Single-User Software

SL01

Operation Manual

PERCo®

SL01 Single-User Software

Operation Manual

TABLE OF CONTENTS

GENERAL

This Operation Manual includes important information about the **SL01 Single-User Software,** its application and main features. The Manual provides straightforward instructions on how to use this software as detailed step-by-step procedures.

The Manual is designed for operators with working knowledge of Microsoft Windows software and operational experience with such common software packages as MS Office, etc.

Application of the SL01 Single-User Software

The software is designed as a single-operator programme appropriate to use for**:**

- administration of employee lists (full names);
- issue of access cards;
- access rights assignment under authorized/non-authorized principle;
- setting and change of access modes;
- hardware configuration;
- database event logging with data exportable e.g. to an Excel file.

STARTING OPERATION

In order to use the **SL01 Single-User Software** (hereinafter referred to as **"**the software**"**), it should be installed at a PC connected to the local area network, LAN.

Establish the Ethernet network connection between the controller and PC with the installed S-20 software.To establish the connection, make sure the controller with determined network settings is connected to the same network segment, or directly to the PC network adapter. To do this, add the new IP-address to the network interface of your PC with the installed S-20 software, or change the existing IP address according to the operating system (e.g. 10.0.0.1) with the network mask given in the controller certificate.

Installation of the software

1. Insert the disc with the licensed software into the CD-ROM drive, wait for the installation program icon to appear.
2. If, by some reason, the installation icon does not appear automatically, use Windows Explorer or any other file manager application to access the disc contents, and run the **Freesetup.exe** program.
3. Follow the Installation Wizard instructions that appear on your screen.
4. Click on the Ready button when the installation is complete.

Starting the software

To start the software:

1. Click on the **Start** button**.**

2. Select **All Programs** → **PERCo** → **Single-User Software** → **Single-User Software**. The software work window will appear on the screen with the Employees section opening on default; subsequent runs of the software will open the last Section where the software was exited. When the software window is reduced, its sign will appear in the System Tray icon as shown below:

Descriptions of corresponding work windows are given in the beginning of each Section.

EMPLOYEES

The **Employees** Section is designed for employees' data entry assignment of access cards with unique ID numbers, allowing and denying of access, authorizing or denying the right to activate/deactivate the Protection mode, inspection of a certain employee's event log over a specified period of time. Click on the Employees tab to open the section.

Employees work window

The work window of the **Employees** section looks as follows:
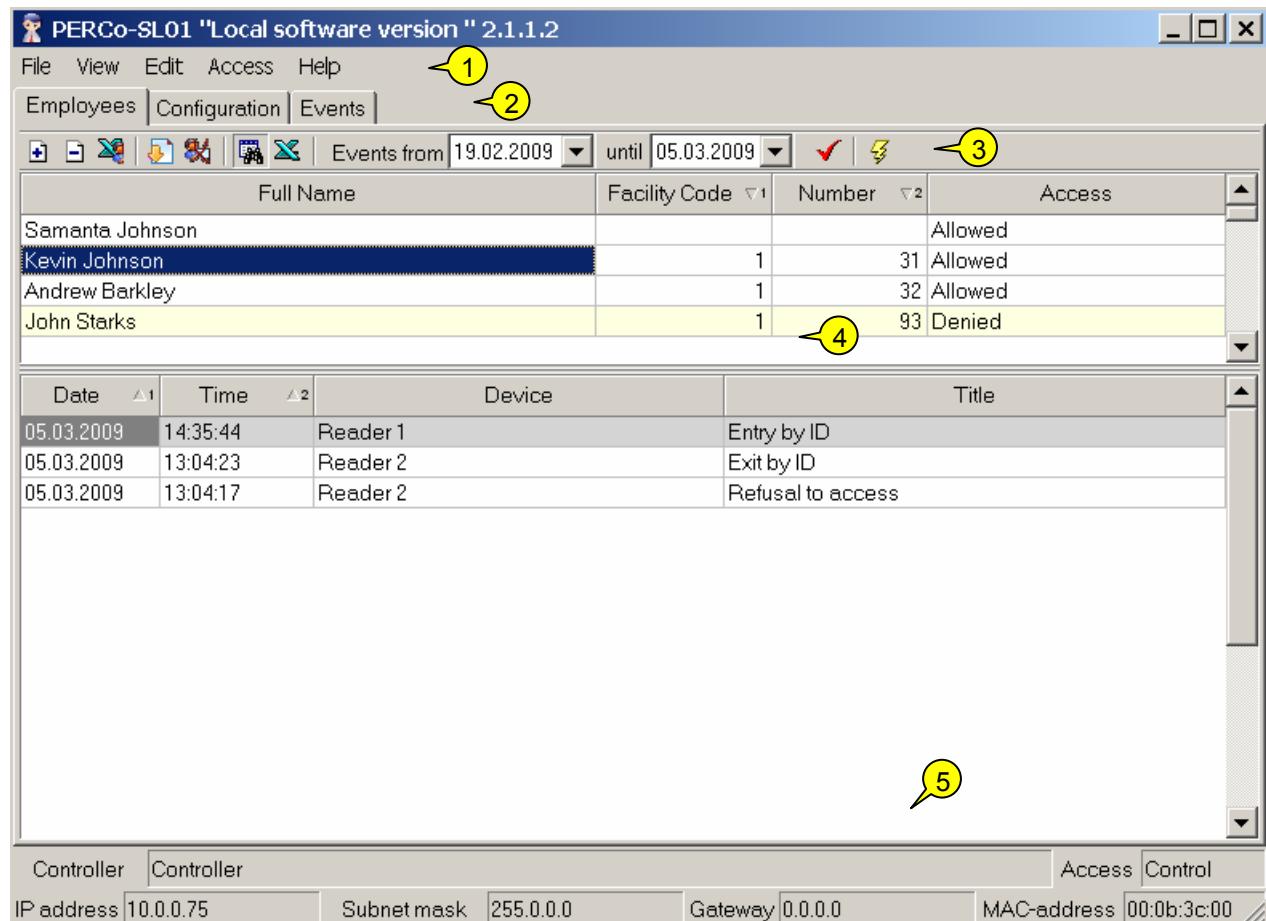
Fig.1. Employees section work window

> **NOTE**
> Rows with data that has not been exported to the controller, and therefore not saved into the system, are highlighted with yellow colour.

1. The window top contains the main menu.

2. There are following section tabs under the main menu: **Employees**, **Configuration**, **Events**.

3. Functional elements of the window are described in the Appendix 1.

4. The central part of the window contains a desktop. The data are given as a table made of several columns, each with a particular functionality. Such a tabular presentation conveniently allows sorting data by various attributes in descending or ascending order. The arrangement of the columns can be easily changed by dragging. The event list related to a selected employee/visitor is located below the desktop.

5. A status line at the bottom of the desktop displays the service information (status of the controller, access mode, IP-address, etc.)

Adding Employee data

After the software installation, the list of the employees is empty. To add an employee:

1. Click on the **Add Employee** button ⊞ . A yellow highlighted line will appear in the list (refer to NOTE к fig.1).

2. Enter the employee's forename (names) and surname, or surname and initials into the **Full Name** column.

3. Press **Enter** button on keyboard to save the employee data in the database.

4. The Access column displays the **Allowed** default option, informing that this employee is authorized to pass through a certain operating device (OD) in the set access mode. For how to authorize/deny access refer to the Access Authorization/Denial section below.

5. On the next stage the employee should be issued an access card. Refer to the **Entering ID number** section below for the access card issue procedure.

> **NOTE**
> You can also add an employee/a visitor by clicking on the **Down** (↓) or **Insert** buttons.

Deleting Employee

To delete an employee from the list:

1. Choose any box in the line containing the data of the employee to be deleted and click on the **Delete Employee button** — ⊟.

2. Click on the Yes button in the appearing confirmation dialog box. The employee and their access card data will be deleted from the database.

> **NOTE**
> Nothing changes in the Event Log when an employee is deleted.

Export of employees

The employees can be exported into files of the following formats:
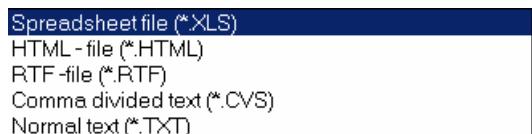
*.**XLS** — Excel document format (default setting);

*.**HTML** — WEB-page format;

*.**RTF** —Word document format;

*.**CVS** — Text document format;

*.**TXT** — Text document format.

To export employees:

1. Click on the **Employee Export button** — .

2. Select the disc and the folder in the opened Export window, specify the file name and extension and click on the Save button:
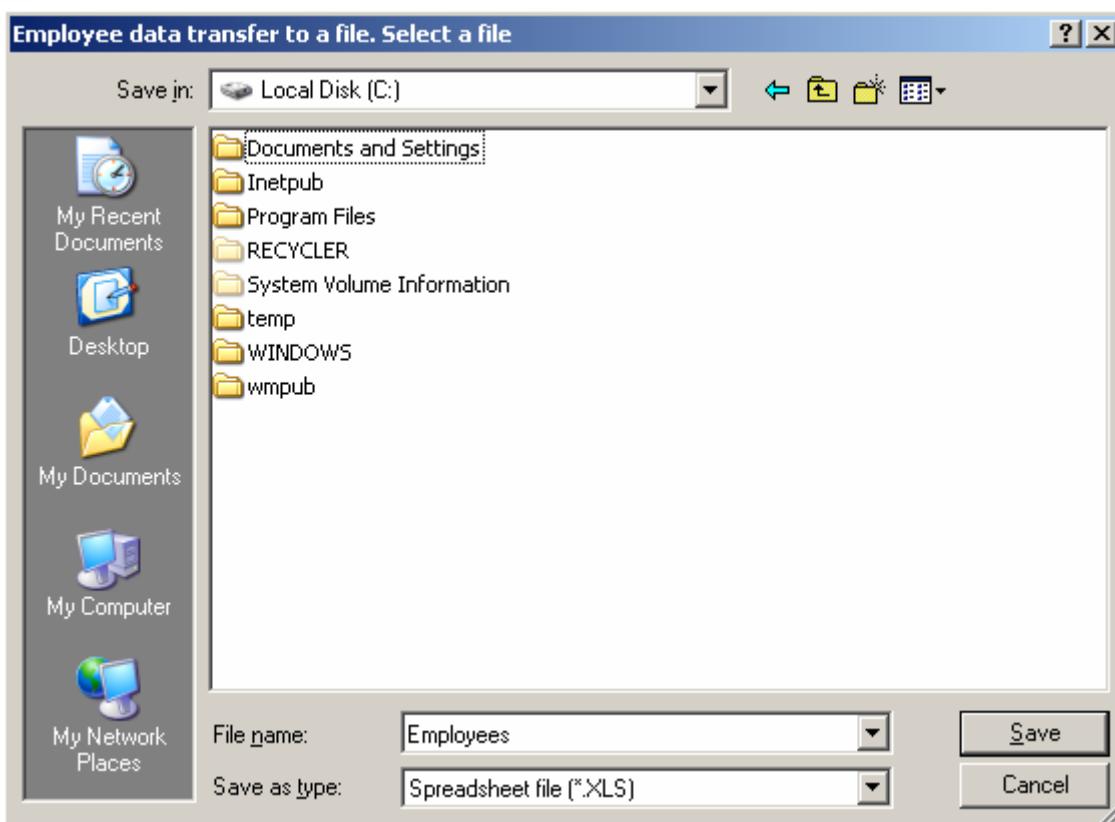
The employee data will be exported into the specified file.

Entering an ID number

There are several types and formats of proximity cards. Not all access cards are issued with their ID numbers visible on the front or rear of the card. In view of this, the software allows for two options of entering an ID number:

- receiving an ID number from a controller
- manual entering of an ID number.

Receiving ID number from Controller

If just a number is shown on the card or no identifying information whatsoever is visible, the only way of receiving an ID number is via a controller.

The controller should be configured before receiving an ID number (refer to the Configuration section, the Controller configuration subsection).

To receive an ID number from a controller:

1. Enter the employee/ visitor information into the Full Name column.

2. Click on the Receive ID from Controller button — . The process of ID number receiving is displayed in the status line.

3. Present the card to the card reader of the controller selected in the Configuration section. The process of receiving an ID number is accompanied by flashing light indication and an audio signal on the controller. To cancel receiving of an ID number, click on the [Cancel] in the status line:

Controller	ID receipt from Controller (6 sec)...		Cancel		Access	Control
IP address 10.0.0.75		Subnet mask 255.0.0.0		Gateway 0.0.0.0	MAC-address	00:0b:3c:00:3c:e5

4. If, during the pre-installed period of time of 100 seconds, the card is not presented to the reader, the following information window appears on the screen:
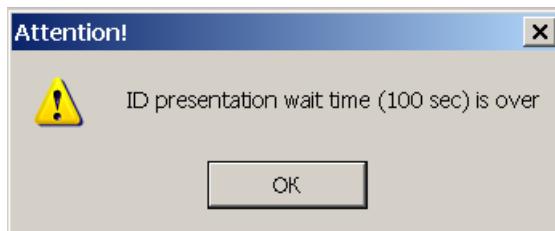
5. Click on the **OK** button**.**

6. If this operation is successful, the values the system received from the access card are shown in the **Facility Code** and **ID Number** columns:

Full Name ▽	Facility Code	Number	Access
Samanta Johnson		1	33 Allowed

7. Click on the **Transfer to Controller** button for correct completion of the operation.

> **NOTE**
>
> ID numbers from the controller are received successively, card by card, with the row to enter a new ID number received from the controller chosen with the cursor. For the next ID number, choose the row with the employee name to enter the ID number and repeat the above procedure.

Manual entering of ID number

If the card series and number are visible, they can be entered manually through the row with an employee data:

1. Enter the card series into the **Facility Code** column. If the first digits are nulls, they will not be visible in the table and are not necessarily to be entered.

2. Enter the visible card number into the **ID Number** column. If the first digits are nulls, they will not be shown in the table and are also not necessarily to be entered.

Facility Code	Number	Access
1	33	Allowed
160	36067	Allowed
160	36386	Allowed
160	36466	Allowed
160	35975	Allowed
160	36596	Allowed

Click on the **Transfer to Controller** button — [icon].

The employee access card is ready for use.

Deleting ID number

To delete an ID number from the controller:

1. Highlight any box in the row with the ID number to be deleted.

2. Click on the **Delete ID from Controller** button — [icon]. The below confirmation window will appear:

Do you want to delete?

Do you want to delete the ID number 160 / 36067?

[Yes] [No]
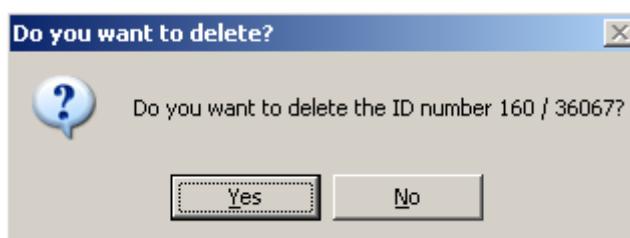
3. Confirm the deletion by clicking on the **Yes** button. Data from **the Facility code** and **Number** columns will be deleted. The ID number will be deleted from the controller.

Access authorization/denial

For all employees/visitors access is allowed by default in a set operating mode (refer to the **Operating Modes** section). Proceed as follows to change this setting:

1. Choose the row with the employee/visitor data and the operating mode to be changed.

2. Choose the Access column and click on the Allowed option. The arrow of the dropdown list will appear on the right side of the column.

3. Click on the arrow and choose the Denied option in the list:

Facility Code	Number	Access
1	93	Denied
1	31	Allowed
1	33	Allowed
160	36067	Denied
160	36386	Allowed
160	36466	Allowed

4. Click on the **Transfer to Controller** button [⚡] to save the changes.

To authorize access, follow the same procedure but choose the **Allowed** option in the list.

Event viewing

The software enables viewing of events related to activities of a selected employee over a specified period of time.

1. Enter the initial viewing date manually or by clicking on the left arrow of the date field in the event viewing time setting box **Events since … until…**, located above the list of the employees: [3/12/2009]
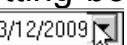
2. Choose the initial viewing date by the below calendar:
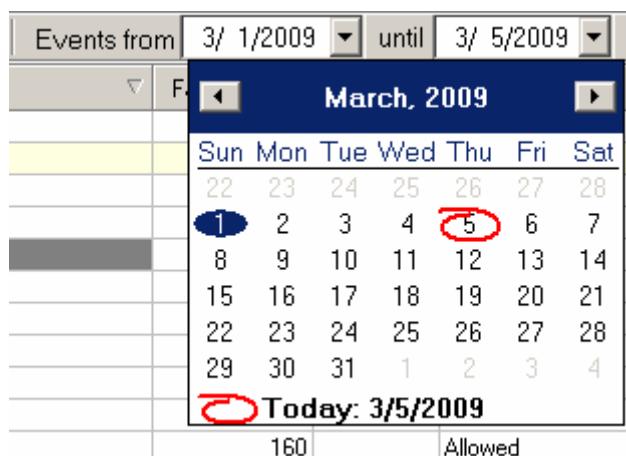
3. Repeat the procedure to set the final viewing date in the right date field. On default this field automatically shows the current date.

4. Choose the row with the specified employee data and click on the **Show Events** [🔍] button. An additional window with the event list over the specified period of time will appear:

Full Name	▽	Facility Code	Number	Access
John Starks		1	93	Denied
Kevin Johnson		1	31	Allowed
Samanta Johnson		1	33	Allowed

Date △1	Time △2	Device	Title
05.03.2009	14:35:44	Reader 1	Entry by ID
05.03.2009	13:04:23	Reader 2	Exit by ID
05.03.2009	13:04:17	Reader 2	Refusal to access

5. Use the **Update Event** List ☑ button for periodical updates of the list. This button is active only in the Event viewing mode.

6. Click again on the **Show Events** button 🔍 to leave the viewing mode.

Event export

The event log of a selected employee over a specified period of time can be saved into a file of the following formats:
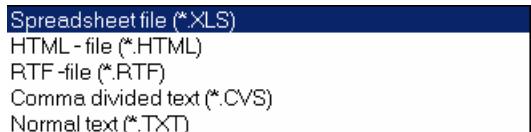
Spreadsheet file (*.XLS)
HTML - file (*.HTML)
RTF -file (*.RTF)
Comma divided text (*.CVS)
Normal text (*.TXT)

*.XLS — Excel document format (default setting);

*.HTML — WEB-page format;

*.RTF — Word document format;

*.CVS — Text document format;

*.TXT — Text document format.

To export events:

1. Choose the row with the employee data in the table.

2. Specify the event viewing period (refer to the Event Viewing section above).

3. Click on the **Show Events** button 🔍 to display the event log. Click on the Event List Update — ☑ to refresh the event list.

4. Click on the **Employee Export** button 📊. Select the disc and folder in the opened window, specify the file name and format, click on the **Save** button:

Event data will be exported into the specified file.
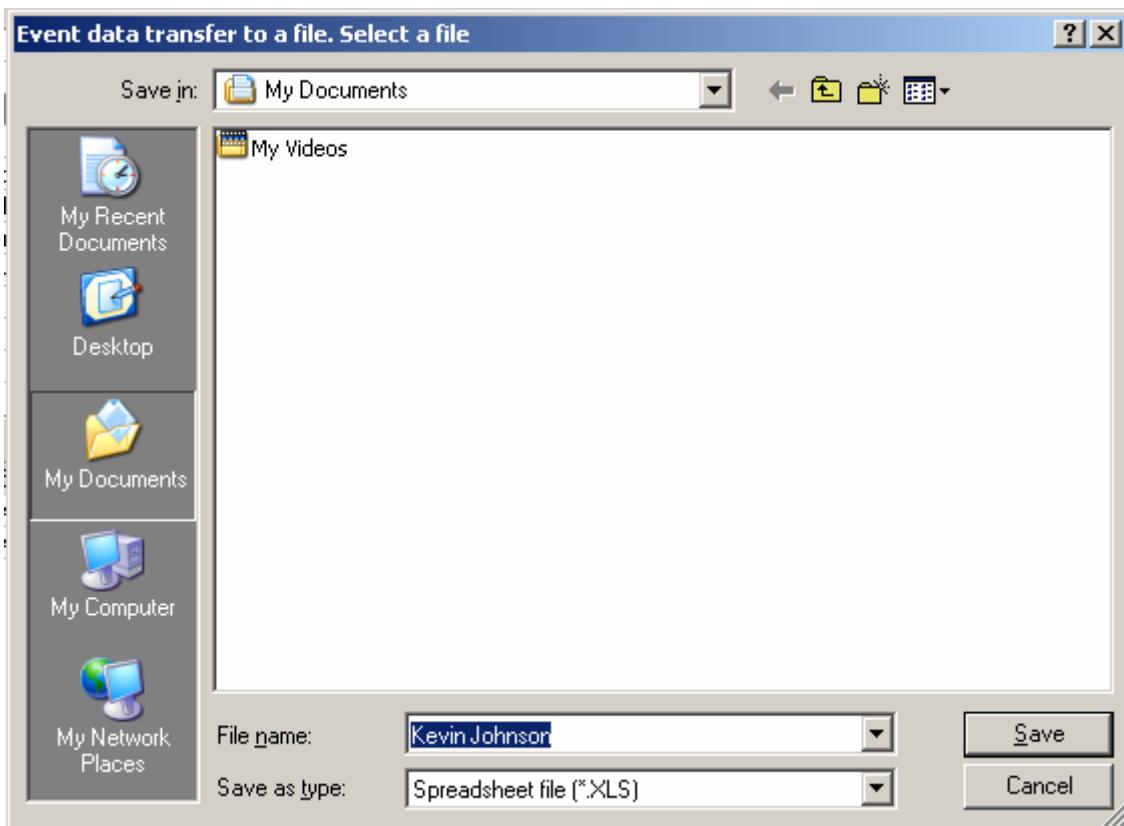
CONFIGURATION

The **Configuration** section refers to settings of the system hardware**:** controllers, readers, operating devices, video cameras. Click on the **Configuration** tab.

Configuration section work window

The **Configuration** section work window looks as follows:
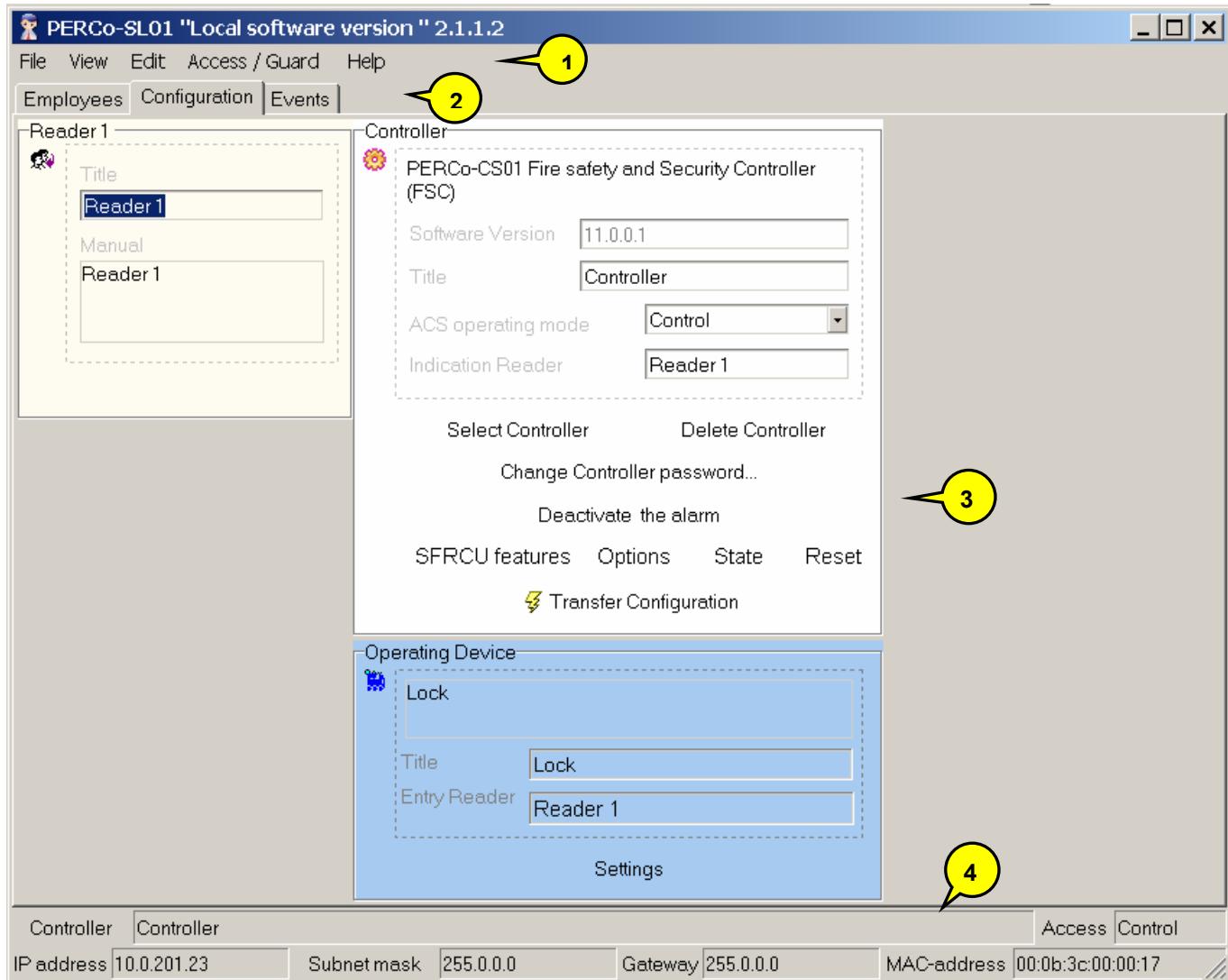
Fig.2. Configuration section work window

1. The top of the window contains the Main menu. Use the **Access** menu for section configuration of the access cards' rights.

2. Section tabs of the following sections are located under the Main menu: **Employees**, **Configuration**, **Events.**

3. The central part of the window contains the desktop with the hardware settings windows for a controller, a reader (or, depending on the controller type, two readers), and an operating device.

4. The bottom of the work window contains a status line to display the service information (status of the controller, access mode, IP-address, etc.)

Controller configuration

Regardless of the number of the controllers installed at the enterprise, the software enables real time operation with only one selected controller. In order to activate another controller, the current controller should be deactivated and another one chosen from the list. The settings are modified in the **Controller** window:

Controller window elements

The **Title** text field is meant for a descriptive name of a controller, for instance **the main entrance Controller**. This provides the operator with information about the selected controller in a convenient form when there are several controllers in the system (refer to the NOTE to the «*Reader window*» section below).

The operator cannot enter any information via the **Title** text field of the controller window; this information is transferred from the hardware to identify a unique device, for instance the **CL02 Lock Controller**.

Use the **Access Mode** dropdown list for selection of the appropriate access mode for the employees entering by card through the operating device served by this controller. Click on the list arrow and select the required mode (the **Control** mode is set on default after selection of the Controller):

> ### NOTE
>
> Use the remote control panel or the **Access** option of the Main menu for a quick change of the operating mode (refer to the *fig.2* description). Refer to the «*Operating modes*»section for further details about the operating modes.

The name of the reader connected to the controller is selected in the **Reader ID** text field, e.g**. Reader 1** that can be used as an ID-number reader during an employee access card issue (refer to the «*Receiving ID-number from Controller*» subsection) in the **Employees** section. The selected reader name will be employed during the current and successive sessions provided that the controller was not deleted or changed (refer to NOTE to the «*Reader window*» section below).

Controller selection

The software enables real time operation with only one selected controller. Select one controller if there are several controllers installed in the system. Each controller comes as a network device, with its own IP-address.

1. Click on the   Select Controller   button. The **Controller selection** window with the list of all devices installed in the system will appear on the screen:
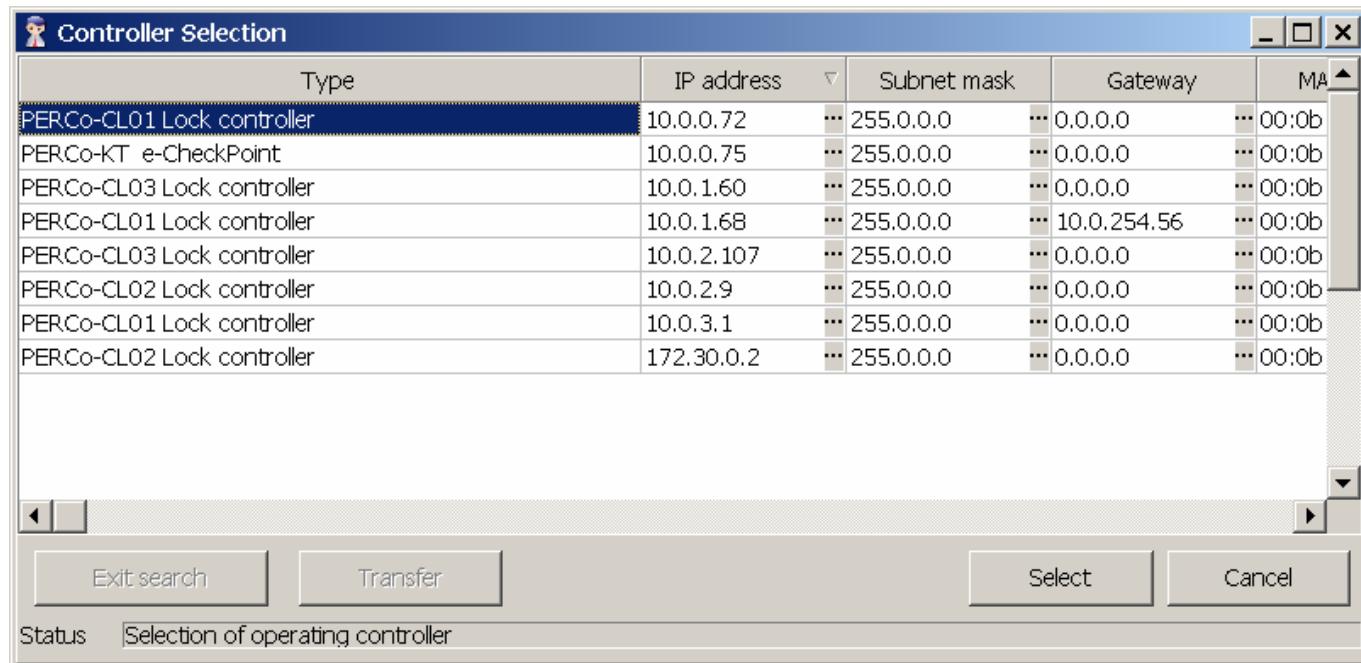
2. When the window is open, an automatic search for all controllers in the network will start, the search flow being displayed in the status line at the bottom of the window. The list contains all the controllers found in the network. This search may take a long time with a large number of controllers connected to the network. When a required controller is found, the search can be stopped by clicking on the **Exit Search** button. For selection, click on the row of the required controller and push the **Select** button.

3. Click on the   ⚡ Transfer Configuration   button to save the settings into the system .

Controller change

The   Delete Controller   button is not meant for deleting a controller from the system configuration but for deactivating of the current controller and subsequent selection of another controller. To change a controller:

1.Click on the [Delete Controller] button. All data in the window fields will be deleted while a message that no controller is selected will appear

```
┌─Controller────────────────────────────────────┐
│ ⚙  Controller is not selected! Select a Controller. │
│                                                │
│   Software Version  [                        ]  │
│                                                │
│   Title             [                        ]  │
│                                                │
│   Operating mode    [              ▼]          │
│                                                │
│   Indication Reader [|             ▼]          │
│                                                │
│        Select Controller      Delete Controller │
└────────────────────────────────────────────────┘
```
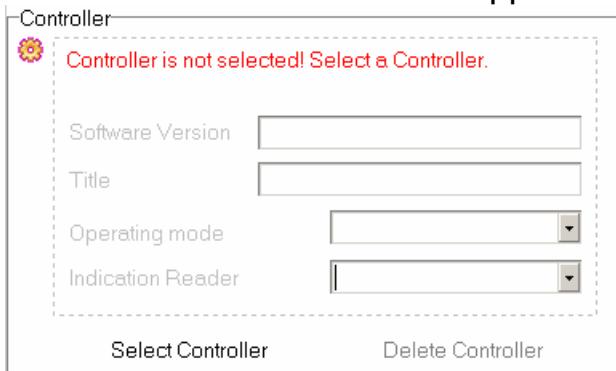
2. Click on the [Select Controller] button to select another controller and repeat the procedure given in the «*Controller Selection*» subsection above.

3. Click on the [⚡ Transfer Configuration] button to save the settings into the system.

Change of Controller settings

Settings of a controller that can be changed are as follows:
- IP- address;
- Subnetwork mask;
- Gateway.

To change any of the above settings:

1. Click on the **Exit search** button in the **Controller selection** window:

Type	IP address ▽	Subnet mask	Gateway	MA
PERCo-CL01 Lock controller	10.0.0.72	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-KT e-CheckPoint	10.0.0.75	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CL03 Lock controller	10.0.1.60	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CL01 Lock controller	10.0.1.68	⋯255.0.0.0	⋯10.0.254.56	⋯00:0b
PERCo-CL03 Lock controller	10.0.11.215	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CL03 Lock controller	10.0.2.107	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CL02 Lock controller	10.0.2.9	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CS01 Fire safety and Security Controller (FSC)	10.0.201.46	⋯255.0.0.0	⋯255.0.0.0	⋯00:25
PERCo-CL01 Lock controller	10.0.3.1	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b
PERCo-CL02 Lock controller	172.30.0.2	⋯255.0.0.0	⋯0.0.0.0	⋯00:0b

Exit search   Transfer   Select   Cancel

Status   Controller search in system network   ▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐▐

2. Choose the controller row in the column with changing settings and click on the ⊡ button on the right side of the current value:

IP address	▽	Subnet mask		Gateway	
10.0.0.72	···	255.0.0.0	···	0.0.0.0	···
10.0.0.75	···	255.0.0.0	···	0.0.0.0	···
10.0.1.60	···	255.0.0.0	···	0.0.0.0	···
10.0.201.18	···	255.0.0.0	···	255.0.0.0	···
10.0.201.23	···	255.0.0.0	···	255.0.0.0	···
172.30.0.2	···	255.0.0.0	···	0.0.0.0	···

3. An **IP-address** window will appear:
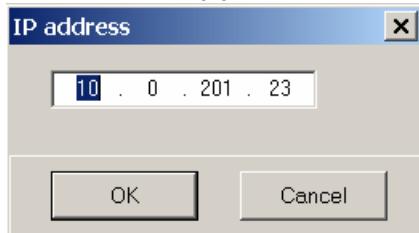
4. Enter new values and click on the **OK** button.

5. Click on the [Transfer] button in the **Controller selection** window.

6. Click on the [⚡ Transfer Configuration] button to save the settings into the system.

Alarm deactivation

The system can be in the alarm state. Click on the **Deactivate Alarm** button to deactivate the alarm:

.
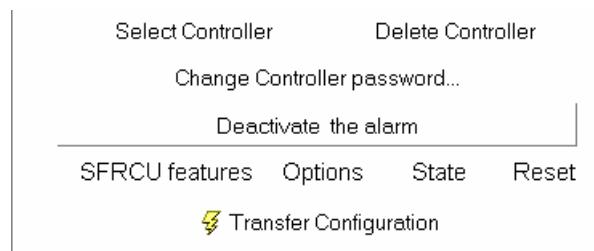
Reader window

Depending on the controller type, one or two readers can be connected to it. The **Reader** window provides the description of a specific reader connected to a specified controller. Two text fields**, Title** and **Manual** are used for this purpose:
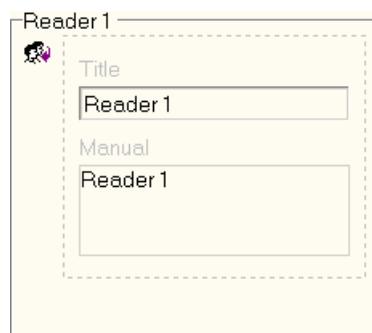
A text in the **Manual** field cannot be changed as it is transferred from the hardware and serves for identification of a unique device.

The **Title** field is used for entering of specifying information about the reader location, e.g., Reader 1: at the **Main Entrance**:
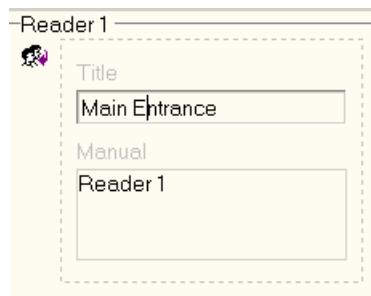
This information will be reflected in the corresponding **Controller** and **Operating device.**

> ### NOTE
>
> Information, entered in the **Title** fields of every device windows, is saved during all current session as well as at the ending of the software operation and its successive run. When deleting (changing) a controller, information entered by the Operator in the **Title** field is replaced by default data (in this particular case— Reader **1**).

Operating Device configuration

Various operating devices can be connected to a controller: electromagnetic and electromechanical locks, turnstiles and other hardware. Such connected devices should be properly configured. For this purpose use the **Operating device** window in the **Configuration** section:
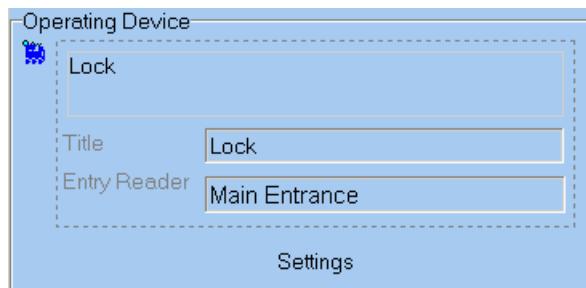
Operating device window elements

The **Title** text field is used for entering of a descriptive name of an operating device (OD), e.g., **Lock** or **Main Entrance Turnstile**. When there are several OD's in the system, this enables fast determination which device exactly is connected to the selected controller. In this particular case, a generic name **Lock** is used as a description.

The **Entry Reader** text field contains name of a reader that comes as the entry reader depending on the passage (access) direction selected in the **Operating Device Settings** dialog box, e.g., **Reader 1**. This name will be used during the current and successive sessions provided that the controller is not deleted or changed (refer to NOTE to the «*Reader window*» section above).

The operator cannot enter any information via the **Title** text field of the controller window; this information is transferred from the hardware to identify a unique device, e.g. **Lock**.

The bottom part of the window contains the **Settings** button, which is used for opening of the **Operating device settings** dialog box:
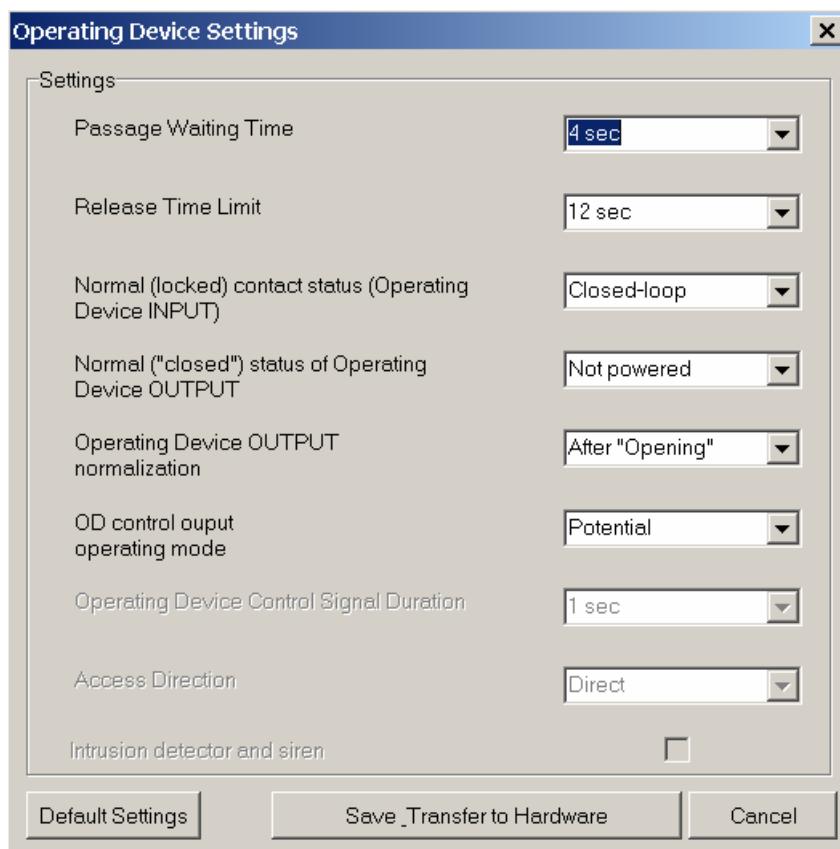
Operating Device settings

The **Operating Device settings** dialog box contains several settings for installation of a specified OD realized as dropdown lists and the three buttons: On Default, Save & Transfer to Hardware and Cancel. Each operating device in the system (various locks types, turnstiles and other hardware) will have different settings. The system determines the settings automatically for all OD's, connected to the controller but the settings can be changed when necessary, in accordance with documentation for a specific operating device.

Some of the settings are interdependent. For example, if the **OD Control Output Operation mode** is **Potential,** the **OD Control pulse duration** setting will be unavailable.

Some of the settings can be changed without referring to the documentation. For example, depending on the number of employees passing through a certain OD, the value of the **Passage waiting time** setting can be increased from **4 seconds** set on default to a higher value. The **Release time limit** setting can also be changed. This setting represents a time window after which a signal is given that the OD is not closed. In case of bidirectional access control, the **Access direction** dropdown list is used. The **Direct** option represents entrance registration by the reader selected as an entry reader in the **Operating Device Settings** dialog box and exit registration by another reader. **The Reverse option** represents entrance and exit registration in the reverse direction.

If only one reader is used, the **Access direction** setting is unavailable.

If in doubt about changing settings, use system default settings for each particular operating device.

Configuration of FACU and FSSC features

The following features are part of the FACU and the FSSC: zones, alarm loops, outputs. Their functional settings are determined by means of the **Outputs, Loops, Zones** dialog window, opened by the **FACU Features** button of the **Controller** window:

.
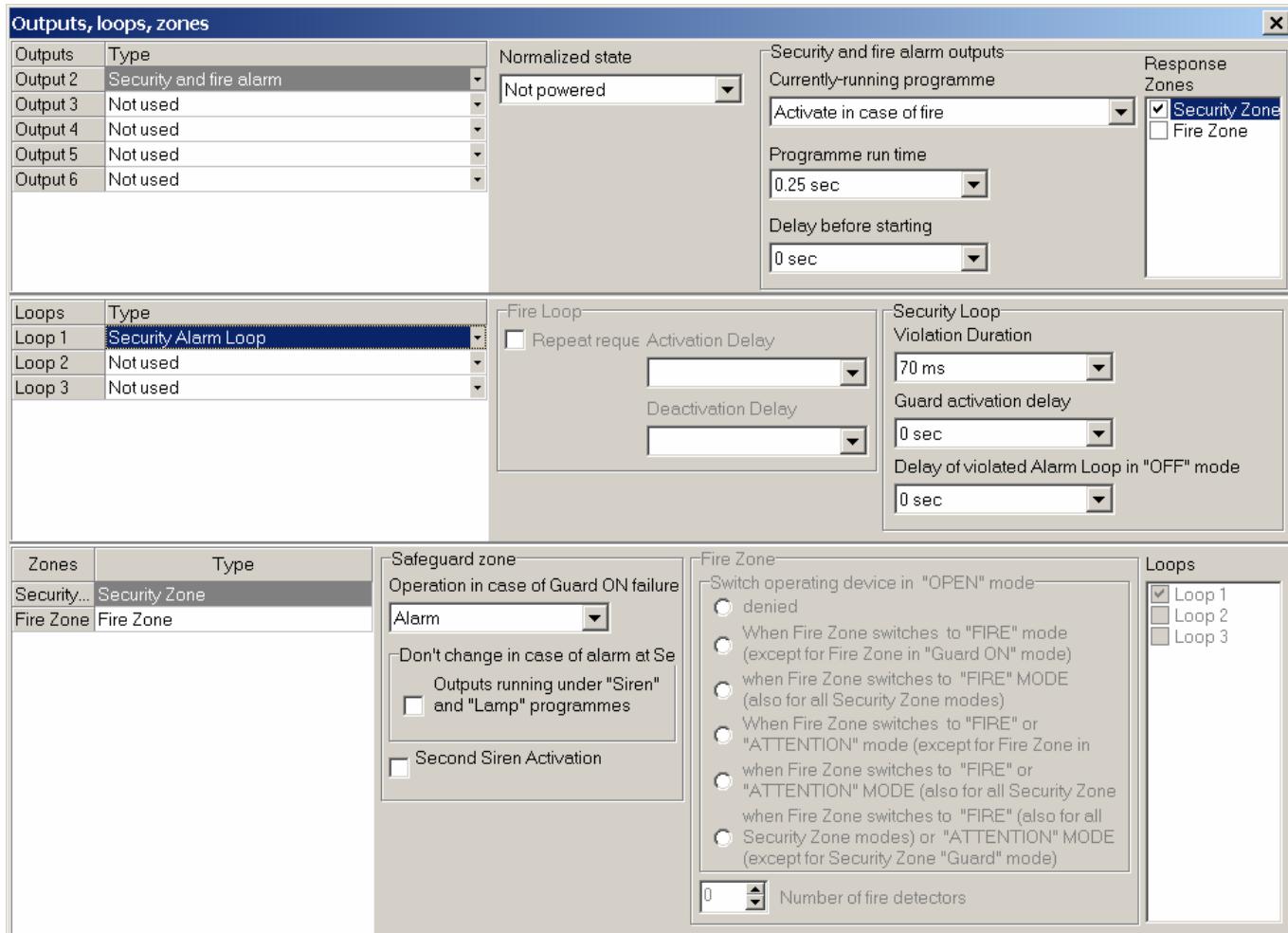
When a new the feature type is selected, its settings will appear on the right of the feature's list (Press the Enter key after selection of the feature type from the dropdown list).

The zones and loops can be related to either security or fire safety, with different settings combined under corresponding headings (**Fire** loop and **Security** loop, **Security** zone and **Fire** zone). Only settings of a selected component type can be changed.

For example, the Second Siren Activation setting is featured by both security and fire zones; therefore it is displayed in the zone list and can always be altered.

There are 2 fixed zones in the FSSC – one is always for security, another is always for fire safety. As a result, all the security loops are automatically placed into the security zone while all the fire loops are in the fire zone. For example, the Second Siren Activation setting is featured by both security and fire zones; therefore it is displayed in the zone list and can always be altered.

Thereby, for the FSSC the checkboxes to include the loops in the zones (the **Loops** list in the right part of the **Zones** toolbar) are disabled.

It is different for the FACU: any zone can be set as either security or fire zone. A certain loop can belong to only one zone. When the loop is included in one zone, it is automatically excluded from another zone.

The FACU has no operation device, so the "OD Switch to Open" setting makes no sense and the corresponding features are unavailable.

The operating device of the FSSC (a lock) is physically connected via the №1 Output, therefore it is absent from the list of outputs and the OD settings are determined in the same way as settings of lock and turnstile controllers (refer to the "Operating device settings" subsection).

Options of the CIU (Control and Indication Unit) operation can be changed with the **Options** button:

.
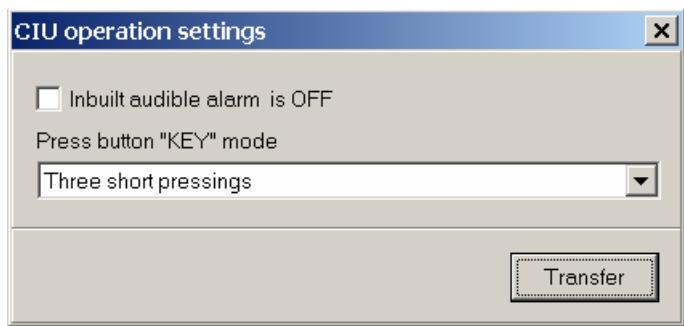
> **NOTE**
> When the CIU inbuilt audio indicator is deactivated, it will switch on only by ACS command.

The **Status** button can help know the FACU (the FSSC) operation settings as well as the status of its features:

Setting	Value
FIRE	No
ATTENTION (pre-ALARM)	No
Fire Zone blocking	No
ACS Alarm (alarm generator)	No
alarm - SFA	No
silent alarm - SFA	No
case is broken-in	Yes
PSU malfunction	No
switching to SPS	No
SPS battery discharge	No
ground leakage	No
connection with CIU	Yes
Buttons unblocking	No
sound deactivation by button	Yes
Access direction ACM	Control
OD status	Unlocked
Detector output №1 status	Standard
Detector output №2 status	Standard
OD status in SFA	
logic state	OFF
physical state	Standard
Zone 1	Security, Guard is OFF
Zone 2	Fire, Guard is OFF
Loop 1	SECURITY
logic state	Guard is OFF
physical state	Standard

The Reset button is assigned a function similar to the **CIU Reset** button's: deactivation of the «Fire», «Attention», «Alarm», «Malfunction».

For more information about the FACU, the FSSC settings and the CIU functional capabilities refer to the **"S-20 Fire alarm and security control units. Operation Manual"**.

Operating modes

The system provides 4 operating modes.

Open. When this mode is activated, the operating device (OD) is unlocked and remains unlocked all time that the operating mode is active. Pressing of the remote control panel (RC) button is ignored. When an authorized card is presented, the corresponding access event is registered by the ID number. Depending on the type of the reader, the indication comes as an LED arrow or green light.

Control. This operating mode is the standard mode of the system functioning. When this mode is activated, the OD gets locked and access is possible by only those cards that conform to all the access authorization criteria.

When an authorized card is presented to the reader, the OD becomes unlocked for the passage waiting time that is set in the **Configuration** section (refer to the subsection «*Operating device settings*» above). Depending on the type of the reader, the indication comes as an LED hand-with-card icon or a yellow light indicator.

Closed. This mode is used for denial of access through an operating device. When this mode is active, the OD gets locked and remains locked all the time that this mode is active. Pressing of the remote control panel (RC) button is ignored. Whatever card is presented, the system registers an event of an authorized access attempt. Depending on the type of the reader, the indication comes as an LED **STOP** sign or a red light indicator.

Conference. This mode is similar to the **Control** mode but with different indication. The yellow and green indicators are used to inform employees that a conference or a reception is being held at the premise and only authorized employees are allowed to enter. So when an authorized card is card is presented, the green light indicates that the access is allowed. When a card is not authorized for this conference, the red light indicates that the access is denied.

EVENTS

The **Events** section allows logging all events for all devices. Unlike the **Employees** and **Configuration** sections of the software, the **Events** section is rather informative than functional.

Events work window

Click on the **Events** tab to open the section work window:
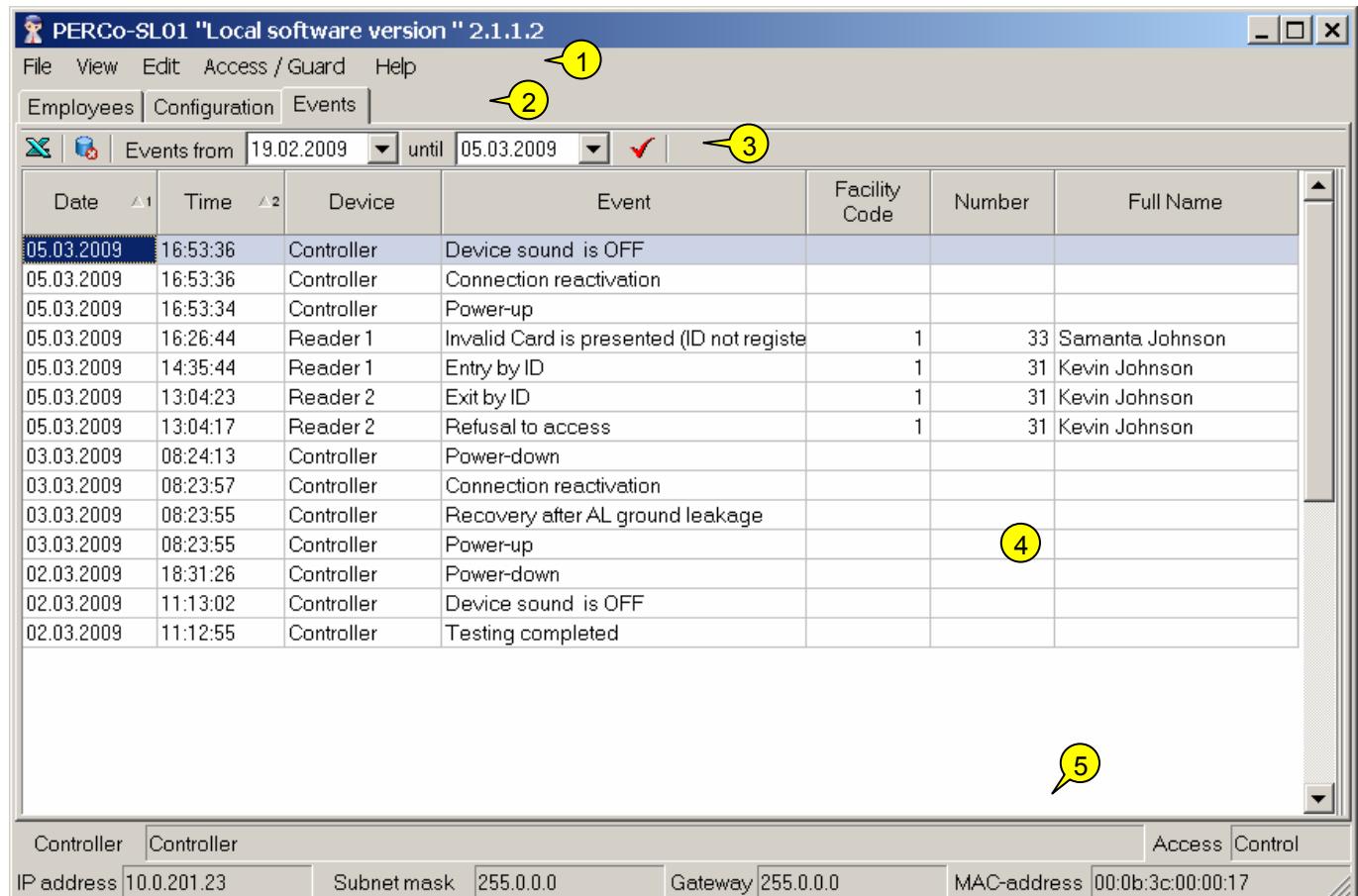
Fig.3. Events section work window

1. The top part of the window contains the Main menu. For the purpose of operating with the event log, the **File** menu is employed.

2. Tabs of the following sections are located under the Main menu:
Employees, **Configuration**, **Events**.

3. Functional elements of the window are described in the «*Appendix 2*». 2.

4. The central part of the window contains a **desktop**. The data are given as a table made of several columns. Such a tabular presentation conveniently allows sorting data by various attributes in descending or ascending order. In the above figure the events are sorted in reverse chronological order i.e. the last event on top. The column order can be easily changed by dragging.

5. The bottom of the work window contains a status line to display the service information (status of the controller, access mode, IP-address, etc.).

To sort the data:

1. Decide on the sorting attribute and click on the heading of the corresponding table column (e.g., **Event**).

2. A darken arrow pointing up (ascending sorting) or down (descending sorting) will appear on the right side of the active column:

Date	Time	Device	Event ▽
06.03.2009	09:40:05	Reader 1	Change of operating mode by Operator command ("Guard" mode)
03.03.2009	08:23:57	Controller	Connection reactivation
05.03.2009	16:53:36	Controller	Connection reactivation
06.03.2009	08:57:12	Controller	Connection reactivation
02.03.2009	11:13:02	Controller	Device sound is OFF
05.03.2009	16:53:36	Controller	Device sound is OFF
05.03.2009	14:35:44	Reader 1	Entry by ID
05.03.2009	13:04:23	Reader 2	Exit by ID
06.03.2009	09:40:05	Security Zone	FZ Guard activation by PC command

3. Click again on the column heading to swap the sorting direction:

Date	Time	Device	Event △
02.03.2009	11:12:55	Controller	Testing completed
06.03.2009	09:40:05	Security Zone	SZ Guard is ON by PC command
06.03.2009	09:40:05	Loop 1	SAL Guard is ON
05.03.2009	13:04:17	Reader 2	Refusal to access
03.03.2009	08:23:55	Controller	Recovery after AL ground leakage
06.03.2009	08:57:10	Controller	Recovery after AL ground leakage
05.03.2009	16:53:34	Controller	Power-up
03.03.2009	08:23:55	Controller	Power-up
06.03.2009	08:57:10	Controller	Power-up

4. To cancel the current sorting click again on the column heading.
Using the **Ctrl** key enable sorting of several columns at once. For this purpose hold the Ctrl key down and repeat the above steps for each column to be sorted. The sorting is completed after releasing the **Ctrl key**.

Event viewing time setting

The software enables viewing of events over a specified period of time. On default all events are automatically entered into the event log immediately after the software installation and until the present moment. To set an event viewing time value:

1. Enter the initial viewing date manually or by clicking on the left arrow of the date field in the event viewing time setting box **Events since … until…**, located above the list of the employees:

2. Choose the initial viewing date by the below calendar:
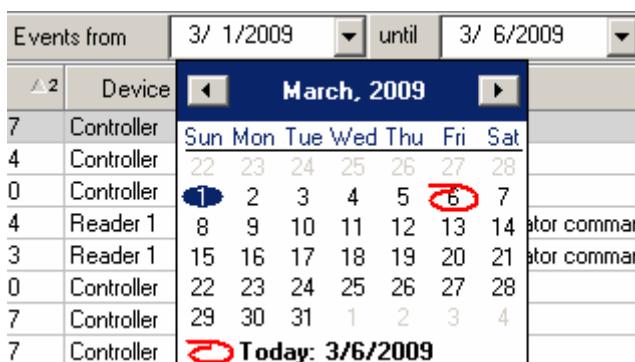
3. Repeat the procedure to set the final viewing date in the right date field. While on default, this field automatically shows the current date.

4. Use the Update Event List button for periodical updates of the list. This button is active only in the Event viewing mode.

The **Full Name** column is filled in with data from the database the moment of an event. Subsequent changes of the data (deletion, name or card number amendments) have no effect on past events. This enables maintaining the event history.

Event types

The **Events** tab displays events received only from the controller.

The types of events are displayed in the **Event** column and provide brief information on what happened at a certain moment. If the event is related to a concrete employee, the employee data is displayed in the **Facility code**, **ID number** and **Full Name** columns.

> **NOTE**
>
> For detailed technical information on the event types refer to the technical specification of the controller you use, subsections 4.3.4.1 - 4.3.4.2. Contact PERCo support service if you need assistance.

Event deletion

The event log size can be fast increasing. In order to delete outdated events:

1.Click on the **Delete Events** button. The **Enter Date Interval** dialog box will appear on the screen:
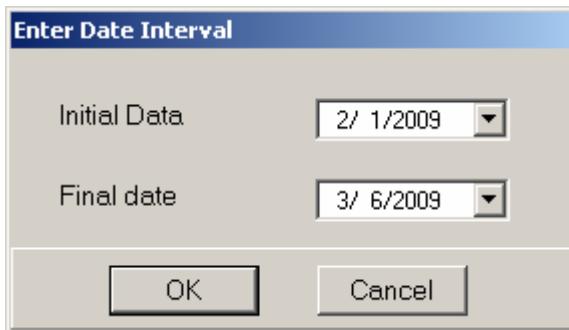
2. Set the initial and final dates of the interval manually or by means of the calendar that is opened by clicking on the arrow of the dropdown list:

3.Click on the «**OK**» button for confirmation**.**
Events over the specified time period will be deleted from the list.

NOTE
Events can also be deleted choosing in the menu
File → Delete Events… then determine date interval.

Event export

An event log for a specified time period (the whole time period on default) can be saved into a file of the following formats:
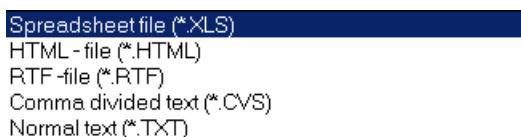
*.XLS — Excel document format (default setting);
*.HTML — WEB-page format;
*.RTF — Word document format;
*.CVS — Text document format;
*.TXT — Text document format.

For event exporting:

1. Set the event viewing time if necessary (refer to the «*Event viewing time setting*» above).

2. Click on the **Update Event List** button to to refresh the event list.

3. Click on the **Event** Export button. In the opened export window select the disc and folder, specify the file name and extension and click on the **Save** button:
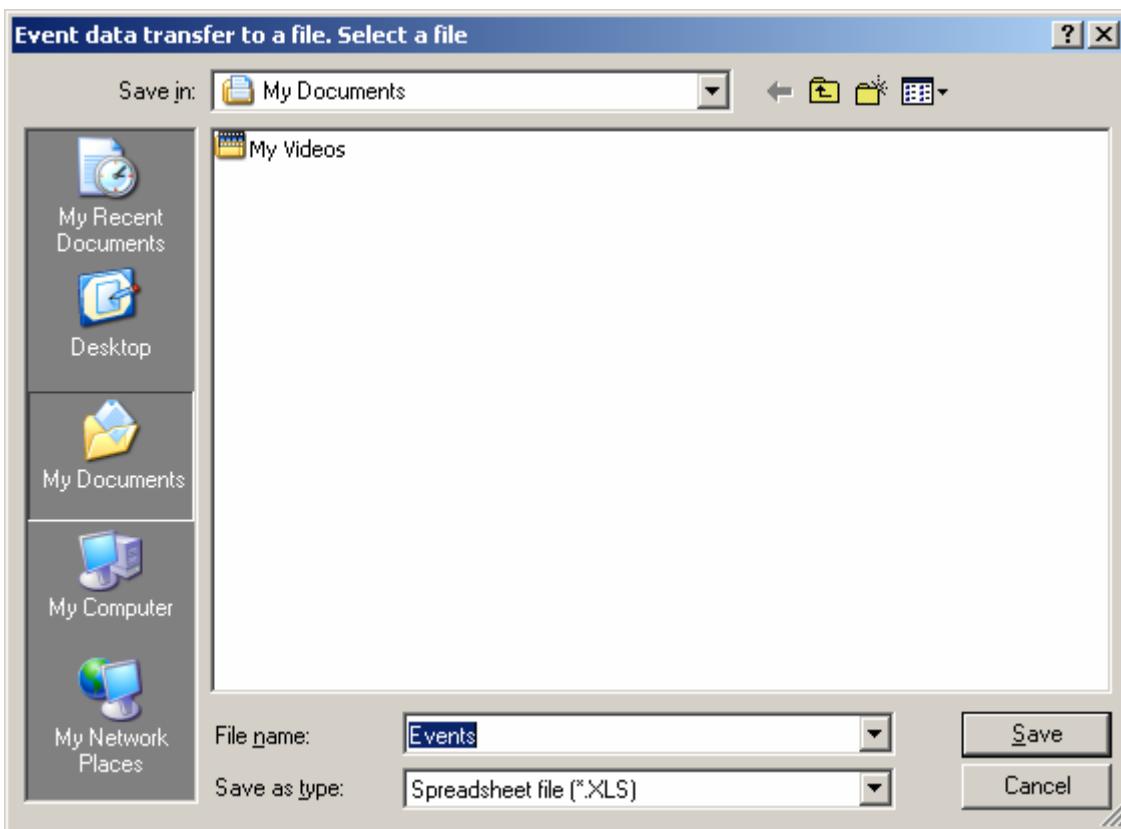
Events data will be exported into the specified file.

GUARD ACTIVATION KEYS (FACU ONLY)

This section is only for creating the list of Guard activation/deactivation keys for SFRCU zones.

The key can be an ID or a combination of digits from 1 to 8 (a PIN-code, from 4 to 8 digits in a key). Use of the keys eliminates unauthorized control over the zones status (before activation/deactivation of the zones guard with CIU, SFRCU awaits either ID presentation or PIN-code entering). The maximum allowed number of keys is 200. Each key has certain designated rights (only Guard activation, only Guard deactivation, only Guard activation/deactivation) and a selection of zones (and consequently, a selection of the related alarm loops) to operate by means of the key. The key can be tied with a random text, for example names of the employees authorized to use it. This text will be visible in the "Name" column (ref. section "EVENTS") for events connected to guard activation/deactivation by key.

To open the section click the **Guard activation keys** tab. The work window of the section will be as follows:
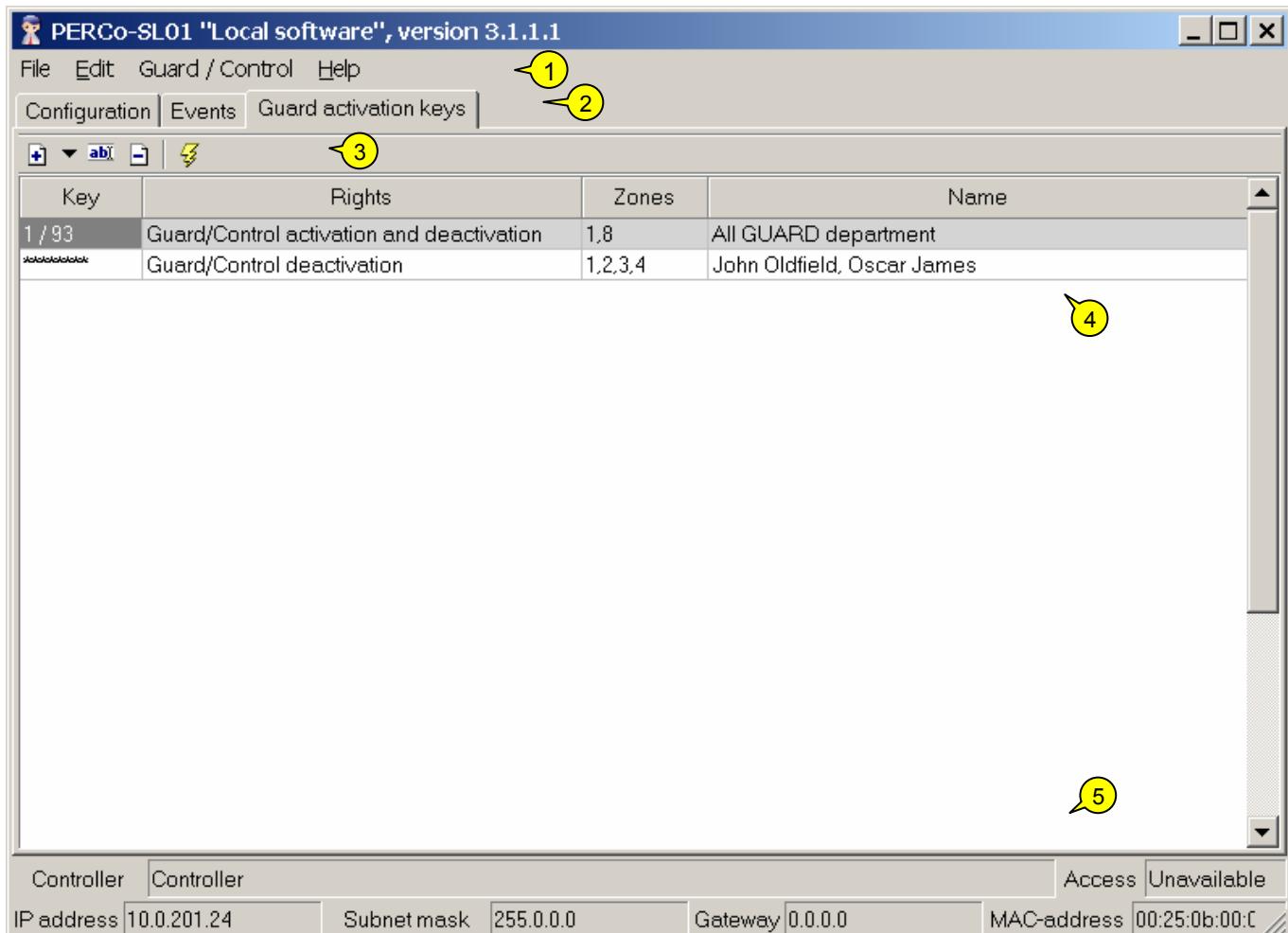
1. The top part of the work window contains the main menu.

2. Under the main menu the tab of the following sections are located: **Configuration**, **Events**, **Guard activation keys**.

3. Functional elements of the window are described in «*Appendix 3*».

4. The central part of the work window contains **the desktop** – the list of keys. The data is given as a table consisting of several columns with different functions. Such representation method allows sorting of the data by various criteria in descending or ascending order. When a key is added/ changed, a bar with the key's parameters will be visible at the bottom of the work window.

5. The lower part of the work window contains the status line, displaying the service information (the controller status, access mode, IP- address, etc.).

Adding a key

The key list is empty upon installation.

To add a key:

    1. Click on the arrow on the right of the ⊞ button (add a key). After that, a menu to select the key type will be highlighted:

2. Once the key type is selected, the bar to enter the key parameters will appear in the bottom part of the work window (the bar composition depends on the key type):

For a PIN-code key

For an ID key

The obligatory parameters are PIN-code (the facility code and the number for the identifying key) and selection of at least one zone. Once the parameters are determined, the "OK" saving the key in the data base becomes available.

The software checks the uniqueness of the key (inside ID's of the selected type), and shows the below window when a duplicate is being saved:

Change of a key

To change a key, click on the [ab] **Change** button. The bar with the key parameters will be visible, same as when a key is being. The type of the key cannot be changed here.

Deletion of a key

To delete a key from the list (from the data base):

1. Select any cell in the line with data of the key to be deleted and click on the **Delete** button — [🗔] .

2. Click the «**Yes**» button in the appearing dialog box

Transfer of keys into SFRCU

To transfer the keys list into SFRCU, click the [⚡] button.

The result of the transfer (successful or faulty transfer) will be displayed in the status line.

For detailed information on use of the key refer to the document **"S-20 Security and Fire safety Receiving and Control Units. Operation Manual".**

FINISHING OPERATION

To finish the operation and exit the the software:

1. Transfer all unsaved data to the controller.
2. Click on the Close button in the row of the heading

or perform the following sequence of commands **File →Exit**:
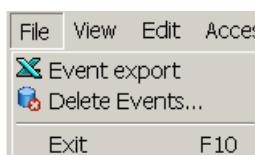
3.Click on the **Yes** button in the exit dialog box:
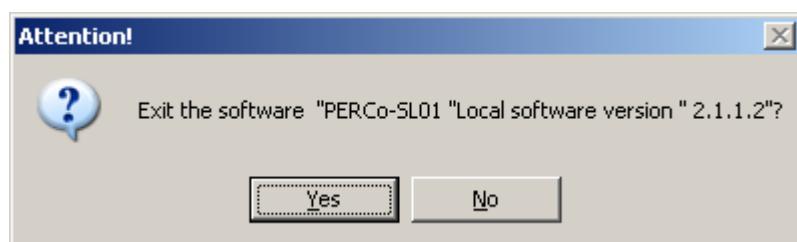
The software will be closed.

APPENDIX 1

The Employees section functional elements.

1 — **Add Employee**
2 — **Delete Employee**
3 — **Export employee**
4 — **Receive ID from Controller**
5 — **Delete ID from Controller**
6 — **Show Events**
7 — **Event Export** (e.g. in Excel)
8 — **Initial Event Viewing Date**
9 — **Final Event Viewing Date** (the current date on default)
10 — **Update Event List**
11 — **Transfer to Controller**

APPENDIX 2

The Events section functional elements.

1 — **Event Export** (e.g. in Excel)
2 — **Delete Events over a period**
3 **—** **Initial Event Viewing Date**
4 — **Final Event Viewing Date** (the current date on default)
5 — **Update the Event List**

APPENDIX 3

The FACU keys section functional elements.
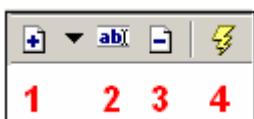
1 — **Add key**
2 — **Change key**
3 — **Delete key**
4 — **Transfer keys to the FACU**

PERCo Industrial

Tel.: +7 812 3216172, +7 812 3298924
Fax: +7 812 2923608

Legal address:
123-V ul. Leona Pozemskogo,
Pskov, 180600, Russia

e-mail: support@perco.ru

www.percoweb.com

PERCo

www.perco.ru