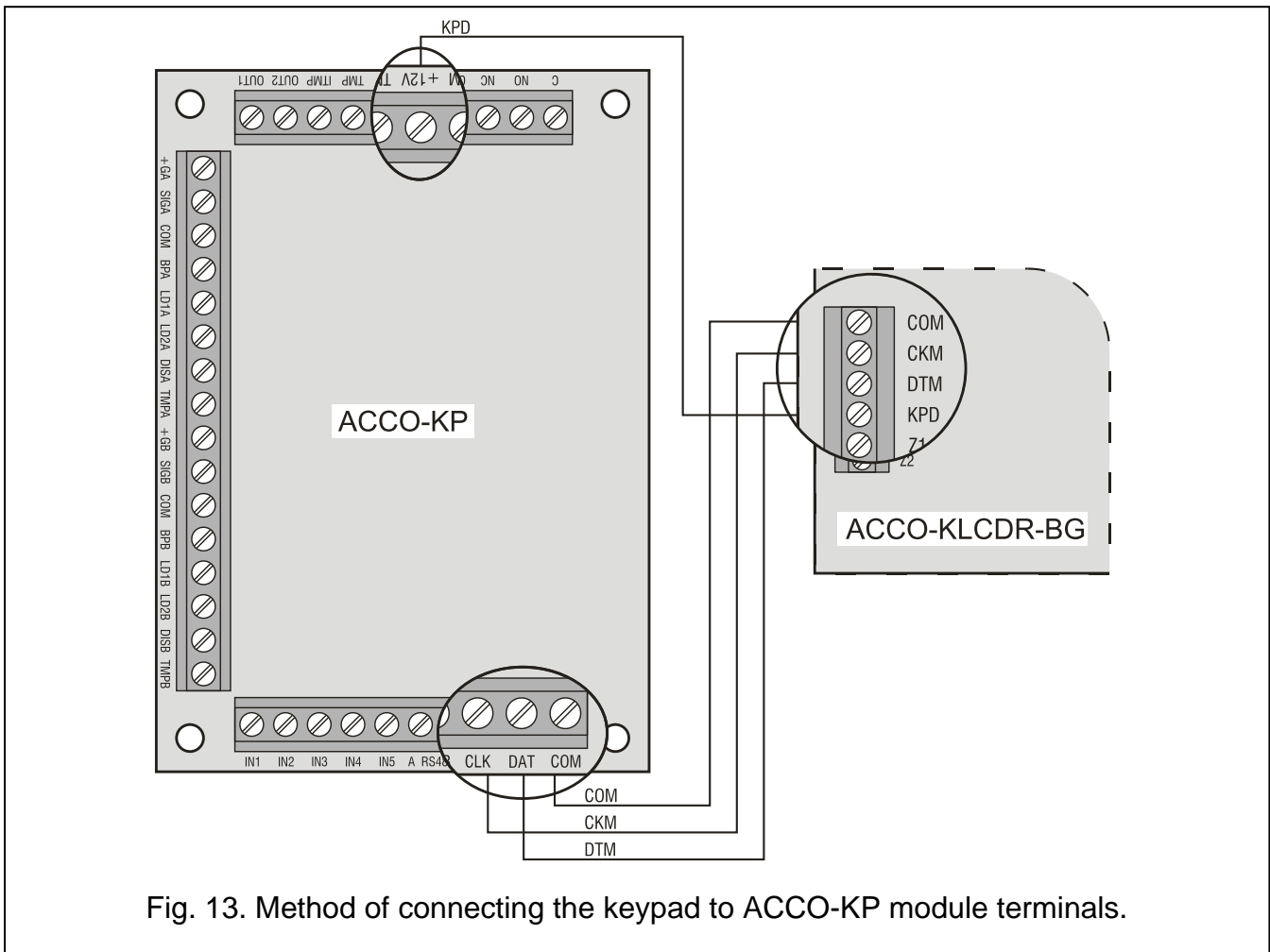
Fig. 13. Method of connecting the keypad to ACCO-KP module terminals.

The module supports keypads with addresses 0 and 1. The keypad with address 0 will serve as terminal A (entry terminal). The keypad with address 1 will serve as terminal B (exit terminal). The information whether the keypad performs the function of terminal A or B can be read out from the display after restarting the keypad (in order to cause the restart, hold down the ▲ and ▼ keys for approximately 10 seconds).

Connecting the LCD keypad with address 0 will switch off the proximity card reader working as reader A. Connecting the LCD keypad with address 1 will switch off the proximity card reader working as reader B.

Never connect two devices (LCD keypads, keypads) which have an identical address.

If the clock and additional information fail to appear on the keypad display after power-up, make sure that:

− the cables connecting the keypad to the module have been properly connected;
− a correct address is set in the keypad.

4.1.1 Connecting the LCD keypad to terminals

The method of connecting the keypad communication bus to the terminals of ACCO-KP and ACCO-KP-PS modules is shown on Fig. 13 and Fig. 14.

Fig. 14. Method of connecting the keypad to ACCO-KP-PS module terminals.
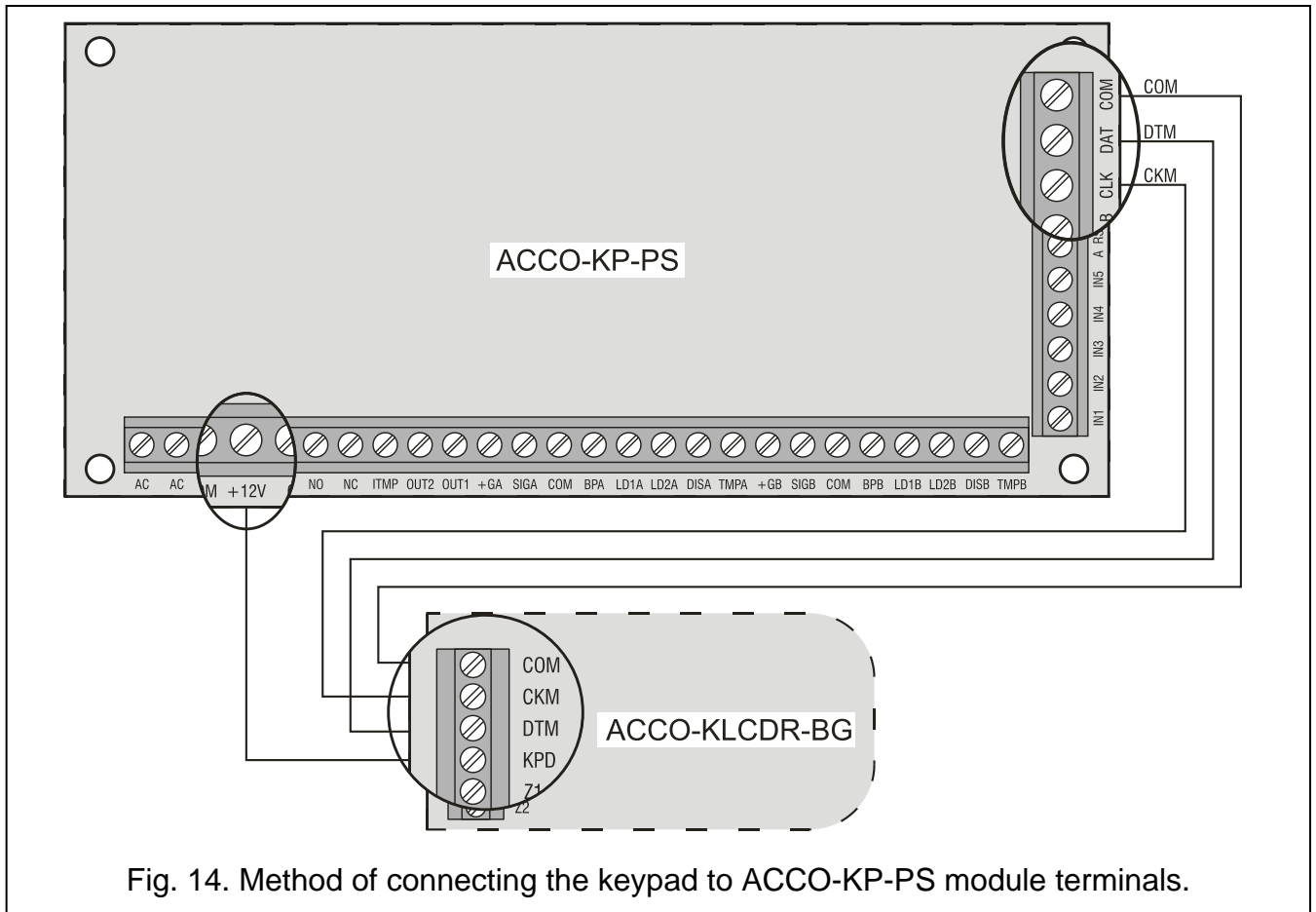
4.1.2 Connecting the LCD keypad to RJ socket

The method of connecting the LCD keypad communication bus to the RJ socket is shown on Fig. 15. The socket is dedicated to connecting the LCD keypad for the duration of programming whenever devices connected to the module do not offer the possibility of its programming.

1 - +KPD
2 - CKM
3 - DTM
4 - COM

Fig. 15. Sequence of wires in the plug connecting LCD keypad with module. 1 – view of plug in socket. 2 – view of plug from pins side.
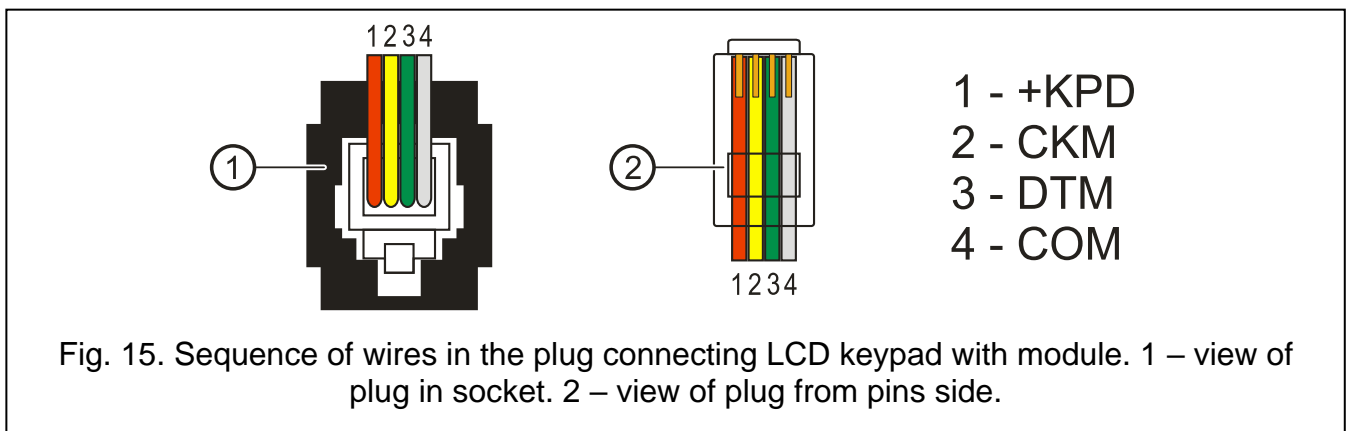
In order to program the module, you can use any LCD keypad supported by the INTEGRA control panels. However, such a keypad is not recommended for everyday operation of the module because of different LED designations. The module can handle the readers in INT-KLCDR-GR and INT-KLCDR-BL LCD keypads with firmware version 1.06 or later.

i | *The above description of programming with LCD keypad does not apply to the access control module being part of the ACCO NET system.*

If one ACCO-SCR-BG keypad and any proximity card reader is connected to the controller module, the address set in LCD keypad must be different from that set in the keypad:

– 1 – if address 0 is set in the keypad,

– 0 – if address 1 is set in the keypad.

If 2 ACCO-SCR-BG keypads are connected to the controller module, you must disconnect one of them from the DAT terminal (green wire), and set in the LCD keypad the identical address, as in the disconnected keypad.

4.1.3 Setting the LCD keypad address

1. Disconnect the keypad supply (KPD) and the data bus cables (CKM, DTM).
2. Short together the keypad terminals CKM and DTM.
3. Connect the keypad supply.
4. Keypad address will be displayed:

```
This LCD address
(n, 0-7): _
```
n=0...7, currently set
keypad address

Fig. 16. Programming LCD keypad address.

5. Change the address to the correct one (0 or 1). The keypad will acknowledge the address setting by 4 short beeps and 1 long beep.
6. Disconnect the keypad supply (KPD).
7. Connect the keypad to the door controller module in the correct way (CKM, DTM and KPD).

4.2 Connecting the ACCO-SCR-BG keypad

The keypad should be connected in accordance with Table 1. The connection is to be made with five-core cable. The distance between keypad and module can be up to 300 m.

The module supports keypads with addresses 0 and 1. The keypad with address 0 will function as terminal A (entry terminal). The keypad with address 1 will function as terminal B (exit terminal).

Wire color	Function	Module terminals			
		ACCO-KP-PS / ACCO-KP		ACCO-KPWG-PS / ACCO-KPWG	
		Reader A	Reader B	Reader A	Reader B
■ brown	power supply	+12V			
□ white	common ground	COM			
■ gray	clock	CLK			
■ green	data	DAT			
■ yellow	bell	IN1…IN5 (chosen module input, programmed as BELL SIGNAL)			
■ violet	reader operation blocking (if the readers are operating in close vicinity to each other, to eliminate mutual interference)	DISA	DISB	DISA	DISB

Table 1. Method of connecting keypad wires to module terminals.

ℹ️ *The violet wire is provided in keypads with firmware version 2.01 or later.*

Connecting the keypad with address 0 will switch off the proximity card reader working as reader A. Connecting the keypad with address 1 will switch off the proximity card reader working as reader B.

Never connect two devices (LCD keypads, keypads) which have an identical address.

The yellow wire is connected to the OC low-current output, controlled by means of the bell button. Press the button to short the output to common ground. The yellow wire (bell) can be connected to the module input programmed as BELL SIGNAL.

4.2.1 Setting the keypad address

1. Disconnect the brown, gray and green wires from the module terminals.
2. Short the ends of gray and green wire.
3. Reconnect the brown wire to the +12V terminal. After the power lead is connected, the keypad will generate 4 short beeps and 1 long beep, and the LEDs designated 📢 [ALARM] and 🔓 [DOOR UNBLOCKED] will start alternately blinking (then the ends of gray and green wire may be separated).
4. Press in turn the keys $\boxed{1}$ and $\boxed{\#}$. The keypad will acknowledge starting the address setting function with 2 short beeps, and the LED designated 📢 [ALARM] will start blinking.
5. Depending on which address is to be set in the keypad, press $\boxed{0}$ or $\boxed{1}$ and confirm with the $\boxed{\#}$ key. The keypad will confirm the address setting by 4 short beeps and 1 long beep.
6. Disconnect the brown wire from the +12V terminal.
7. Connect correctly to the module the following wires: gray (CLK), green (DAT) and brown (+12V).

4.3 Connecting the proximity card readers

The readers with support for EM-MARIN data transfer format (used for communication with devices manufactured by SATEL) should be connected using the cable in accordance with Table 2. The length of the cable connecting reader with module should not exceed 30 m.

i *In case of CZ-EMM3 and CZ-EMM4 readers the brown wire must be connected to the module.*

The violet wire in the CZ-EMM4 reader is connected to the OC low-current output, controlled by means of the bell button. When the button is pressed, the output is shorted to common ground. The violet wire (bell) can be connected to the module input programmed as BELL SIGNAL.

The black wire available in the CZ-EMM3 and CZ-EMM4 readers is not used and should not be connected to any terminal of the module.

Wire color	Function	Module terminals			
		ACCO-KP-PS / ACCO-KP		ACCO-KPWG-PS / ACCO-KPWG	
		Reader A	Reader B	Reader A	Reader B
red	supply (12 VDC ±15%)	+GA	+GB	+G	
green	data	SIGA	SIGB	SIG1A	SIG1B
blue	common ground	COM	COM	COM	
yellow	sounder control	BPA	BPB	BPA	BPB
pink	LED green color control/ green color LED control	LD1A	LD1B	LD1A	LD1B
gray	LED red color control/ red color LED control	LD2A	LD2B	LD2A	LD2B
brown	reader operation blocking (if the readers are operating in close vicinity to each other, to eliminate mutual interference)	DISA	DISB	DISA	DISB
white	presence control	TMPA	TMPB	TMPA	TMPB
violet	bell (in CZ-EMM4 only)	IN1…IN5 (selected input of the module, programmed as BELL SIGNAL)			
black	*unused* (in CZ-EMM3 and CZ-EMM4 only)	*do not connect*			

Table 2. Method of connecting the reader wires to the module terminals.

4.4 Connecting the Wiegand readers

The readers should be connected according to Table 3. The length of cable connecting the reader with the module should not exceed 30 m.

Wire color	Function	Module terminals		Designation for WIEGAND 26
		Reader A	Reader B	
🟥 red	power	+G		+12V
🟦 blue	common ground	COM		COM
🟩 green	data (0)	SIG1A	SIG1B	OUT0
⬛ black	data (1)	SIG2A	SIG2B	OUT1
🟨 yellow	sounder control	BPA	BPB	BEEP
🟪 pink	green color LED control	LD1A	LD1B	LED-G
⬜ gray	red color LED control	LD2A	LD2B	LED-R
🟫 brown	reader operation blocking	DISA	DISB	HOLD
⬜ white	presence control	TMPA	TMPB	TMP
🟪 violet	bell (in CZ-EMM4 only)	IN1…IN5 (selected input of the module, programmed as Bell signal)		BELL

Table 3. Method of connecting the reader wires to the module terminals.

4.5 Connecting DALLAS iButton readers

The DALLAS iButton readers only work with the ACCO-KPWG-PS and ACCO-KPWG modules. The readers should be connected with cable, according to Table 4. The length of the cable connecting the reader to the module should not exceed 30 m.

Wire color	Function	Module terminals ACCO-KPWG-PS / ACCO-KPWG	
		Reader A	Reader B
🟫 brown	red LED anode	LD2A	LD2B
⬜ white	data	SIG1A DISA	SIG1B DISB
⬜ gray	common ground	COM	COM
🟩 green	green LED anode	LD1A	LD1B
🟨 yellow	LED cathode	COM	COM

Table 4. Method of connecting the reader wires to the module terminals.

ℹ️ When connecting the A reader, remember to connect the SIG1A and DISA terminals with an additional wire. Similarly, in the case of the B reader, be sure to link the SIG1B and DISB terminals.

4.6 Connecting CZ-USB-1 proximity card reader

Connect the CZ-USB-1 reader to the computer USB port. When the LED goes on, the reader is ready for work.

4.7 Connecting activators and sensors of the controlled door

The device which is to activate the door should be connected to the suitable terminals of the relay output. The sensor monitoring the door status should be connected to one of the module inputs (by default, the input 1 is programmed as the Door status control, NO type, but it is possible to select any of the five inputs and program it accordingly).

4.8 Mantrap / airlock

The mantrap / airlock consists of at least 2 doors and requires the use of 1 controller module for each door (see Fig. 17). In the mantrap / airlock configuration, both doors cannot be opened simultaneously.
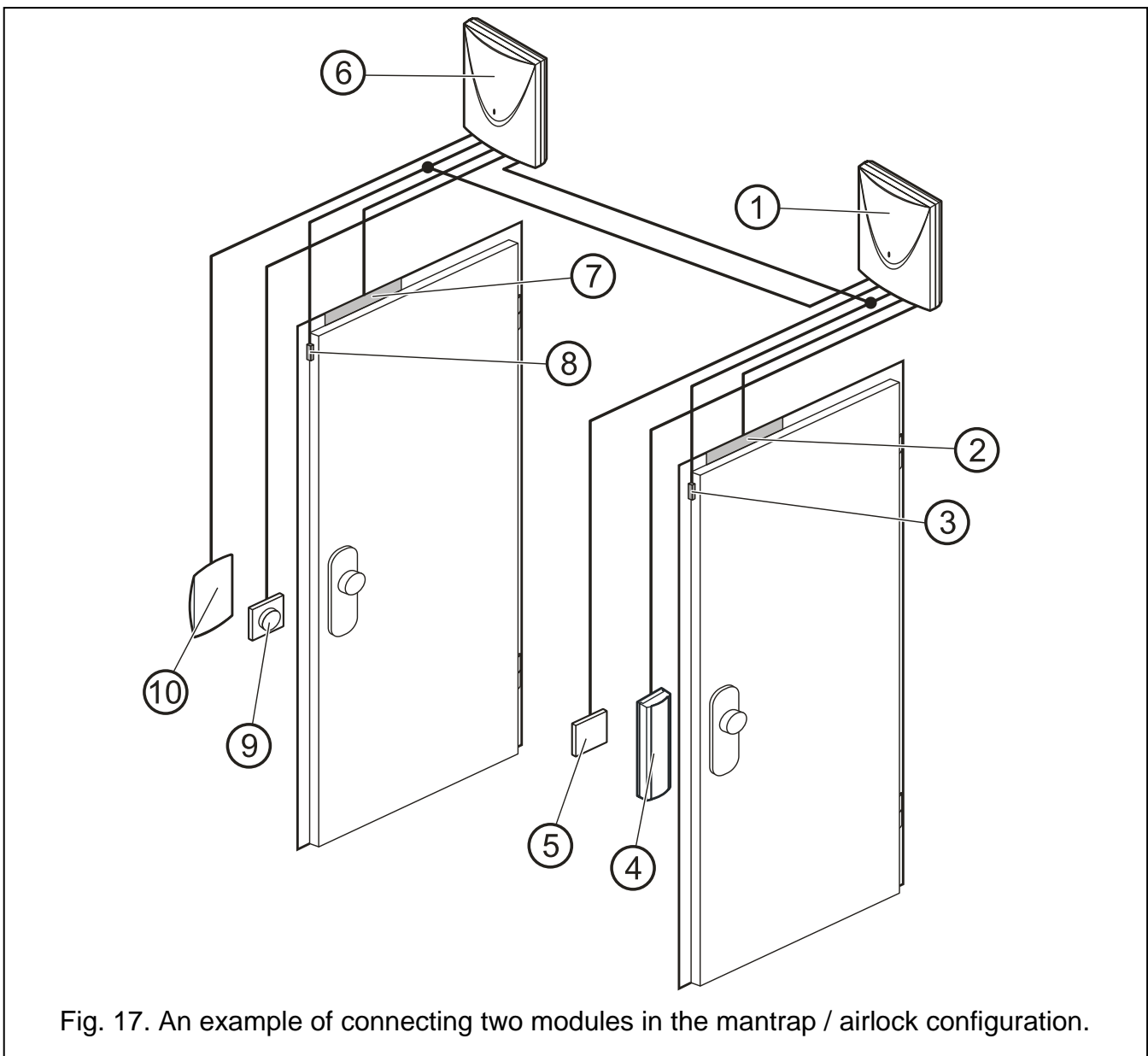
Fig. 17. An example of connecting two modules in the mantrap / airlock configuration.

Explanations for Fig. 17:

1 – **module 1** supervising the door 1.

2 – **door 1 activator** (electromagnetic lock controlled from the relay output of module 1).

3 – **door 1 status sensor** (magnetic detector connected to the module 1 input programmed as DOOR STATUS CONTROL and the module 2 input programmed as SLUICE CONFIGURATION).

4   – **entry terminal** (proximity card reader connected as reader A do the module 1).

5   – **button unlocking the door 1** (connected to the module 1 input programmed as UNLOCK BUTTON – substitutes the exit terminal for the door 1).

6   – **module 2** supervising the door 2.

7   – **door 2 activator** (electromagnetic lock controlled from the relay output of module 2).

8   – **door 2 status sensor** (magnetic detector connected to the module 2 input programmed as DOOR STATUS CONTROL and the module 1 input programmed as SLUICE CONFIGURATION).

9   – **button unlocking the door 2** (connected to the module 2 input programmed as UNLOCK BUTTON – substitutes the exit terminal for the door 2).

10 – **exit terminal** (proximity card reader connected as reader B to the module 2).

i | *In the case of mantrap / airlock consisting of 3 or more doors, remember to correctly connect the magnetic contact detectors. Each detector of this type connected to an input programmed as DOOR STATUS CONTROL of one of the modules, must be also connected to inputs programmed as SLUICE CONFIGURATION of all other modules creating a mantrap / airlock.*

4.9 Connecting power supply

4.9.1 ACCO-KP / ACCO-KPWG module

The ACCO-KP / ACCO-KPWG module requires supply with direct voltage 12 V (±15%). You can use the APS-412 power supply unit, manufactured by SATEL, as supply source for the module. When selecting the power supply, take into account the balance of currents in the system. The power supply cable and common ground should be connected to the respective module terminals (+12V and COM). After power supply is turned on, the module starts up (the green LED on the electronics board goes on) and is ready for operation.

4.9.2 ACCO-KP-PS module

The ACCO-KP-PS / ACCO-KPWG-PS module requires supply with alternating voltage 18 V (±10%). The transformer secondary winding should be used as supply source for the module. It is recommended that a transformer with at least 40 VA capacity be used.

⚠ | **Never connect two devices with power supply unit to one transformer.**

Before hooking up the transformer to the circuit from which it will be supplied, remember to deenergize the circuit.

Because the ACCO-KP-PS / ACCO-KPWG-PS door controller module has no power switch, it is important that the device owner or user be advised on how the device is to be disconnected from the mains (e.g. by showing the cut-out in the module supply circuit).

The transformer should be permanently connected do the 230 VAC mains voltage. Therefore, before you are about to make the cabling, familiarize yourself with the facility electrical installation. Select the circuit which is always energized as your supply circuit. The circuit should be protected by an appropriate safety device.

12 V / 7 Ah battery should be connected to the ACCO-KP-PS / ACCO-KPWG-PS door controller module as an emergency power source.

To connect power supply to the module, proceed as follows:

1. Switch off supply in the 230 VAC circuit to which the transformer is to be connected.

2. Connect the 230 VAC cables to the terminals of transformer primary winding.

3. Connect the terminals of transformer secondary winding to the AC terminals on the module electronics board.

4. Switch on the 230 VAC supply in the circuit to which the transformer is connected. Measure the voltage across the batter leads (the correct value is between 13.6 and 13.8 VDC) and check that all devices connected to the module are properly supplied.

5. Switch off supply 230 VAC.

6. Connect the battery. The module will not start after the battery alone is connected.

i | *If the battery voltage drops below 11 V for longer than 12 minutes (3 battery tests), the module will signal low battery. After the voltage drops to approx. 9.5 V, the battery will be disconnected.*

7. Switch on the 230 VAC supply in the circuit to which the transformer is connected. The module is ready for operation.

The above-mentioned sequence of switching on power (the battery first, and then the 230 VAC mains) will enable proper operation of the power supply unit and electronic safety circuits of the module, thus preventing failures due to possible installation mistakes. If a situation occurs, when entire disconnection of the power supply is necessary, then switch off the mains first, and then the battery.

5.   Addressing the module

Setting an individual address is required, if the ACCO-SOFT-LT program is to support several modules or if the module is to work in the ACCO NET system. The module addresses must not be repeated.

For setting the module address, use the DIP-switches provided on the electronics board (see Figures 1, 2, 3 and 4). Eight DIP-switches make it possible to set 256 different addresses (from 0 to 255). **Address 0 must not be set.** In order to determine the module address, add together the values set on individual DIP-switches, according to Table 5. When the address is set, it can be checked in the LCD keypad connected to the module (not applicable to ACCO NET system) by using the function ADDRESS (SERVICE MODE →MODULE DATA →ADDRESS) or in the ACCO-SOFT-LT / ACCO Soft program.

DIP-switch number	1	2	3	4	5	6	7	8
Numerical value (for switch in ON position)	1	2	4	8	16	32	64	128

Table 5.

address: 150   address: 196

Fig. 18. Examples of setting address on DIP-switches.
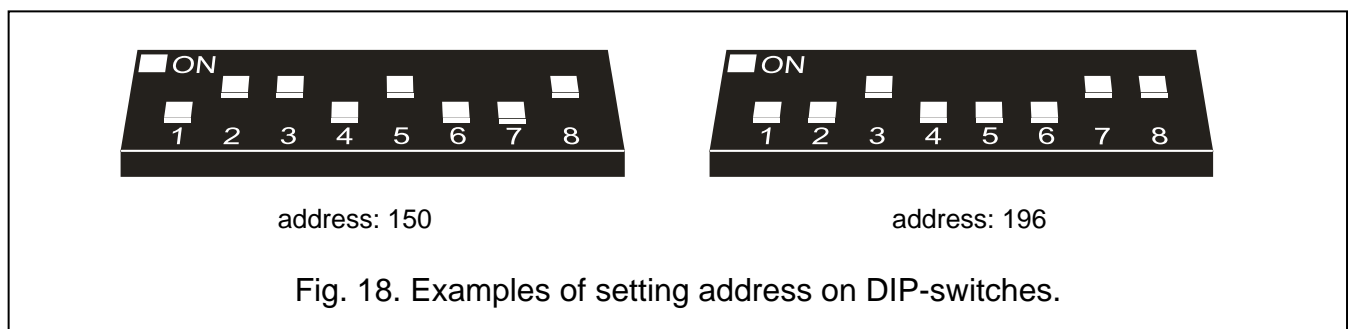
6.   Programming the module

$\boxed{i}$ *In the case of the ACCO NET system, you must not:*
   – *connect the computer to the RS-485 bus via the ACCO-USB converter;*
   – *connect the module to the computer through the RS-232 port.*

   This section does not apply to the access control module, which is part of the ACCO NET system.

You can configure for work the door controller module by means of the LCD keypad or PC computer with the ACCO-SOFT-LT program installed.

You can connect the LCD keypad to the module as a terminal unit. Connecting the LCD keypad for the programming time only is also possible due to the RJ socket provided on the electronics board.

The computer can communicate with the module in two ways:

1. RS-232. Connect the module port to the COM serial port of the computer by means of the USB-RS converter manufactured by SATEL.

2. RS-485. Connect the module port to the bus connecting the modules into a system. Connect the computer to the bus by means of the ACCO-USB converter manufactured by SATEL (for description of the connection method, see the converter manual).

Programming by means of the ACCO-SOFT-LT should be done in the same way for both communication methods.

6.1 Programming from LCD keypad

The LCD keypad makes it possible to configure the module as well as to add and remove users in the module to which the LCD keypad is connected. Editing the access schedules is not available in the LCD keypad.

$\boxed{i}$ *Adding and removing users by means of the LCD keypad in case of the modules operating within the access control system is not recommended.*

The programming is carried out by means of functions available in the service mode. In order to start the service mode, enter code of the user with ADMINISTRATOR authority and press the $\boxed{* \circlearrowleft}$ key. Using the key designated ▲ or ▼, find the SERVICE MODE item in the menu which will be displayed. When the display arrow indicates the a.m. item, press $\boxed{\# \; \spadesuit}$, $\circledcirc$ or ▶. The service mode is signaled by the $\boxminus$ [SERVICE] LED lighting up.

6.1.1 Service mode menu

Navigation through the service mode menu is possible by means of the arrow keys and the $\boxed{* \circlearrowleft}$, $\boxed{\# \; \spadesuit}$ or $\circledcirc$ key. The ▼ and ▲ keys enable scrolling through the list of functions. In order to enter the submenu or start the selected function, press the ▶, $\boxed{\# \; \spadesuit}$ or $\circledcirc$ key. In order to quit the submenu, press ◀ or $\boxed{* \circlearrowleft}$. In order to quit the submenus and functions where options and parameters are programmed, confirm the introduced changes by pressing the $\boxed{\# \; \spadesuit}$ or $\circledcirc$ key, or, if you exit without making any changes – by pressing the $\boxed{* \circlearrowleft}$ key.

```
Users ──────────┬── Add user
                └── Find user

Inputs ──────── Input n ────────┬── Function
                                └──Sensitivity
```

Outputs ──────── Output *n* ──────── OUT*n* function
                                       ├─ Operation time
                                       └─ Polarity

Access mode ──── Card or code
                 ├─ Card and code
                 ├─ Code only
                 └─ Card only

Door ──────── Options ──────── Door status control disable
                              ├─ Unauthorized open – event
                              ├─ Unauthorized open – alarm
                              ├─ Off if door open
                              └─ Off if door closed
              └─ Times ──────── Access time
                              ├─ Door open time
                              ├─ Unblocking start
                              ├─ Unblocking end
                              ├─ Blocking start
                              └─ Blocking end

Module ──────── Options ──────── Terminal A
                                 ├─ Terminal B
                                 ├─ Anti-passback
                                 ├─ APB – event only
                                 ├─ Anti-Scanner
                                 └─ Time pattern
                ├─ Data format A** ──────── DALLAS
                                         ├─ WIEGAND 26
                                         └─ EM-MARINE
                ├─ Data format B** ──────── DALLAS
                                         ├─ WIEGAND 26
                                         └─ EM-MARINE
                ├─ Clock ──────── Set time & date
                               ├─ Clock adjustment
                               ├─ Daylight saving
                               ├─ DST starts
                               └─ DST ends
                └─ Times ──────── APB resetting time
                               └─ AC loss delay *

LCD ──────── Clock format
            └─ Options ──────── Work time log
                             ├─ Show name
                             └─ Show name-2nd

Backlight ──────── A Backlight
                   └─ B Backlight

Module data ────── Address
                  ── Module ID
                  ── Firmware version

Service end

6.1.2 Data entry

Digital data (e.g. user ID number, time, etc.) should be entered by means of respective numerical keys. Where a digit is to be entered, the cursor flashes. It can be moved by means of the ◄ and ► keys.

The LCD keypad keys make it also possible to enter other characters in the user name entry function. Press the key repeatedly to change the character to another one, according to Table 6. The cursor flashing at the place of the character being entered can be moved by means of the ◄ and ► keys. Press the ▲ key to move the cursor to the left, deleting the character that was previously in that place. Press the ▼ key to enter the space character in the cursor place (if any other character was there previously, it will be moved by one position to the right).

Key	Characters available on next keystroke
1	1 ! ? ' ` ↵ " { } $ % & @ \ ^ | ⴺ #
2	A a B b C c 2
3	D d E e F f 3
4	G g H h I i 4
5	J j K k L l 5
6	M m N n O o 6
7	P p Q q R r S s 7
8	T t U u V v 8 · ■ █ ⏸ ↑ ← → ↓
9	W w X x Y y Z z 9
0	0 . , : ; + - ✳ / = _ < > ( ) [ ]

Table 6. Characters available in LCD keypad.

6.1.3 Programming bit options

Enabling an option is indicated on the display by the ⏸ character next to the given option name. If the option is disabled, it will be indicated by the · character. Press any numerical key to enable / disable the option.

6.2 ACCO-SOFT-LT program

i   *Modules with the firmware version 3.05 require the ACCO-SOFT-LT program in version 1.07.006. Information about modules with an earlier firmware version are available at www.satel.eu*

The ACCO-SOFT-LT program enables configuration from 1 to maximum 255 modules in the system. The access schedules and the users are created by means of the program and are global by nature. The access schedules are saved in all modules supported by the program. The user related data are only saved in the modules which are accessible to those users.

Owing to the ACCO-SOFT-LT program, the administrator gets an extra tool to supervise operation of the system, such as visualization of the module status, or readout of events. The advanced filtering function makes it possible to extract the events which are needed by the administrator at the moment. This function enables, among other things, displaying events related to the personnel presence at the workplace and using them afterwards in order to calculate the attendance time.

Using the program, it is possible to copy data between the modules.

6.2.1 Installation and first start of the program

i *You must have administrator privileges to run the installation and start the ACCO-SOFT-LT program.*

1. Start the installation program and indicate the directory where the program is to be installed.
2. Start the ACCO-SOFT-LT program. Access to the program is protected by a password. When running the program for the first time, you will get access on the basis of default password, which is already entered. The default password can be read then (see Fig. 19). **It is recommended that the password of access to the program be changed after the first start.** In order to do so, open the main menu of the program, enter the FILE menu and select PROGRAM ACCESS, and then CHANGE PASSWORD. To change login or add other users who will be authorized to use the program, enter the FILE menu and select PROGRAM ACCESS, and then PROGRAM USERS.
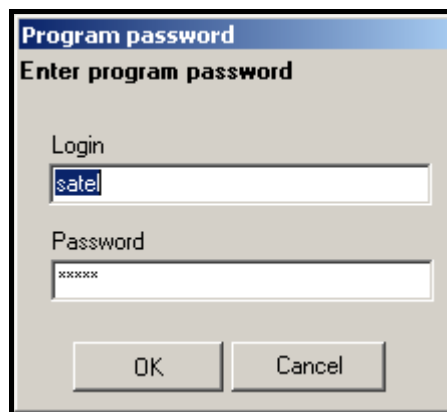
Fig. 19. Password entry window on the first start of the program.

i *Entering three invalid passwords will terminate the program.*
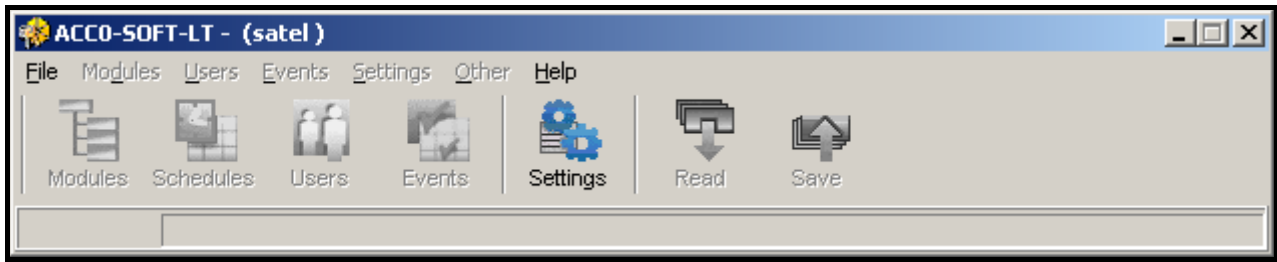
Fig. 20. Program menu bar after login.

3. After logging in, the only active button on the menu bar will be the one designated as SETTINGS. If it is necessary to change the language version of the program, click on the button. When the SYSTEM SETTINGS window will open, select the required version in the window, close the program and then log in again, as the change of language version will only take effect after the program is restarted.

4. Create a configuration file in which all information related to the module (system consisting of several modules) served by the program will be saved. For this purpose, open the FILE menu and select the NEW item. The window shown on Fig. 21. will open. You have to fill in the SYSTEM NAME and SYSTEM IDENTIFIER fields and select the computer port through which communication with the module(s) will be effected. Next, click on the FIND button (the module or modules connected to the indicated computer port will be found by the program itself) or directly on the OK button.

1 - enter the system name in this field. The configuration file will be saved under this name on the computer. The field must be filled.

2 - in this field, you can give additional information on the system.

3 - enter the system identifier in this field. It can include up to 10 characters. You can enter digits from 0 to 9 and letters from A to F. The field must be filled.

4 - select the computer port through which communication with the module / modules will take place.

5 - click on the button with your mouse cursor to start the procedure of searching for modules connected to the indicated port of the computer.
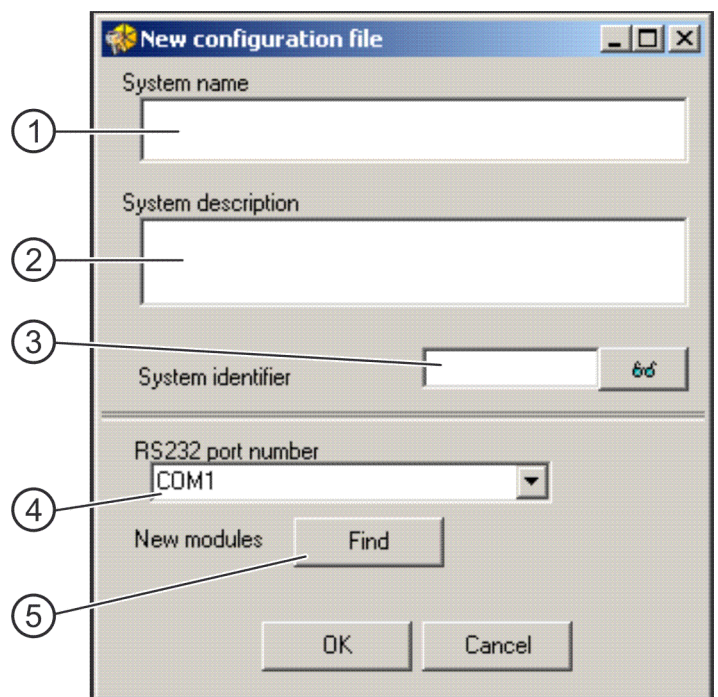
Fig. 21. Window enabling parameters of a new configuration file to be determined.

5. After creating the configuration file (or opening the already existing file) the appearance of the program menu bar will change (see Fig. 22). The entire menu will be available, including the other buttons.
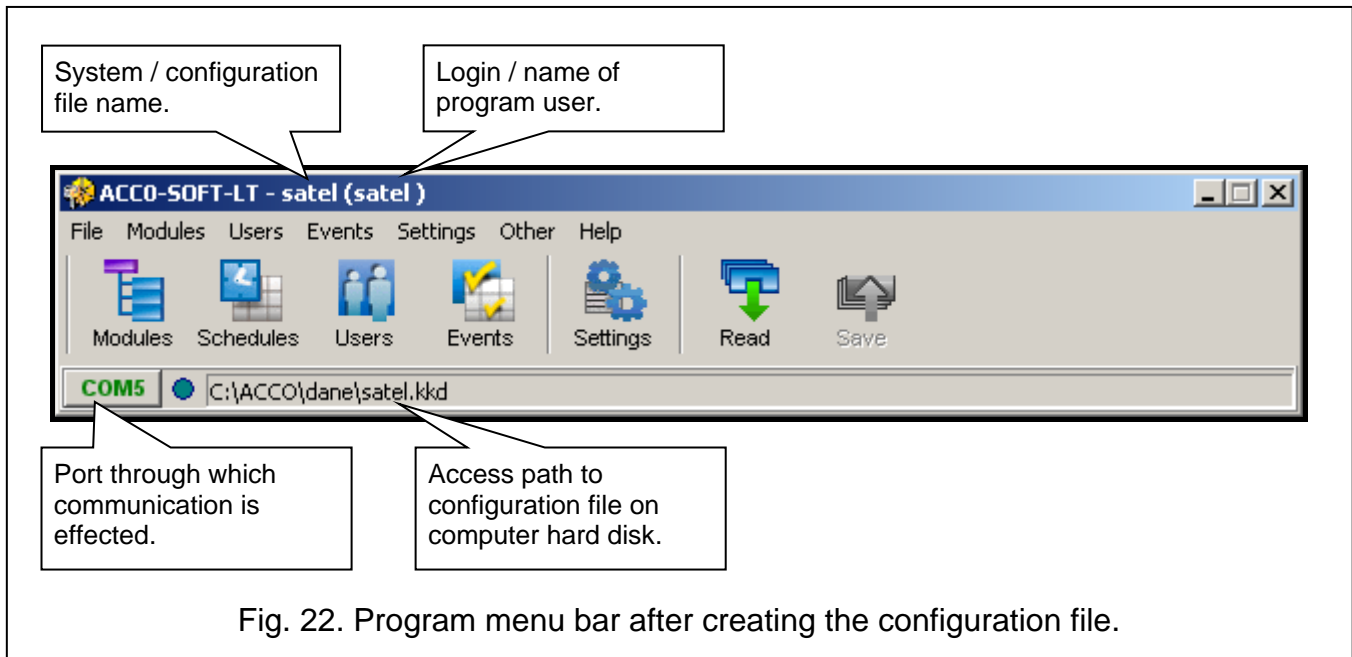
Fig. 22. Program menu bar after creating the configuration file.

6. Click your mouse on the button designated MODULES. The MODULES LIST window will open. If the module search function was not started in the NEW CONFIGURATION FILE window before, you can start it now by clicking on the button designated FIND. You can also add modules manually, after clicking on the ADD button. The list of all modules (found by means of the module search function or added manually) is displayed on the left-hand side of the window. Displayed on the right are settings of the module selected the list.

7. Each new module must be registered so that the program can establish communication with it and, consequently, to enable reading and writing the data. To register a single module, use the REGISTER MODULE command, available in the MODULE menu. Provision is made for registering all modules by means of the REGISTER ALL MODULES command, also available in the MODULE menu.

i | *During registration, the System identifier (the same that was defined in the New configuration file window) is saved in the module. If a module which has a different identifier (was registered in another system) is added to the system, registration of such an identifier in the new system means deletion of all data and restoration of default settings.*

8. Having registered the module, the program will automatically read data from it (this applies to the modules with factory settings and the modules having a consistent identifier of the system). You can proceed to configuring the module.

9. Having configured the module(s), save the new settings. The SAVE button in the modules window enables saving the data to the selected module. The SAVE button available on the program menu bar (see Fig. 22) makes it possible to save the data to all system modules whose settings have been changed.
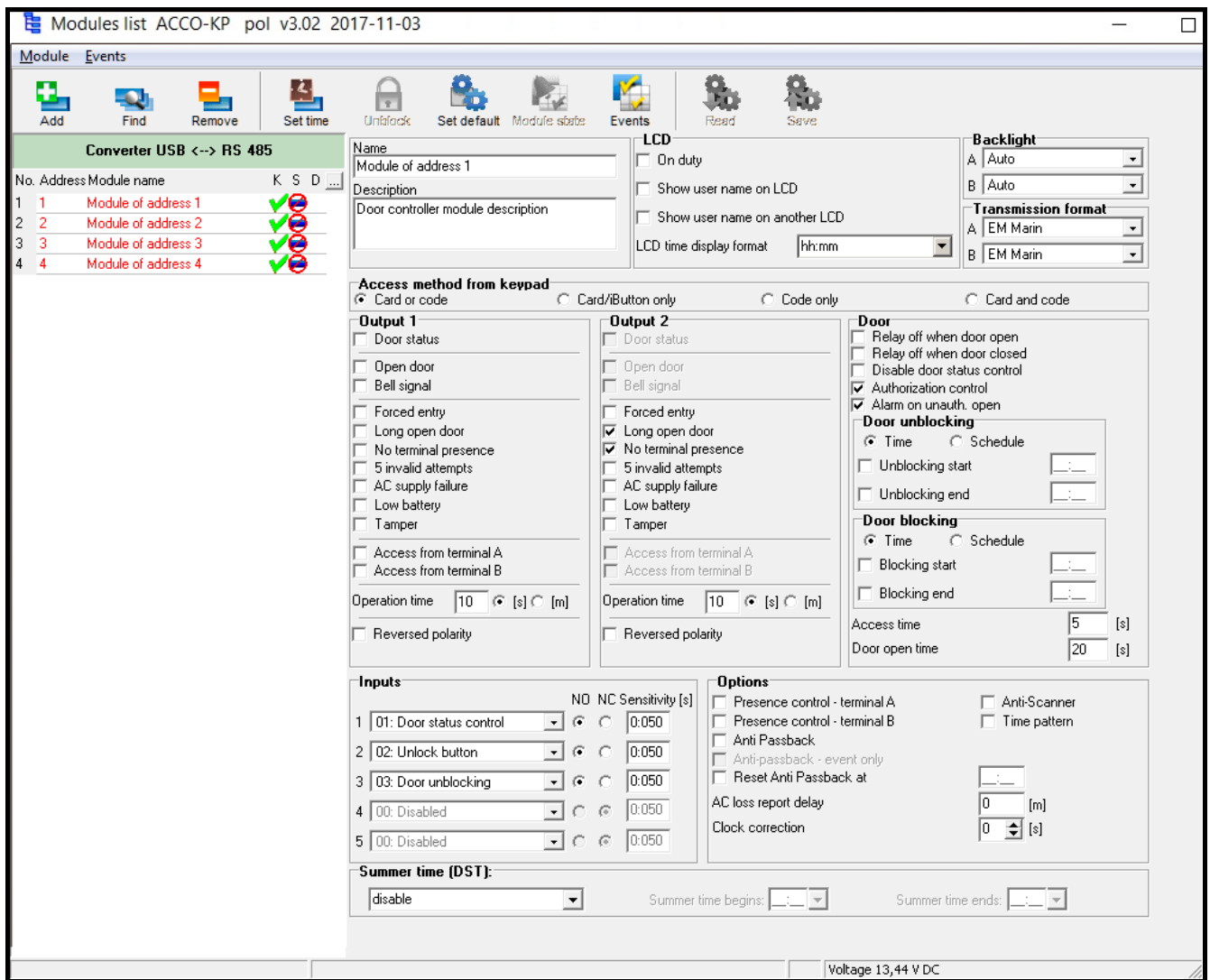
Fig. 23. The MODULES LIST window with modules which are still unregistered.

6.3 Module functions and options

Presence control – terminal A / B

With the option enabled, the module checks presence of keypads and proximity card readers working as terminal A or B. The presence of keypads will be checked first, and only then the presence of proximity card readers. In practice, it may mean that after disconnecting the LCD keypad / keypad, the module will also report lack of the reader, despite the fact that the reader has never been connected to the module. Registering such an event does not mean erroneous operation of the module, but results from the assumed solutions which allow for a temporary connection of the LCD keypad for service purposes (see: CONNECTING THE ACCO-KLCDR-BG / ACCO-KLCDR-BW KEYPAD). If this option is disabled, the module will in no way report a missing terminal (the alarm will not be generated, the event will not be saved and the NO TERMINAL PRESENCE output will not be activated).

i | *The module is unable to verify the presence of DALLAS iButton readers. If you connect this type of reader, do not enable the PRESENCE CONTROL - TERMINAL A/B option.*

Anti-passback

The function enables control of the user movement direction. The user will not get access from the terminal A (entry terminal), if information is in the module memory, that he has already gain access and opened the door from that terminal, but at the same time no information has appeared about gaining access and opening the door from the terminal B (exit terminal). The situation is similar in case of the terminal B. Therefore, it is impossible to pass several times in the same direction: every entry through the door must be followed by an exit. The function requires that both terminal units be installed (none of the terminals can be substituted e.g. by the unlock button).

i | *If the door status is not monitored, operation of the function is limited to registering the event (similarly as when ANTI-PASSBACK – EVENT ONLY option is enabled).*

Anti-passback – event only

Operation of the ANTI-PASSBACK function can be limited to logging in the events memory the cases of user passing in the same direction. The user will be able to unlock the door from one terminal side any number of times.

Reset Anti-passback

It is possible to define the time at which the ANTI-PASSBACK function will be reset, i.e. the users will be able to unlock the door by means of any terminal.

Anti-Scanner

When this option is enabled, 5 attempts to get access on the basis of an unknown card, unknown iButton or code within 3 minutes will block the terminals for about 5 minutes. The user having access to the door can unblock the terminals before expiry of this time by holding the card / iButton in front of the reader for approx. 3 seconds.

Time pattern

If the modules are connected to the RS-485 bus, the clock of one of them can serve as the pattern for the other ones. It enables synchronization of the clocks in all modules. The option should be enabled for 1 module only (the ACCO-SOFT-LT program does not allow for enabling the option for several modules).

AC loss report delay

This function applies to the ACCO-KP-PS and ACCO-KPWG-PS modules. It makes it possible to define the time during which the module can do without the AC supply. After expiry of this time, a failure will be reported. The time is programmed in minutes and its maximum value is 255 minutes. Entering the value 0 means that the AC supply failure will not be reported.

Clock correction

The function enables the clock settings to be adjusted once every 24 hours (at midnight) by a defined time, if the module clock is inadequate. The correction time is programmed in seconds. The maximum correction can be ±15 seconds per 24 hours.

Summer time (DST)

The module can automatically adjust the clock settings due to the change from standard time to summer time (DST) and vice versa. The following correction schemes can be selected:

− no correction,

− correction according to the European Union rules,

− correction by 1 hour according to dates,

− correction by 2 hours according to dates.

Summer time begins

The function is available, if the module clock settings are to be corrected by 1 or 2 hours according to dates. It enables entering the date (day, month) when the module clock is changed to summer time (shifted forward).

Summer time ends

The function is available, if the module clock settings are to be corrected by 1 or 2 hours according to dates. It enables entering the date (day, month) when the module clock is changed to standard time (shifted back).

6.4 Functions and options related to the door

Relay off when door open

If this option is enabled, the relay controlling the door activation device will be switched off as soon as the door is opened.

Relay off when door closed

If this option is enabled, the relay controlling the door activation device will be switched off as soon as the open door is closed.

> *i* | *If none of the options determining the moment of switching the relay off is enabled, the relay will only be switched off after expiry of the ACCESS TIME.*
>
> *In the following cases the relay will be switched off after expiry of the ACCESS TIME, despite enabling one of the options which determine the moment of switching the relay off:*
> – *none of the inputs informs about the door status (the door status monitoring sensor has not been installed),*
> – *the DISABLE DOOR STATUS CONTROL option has been enabled,*
> – *the user has got access, but has not opened the door.*

Disable door status control

Enabling this option is recommended if no information on the door status can reach the module (the status sensor has got damaged or, for some reason, has not been connected). This will prevent generating wrong events. When the option is enabled, unlocking the door is recognized as equivalent to opening the door. This means that unlocking the door from the terminal A side will generate the event informing about entry without door status control, and from the terminal B side – about exit without door status control. Some events are not generated (e.g. events informing about forced opening of the door, long open door, etc.).

When the DISABLE DOOR STATUS CONTROL option is enabled, the ON DUTY option is disabled. Correct execution of the ANTI-PASSBACK function is also impossible, i.e. after it is enabled, the user can unlock the door from one terminal side any number of times. Additional information will only be registered when the door is opened again from the same terminal side (similarly as when the ANTI-PASSBACK – EVENT ONLY option is enabled).

> *i* | *The DISABLE DOOR STATUS CONTROL option is to be only enabled in emergency situations, since it seriously affects functionality of the access control.*

Authorization control

If the option is enabled, opening the door without authorization will generate an event informing about the fact.

Alarm on unauthorized open

If the option is enabled, opening the door without authorization will generate alarm and a "Forced entry" event.

6.4.1 Door unblocking

You can choose whether the door is to be unblocked on the basis of predefined time or access schedules (select a schedule from the drop-down list).

Unblocking start

The time when the door unblocking is enabled. Hour and minutes are to be programmed. Programming the value 99:99 in the LCD keypad will disable the function.

Unblocking end

The time when the door unblocking is disabled. Hour and minutes are to be programmed. Programming the value 99:99 in the LCD keypad will disable the function.

6.4.2 Door blocking

You can choose whether the door is to be unblocked on the basis of predefined time or access schedules (select a schedule from the drop-down list).

Blocking start

The time when the door blocking is enabled. Hour and minutes are to be programmed. Programming the value 99:99 in the LCD keypad will disable the function.

Blocking end

The time when the door blocking is disabled. Hour and minutes are to be programmed. Programming the value 99:99 in the LCD keypad will disable the function.

> *i* *You can choose an access schedule, if not all of the created weekly schedules (see section: ACCESS SCHEDULES) have been used when programming the user settings. You cannot use the same schedule for unblocking and blocking the door.*

Access time

The time period during which the relay will change its status after access is granted, enabling the door to be opened. It can be programmed within the range of 1 to 60 seconds.

Door open time

The time during which the door can remain open after the relay is switched off. If the door stays open longer than for the specified time, the corresponding event will be generated. Additionally, the output programmed as LONG OPEN DOOR will be activated. The time can be programmed within the range of 1 to 60 seconds.

6.5 Functions and options related to the LCD keypad

On duty

With this option enabled, the following message will be displayed after unlocking the door:

```
— On duty
 (press ↑)
```

If the entry / exit is connected with business duties, the user should press the ▲ key. Suitable information will then be added to the event details. This information is useful, if the user passes registered by the door module are to help in determining the work time of the users.

> *i* *The function will not be executed, if the door status is not controlled or the door is open.*

Show user name on LCD

If the option is enabled, the name of the user who unlocked the door will be displayed on the LCD keypad.

Show user name on another LCD

If the option is enabled, the name of the user who unlocked the door will be displayed on the other LCD keypad.

Display format

The function makes it possible to choose how the time and date will be displayed on the keypad screen.

6.6 Backlight settings

You can specify the rules of backlighting for the keys and display in LCD keypads / keypads connected to the module. The following options are available:

− backlight off;

− automatic backlight (switched on by pressing any key or presenting the card);

− permanent backlight.

6.7 Transmission format

If you have selected:

− DALLAS format for one of the readers, the same format will be automatically set for the other reader. There is no option to select 2 different formats, if one of them is DALLAS;

− WIEGAND format for one of the readers, in both terminals connected to this controller you should choose the CARD/IBUTTON ONLY method of access;

i | *In the WIEGAND format, double-tapping the same card (identifier) on the reader is interpreted as holding the card. Not all readers will support this feature. Please check your readers for this functionality.*

It is recommended that the SATEL's CZ-EMM3 and CZ-EMM4 proximity card readers work in the EM Marin format.

− EM-MARIN format, you can choose one of the four available access methods.

7.   Users

i | *This section does not apply to the access control module, which is part of the ACCO NET system.*

It is possible to register 1024 users in the module. Each of the users is characterized by:

Name – which facilitates identification of the users. It can consist of up to 16 characters.

ID number – a 5-digit number assigned to the user during the procedure of adding a new user.

Card – a passive transponder in the form of proximity card, key fob etc. authorizing the user to get access to the door.

DALLAS iButton – an electronic key with unique and unchangeable code authorizing the user to obtain access to the door.

i | *No card added using the Wiegand reader will be supported by the ACCO-KLCDR keypads.*

The DALLAS iButton can be only assigned to users who are authorized to access the doors served by iButton readers connected to the ACCO-KPWG-PS and ACCO-KPWG modules.

Code – a sequence of 4 to 12 digits authorizing the user to get access to the door.

Access schedules – time limits within which the user is authorized to get access to the door (editing the schedules is available in the ACCO-SOFT-LT program).

Rights – additional functions available to the user. The following rights can be granted:

> **Administrator** – adding and removing users, module configuration in the service mode.
> **Switching** – unblocking / blocking the door.
> **Change code** – editing own code.

Additionally, the ACCO-SOFT-LT program makes it possible to enter the user's first and last name (which are not necessarily identical with his name in the system), account number and description. A photograph can also be assigned to the user.

On starting the module with default settings (first run), there is one registered user with the name "Administrator" and ID number 00001, having all the rights and using the code 12345.

> *i* | *The "Administrator" user's default code should be replaced by another one.*

The user with ID number 00001 cannot be deleted from the module. His ADMINISTRATOR and CHANGE CODE rights cannot be revoked either.

Adding / editing / removing users is possible by means of the LCD keypad or the computer with ACCO-SOFT-LT program installed. The LCD keypad only enables adding and removing users in the module to which it is connected. The ACCO-SOFT-LT program makes it possible to create / edit / remove users in all modules included in the system. Additionally, it enables creating **user groups**.

7.1 Adding new users

The new user is automatically assigned the ID number, name, CHANGE CODE authority, and in the access schedule - the right to always unlock the door. All these parameters can be edited and modified. Additionally, to allow the new user to use the door, he must be assigned a proximity card, iButton or code.

7.1.1 Adding a new user by means of LCD keypad

New users can be added by means of the ADD USER function. Having programmed all the user parameters, press the ✳ ☐ key. According to the command displayed on the keypad, press the # ♠ or ⓞⓚ key to save the new user, or the ✳ ☐ key to cancel adding the user.
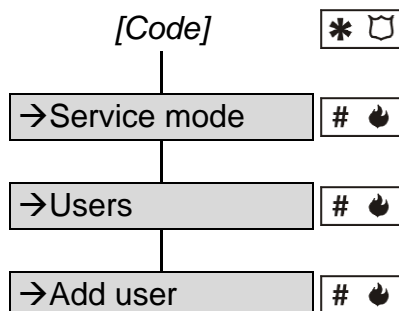
Diagram 1. The manner of starting the ADD USER function in LCD keypad.

> *i* | *The user will only be added to the module to which the LCD keypad is connected.*

7.1.2 Adding new users by means of the ACCO-SOFT-LT program

1. Click with your mouse cursor on the button designated USERS, which is available on the program menu bar (see Fig. 22). The USERS window will open (see Fig. 24).
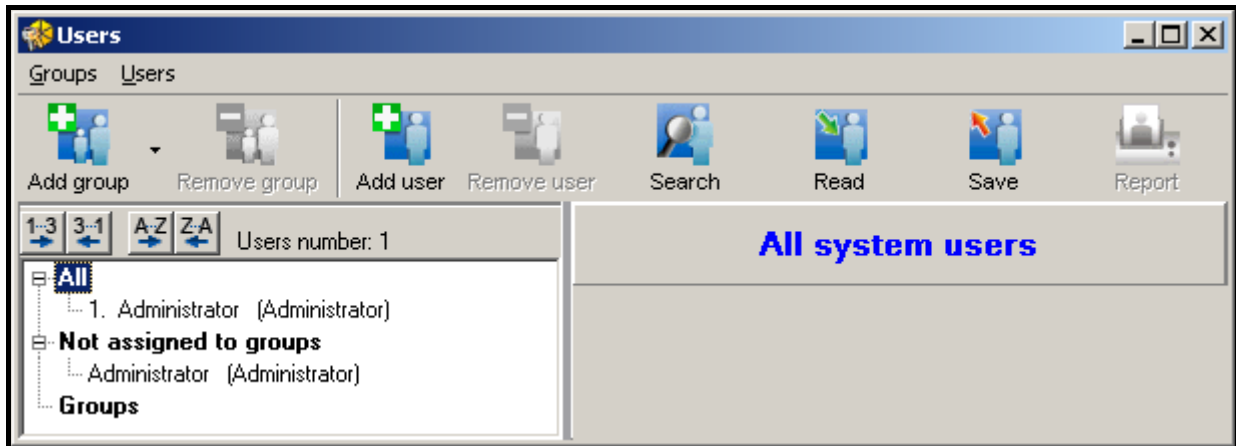
Fig. 24. View of the USERS window before adding the users.

2. Click with your mouse on the button designated ADD USER. The CREATE USERS window will open (see Fig. 25).

3. Select the number of users, you want to create.

4. Select settings for the new users. In case of the module(s) with factory settings, you can select the default settings or ADMINISTRATOR settings as a pattern. This feature enables new users to be created, based on the settings of already existing users and user groups. The user being created will be granted the same rights, will be assigned to the same modules and will get the same access schedules as in the pattern. In case of the default settings it means the right to change the code, no assignment to the modules and an access schedule authorizing the user to always unlock the door.

5. Determine whether the user is to receive the code automatically. The code may be generated on the basis of user ID number (5-digit code) or randomly (number of digits in the code: from 4 to 12). Indicate whether the user should change the code after the first login.

6. Click with your mouse on the APPLY button. The CREATE USERS window will close. The new user(s) will appear in the list in the USERS window. The name of the users which are saved in any module and whose names have not been changed in the program will be displayed with black color. The name of the users whose settings are to be saved in the module(s) will be displayed in red. The name of the users who are not saved in any module will be displayed in gray.
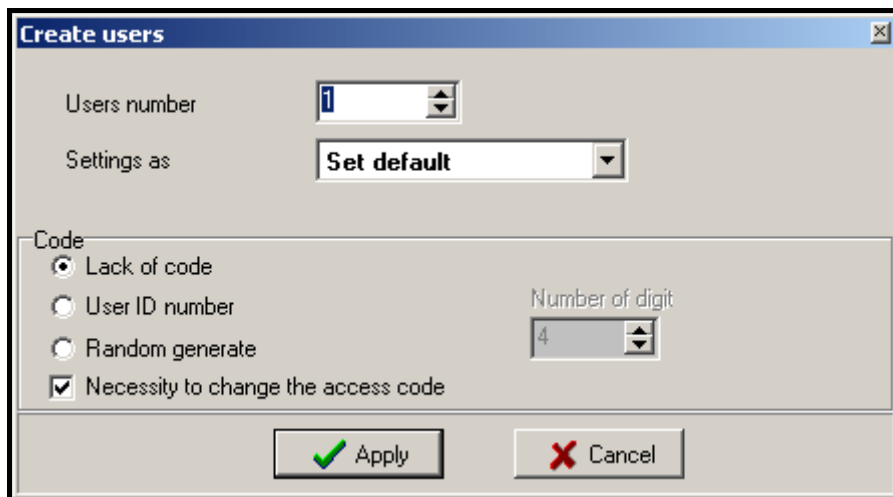
Fig. 25. Window for adding new users.

7. Enter the last name, first name and display name of the user (16 characters) in the USER DATA tab. The display name will be created automatically after entering the user's last and first name, however it can be independent of them. The display name only is saved to the module. In the ACCO-SOFT-LT program, this name is displayed in brackets in the USERS window (see Fig. 26).
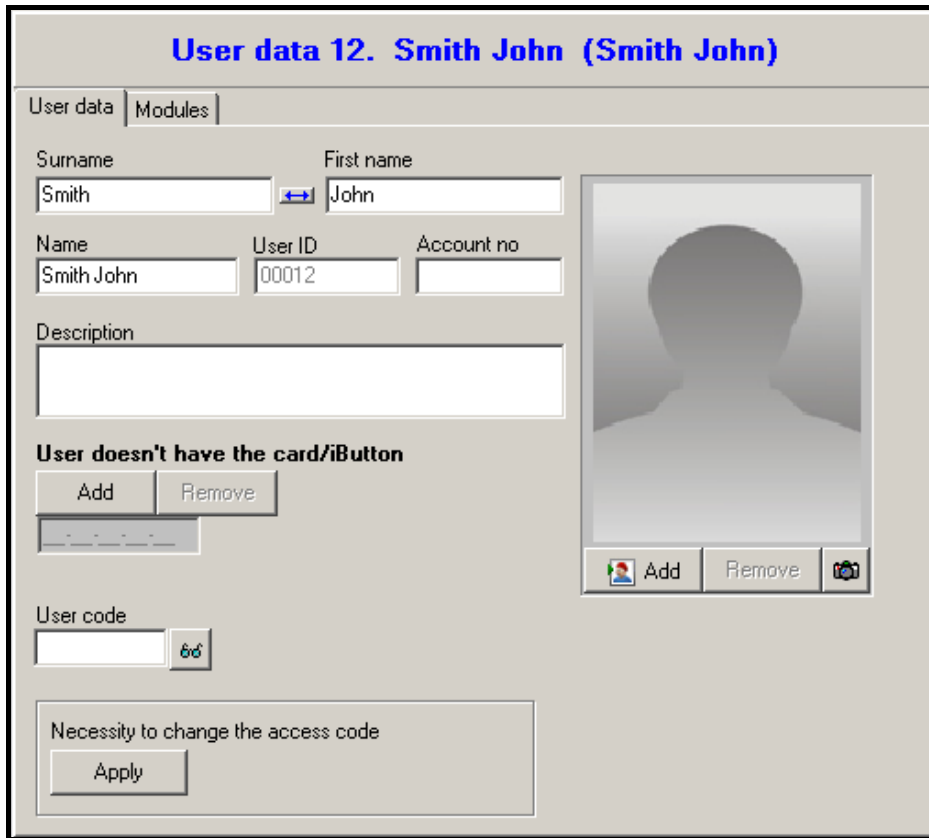
Fig. 26. User data tab in the USERS window.

8. If the user is also to use the card / iButton, click with your mouse on the ADD button. The CARD / IBUTTON READING window will open (see Fig. 27).
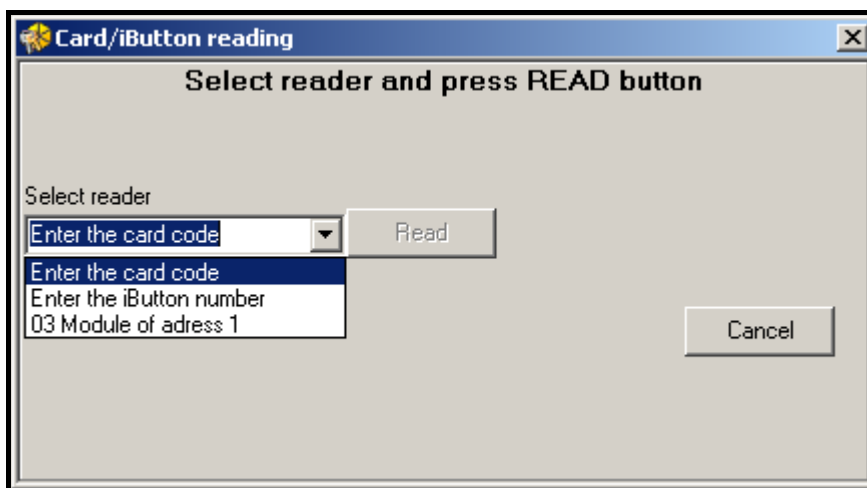
Fig. 27. Window for adding card / iButton to the user.

9. When adding a card, select how it should be added: by entering the card number, or by reading the card on the reader connected to the ACCO-USB converter, on the CZ-USB-1 reader or on any terminal unit (if added by means of the Wiegand terminal, the card will not be supported by the keypad) connected to one of the system modules.

10. When adding an iButton, select how it should be added: by entering the iButton number, or by reading in the iButton by means of the reader connected to the ACCO-KPWG-PS or ACCO-KPWG module.

11. Enter the number or read in the card / iButton.

12. Click with your mouse on the CONFIRM button. The CARD / IBUTTON READING window will close.

13. If the code is to be changed by the user, click on the APPLY button. A suitable message will be displayed in the program window. The user using the LCD keypad will be informed of the necessity to change the code.

> *i*   *The user must be authorized to change the code.*

14. Optionally, add description, account number and photograph of the user.

15. Click with your mouse on the MODULES tab (see Fig. 28).

Fig. 28. MODULES tab in the USERS window.

16. Indicate the modules to which the user data are to be saved.

> *i*   *The user may only get access to the doors supervised by the modules to which his data have been saved. This access is defined in detail by means of the access schedules. The user has no access to the door, unless his data are saved to the module controlling this door.*

17. Select the access schedule for each door.

18. Determine the user rights for each module.

19. Determine whether the user passes in the particular modules are to be limited.

20. End the procedure of user adding by clicking on the SAVE button (see Fig. 24).

7.2 Editing users

It is possible to edit all the user's parameters except for his ID number.

7.2.1 Editing a user by means of LCD keypad

The user parameters can be modified by means of the EDIT USER function. Having completed editing the user, press the ✱ ☾ key. According to the command which will appear on the display, press the # ♠ or ⓞⓚ key to save the changes, or ✱ ☾ to cancel saving the changes made.

```
                    [Code]        ✳ 🗇
                       │
              →Service mode    # ♠
                       │
                 →Users         # ♠
                       │
                →Find user      # ♠
          ┌────────────┼────────────┐
  →Find by name  # ♠   →Find by ID   # ♠   →Find by card   # ♠
       │                    │                    │
┌──────────────┐   ┌──────────────┐   ┌──────────────┐
│Select the user│   │ Enter the user│   │  Read the user│
│  from list    │   │   ID number   │   │     card      │
└──────────────┘   └──────────────┘   └──────────────┘
          └────────────┼────────────┘
                →Edit user      # ♠
```
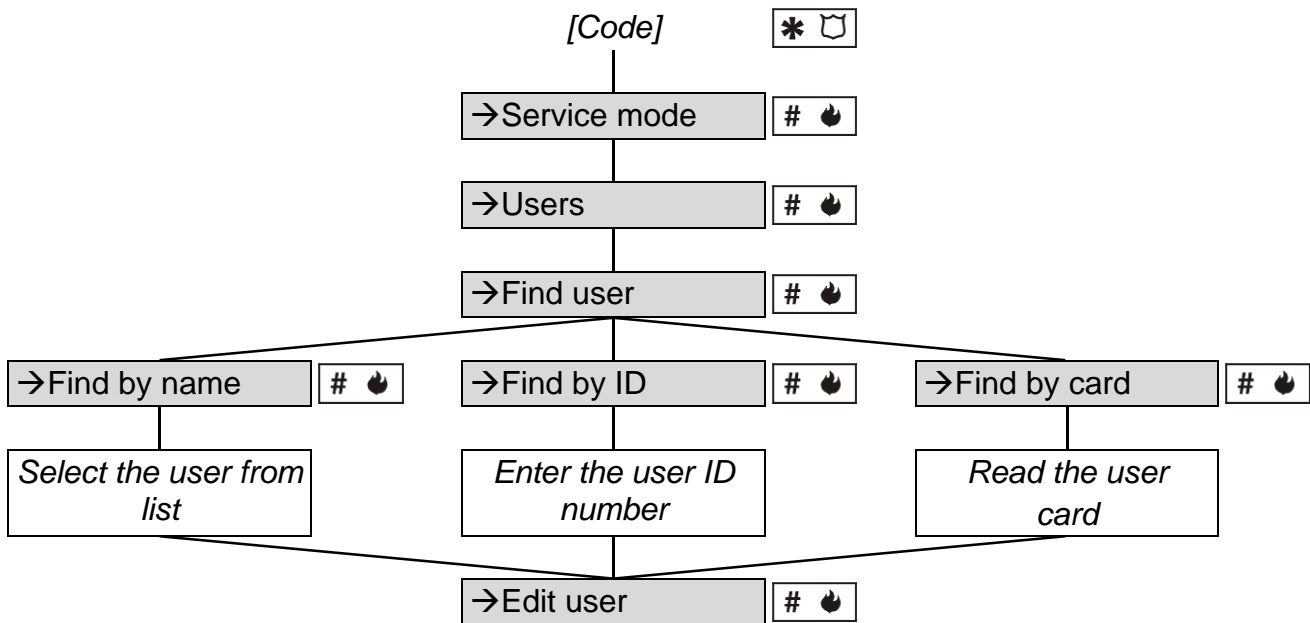
Diagram 2. The manner of starting the EDIT USER function in LCD keypad.

i | *The user related changes which have been made in the module by means of the LCD keypad will be automatically sent out to other modules, if they are connected by means of the RS-485 bus.*

7.2.2 Editing a user by means of ACCO-SOFT-LT program

In order to modify the user parameters, open the USERS window and select from the list the user whose data you want to change. To make easier finding the user in the list, the program provides the FIND function. Owing to this function, you can find the user based on the name (or part of the name), ID number, account number, module where it is saved proximity, card or iButton (the card code / iButton must be read by the reader).

Having entered changes in the user settings, save them to the module(s) by clicking on the SAVE button. Only saving the changes to the module(s) will end the user editing procedure.

i | *If the user(s) is simultaneously edited by means of the ACCO-SOFT-LT program in the given module and from the level of LCD keypad connected to that controller, then, selecting in the program:*

– the SAVE function – OMITTED. DATA EDIT MODE message will display in the USERS SAVING window. The changes entered by means of the program will have priority, while those entered by means of the keypad will be disregarded by the program.

– the READ function – OMITTED. DATA EDIT MODE message will display in the USERS READOUT window. In such a case you should stop entering changes by means of the keypad.

7.3 Removing users

7.3.1 Removing a user by means of LCD keypad

You may remove the user by means of the REMOVE USER function. On starting the function, a message will be displayed, according to which you have to confirm the command to remove the selected user by pressing the # ♠ or ⓞⓚ key (press another key to cancel removing the user).
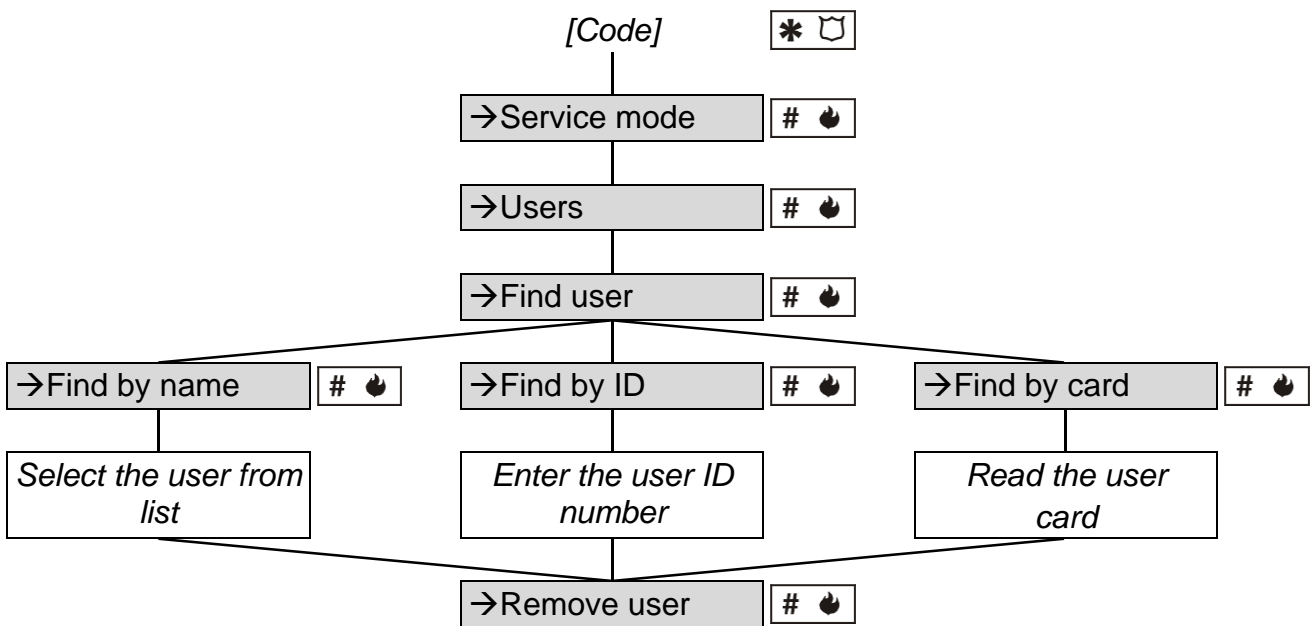
Diagram 3. The manner of starting the REMOVE USER function in LCD keypad.

i | *The user will only be removed from the module to which the LCD keypad is connected.*

7.3.2 Removing a user by means of ACCO-SOFT-LT program

In order to remove a user, open the USERS window and click with your mouse on the user you want to remove. The FIND function makes finding the user easier (see: EDITING A USER BY MEANS OF ACCO-SOFT-LT PROGRAM). Having selected the user, click with your mouse on REMOVE USER (button or command in the USERS menu). When the program window will open, confirm the intention of removing the user, or cancel removing the user.

The changes made must be saved. Only saving the changes to the module(s) will end the procedure of removing the user.

7.4 User groups

The ACCO-SOFT-LT program enables creating user groups which facilitates management of the users. The users belonging to a group have identical:

– modules to which their data are saved (access to doors supervised by these modules);
– schedules of access to the doors;
– rights.

It is possible to create up to 255 groups.

i | *Only after a group is created and its parameters configured, you can assign users to the group.*

| *Users assigned to the same group can have a different number of entries defined by the ENTRIES LIMIT parameter.*

7.4.1 Creating a user group

1. Click with your mouse on the button designated USERS, available on the program menu bar (see Fig. 22). The USERS window will open (see Fig. 24).
2. Click with your mouse on the button designated ADD GROUP. The new group will appear in the list on the left-hand side of the USERS window.
3. Assign a name to the group.
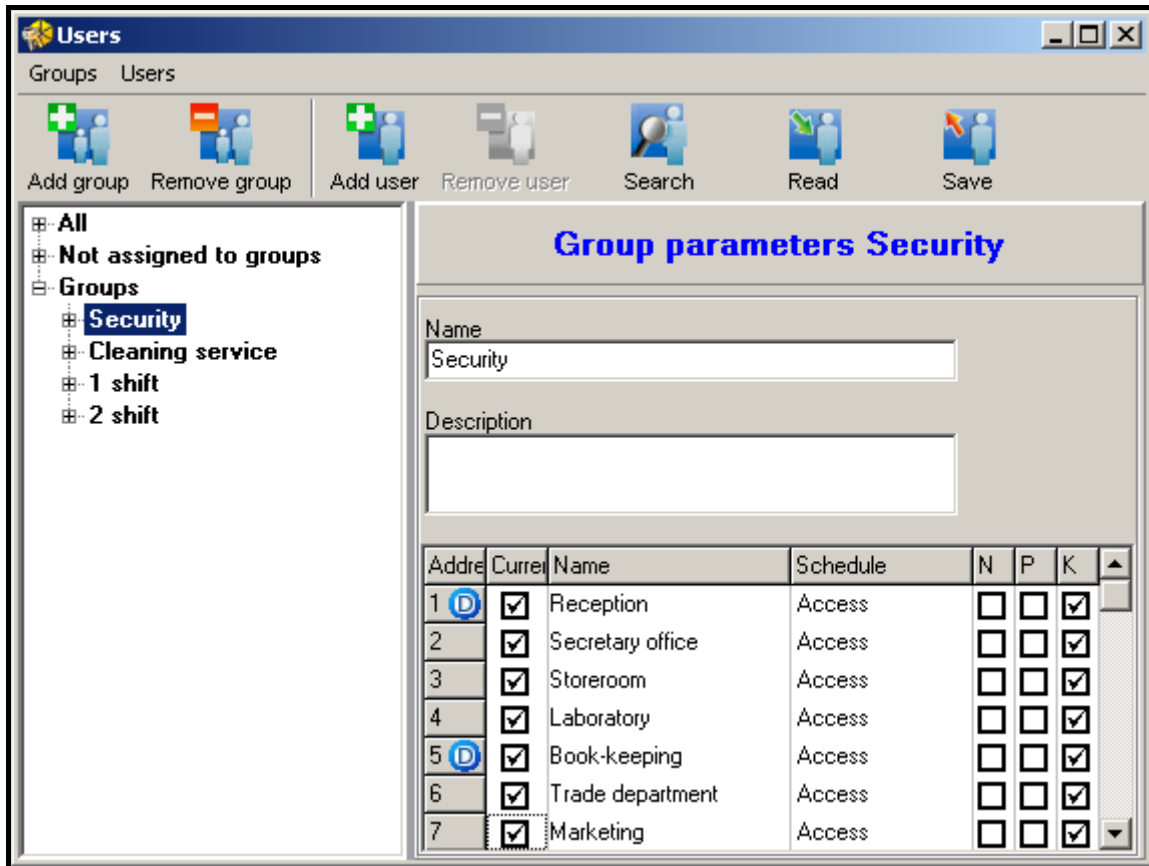
Fig. 29. An example of user group settings.

4. Indicate the modules to which the data of users belonging to the group are to be saved.
5. Select an access schedule for each door.
6. Define the user rights for each module.
7. Having defined settings of the group, you can assign users to it. The users created earlier can be assigned to the group, e.g. by the "drag and drop" method. The newly created users will be assigned to a selected group, if that group is selected in the SETTINGS AS field of the CREATE USERS window (see ADDING NEW USERS BY MEANS OF ACCO-SOFT-LT PROGRAM and Fig. 25).

i | *If, when editing a user belonging to the group, one of the parameters defining the group (rights, weekly access schedule, available doors) is changed, the user will be removed from the group and transferred to the category of users not assigned to groups.*

8. Save the user data to the module(s) by clicking on the SAVE button.

7.4.2 Automatic assigning of user to a group

1. Click your mouse on the USERS button on the program menu bar (see Fig. 22). The USERS window will open (see Fig. 24).
2. Click on the name of one user not assigned to any group. The user data will be displayed on the right-hand side. Select the MODULES tab.
3. Click on the GROUP button (see Fig. 28). The user will be assigned to a group with parameters corresponding to the user's parameters or a new group will be created.
4. If a new group is created, give it a name.
5. Save the changes made to the module(s) by clicking on the SAVE button.

7.4.3 Automatic grouping of users

1. Click on the USERS button, available on the program menu bar (see Fig. 22). The USERS window will open (see Fig. 24).

2. Click on the ▪ button and select the GROUP THE USERS command (see Fig. 29). The users not assigned to any group will be assigned to the first available group with parameters corresponding to those of the given user. If there is no group corresponding to the user parameters, a new group will be created.

3. If a new group is created, give it a name.

4. Save the changes made to the module(s) by clicking on the SAVE button.

7.4.4 Editing a user group

In order to modify the parameters of a user group, open the USERS window and select from the list the group whose settings are to be changed.

Having made changes in the group parameters, save the users data to the module(s) by clicking on the SAVE button. Only saving the data to the module(s) will end the procedure of editing the user group.

7.4.5 Removing a user group

In order to remove a user group, open the USERS window and select from the list the group which is to be removed and then click with your mouse on the REMOVE GROUP button. When the program window will open, confirm the intention to remove the group or cancel the deletion. After deletion of the group, the users who were previously assigned to it, will be users with individual parameters.

Save the users data to the module(s) by clicking on the SAVE button. Only saving the data to the module(s) will end the procedure of removing the user group.

7.5 User(s) report

The REPORT button will be activated at the moment of highlighting the user name: one, a few or all of them. The user(s) report will provide information on the selected users. Click on the REPORT button to open the REPORT PARAMETERS window, where you can define parameters of the report generated in PDF format.
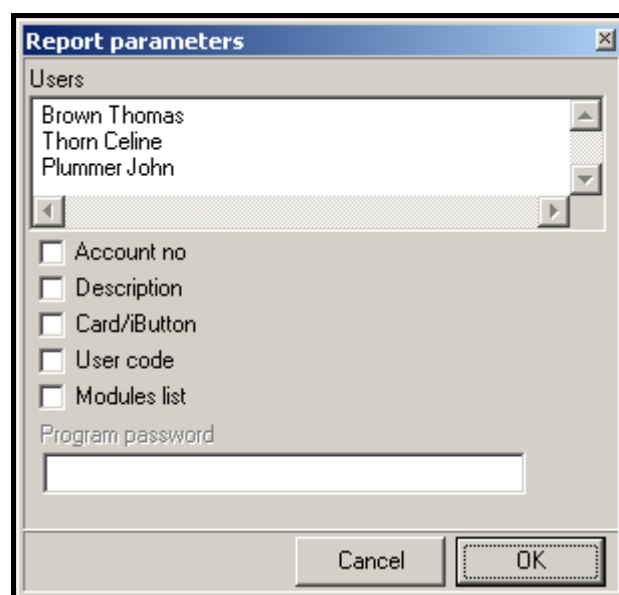
Fig. 30. REPORT PARAMETERS window.

7.5.1 Creating a user(s) report

1. Select one, a few or all users (press the Ctrl key and highlight the user names with the mouse pointer).
2. Click your mouse on the REPORT button.
3. A list of the names of selected users will be displayed in the USERS field, REPORT PARAMETERS window.
4. Select the user related information which should be included in the report:
   – ACCOUNT NUMBER;
   – DESCRIPTION;
   – CARD / IBUTTON (the parameter requires entering program access password);
   – USER CODE (the parameter requires entering program access password);
   – MODULES LIST.
5. Click on the OK button to generate the report.

7.6 Access schedules

An access schedule should be assigned to each user, i.e. it should be defined on which days of the week and at what time the user will have access to the door. Creating, editing and removing the access schedules is only possible by means of the ACCO-SOFT-LT program. The access schedule is created on the basis of weekly schedules, daily schedules and time slots.

Weekly schedule – defines the user access to the door throughout the week. Each user can be assigned 1 of 256 schedules with numbers from 0 to 255. Two of these schedules are already defined: 0 – Access (the door will be always unlocked to this user) and 255 – Access denied (the door will be always locked to this user). You can create the remaining 254 weekly schedules by selecting suitable daily schedules for each day of the week.

Daily schedule – defines the user access to the door over the course of 24 hours. From among the general number of 256 daily schedules, 2 are predefined: 0 (the door will be unlocked to this user round the clock) and 255 (the door will be locked to this user round the clock). You can create the remaining 254 daily schedules, based on the time slots. The daily schedule must consist of at least one time slot.

Time slot – defines period of time within 24 hours, when the user has access to the door. You can create up to 256 time slots. When programming, you must define from when (hour and minutes) to when (hour and minutes) the door is to be available to the user.
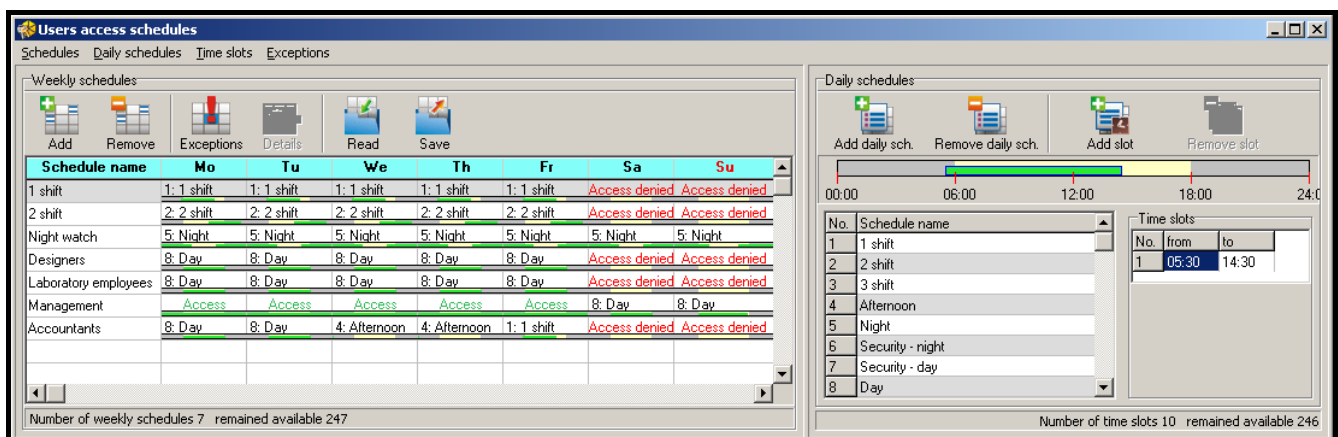
Fig. 31. Window with access schedules.

Additionally, you can define up to 60 days / exceptional periods which have global character. On holiday(s), exceptional daily schedules, i.e. different rules of access to the door, may be valid. You can create up to 128 exceptional daily schedules. You have to determine for each weekly schedule, which exceptional daily schedule is to be valid during the exceptional day / period. If no exceptional daily schedule is selected, the access rules defined in the weekly schedule will also hold good during the holiday(s).

7.6.1 Creating the access schedule

1. Click with your mouse on the button designated SCHEDULES, available on the program menu bar (see Fig. 22). The USERS ACCESS SCHEDULES window will open (see Fig. 31).
2. Click with your mouse on the button designated ADD. A weekly schedule will be displayed in the window. By default, this schedule assumes full user access during all days of the week.
3. Assign a name to the created schedule.
4. Click with your mouse the button designated ADD DAILY SCHEDULE. The daily schedule will be displayed in the list. At the same time, a time slot will be created for the schedule.
5. Assign a name to the created schedule.
6. Define the time slot parameters (from when to when the door is to be available to the user). If necessary, add further time slots by clicking on the button designated ADD SLOT.
7. If necessary, create next daily schedules.
8. Assign the daily schedules to the selected days of the week in the weekly schedule.
9. Save the created access schedule to the module(s) by clicking on the SAVE button.

7.6.2 Creating exceptions

1. Click with your mouse on the button designated EXCEPTIONS, available in the USERS ACCESS SCHEDULES window (see Fig. 31). The EXCEPTIONAL DATES CALENDAR window will open (see Fig. 32).
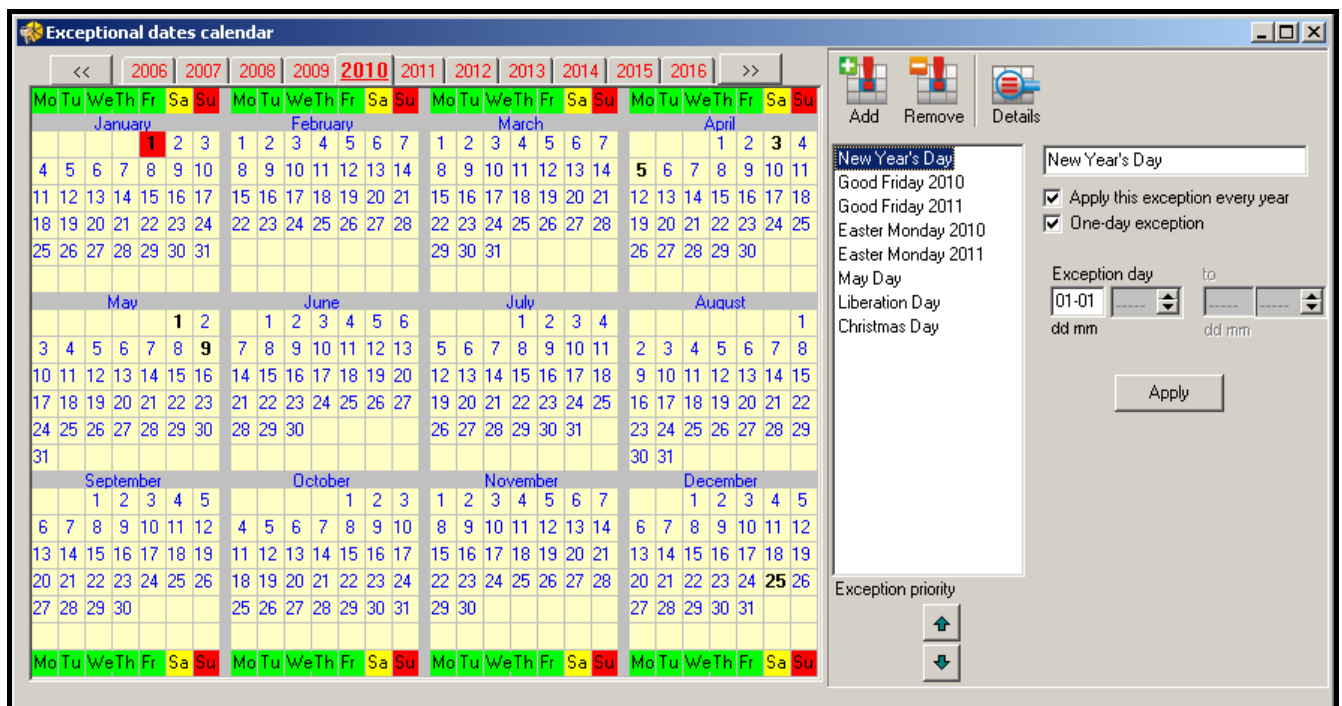
Fig. 32. Window with exceptional dates calendar.

2. Click with your mouse on the ADD button. The new exception will appear in the list.

3. Assign a name to the created exception.

4. Indicate whether the exception is to be applied every year, or not.

5. Indicate whether the exception is to be valid on one day, or over a period of time.

6. Depending on previously made selections, define the exception date, or the beginning and end of the exception.

7. Click with your mouse on the APPLY button to finish the procedure of defining the date / exceptional period.

8. Click on the DETAILS button. The EXCEPTIONS DETAILS window will open.

9. Click with your mouse on the button designated ADD SCHEDULE. The exceptional daily schedule will be displayed in the list. At the same time, a time slot will be created for the schedule.

10. Assign a name to the created schedule.

11. Define the exceptional time slot parameters (from when to when the door is to be available to the user). If necessary, add further time slots by clicking on the button designated ADD SLOT.

12. If necessary, create next exceptional daily schedules.

13. For selected weekly schedules, assign the exceptional daily schedules to suitable exceptions (the list on the right-hand side of the window).

14. Save the access schedule data to the module(s) by clicking with your mouse pointer on the SAVE button in the USERS ACCESS SCHEDULES window.
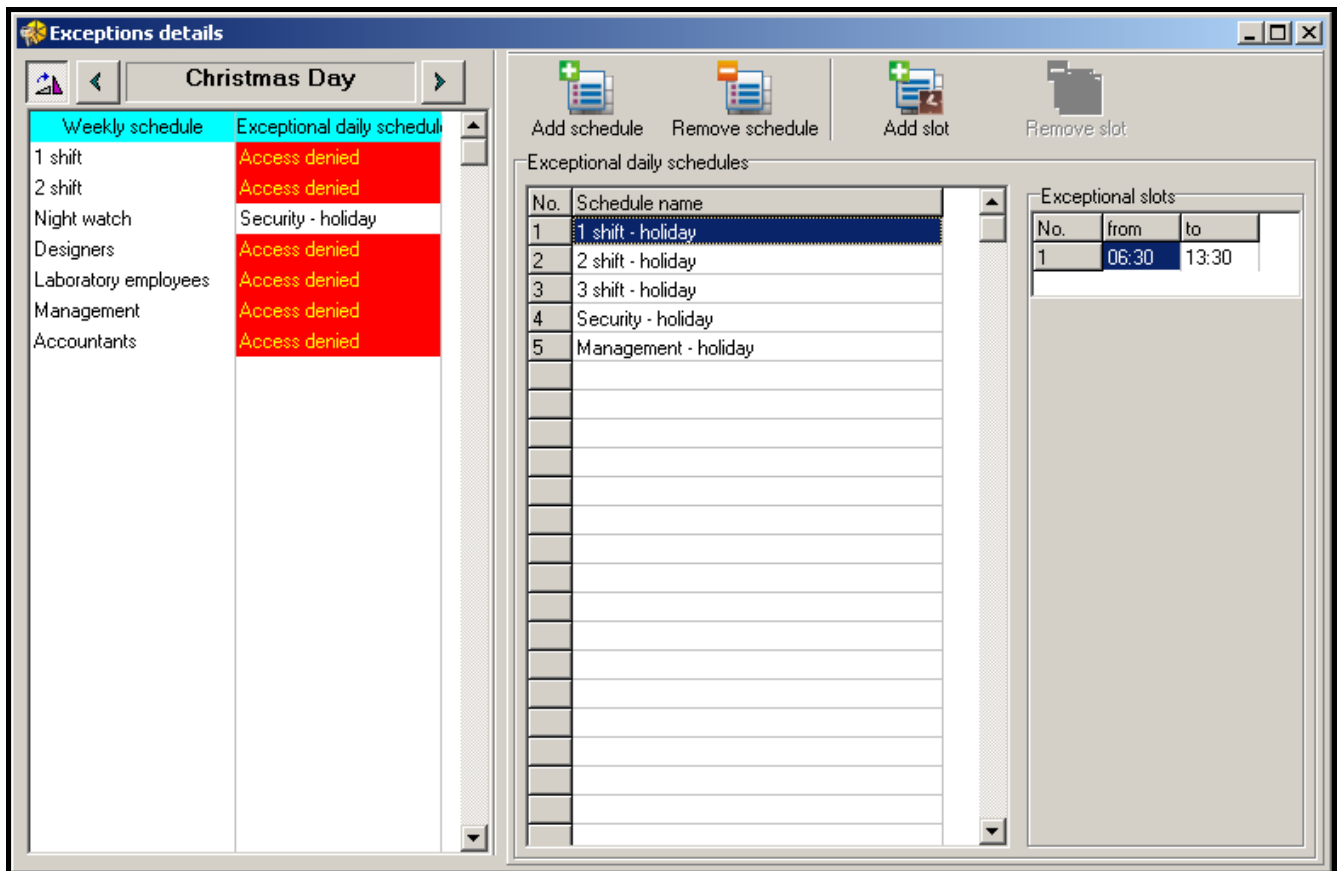
Fig. 33. EXCEPTIONS DETAILS window.

7.7 Presence reports

The ACCO-SOFT-LT program enables generating a presence report. Thus you can gather information on the time spent by user(s) on the premises. There is an option provided to generate a report in PDF format.

You can open the PRESENCE REPORT window in two ways:

− in the main menu, select the EVENTS command / button. In the window that will open, go to the menu and select the EVENTS command, then select PRESENCE REPORT (see Fig. 34);

− in the main menu, select the OTHER command and then select PRESENCE REPORT.
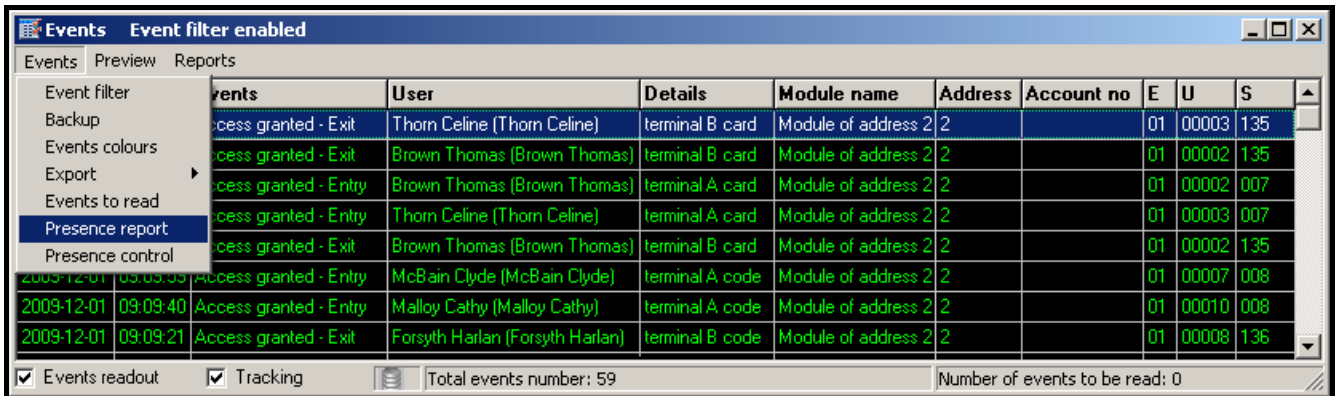
Fig. 34. PRESENCE REPORT command in the EVENTS window.
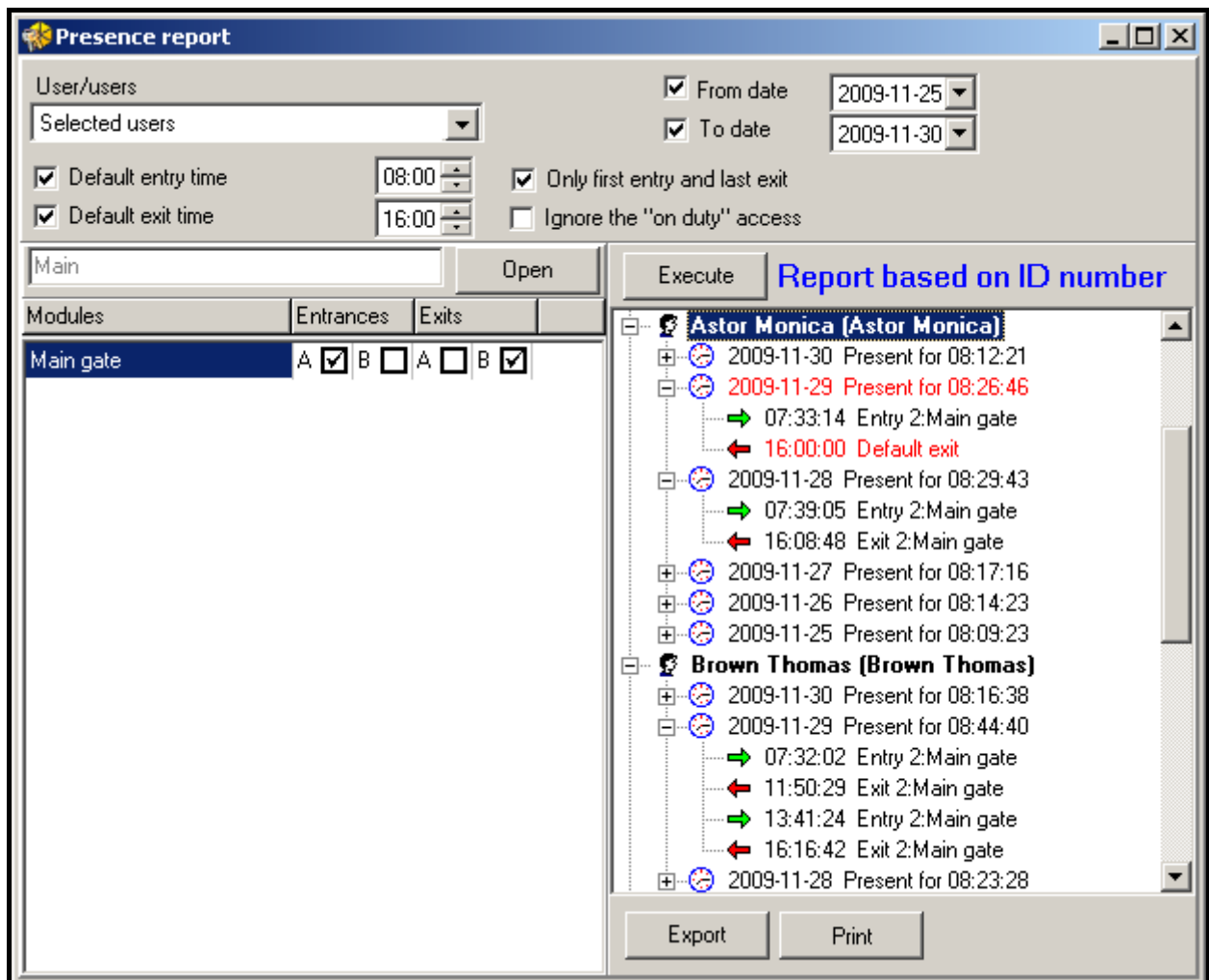
Fig. 35. PRESENCE REPORT window.

7.7.1 Creating a presence report

1. Determine which users are to be included in the report. You can do it in two ways:
   - In the USER/USERS field, enter the user name or a part of it – all persons meeting this criterion will be included in the report. Users will be distinguished in the report by their name, i.e. the user having the same ID number, but a different name will be treated as another person.
   - Using your mouse, click on the ▼ button next to the USER/USERS field to open the selection list. Select from the list those users who are to be included in the report. Users will be distinguished in the report by their ID number, i.e. the users having the same ID, but a different name will be treated as one person (all the names will be included in the report).
2. Define the report time slots:
   - in the FROM DATE field, enter the date from which all the user(s) entries and exits will be included in the report. If you do not enable this option, the report will include all the user(s) entries and exits from the moment when the program was installed.
   - in the TO DATE field, enter the date up to which all the user(s) entries and exits will be included in the report. If you do not enable this option, the report will include all the user(s) entries and exits up to current date.
3. Where the user can enter or leave the premises without registering the fact by the access control, there is an option to define the default hours for entering or leaving the premises. They should be entered in the DEFAULT ENTRY TIME and DEFAULT EXIT TIME fields. The program will use the default entry time when there is no information on the user entry, and the default exit time when there is no information on the user exit.
4. If the report is to record the user presence time during the day without taking any work breaks into account, select the ONLY FIRST ENTRY AND LAST EXIT field.
5. If the report is to be generated without taking the "on duty" passes into account, select the IGNORE THE "ON DUTY" ACCESS field.
6. The report is generated on the basis of entry / exit rules. Click on the OPEN button to open the ENTRY/EXIT RULES window, where you can select one of the available rules. Confirm your selection by using the OK button. The rule settings will be displayed in the window below. If none of the entry / exit rules has been defined yet, click on the OPEN button. In the ENTRY/EXIT RULES window, click on the ADD button. The DOORS window will open. Give a name to the new rule. Then, indicate for each module which terminal (A or B) will function as entrance to and which one as exit from the premises, and confirm your choice by pressing OK. The defined entry / exit rule will be added to the list.
7. Click your mouse on the EXECUTE button. A report on the presence of selected users will be generated in the window, according to preset parameters. The report consists of the user name and the list of user presence dates with specification of entries and exits. Information on the recorded time will be displayed next to the date. Displayed in red color is the date of day on which the user presence data are incomplete (they can be completed, based on the preprogrammed parameters).
8. There is an option provided to export and/or print out the report. Click your mouse on the EXPORT button to export the presence report to file in the CSV, Excel or Symfonia format. Run the EXPORT command and select the format to open a window where you should choose the location to store the file. In order to print out the report in PDF format, click on the PRINT button.

*The defined entry / exit rules are saved and stored in the ACCO-SOFT-LT program data base (file extension *.s3db). If the data base is deleted, all the rules will have to be programmed once more.*

7.8 Presence control

The ACCO-SOFT-LT program makes the PRESENCE CONTROL tool available to the administrator. Thus you are able to find out whether or not the given user stays within the area defined for him/her.

You can open the PRESENCE CONTROL window in two ways:

− in the main menu, select the EVENTS command / button. In the window that will open, go to the menu and select the EVENTS command, then select PRESENCE CONTROL (see Fig. 34);

− in the main menu, select the OTHER command and then select PRESENCE CONTROL.

The PRESENCE CONTROL window will be displayed, in which, after suitable options are selected, a list of all users will appear. The list shows data about the number of present and absent users. Information on the method of monitoring the user presence, depending on the settings, can be shown under the name of each user.
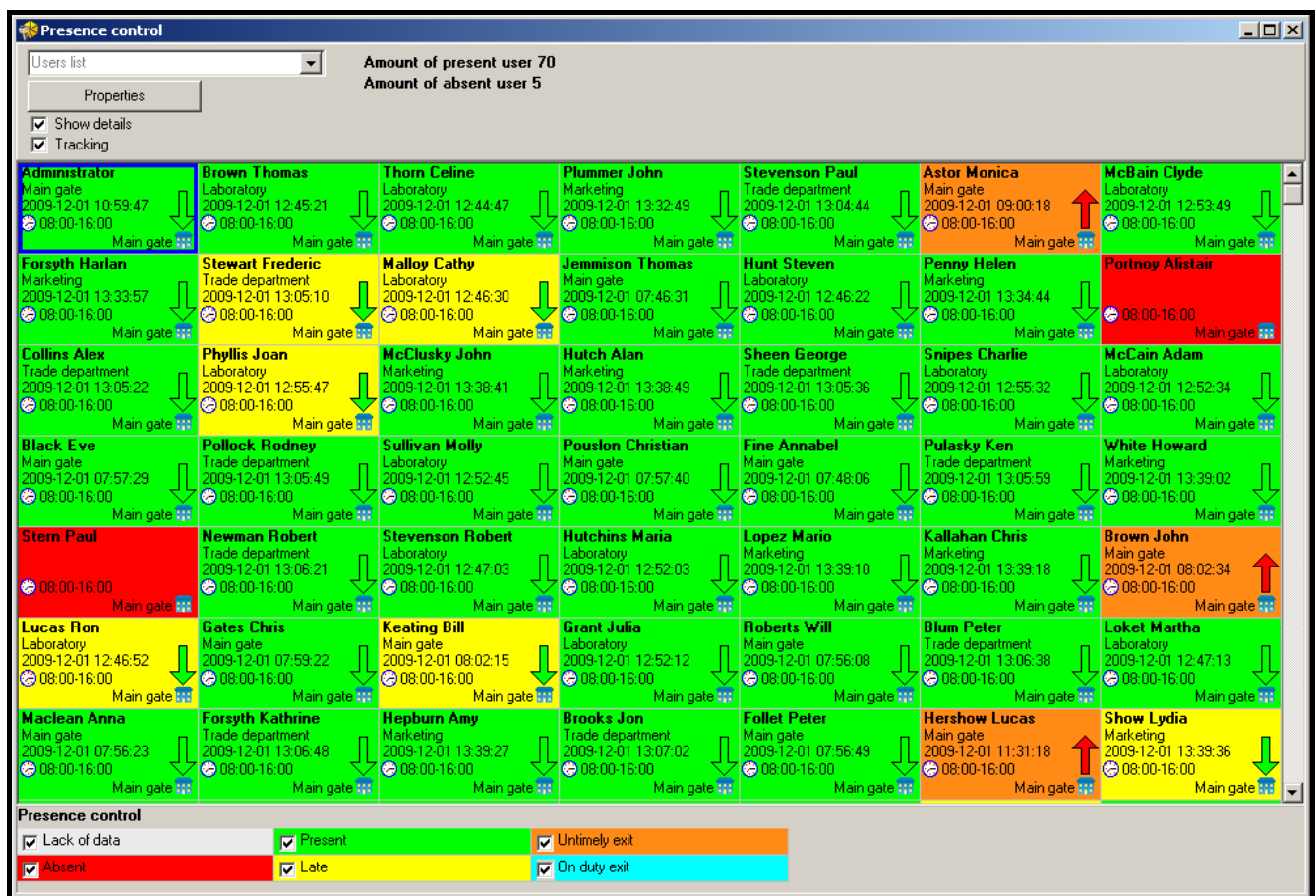
Fig. 36. PRESENCE CONTROL window.

7.8.1 Creating presence control list

1. Select one, a few, a group or all users in the USERS LIST field. The list of selected users will appear in the window below.

2. Using the mouse cursor, select one of the users, and then, if necessary, holding down the left mouse button, select all users or just the required ones (you can also select users by holding down the Shift key and the left mouse button).

3. Click on the PROPERTIES button. A window will open where, depending on the information you want to obtain about users, you can:

– select the entry / exit rule, so that it can be determined when the user left the premises (see: description of creating the rules, section "Creating a presence report").

– define the way of monitoring the entry / exit time:

OUT OF CONTROL – the presence control function will be disabled (only information on the module recently used by the user will appear);

ACCORDING TO HOURS – the presence will be monitored according to the defined time;

ACCORDING TO SCHEDULE – the presence will be monitored according to the selected or defined weekly schedule.

– define the default time of leaving the premises, if the user can leave the premises without registering of this fact by the access control.

4. Select the SHOW DETAILS field, if the parameters defined in the PROPERTIES window are to be displayed at the user name.

5. Select the TRACKING field, if the user whose pass was registered by the access control as the last one is to be selected with a dark blue frame.

6. Select the user presence information which is to be displayed (e.g. presence, being late, etc.).
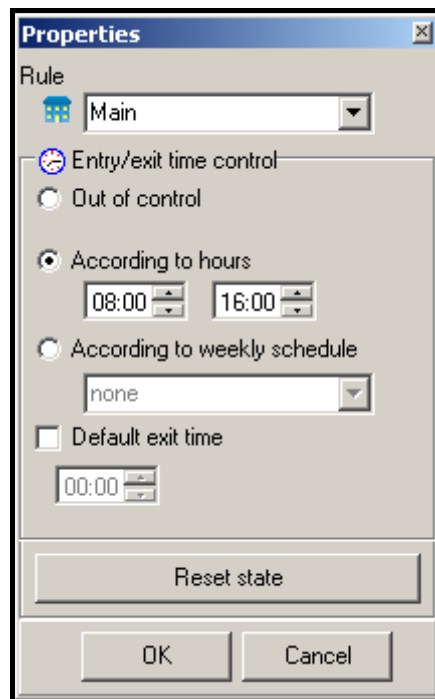
Fig. 37. PROPERTIES window.

Adding new users to the system will not result in their being automatically displayed in the PRESENCE CONTROL window. You must define how they are to be displayed, according to the above-described procedure.

The defined parameters of the users, whose presence status is to be monitored, are saved and stored in the ACCO-SOFT-LT program data base (file extension *.s3db). If the data base is deleted, all the settings will have to be programmed once more.

8. Using the module

This section does not apply to the access control module, which is part of the ACCO NET system.
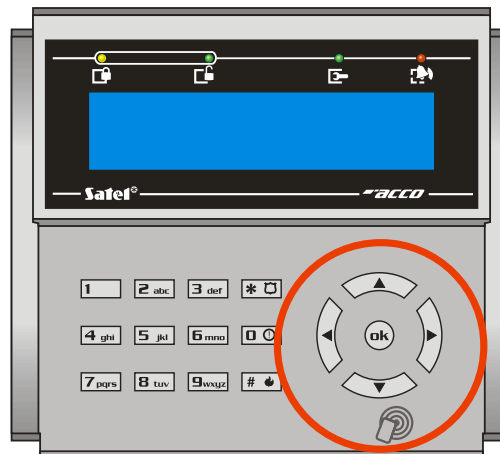
Fig. 38. The area where you have to put the transponder against the ACCO-KLCDR-BG keypad. In case of other terminal units, the user can put the transponder to the terminal at any place.

8.1 Unlocking the door

8.1.1 Unlocking the door with identifiers

Placing the card in proximity of the terminal (to a distance enabling the card code to be read), touching the reader with the iButton or entering the code and confirming it with the $\boxed{\#}$ or $\textcircled{ok}$ key will start the procedure of user verification. If the entry of another identifier is additionally required, this will be signaled by 3 short beeps (and also by corresponding message on the LCD keypad display). Then, enter the code or present your card to the terminal.

If the user can get access, the terminal (except the CZ-DALLAS reader) will signal unlocking the door by a short beep. The module relay will become activated for the time programmed as the ACCESS TIME. Then the door can be opened freely. Depending on the module settings, the relay will be switched off after opening / closing the door (if the door status is not controlled or the user decides not to open the door, the relay will be switched off after expiry of the ACCESS TIME). The door should be closed before expiry of the time programmed as DOOR OPEN TIME.

The door will stay locked if the card/iButton and/or code are unknown (2 long beeps) or the user cannot get access. The user registered in the module, and using a valid code or card/iButton, may be denied access in the following cases:

- the keypad will only grant access based on the card, while a code has been entered (1 long beep);
- the keypad will only grant access based on the code, while a card has been read in (1 long beep);
- the access schedule does not provide for granting permission to pass at that moment (3 long beeps);
- the door is blocked (3 long beeps);
- the user's defined entries limit is exceeded (3 long beeps);
- the user is trying to get access at the terminal, from the side of which he has already unlocked and opened the door (3 long beeps) – the ANTI-PASSBACK function is running;
- the module operates in the mantrap / airlock configuration and the other door is open (3 long beeps);
- the terminal is blocked (1 very long beep) – the ANTI-SCANNER function (holding the card / iButton by the authorized user for 3 seconds will unblock terminals).

Unlocking and opening the door by means of the terminal A will be registered as an authorized entry (event: "Access granted – entry"), and by means of the terminal B as an authorized exit (event: "Access granted – exit"). Cancellation of the door opening after being granted access at the terminal A will be registered as cancellation of the entry (event: "Access granted – entry. Door not opened."), and after being granted access at the terminal B – as cancellation of the exit (event: "Access aborted – exit. Door not opened."). In case of the access refusal, there will also be registered information on whether it was refusal of permission to enter (terminal A), or refusal of permission to exit (terminal B).

8.1.2 Unlocking the door without user identification procedure

The door can be also unlocked, bypassing the access control procedures, by using the module input programmed as the UNLOCK BUTTON. The input can be controlled by means of the button or other device. Appearance of the control signal will unlock the door for the time programmed as the ACCESS TIME (the time of the control signal being supplied to the input has no effect on the door unlocked time).

8.2 Blocking the door

8.2.1 Blocking the door with the use of identifiers

The door can be blocked by the user having the SWITCHING authority. The user can only block the door when he has access to the door, according to the access schedule.

> *i* | *If door status control is disabled, door can be blocked only by means of LCD keypad and code.*

In order to block the door by means of the proximity card / iButton:

1. Make sure that the door operates in normal mode and the door is closed.
2. Place the card in proximity of the reader / touch the iButton to the reader and hold it for about 3 seconds. The terminal (except the CZ-DALLAS reader) will signal blocking the door by 2 short beeps.

> *i* | *If, according to the module settings, the user is to be identified in the LCD keypad / keypad on the basis of card and code, or code only, then the function of blocking the door by means of card will be unavailable in the keypad.*

In order to block the door by using the code and LCD keypad:

1. Enter the code and confirm with the ✱ ☉ key.
2. Scrolling through the menu by means of the ▲ and ▼ keys, find the BLOCK DOOR function.
3. Press the # ♠ or ⓞⓚ key. 2 short beeps will confirm that the door is blocked.

In order to block the door by using the code and ACCO-SCR-BG reader:

1. Make sure that the door operates in normal mode and the door is closed.
2. Enter the code and confirm with the ✱ key. 2 short beeps will confirm that the door is blocked.

8.2.2 Blocking the door without user identification procedure

The door can be blocked by using the module input programmed as DOOR BLOCKING or ALARM – BLOCK DOOR (see: INPUTS). The input can be controlled by means of a switch, alarm control panel, etc. Additionally, the door blocking can be effected by the use of timer or access schedule not used when programming the user settings. For the timer, it is possible to

program the start / end of blocking in the module. Where an access schedule is used, the door will be blocked at the time defined by the schedule.

i *Switching to the normal operation mode or unblocking the door blocked with the use of* ALARM – BLOCK DOOR *type of input is only possible by means of the procedure that requires the use of identifier.*

The timer and the programmed schedule have no priority. This means that occurrence of other events in the module can change the door status before expiry of the specified blocking time.

Blocking the door by means of the timer, schedule or module input programmed as DOOR BLOCKING *is impossible, if the door has been unblocked by means of the* FIRE – UNBLOCK DOOR *type of input.*

8.3 Unblocking the door

8.3.1 Unblocking the door with the use of identifiers

The door can be unblocked by the user having the SWITCHING right. The user can only unblock the door when he has access to the door, according to the access schedule.

i *If door status control is disabled, door can be unblocked only by means of LCD keypad and code.*

In order to unblock the door by means of the proximity card / iButton:
1. Make sure that the door operates in normal mode, and then open the door.
2. Place the card in proximity of the reader / touch the iButton to the reader and hold it for about 3 seconds. The terminal (except the CZ-DALLAS reader) will signal unblocking the door by 2 short beeps.

i *If, according to the module settings, the user is to be identified in the LCD keypad / keypad on the basis of card and code, or code only, then the function of unblocking the door by means of card will be unavailable in the keypad.*

In order to unblock the door by using the code and LCD keypad:
1. Enter the code and confirm with the $\boxed{* \; \circlearrowright}$ key.
2. Scrolling through the menu by means of the ▲ and ▼ keys, find the UNBLOCK DOOR function.
3. Press the $\boxed{\# \; \spadesuit}$ or $\boxed{\text{ok}}$ key. 2 short beeps will confirm that the door is unblocked.

In order to unblock the door by using the code and ACCO-SCR-BG reader:
1. Make sure that the door operates in normal mode, and then open the door.
2. Enter the code and confirm with the $\boxed{*}$ key. 2 short beeps will confirm that the door is unblocked.

8.3.2 Unblocking the door without user identification procedure

The door can be unblocked by using the module input programmed as DOOR UNBLOCKING or ALARM – UNBLOCK DOOR (see: INPUTS). The input can be controlled by means of a switch, alarm control panel, fire protection system, etc.

The ACCO-SOFT-LT program enables unblocking the door by means of the UNBLOCK button, available in the MODULES LIST window (when the door is toggled into unblock status, the button description will change into CONTROL).

Unblocking the door can be effected with the use of timer or access schedule not used when programming the user settings. For the timer, it is possible to program the start / end of unblocking in the module. Where an access schedule is used, the door will be unblocked at the time defined by the schedule.

> i *Switching to the normal operation mode or blocking the door unblocked with the use of FIRE – UNBLOCK DOOR type of input is only possible by means of the procedure that requires the use of identifier.*
>
> *The timer and the programmed schedule have no priority. This means that occurrence of other events in the module can change the door status before expiry of the specified unblocking time.*
>
> *Unblocking the door by means of the timer, schedule, module input programmed as DOOR UNBLOCKING, or ACCO-SOFT-LT program is impossible, if the door has been blocked by means of the ALARM – BLOCK DOOR type of input.*

8.4 Restoring the door to normal operation mode

8.4.1 Restoring normal operation mode of the door with the use of identifiers

The normal operating mode of blocked / unblocked door can be restored by the user having the SWITCHING authority. He can only do so by using the proximity card / iButton or code when he has access to the door, according to access schedule. In case of the door status control disabled, door can be restored to normal operating mode only by means of LCD keypad and code.

In order to restore the normal operating mode of the door by means of proximity card / iButton, hold the card in front of the reader / touch the iButton to the reader for approx. 3 seconds. The terminal (except the CZ-DALLAS reader) will signal restoration of the door to the normal operating mode by 2 short beeps.

> i *If, according to the module settings, the user is to be only identified in the LCD keypad / keypad on the basis of code, or card and code, then restoring the normal operating mode is possible by means of code only.*

In order to restore the door to its normal operating mode with the use of code and LCD keypad:

1. Enter the code and confirm with the $\boxed{* \ \circlearrowleft}$ key.
2. Scrolling through the menu by means of the ▲ and ▼ keys, find the NORMAL MODE function.
3. Press the $\boxed{\# \ \spadesuit}$ or ⓞⓚ key. 2 short beeps will confirm that the normal operation mode of the door has been enabled.

In order to restore the normal operating mode of the door with the use of code and ACCO-SCR-BG reader, enter the code and confirm with the $\boxed{*}$ key. 2 short beeps will confirm that the normal operation mode of the door has been enabled.

8.4.2 Restoring normal operation mode of the door without the user identification procedure

When unblocked, the door can be switched over to the normal operating mode by means of the CONTROL button, available in the MODULES LIST window of the ACCO-SOFT-LT program (when the door is switched to the normal operating mode, the button description changes to UNBLOCK). This does not apply to the door unblocked by means of the FIRE – UNBLOCK DOOR type of input.

8.5 Audible signaling

The user identification devices (keypad, proximity card reader) generate beeps of informative character:

1 short beep – access granted and door unlocked.

2 short beeps – blocking, unblocking or restoring the door to normal mode.

3 short beeps – waiting for the second identifier to be entered.

1 long beep – access denied – card or code are known, but the user cannot unlock the door because:

– the LCD keypad / keypad only grants access, based on the code, but the card has been used;

– the LCD keypad / keypad only grants access, based on the card, but the code has been entered.

2 long beeps – access denied – card or code unknown.

3 long beeps [after placing the card in proximity of the terminal or entering the code and confirming it with the $\boxed{\#}$ key] – access denied – card or code are known, but the user cannot unlock the door because:

– the access schedule does not provide for granting permission to pass at that moment;

– the door is blocked;

– the defined user entries limit is exceeded;

– the user is trying to get access at the terminal, from the side of which he has already unlocked and opened the door – the ANTI-PASSBACK function is running;

– the module operates in the mantrap / airlock configuration and the other door is open;

3 long beeps [after placing the card and hold it in proximity of the terminal for about 3 seconds or entering the code and confirming it with the $\boxed{*}$ key] – change of door status (blocking / unblocking / normal mode) cannot be done – door status control is disabled.

1 very long beep – access denied – the terminal is blocked – ANTI-SCANNER function (holding the card by an authorized user for 3 seconds will unblock the terminals).

Long beep lasting 10 seconds – alarm. There can be the following causes for the alarm:

– opening the door by force;

– 5 attempts to get access on the basis of unknown identifier (ANTI-SCANNER function);

– activation of the FIRE – UNBLOCK DOOR type of input;

– activation of the ALARM – BLOCK DOOR type of input;

– tamper of the door controller module (ITMP controller module input is isolated from the common ground);

– tamper of keypad;

– loss of communication with the terminal (no terminal).

9. Module factory settings

| *i* | *This description does not apply to the access control module, which is part of the ACCO NET system.* |

The below described settings refer to a new module. The SET DEFAULT button available in the MODULES LIST window will not restore all the factory settings of the module. Only the settings available in the MODULES LIST window will be restored. The user list, time schedules and event log, which were saved to the module memory, will be retained without changes.

Module

All the module related options and functions are disabled.

Module inputs

Input 1: Door status control. NO type. Sensitivity: 50 ms.

Input 2: Unlock button. NO type. Sensitivity: 50 ms.

Input 3: Door unblocking. NO type. Sensitivity: 50 ms.

Input 4: Unused. NC type. Sensitivity: 50 ms.

Input 5: Unused. NC type. Sensitivity: 50 ms.

Module outputs

Output 1: Forced entry. 5 invalid attempts. Operation time: 10 seconds.

Output 2: Long open door. No terminal presence. Operation time: 10 seconds.

Door

Enabled options:

    Authorization control,

    Alarm on unauthorized open.

Access time: 5 seconds.

Door open time: 20 seconds.

Other functions and options are disabled.

LCD keypad

Time format on LCD keypad: hh:mm.

Other options are disabled.

Backlight A/B

Auto.

Transmission format

EM Marin.

Access method

Card or code.

Users

"Administrator", ID number 00001, having the ADMINISTRATOR and CHANGE CODE rights and using the code 12345.

10. Specifications

10.1 ACCO-KP-PS / ACCO-KPWG-PS module

Supply voltage .... 18 VAC ±10%

Power supply output voltage, rated .... 12 VDC ±15%
Power supply output current .... 1.2 A
Maximum current consumption .... 110 mA
Maximum relay switching voltage .... 250 VAC
Maximum relay switching current .... 8 A
+12V output rating (at 25°C temperature) .... 1,1 A
Current-carrying capacity, OC type outputs .... 50 mA
Battery charging current .... 350 mA
Recommended battery .... 12 V / 7Ah
Working temperature range .... -10 °C … +55 °C
Electronics board dimensions .... 151 x 70 mm
Weight .... 113 g

10.2 ACCO-KP / ACCO-KPWG module

Supply voltage, rated .... 12 VDC ±15%
Average current consumption .... 110 mA
Maximum relay switching voltage .... 250 VAC
Maximum relay switching current .... 8 A
Current-carrying capacity, OC type outputs .... 50 mA
Working temperature range .... -10 °C … +55 °C
Electronics board dimensions .... 73 x 104 mm
Weight .... 235 g

10.3 ACCO- KLCDR-BG / ACCO-KLCDR-BW keypad

Supply voltage, rated .... 12 VDC ±15%
Current consumption, maximum .... 160 mA
Current consumption, average .... 60 mA
Reader working frequency .... 125 kHz
Working temperature range .... -10 °C … +55 °C
Enclosure dimensions .... 140 x 126 x 26 mm
Weight .... 236 g

10.4 ACCO-SCR-BG keypad with proximity card reader

Supply voltage, rated .... 12 VDC ±15%
Maximum current consumption .... 110 mA
Current-carrying capacity, BELL output .... 30 mA
Reader working frequency .... 125 kHz
Working temperature range .... -20 °C ... +55 °C
Enclosure dimensions .... 47 x 158 x 24 mm
Weight .... 237 g

11. History of changes to the manual

Shown below is the description of changes to the manual for controller, firmware version v 2.0.

Date	Firmware	Introduced changes
2009-09	2.02	• Section "General" (p. 3) was modified. • New module diagrams were added to section "Electronics board"; the section was updated (p. 5). • Section "Inputs" was updated (p. 7). • Section "Outputs" was updated (p. 7). • Table in section "Connecting the proximity card readers" was updated (p. 20). • Section "Service mode menu" was updated (p. 25). • Program description was modified and figures changed in section "ACCO-SOFT-LT program" (p. 28). • Section "Module functions and options" was updated (p. 31). • Section "Functions and options related to the door" was updated (p. 33). • Section "Functions and options related to the LCD keypad" was updated (p. 34). • Section "Transmission format" was added (p. 35). • Note about optional assignment of cards by Wiegand format supporting terminals was added to section "Users" (p. 35). • Figures were changed and program description modified in section "Adding new users" (p. 36-39). • Note about simultaneous user editing by means of program and keypad was added to section "Editing a user by means of ACCO-SOFT-LT program" (p. 40). • Note about ENTRIES LIMIT was added and a figure was changed in section "User groups" (p. 42). • Section "Automatic assigning of user to a group" was added (p. 42). • Section "Automatic grouping of users" was added (p. 43). • Section "User(s) report" was added (p. 43). • Contents was updated and a figure changed in section "Access schedules" (p. 44). • Section "Presence reports" was added (p. 47). • Section "Presence control" was added (p. 49). • Contents was updated and a figure added to section "Using the module" (p. 51, 52-53). • Section "Audible signaling" was updated (p. 55).
2011-03	2.03	• Section "General" (p. 3) has been modified. • Information on terminals to connect CZ-DALLAS reader has been added (p. 6). • Section "Outputs" has been updated (p. 8). • Section "Devices interfacing with the module" has been updated (p. 8). • Section "CZ-DALLAS DALLAS iButton readers" has been added (p. 13). • Section "Access control installation" has been modified (p. 14). • Section "Connecting DALLAS iButton readers" has been added (p. 21). • Section "Service mode menu" has been updated (p. 25). • Figure has been changed in section "Installation and first start of the program" (p. 31). • Section "Module functions and options" has been updated and note referring to the "Presence control - Terminal A/B" has been added for CZ-DALLAS reader (p. 31). • Section "Transmission format" has been updated (p. 35). • Section "Users" has been modified (p. 35). • Section "Adding new users by means of the ACCO-SOFT-LT program" has been modified (p. 36). • Section "Editing a user by means of ACCO-SOFT-LT program" has been modified (p. 40). • Figure has been changed in section "Creating a user group" (p. 42). • Section "User(s) report" has been modified (p. 43). • Section "Using the module" has been updated (p. 50-54). • Section "Module factory settings" has been updated (p. 56).

			• Section "Specifications" has been updated (p. 56).
2011-11	2.03		• Illustration in section "ACCO-KLCDR-BG / ACCO-KLCDR-BW keypad" has been changed (p. 9). • In section "Users", the note on assignment of cards to the users by means of terminals supporting Wiegand format has been modified (p. 35). • In section "Adding new users by means of the ACCO-SOFT-LT program", information that the keypad may incorrectly handle cards added by means of Wiegand terminals has been added (p. 38). • Illustration in section "Using the module" has been changed (p. 50).
2014-09	2.03		• Section "Connecting the ACCO-SCR-BG keypad" has been updated (p. 18). • Section "Connecting the proximity card readers" has been updated (p. 20). • Section "Connecting the Wiegand 26 readers" has been added (p. 20).
2015-04	3.00		• The manual has been updated by adding information on the module working as part of the ACCO NET system. • Section "CZ-USB-1 proximity card reader" has been added (p. 14). • Section "Connecting CZ-USB-1 proximity card reader" has been added (p. 21). • Information on required versions of ACCO-SOFT-LT program has been added (p. 27).
2018-12	3.02		• Information about third-party devices sending data in WIEGAND format, supported by the access control module, has been added (p. 3). • Content of the "Electronic board" section has been updated (p. 4). • Content of the "Inputs" section has been updated (p. 7). • Content of the "Outputs" section has been updated (p. 7). • Content of the "Devices interfacing with the module" section has been updated (p. 8). • "Third-party readers" section has been added (p. 14). • Content of the "Mantrap / airlock" section has been updated (p. 22). • Content of the "Programming the module" section has been updated (p. 25). • Drawing in the "Installation and first start of the program" section has been changed (p. 31). • Content of the "Transmission format" section has been updated (p. 35). • Information about CZ-USB-1 reader has been added (p. 38).
2019-11	3.04		• Note on how to install and start the ACCO-SOFT-LT program has been added (p. 28).
2021-04	3.05		• Content of the "CZ-EMM3 and CZ-EMM4 proximity card readers" section has been updated (p. 12). • Note on the WIEGAND format has been added (p. 14). • Content of the "Connecting power supply" section has been updated (p. 2335). • Information on the required versions of the ACCO-SOFT-LT program has been updated (p. 27). • Note on the WIEGAND format has been updated (p. 35).

The declaration of conformity may be consulted at www.satel.eu/ce