User Manual
TSE 5400 Software Light

Dear Customer,

Thank you very much for your decision for the TSE 5400 Software Light.

The configuration and administration of the complete locking system is based on the TSE 5400 Light software. Additionally, TRSE 6000 BURG-WÄCHTER safe electronics (safe systems) can be administered using the software version 4.1 with the USB adapter 2.1. The particularities, which should be taken into account when administering the safe electronics, are described in a separate chapter. Please read also the User Manual for TRSE 6000 in this respect.

In connection with this software, also the last 2400 events per cylinder, or the last 1000 events per safe electronics can be additionally read.

Using the TSE Software Light, you can administer up to 8 users and 15 locks.

The operation is based on a pin code and/or an E-Key.

Permanent radio communication between the cylinder and the software is not necessary.

A link between the USB adapter and the computer over the USB interface is necessary for data transmission. For data transmission, a maximum distance of 20m (typical value) should be provided. This value depends on the environment and thus can vary.
All data transmissions are bidirectional, this meaning from the E-Key to the lock or computer, from the keyboard to the lock and from the computer to the lock and vice versa. Communication of security-relevant data is AES-encrypted.

Table of contents

1 Installation in Windows XP, Windows Vista and Windows 7

Systems requirements: Windows XP, Windows Vista or Windows 7 in standard configuration, USB port.
Installation of drivers and software:
Insert the CD and the drivers and the software are installed automatically. Should this not be the case, the

Light.exe

shall be selected by a double-click in the Explorer and the Windows installation sequence executed.

In case the drivers are already present in your computer, they are recognized and the following window is displayed:

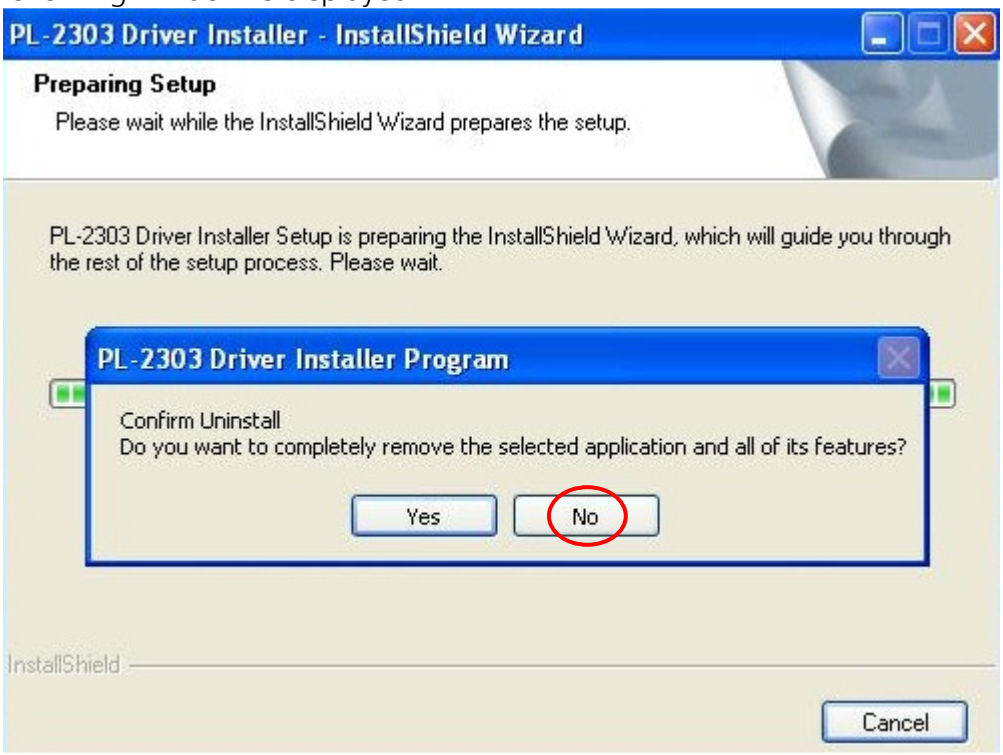

Abb. 1: Installation completed

Reject this prompt and follow the subsequent instructions. After a reboot of the computer, the USB adapter must be plugged to the USB port of the computer in order to be recognized by the system.

In case of problems with the drivers, they can be installed manually. You will find all the necessary drivers in the installation directory. For this purpose, execute the file

PL2303_Prolific_Driver_Installer.exe

and follow the instructions.

The installation has been completed. Now you can work with the program.

2 Programming of safe electronics

Besides administration of access doors, also safe electronics can be administered using the software. Different conditions apply to this administration, which are described in detail in this chapter or at the corresponding points in the software. **Please read also the User Manual for TRSE 6000 and TRSE 6000 FP in this respect.**

Attention: In case of administration of safe electronics using the software, the data must be stored on a removable data carrier. Their saving in a computer is not admissible and is not allowed by the system.

If the safe electronics data is administered using the software with the program not starting from a removable data carrier, the following error message is displayed:

Fig. 2: Prompt on removable data carrier

Start the program from a removable data carrier.

The system also identifies that the DAT folder is copied from the removable data carrier to the computer hard disk and denies the access.

The removable data carrier should be stored at a safe place (e.g. a safe) after the programming. Please note that the software links to the desktop or the Start menu do not exist any more after the copying to the removable data carrier, however, they can be created manually when required.

In order to enhance the protection against intrusion, the following points should be observed:

For locking systems with material code carriers, e.g. an E-Key:

- The code carrier should be consistently stored safely, so that it is accessible only to the authorized persons.

- In case of a loss of the code carrier, the lock should be immediately replaced or converted to a new combination by changing the coding, and/or the code of the lost code carrier should be blocked/deleted.

For locking systems requiring a code:

- No personal data (e.g. dates of birth) or other data, for which a link can be derived to the code owner, should be used for coding.

- If the code is stored in writing, such document should be consistently stored safely, so that it is accessible only to the authorized persons.

Attention: Any changes of the administrator code and of the user codes shall be made with the safe door opened.

When the locking system has been reset to another code, this new code should be repeatedly used with the safe door opened.

Please note that the number of users in the safe electronics is restricted to 9 pin code users and one administrator on account of the lock security class. Besides this, up to 299 E-Keys can be stored per unit.

In case you posses safe electronics with a fingerscan unit, up to 20 fingerscans can be additionally created. Presently, fingerscan data are stored into the safe electronics directly. When programming is done using the software, these fingerscans remain in the electronics, provided the control field *"Fingerscan data to be overwritten!"* is **not** checked (refer to Chapter Data transmission).

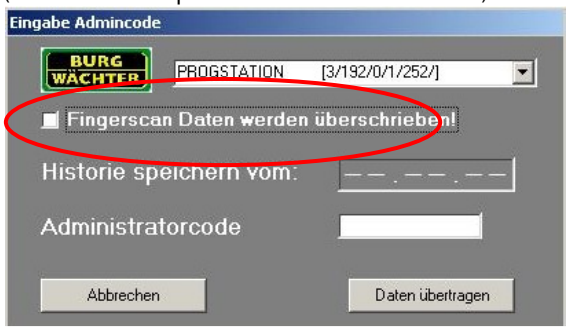

Fig. 3: Inquiry during programming

When programming fingerscan safe electronics, the following shall be born in mind:

- At least two opening codes shall be entered to open the safe using fingerprint; another opening code must be entered in addition to fingerscan. This can be either another fingerscan, but also a pin code or an additional E-Key.
- All the fingerscans are stored in the system with a value of ½. In order to acquire the authorization to open, a value of at least 1 must be achieved. A pin code for the opening must therefore be entered with a value of at least ½. A similar case is opening with an additional fingerscan (a total value of 1). Please read the corresponding chapter on setting the values (rights).
- For safe electronics versions V4.1 and **lower, the right FS+ must be selected in the rights management of the software.** This applies to pin code, as well as to **E-Key**.

Attention: For security reasons as related to programming using the software, it is not allowed to communicate all the opening codes to a single user in case three opening codes are used (value A fingerscan is ½, value B 1/3, value C 1/3).

Example:
User A has defined his finger in the system as opening code (its value is ½). This user can be still authorized in the system with an additional opening code with a value of 1/3. A user B now needs an additional opening code with a value of at least 1/3.

In data transmission, an error message is created when the number of users is exceeded. In such case, the assignment of users for safe electronics shall be adjusted in the user administration menu. **No data transmission is possible without such adjustment.**

3 Program start

The following window is displayed after the program is started.

Fig. 4: Start window

A green square in the bottom left screen area indicates that a valid USB adapter is connected to the computer, a red square means that either no USB adapter has been plugged or the drivers have not been installed appropriately. In case a yellow square is indicated, a USB adapter invalid for the particular software is plugged in (e.g. an adapter intended for the TSE Software System).
The system automatically recognizes whether a USB adapter applicable for the particular software is plugged.

All the settings can be made in the menu bar. They are described in detail in the subchapters.

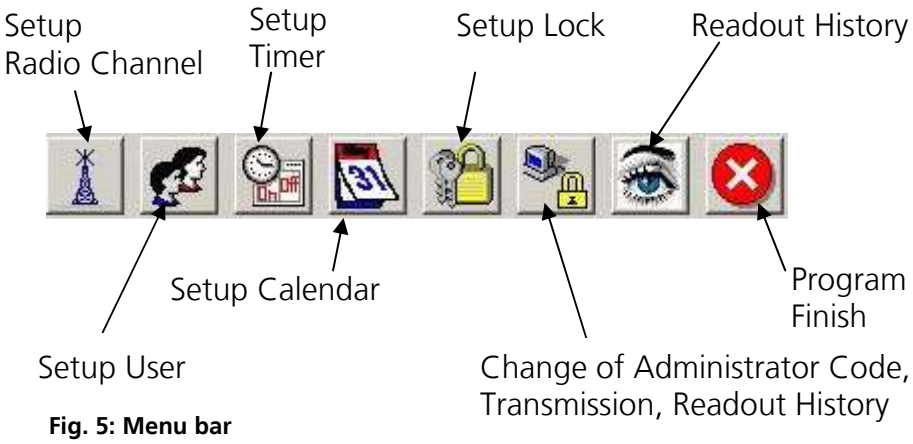

Fig. 5: Menu bar

The File menu allows you to set up the language and select the USB port. When the USB port setup is selected, a window opens, in which the port is indicated, to which the USB adapter is connected.
Automatic USB port identification is activated in the default state.

The specifications have to be saved.

Fig. 6: Adjustment of USB port

3.1 Setup Radio Channel

In this menu item the radio channel for data transmission is specified. This is of fundamental importance, as the radio channel selected here defines the channel setup of the executive unit.
The following window opens when the Setup Radio Channel menu item is selected:

Fig. 7: Selecting radio channel

Channel setup of the units can be made here. Channel 1 is always preset as a default value. If another channel is selected for data transmission, it is used automatically when data transmission takes place. Data transmission is executed in the newly defined channel. Attention: The new radio channel should be, if available, adjusted in advance using the keyboard. Also the E-Key must be adjusted to this radio channel (chapter Synchronizing E-Key).
For this purpose the menu item Admin Setup Radio Channel* shall be selected. The radio channel can be changed after entering the administrator code. **The radio channel indicated on the keyboard display must correspond to the channel selected in the software*. Otherwise data transmission is not possible.**

The radio channel selected in the *Setup Radio Channel* menu item will be used for all locks.

In any case, the default factory-set or the selected radio channel must be saved using the  icon.

In case other devices (e.g. W-LAN, Bluetooth, Bluetooth Headsets, etc.) interfere with wireless transmission, an radio channel should be adjusted as far as possible from the three channels.

*only if keyboards (Pin-code units) are placed

3.2 User administration

User administration can be accessed using the icon  on the start page. The individual users can be edited here.

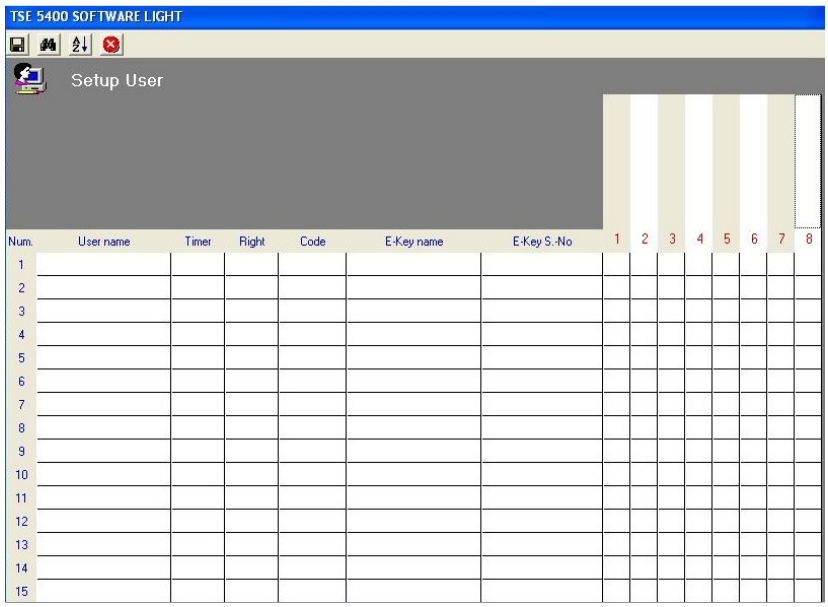

Fig. 8: User administration

Users can be created and configured in this menu item. For example particular rights and opening codes are assigned to a user. Besides this, an E-Key as the opening medium and timers for limited access can be allocated to the user.
The horizontal heading bar of the table is automatically filled with lock names of the doors, as soon as specifications are made in the *Setup Locks* menu item.
The following table provides information on the individual entry options, with detailed information in subchapters:

Selection fields	Entry/selection options
User name	Max. 16 characters long. After the name is typed in the timer and the rights are set, which can be changed afterwards. Special characters are not allowed. e.g. Walter Schmidt
Timer	- (no timer)
	A
	B
Right	1 Full individual access right
	1/2 Access only with an additional person
	1/3 Access only with two additional persons
	0 No access
	Admin Complete access and programming rights
	FS+ for safe electronics with fingerscan unit in certified mode
Opening code	6-digit numeric entry e.g.: 547896 or 6-digit character entry e.g.: Summer (this corresponds to the entry of 766637 on the keyboard)
Description	Identification of the E-Key max. 16 characters long e.g. Building door

E-Key Ser. No	Functions for the use of E-Key

Fig. 9: Entry options in user administration

When the configuration has been completed, the user record is stored in the system using the icon  .

For an easier work with door assignments it is possible to fill several fields at the same time using the cursor keys (e.g. for faster allocation of the individual doors). For this purpose, the mouse pointer must indicate the initial field (do not click). The required fields can be then marked using the *Shift* key and the arrow keys. The fields are then posted with *Enter*. If these fields are already filled, their deletion can be achieved in a similar way, in which case the function works inversely.
If a user should be completely deleted, this can be done by selecting the function *Delete* using the right mouse button over the corresponding *User name* field. Individual fields can be deleted by marking the corresponding field and applying the Delete function (right mouse button).

3.3 Setup Timer

Access times are defined here, which can be subsequently assigned to the users.
If no access times are assigned to a user (the field in the user administration remains empty), the user is authorized to access with no time restriction.

Using the Timers button you reach the *Setup Timer* menu item.

Fig. 10: Timer

Here you have a possibility to define two different timers A and B with four time windows each, which are repeated weekly. Timer A, timer B, or no timer at all can be then assigned to a user. If a user is assigned a timer, the lock is blocked for him outside the defined time window. An exception is the administrator, who always has permanent access.
By double clicking the corresponding field, either a popup window (Day column) opens, or you can enter values (columns Beginning and End).
Attention: If no time period is specified, the particular lock is open with no restriction for the assigned user.

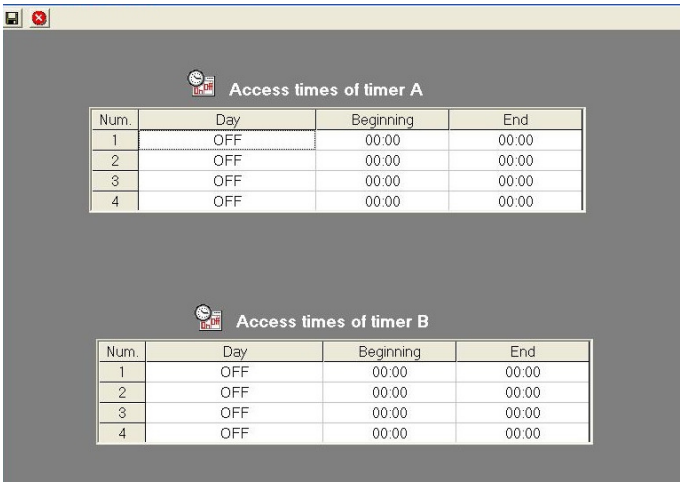

Fig. 11: Timers

The entries can be saved using the  icon.

3.4 Setup Calendar

Holidays and vacations are defined here. A single day or a period of time can be selected. Permanent, i.e. annually repeated, and individual, i.e. each year differing, holidays are distinguished.
You can call the calendar functions using the Calendar menu item.

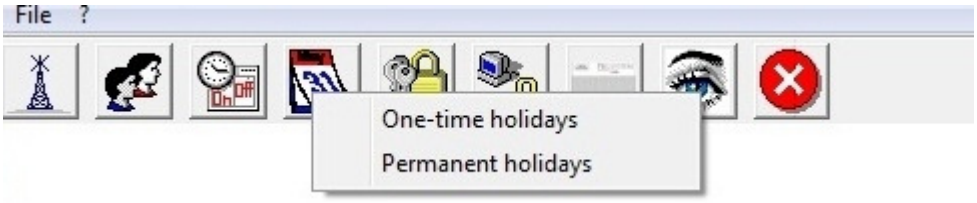

Fig. 12: Selecting holidays

During the programmed holidays/vacations, the lock is blocked for the users subject to a timer function.
This does not apply to all other users and for the administrator.

3.4.1 Calendar of permanent holidays and vacations

Permanent holidays are fixed to a certain date, such as New Year or Christmas. They are transferred to all subsequent years and do not need to be programmed again. You can enter your definition by double clicking the corresponding field.

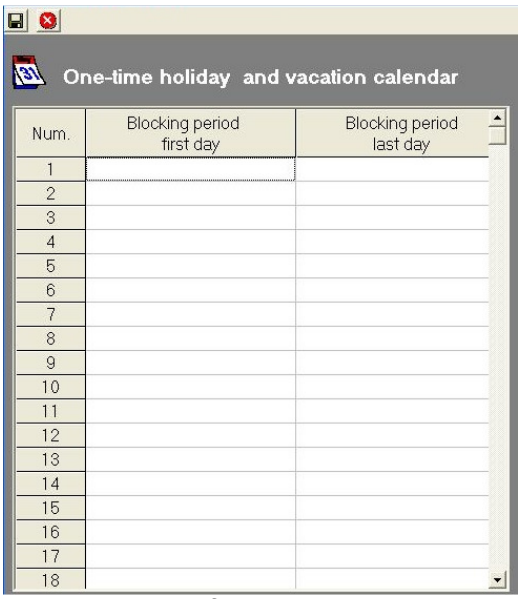

Fig. 13: Calendar of individual holidays and vacations

3.4.2 Calendar of holidays and vacations

This is a calendar with one-time holidays such as Easter or leave. This data is automatically deleted in the executive unit after expiry. You can enter your definition by double clicking the corresponding field.

Fig. 14: Calendar of permanent holidays and vacations

The entries can be saved using the  icon.

3.5 Access rights

The access rights are configured and assigned to the individual users in the *Setup User* menu. In the rights management, a total value of exactly 1 must be achieved for access authorization. From version 2.8 of the executive unit, the opening is allowed also in case the value of 1 is exceeded.

1	Full individual access right
1/2	Access only with an additional person
1/3	Access only with two additional persons
0	No access
Admin	Complete access and programming rights
FS+	for safe electronics with fingerscan unit version 1.0. This right is omitted for safe electronics versions 1.1 and higher.

Fig. 15: User rights

The right **FS+** shall be selected only for safe electronics version 1.0 in combination with fingerscan. With higher versions, the authorization to open for safe electronics with fingerscan is based on the authorization rights. The value of fingerscan is automatically set to ½ for safe electronics with fingerscan. The authorization to open is then reached thanks to a combination with an additional user with a similar half value or with two users with values of 1/3.

3.6 E-Key serial number

In the *Setup User* menu item, E-Keys can be stored, searched for, edited and described. It is also possible to synchronize newly an E-Key in case a change of the radio channel takes place.

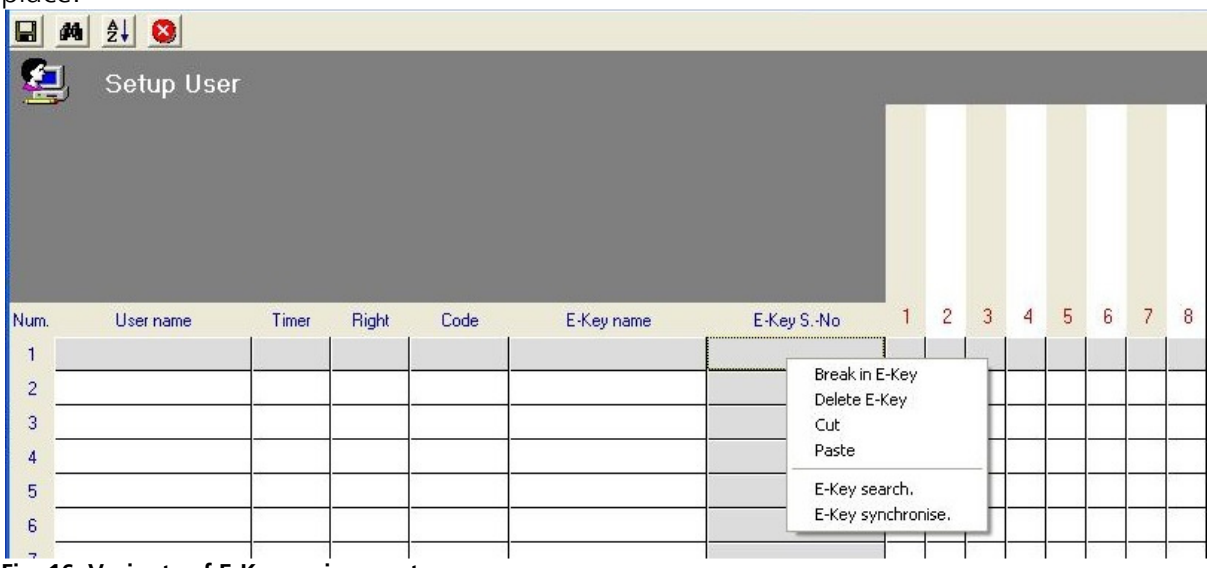

Fig. 16: Variants of E-Key assignment

The following individual options are available using the left mouse button, which are selectively discussed below:

- Break in E-Key
- Delete E-Key
- Cut
- Paste
- Search for E-Key
- Synchronize E-Key

Before storing an E-Key, the radio channel of the lock in the software must be specified. It must correspond to the keyboard radio channel.
It is necessary to take into account that an E-Key can be created always for a single user only.

From version 2.8 of the executive unit, also the E-Key is subject to the settings made under the menu item User administration with regard to access authorizations. If a user has the right ½ here, he is still not allowed to open with E-Key and code, although his total makes the right 1. He needs an additional user in order to open and thus achieve a right of at least 1.

3.6.1 Break in E-Key

When storing an E-Key, it is first necessary to identify, whether this is a unit without any prior E-Key assignment, or whether the E-Key is already in use and had been already assigned to a lock at least once.
If the E-Key has not been assigned to any unit yet, you have to press the button on the E-Key only once and the LED flashes three times briefly.
If an E-Key is to be assigned, which had already been assigned to a unit before, it shall be brought into the programming mode by pressing the button for approximately 10s. When this mode has been achieved, the LED on the E-Key flashes three times briefly.

To break in an E-Key, proceed as follows:

- Click the field *E-Key ser. No*, and a popup window opens
- Choose *Store E-Key*
- A window is displayed with an inquiry on blocking of the subsequent channel changes on the keyboard.

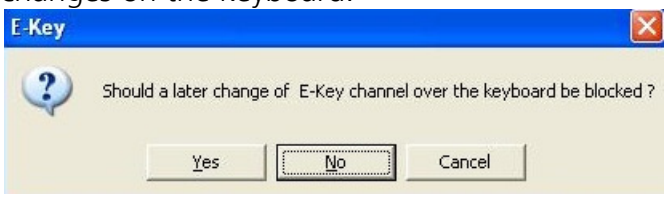

Fig. 17: Channel changes

- The following note is displayed in both cases:

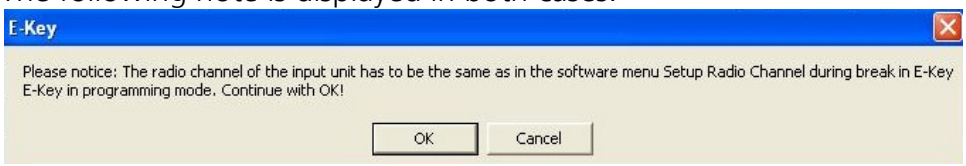

Fig. 18: Channel changes

- Decide on whether channel changes should be blocked or not.
- Bring the E-Key into the programming mode and start data retrieval by *ENTER*

The serial number is automatically displayed in the corresponding field.

3.6.2 Search for E-Key

To break in an E-Key, e.g. after it has been searched for, proceed as follows:

- Click the field *E-Key ser. No*, and a popup window opens
- Select E-Key search
- Bring the E-Key into the programming mode (by pressing the button on the E-Key for approximately 10s until the green LED flashes three times briefly) and start data retrieval by ENTER

The appropriate user is marked in the window.

3.6.3 Synchronize E-Key

In case the system radio channel has been changed in the course of programming, all the relevant E-Keys have to be adjusted to the newly active system radio channel, the E-Keys have to be synchronized. In order to indicate this also visually, the serial number of the E-Key in the Setup User window is displayed in red.
In this situation, the following steps shall be taken:

- Click the field *E-Key Serial. No*, and a popup window opens
- Select E-Key synchronize
- Bring the E-Key into the programming mode (by pressing the button on the E-Key for approximately 10s until the green LED flashes three times briefly) and start data retrieval by ENTER
- The color of the serial number changes from red to black and, besides that, a message is displayed that the adjustment was successful.

3.6.4 Additional E-Key functions

Using the three additional functions, E-Keys can be deleted and, for the purpose of a faster editing, cut from a user and, if required, newly assigned to another user.

3.7 Setup Locks

This menu item is intended for configuration of doors, in which the user sets should be read. Using the  icon, you can reach the *Adjustment locks* window.

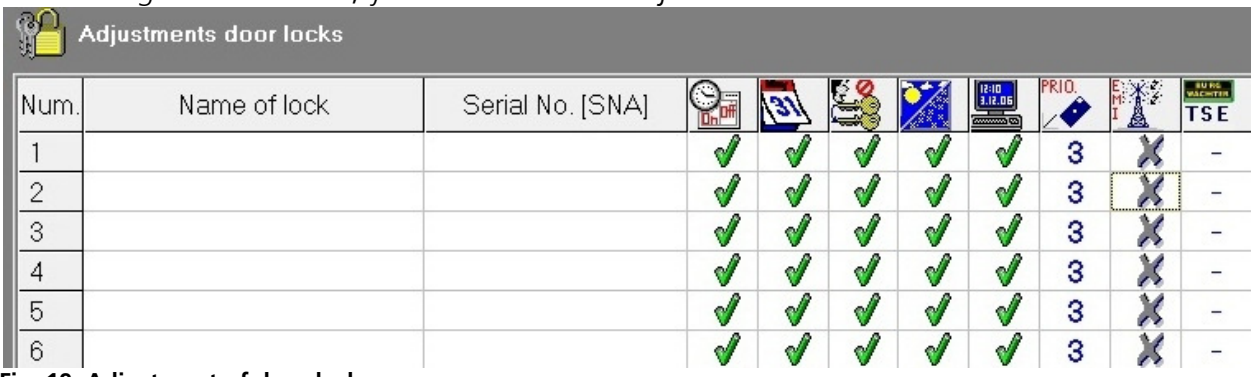

Fig. 19: Adjustment of door locks

The following selection options are available there:

Selection fields	Entry/selection options
Name of lock	Max. 10 characters long e.g. Building door
Serial number	Selection: manually or automatically

Timer adjustment; if deactivated, the lock is not subject to the data entered in the Timer adjustment window	Green check: active Red X: inactive
Calendar adjustment; if deactivated, the lock is not subject to the data entered in the Calendar adjustment window	Green check: active Red X: inactive
Automatic switchover from summer to winter time and vice versa	Green check: active Red X: inactive
Accept current time/date from PC	Green check: active Red X: inactive
Priority definition	Selection
EMI setup	Green check: active Red X: inactive
Burg-Wächter product type	Indication of the product type AWE executive unit - STE control unit

Fig. 20: Selections for adjustment of door locks

In the *Priority definition* selection field, you have an opportunity to influence the response characteristics of the lock when the E-Key is used.
If the appropriate door is not opened when the E-Key is used, you can increase the priority of this door or decrease the priority of the door opened incorrectly. The default value is 3, the highest priority is 5, the lowest 1.
An adjustment of this value is usually not necessary.

In case the system is located in an environment with a very strong electromagnetic interference (EMI), which can have a negative impact on the remote transmission intended for the lock, it can be better adjusted to this situation by activating the EMI field. The function is generally not active X and this should be generally never changed. In case the system is located in an environment with a very strong external electromagnetic activity, the function can be activated by clicking the appropriate field √.
If a grey cross is displayed in the field, the function cannot be activated. Activating of this function is possible from version 2.3 of the executive unit only.

When you use the options provided by the left mouse button in the field *Serial number*, you can choose between an automatic identification (*Storing executive unit*) and the manual entry of the serial number. Besides this, you can change the existing settings under the menu item *Configuration.*

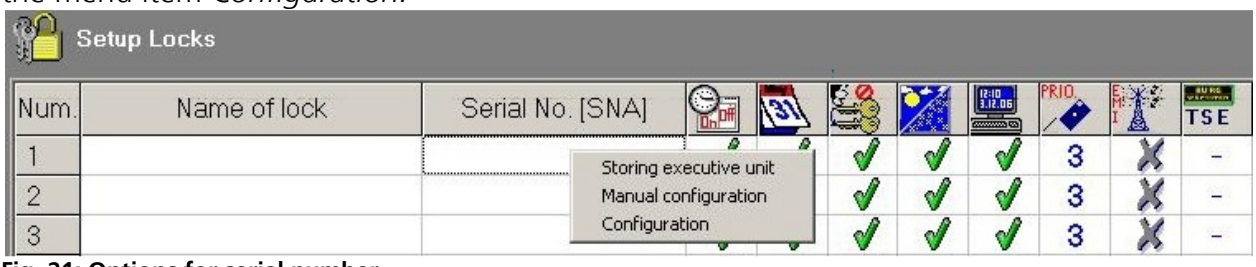

Fig. 21: Options for serial number

Please note the differences in storing safe electronics (programming of safe electronics).
The configuration must be made using a removable data carrier. If the software is not started from a removable data carrier, an error message is displayed when the serial number is being entered. The safe electronics cannot be stored. Copy the software on a removable data carrier and then enter the serial number again.

3.7.1 Storing executive unit

When *Storing executive unit* is used, the serial number is automatically identified. For this purpose, you have to prove your authorization by entering the administrator code.

Fig. 22: Entry of administrator code

In case several units are within the operating range, you can select the required ones. After entering the administrator code, the *Data transmission* button must be selected. Different procedures apply here depending on the version of the USB adapter. Older USB adapters break the search when a connection has been successfully found. New USB adapters from version 1.6 go through all the 12 frequency channels and indicate, for each RADIO channel, the unit with the strongest signal (RSSI). Also an automatic identification of the unit as executive or control unit is provided here. From this version on, automatic recognition is provided on whether an executive unit or the electronic TSE Wireless control unit was found (refer to the *Configuration* menu item).
This process is illustrated in the following figure:

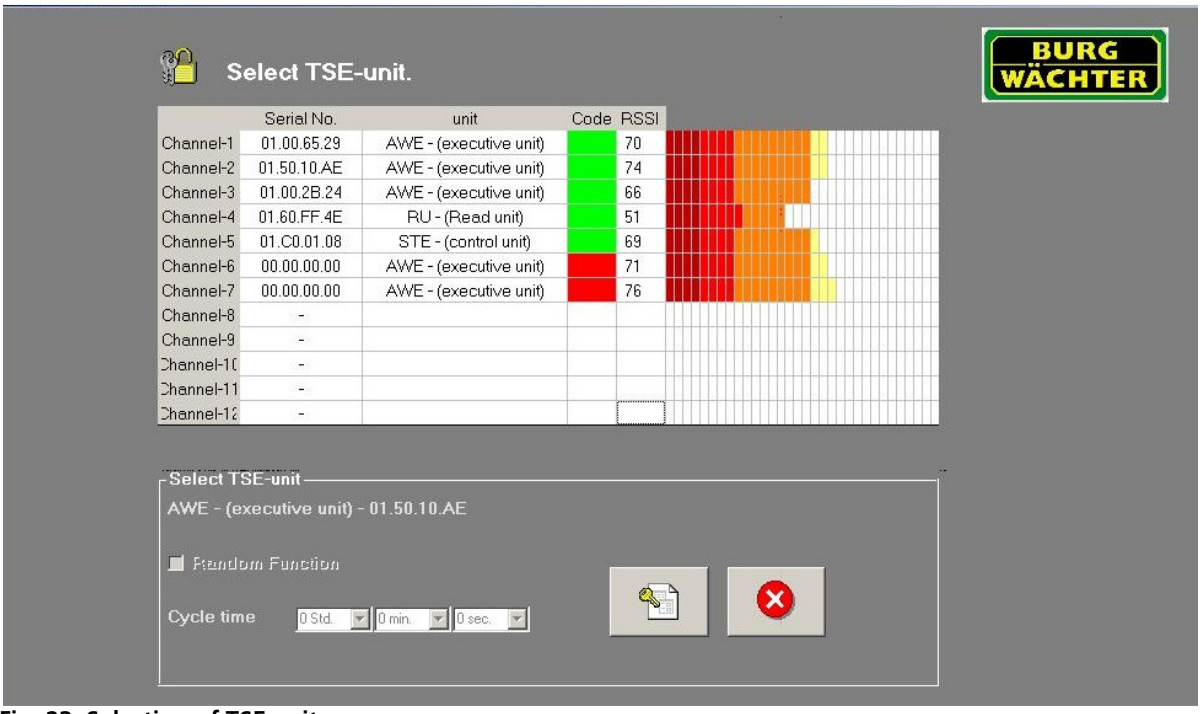

Fig. 23: Selection of TSE units

The radio channels are indicated in the left column.

This window shows all the units located within the operating range, disregarding the validity of the administrator code. In case the administrator code is not valid, an invalid number is displayed in the Serial number column (00:00:00:00).

If 2 units are superimposed on a **single** radio channel, the serial number is displayed with the highest signal strength (RSSI). This is then the unit that will be addressed when wireless transmission takes place. If a wrong unit is addressed, the USB adapter should be brought closer to the unit to be broken in. If this still does not lead to the desired result, remove the batteries from the wrongly responding unit temporarily during the breaking in process.

The *Code* column indicates the status of recognition of the administrator Code (green = password OK; red = password incorrect).

In this example, five units respond, out of which two have the appropriate administrator code.

Choose the desired unit and confirm it with  .

3.7.2 Manual entry

Manual configuration can be used if the serial number is known or if automatic storing is not successful.
The serial number (SNA) can be found either on a separate accompanying tag provided with the executive unit or on the display of the input unit under the *Info* menu item. Only the first two characters can be read without the administrator code.

3.7.3 Configuration

Under the *Configuration* menu item, the TSE unit can be defined as an executive unit or a control unit (TSE 6201 CONTROL), or an already existing assignment of the switching times or of the Random function can be changed. This looks as follows:

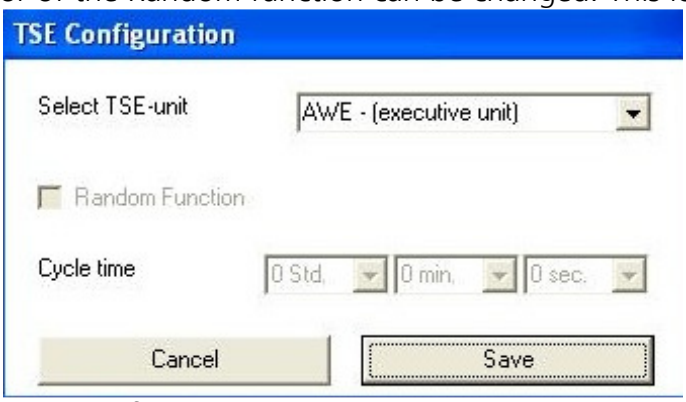

Fig. 24: Configuration

If a control unit should be configured, you can use the Random function (random control). The unit is then configured for the defined time in a random order.

Important: The unit to be programmed must be located in an immediately vicinity to the TSE Light adapter. All the other units to be programmed or already programmed must be clearly separated from there.

When new door locks are registered, please take care that all units are provided with new batteries.

The entries have to be saved.

3.8 Data transmission

The entire communication between the computer and the units is performed in the *Data transmission* menu item; beside this, also the administrator code can be changed and the history read here.
The entry of the administrator code is necessary for all data transmission functions. This code is factory-set to 123456.

Attention: Data transmission overwrites completely the existing data record. Any changes programmed manually in the lock will be overwritten!
An exception are the fingerprints stored in the safe electronics. They are not overwritten by programming!

If you have not read the history when programming, the events that occurred up to the moment of new programming are no more available.

When data is transmitted to the lock, the system inquires whether the history stored in the lock should be transferred to the PC and stored there.

An overview of all preconfigured locks can be viewed in the data transmission window, and its editing is no more possible here.

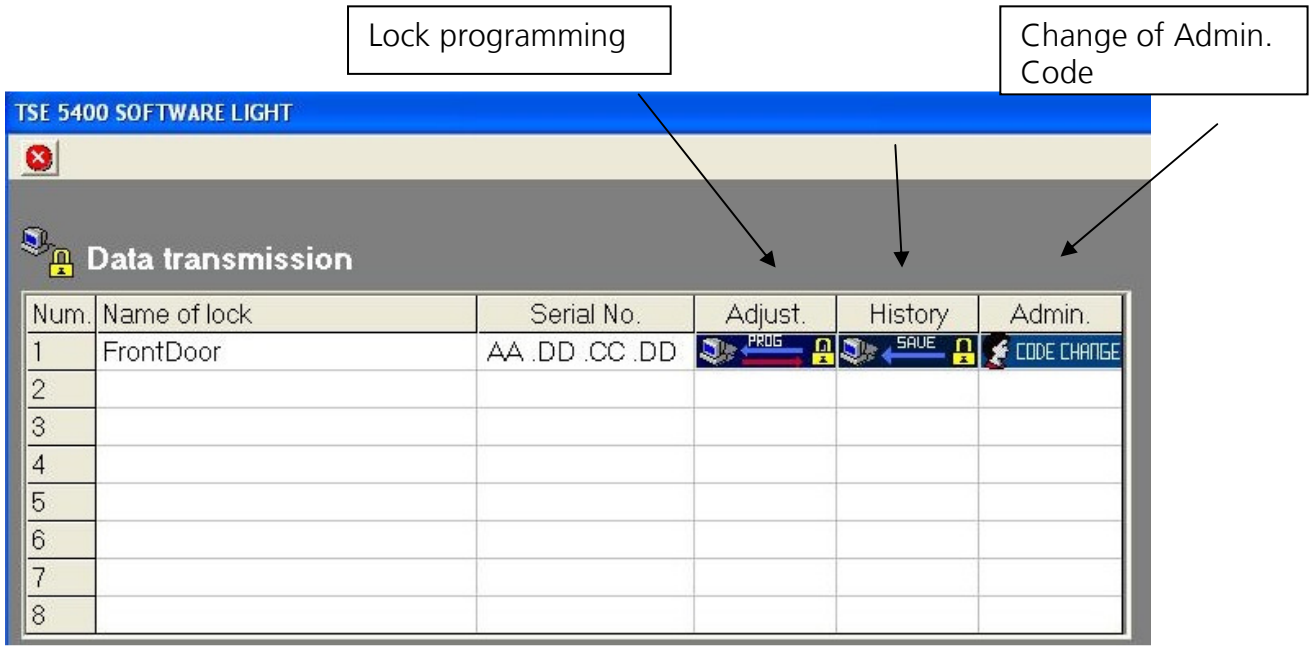

Fig. 25: Lock overview on data transmission

The software automatically verifies whether the number of the selected users is allowed with the corresponding ident medium for the particular lock. If it is exceeded, the number of users has to be correspondingly corrected in the *User administration* menu.

To program the locks, proceed as follows:

- Click the Prog. symbol in the *Setup* column
- Decide on whether the history should be read or not. If the history should be read out, the field *Save history from* is to be active and the date, from which the history should be stored, can be selected after a double click. If the history should not be

read out, the History field should be inactive.

- The following screen is displayed with the current date for the history (in case the storing of history was confirmed):

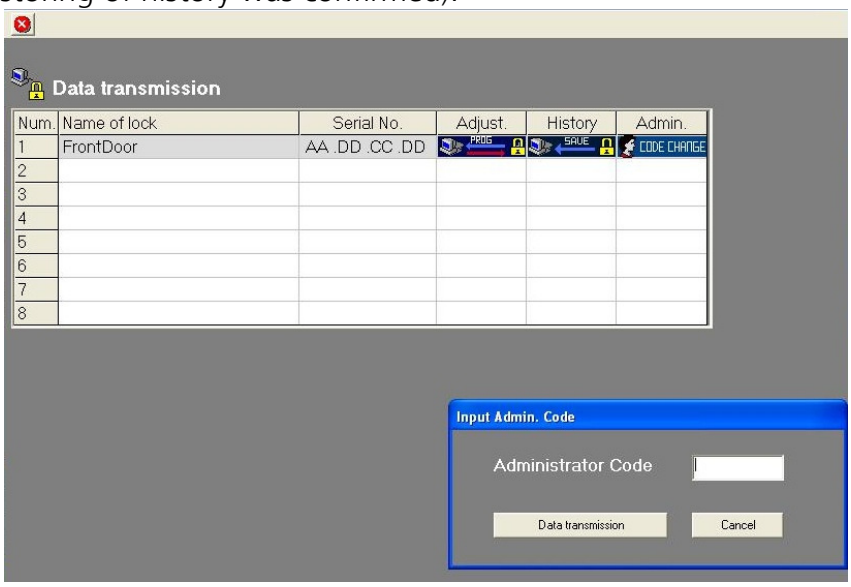

Fig. 26: Data transmission

- Enter the Administrator Code
- Click *Data transmission*

The history data is saved in the source path (installation path of the program).

3.8.1 History

In connection with this software, the last 2400 events per cylinder, or the last 1000 events per safe electronics can be read out.

The current history of a lock can be read out using the *Data transmission* menu item. All the data is then saved in the *Hist* folder of the source path (installation path of the program).

- Select the symbol 

- Enter the date, from which the history should be read out
- Enter the Administrator Code and click *Data transmission*

The history can be viewed also using the  button in the menu bar of the start window.

3.8.2 Changing the Administrator Code

Proceed as follows:

- Click the *Code Change* symbol

- A window appears, in which the old code and two times the new code have to be entered.

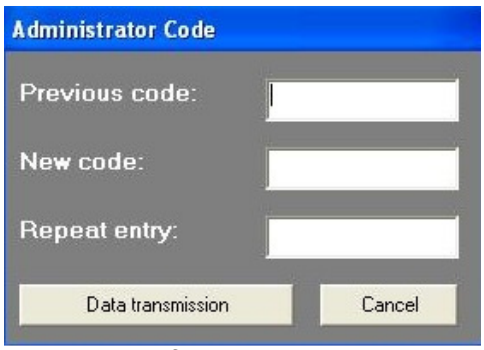

Fig. 27: Entry of administrator code

- Click *Data transmission*

Both when programming the lock and when reading out the history, the current battery status is displayed in the transmission window, from the moment it has been stored in the history.

4 Adjustments

Use *File => Setup USB port* to manually adjust the COM ports. However, this is necessary only in case the USB adapter is not automatically recognized by the system, which occurs only in exceptional cases.
You can identify, to which COM port of your PC the USB adapter is connected, under: Start => Adjustments => System management => System => Hardware => Device Manager => Connections.

The USB-COM port must be within a range of 1 to 15.