Content

Go to main-help ACL32

1 General

The scope of this documentation is to give the information to set up the intelligent door controller **XMP-K32** and **XMP-K32Lite** with the **small system ACL32**.

During operation certain parts of the **XMP-K32/K32lite** carry dangerous voltage. Because of that, the neglect of the safety references given in this documentation can have the consequence of heavy bodily injuries and material damages. Therefore, the installation as well as the start-up of the equipment should be reserved obviously for trained personnel.

2 Program versions

The documentation refers to the following program versions:

W3K32p	Version 2.1 (Jan 08.2006)
K32.bin	Version 2.9 , BD 20.02.2006

3 Setting up the door controllers XMP-K32 / K32lite with ACL32

A mouse click on the menu-button **K32-Parameters** of the system configuration opens the screen shown in Fig. 1.

The program consists of 6 menus located on the left side of the screen (***Parameters***, ***Attributes***, ***Time-Schedules***, ***Routines***, ***Alarming*** und ***LINUX-Parameters***.).
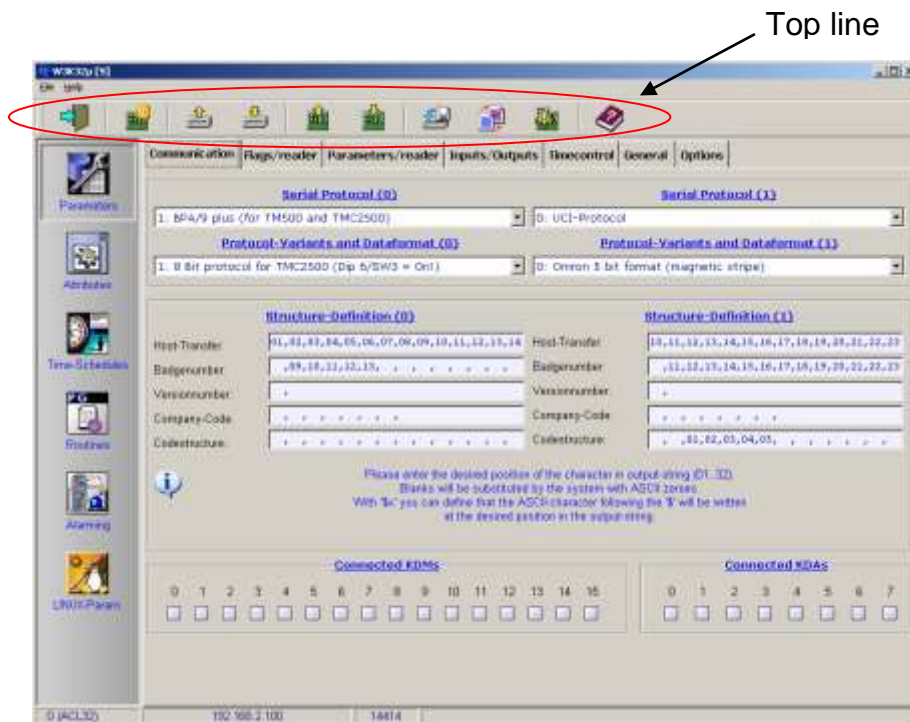
Top line

Fig. 1: Top line of the K32 parameters screen

Meaning of the topline-menu buttons:

	Exit program, go back to the system configuration
	Reboots the K32/K32lite. Cold- or warm-start can be chosen. A cold-start deletes all stored data into the door controller.(Reader, personal data, profiles) This makes only sense if generally new data has to be downloaded to the door controller.
	K32 data/ parameters will be load from a file on the central computer. One file is responsible for each door controller.

	K32 data/ parameters will be saved into a file on the central computer. One file is responsible for each door controller.
	Upload of data/ parameters from K32/ K32lite
	Download of data/ parameters into the K32/ K32lite
	Data/ parameters of another K32/ K32lite can be imported.
	The current data/ parameters will be overwritten by default values.
	A sub-menu with 4 utility functions opens.
Function 1	**Show dipswitches.** Several functionality of the door controller are activated by dipswitch. To get easy information about the actual settings the 4 dipswitches (SW1..SW4) of the K32/K32lite can be displayed
Function 2	**Download new firmware** The software of the door controller K32/K32lite will be extended continuous with new functions and readers. If needed new software can be downloaded into the door controller K32/K32lite.
Function 3	**Activating additional features** The controllers K32 or K32lite can be upgraded with special software-activation-codes. Depending to the type of controller a screen with activation possibilities appears. Activated features are displayed by a green hook. To activate a feature you receive a serial number depending 10-digit code from the manufacturer. Typing the code into the box and clicking the activation button the feature will be activated.
Function 4	**Display error log.** Normally the error log should not contain entries. However, if this should be the case, the content should be copied into a file (via clipboard) and to be send to our service hotline. This can be very meaningful for an error tracing.
	Opens the online help

3.1 Parameters

The first menu program *Parameters* consists of 7 registry cards where all attributes of the XMP-**K32/K32lite** and peripheral devices like connected card readers can be specified

Peripheral devices can by example be card readers, door contacts, extension modules (KDM16, KDA24), alarm contacts and so on.

Further on the communication protocols, data structures and timings must be set for the **XMP-K32/K32lite.**

The 7 registry card of the menu *Parameters* are described below.

3.1.1 The registry card C*ommunication*

Choice of card reader-protocol

Choice of badge structure

Activation of input extension modules

Activation of output extension modules
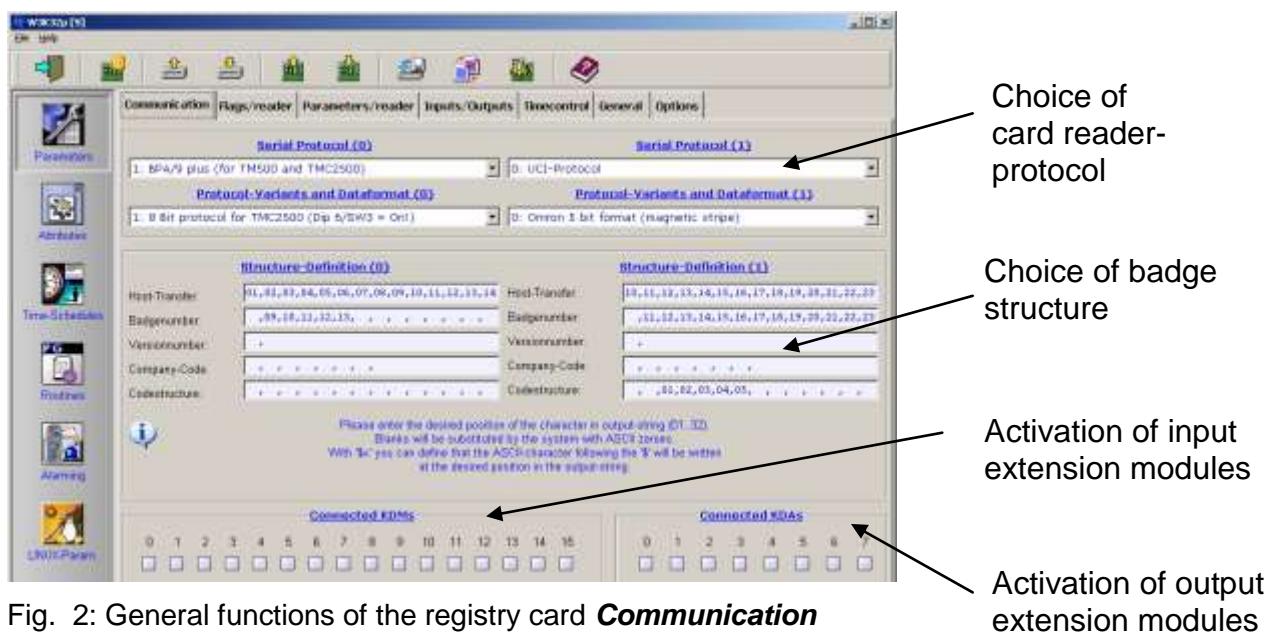
Fig. 2: General functions of the registry card *Communication*

In the registry card *Communication* the data transmission between **XMP-K32/K32lite** and connected card readers as well as the interpretation of badge data can be specified. The screen is divided vertically in two sides to specify two independent types of card readers and types of badges (0) and (1). The first step is to specify the reader protocol 'Serial Protocol' . Afterwards the data type of the selected card reader can be chosen 'Protocol-Variants and Data format'. Information about specific values is given in the datasheets of each card reader type.

Hint
Protocols and data formats will be extended continuously. Depending on the software revision different choices are possible.

The transmitted badge information are defined by the 'Structure- Definition'.   The card reader transmits maximum 32 digits to the door controller. These digits can consist of badge number, revision number, company code and pin-code. The position and type of the digits is described below.

Host-Transfer:

The XMP-K32 always transmits 14 characters to the computer.
The sequence of the 14 characters which are transmitted to the master computer is defined here as a selection from the maximum 32 characters [01..32] received from the reader.

Example: (01,02,03,04,05,06,07,08,09,10,11,12,13,14)

Blanks (empty fields) are replaced by ASCII zeros from the system.
An input of the form '$x' (x = ASCII character) causes the appearance of the ASCII character that follows after the $ character at the appropriate position of the output string.

Badge number:
By entering data positions into these fields (assuming from the data positions transmitted by the reader) the sequence of the card identification number for offline mode is defined here.
Attention: Card reader data is always transmitted by 14 digits, not defined digits are filled with zero automatically.

Version number:
By entering data positions into these two fields (assuming from the data positions transmitted by the reader) a version number can be defined.

Company-Code:
By entering data positions into these fields (assuming from the data positions transmitted by the reader) the sequence of a company code for the online and offline mode is defined.

Code structure:
By entering the pin code data positions into these fields (assuming from the pin code data positions transmitted by the reader) the sequence for the pin code evaluation is defined for the system.

In the bottom area of the window additional input-output modules can be activated. These extension modules KDM16 or XMP-KDA24 are connectable to the second serial interface of the **XMP-K32/K32lite**. A hook in the box activates the selected extension module with the corresponding hardware address (Dipswitch setting on the module).

3.1.2 The registry card *Flags/reader*

In the registry card *flags/readers* the **XMP-K32/K32lite** gets information about general and special functional properties of the up to 8 connected card readers.
The standard delivery of the K32/K32lite allows the connection of up to 4 readers to the controller. To connect more readers the door controller must be upgraded by the '8-reader' Software-extension. It is recommended to use also the 8-reader connection terminal with integrated power supply.
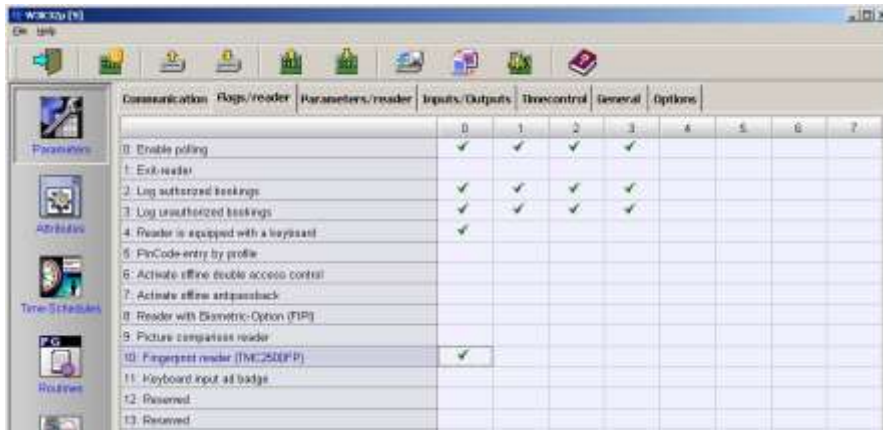
Fig. 3: Registry card *Flags / reader*

Meaning of the input fields of the registry card *Flags / reader*

0: Enable polling	Setting the flag activates the polling to the reader after the next K32 parameter download. **The flag should be set only, if the reader with the appropriate address is actually connected to the XMP-K32.**
1: Exit-reader	Setting of this flag defines the inside reader of a reader pair for Antipas back operation (reader 1 and reader 2, reader 3 and reader 4). **The first ('even') reader of such a pair always must be set as exit or inside reader.** In this situation two readers influence the same door control periphery (door opener, door contacts). For this reason only the data points for the outside reader is set. Furthermore the settings for the room balancing must be executed (e.g. (from 1 to 2) and (from 2 to 1) or (from 3 to 4) and (from 4 to 3)).
2: Log authorized bookings	Authorized bookings at this card reader are stored into the XMP-K32.
3: Log unauthorized bookings	Unauthorized bookings at this card reader are stored into the XMP-K32 (in offline mode).

4:	Reader is equipped with a keyboard	The connected card reader is equipped with a keyboard for pin code input.
5:	Pin Code-entry by profile	A pin code input at this card reader is only then required if the appropriate profile is defined so. This option does not work with all reader types!
6:	Activate offline double access control	The double access control in offline mode is activated for this reader. The time for this double access control is specified in the registry card *General* in the field ,*Number of seconds for double access control'*.
7:	Activate offline Antipas back	The Antipas back is activated on the selected K32/K32lite
8:	Reader with Biometric-Option (FIPI)	Not used with ACL32.
9:	Picture comparison reader	Not used with ACL32.
10:	Fingerprint reader (TMC2500-FP)	This is a biometric fingerprint reader

3.1.3 The registry card *Parameters/r*eaders

In the registry card ***Parameters/readers*** the following settings for the card readers and the periphery connected to the **XMP-K32** are made:

- definition of the control and supervision times for relay outputs and analog inputs, respectively, for the door control;
- activation of the functions for relay outputs and analog inputs;
- definition of a default identifier (SA/SAM) for the appropriate card reader;
- setting of room numbers;
- definition of the structure type for the identification number, the serial interface and the protocol or the data format (according to the definitions in the registry card ***Communication***).

Fig. 4: Registry card ***Parameters /reader***

Meaning of the input fields of the registry card *Parameters/ reader*

Maximum door open time:	The maximum door open time in seconds is specified here. This is the maximum time, which may pass between opening and closing the door, before an alarm will be released.
Reserved time 1:	Reserved time. Not used at the moment.
Pass through timeout:	This is the maximum time interval, which may pass between bookings and pass through (activation or release of the pass through contact). During this time the reader is blocked and on the reader display the message 'Terminal blocked' will appear.
Reserved time 2:	Reserved time. Not used at the moment.
On-time for door opener:	The maximum effective period (on-time) for the first door relay of the respective card reader is entered here.
On-time for alarm-relay:	The maximum effective period (on-time) for the second relay is entered here, if this is set as alarm output (function of the relay output 1 = 2). Otherwise the max. door opening time is valid.
Function of analog input 0:	0: Disabled 1: Doorframe contact active 2: Reader handles doorframe contact By this reader (with BPA/9 protocol) the door supervision is controlled externally. This function is important for integration of older reader installations on basis of BPA/9 protocol and integrated door supervision. The door supervision and/or door control is carried out directly by the reader here. The alarms resulting from it are registered and processed by the **XMP-K32** as if it would concern supervision and control contacts of the **XMP-K32** itself. **Important: With this function no supervision times may be activated.**
Function of analog input 1:	0: Disabled 1: Pushbutton connected (For opening with alarm bridging) 2: Handle contact connected
Function of analog input 2:	0: Disabled 1: Pass through contact active
Function of analog input 3:	0: Disabled 1: Reader blocking input active 2: Pass through reset contact
Function of analog output 0:	0: Disabled **Note:** For the parameter setting of an Antipas back system the inside reader should be an 'even reader' (address 0, 2, 4 or 6) and the outside reader an 'odd reader' (address 1, 3, 5, 7). If the readers 0 and 1 work as Antipas back reader pair, the function for the relay output of reader 0 should be set on '0' and for reader 1 this function should be set on '1'. By this constellation an authorized booking at reader 0 as well as at reader 1 activates the same door opener relay (BO2). 1: Door striker active 2: Door striker is reset when door opens (according to VDS)

Function of analog output 1:	0: Disabled 1: ON while door opening is allowed (external alarm system is bridged) 2: Alarm output (badge related alarms, e.g. *Badge not valid*) with → **on-time of alarm relay.**
Default-Identifier (SA/SAM):	Each reader can get its own default identifier (e.g. **A0** = access**, B1** = coming, **B2** = going**)** by entering this identifier into this field. After a booking this identifier (together with the card information) is send to the control system. If this field remains free, then the identifier of the reader (e.g. TMC2503) is send. The card readers identifier is determined, e.g. on basis of a key action at the reader (***coming*** or ***going***). With readers, which do not sent an own identifier (e.g. TMC450N) the identifier type A0 will be send to the control system automatically.
From room: **To room:**	Virtual room numbers can be entered here. These numbers are used for Antipas back in offline mode (also global!). Values from 0 to 254 are allowed. A special case is the room number –1, which marks an 'undefined' room. If a person is in room –1 the 'anti pass back' is deactivated temporarily, i.e. the person can go into every other room. After restarting the K32, first, all persons are set as are being in room –1 (to prevent problems). It is recommended, however, not necessary absolutely, to use the same room numbers for the control system and for the K32. With very large system with more than 255 rooms, of course, this is no longer possible. The assignment of the room names is realized in the menu option **Rooms** (W3ROOM.EXE) of the parameter set for the door control units. **The Antipas back option is only possible with a inside/outside reader pair.**
Structure-Definition (0 or 1)	The code number (0 or 1) for the structure definition of the card reader must be entered here (see registry card **Communication**).
Serial protocol (0 or 1)	The code number (0 or 1) for the serial protocol of the card reader must be entered here (see registry card **Communication**).
Protocol-Variant / Data format (0 or 1)	The code number (0 or 1) for the protocol variant and/or the data format of the card reader must be entered here (see registry card **Communication**).

3.1.4 The registry card *Inputs/Outputs*

In this registry card the assignment of the inputs and outputs of the door control unit to the appropriate card reader takes place.
Here can be selected between standard configuration and a free definable configuration.
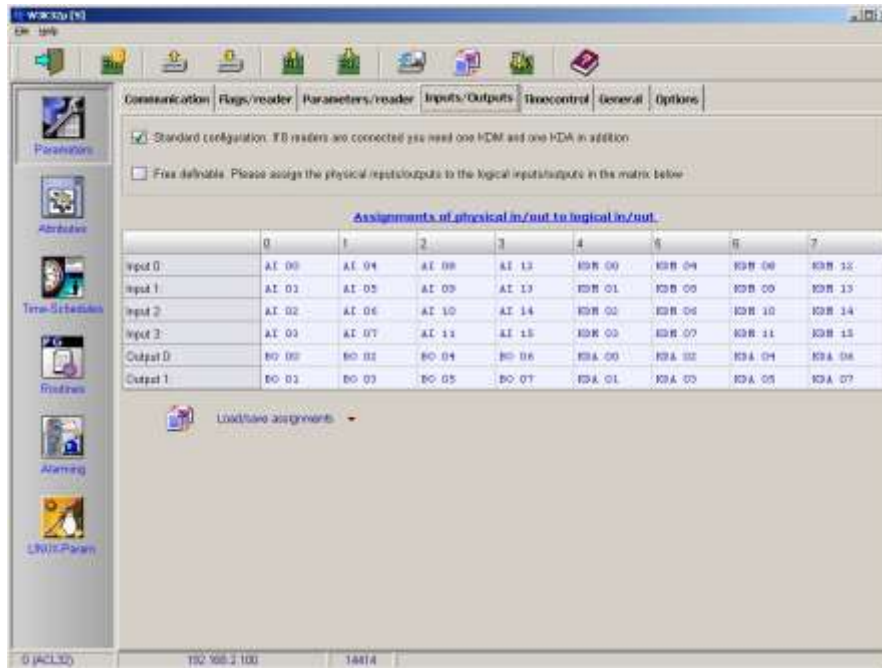
Fig. 5: Registry card *Inputs/Outputs*

Standard configuration:
In case of 8 reader operation a KDM16 and a KDA24 (both with the hardware address 0) are needed in order to reach the necessary number of inputs and outputs.

Free definable:
By selecting this option it is possible to assign outputs and inputs for the reader on individual way. To do this the operator can use the scroll down menus in the matrix.

Load/save assignments
With this selection menu it is possible to load or save frequently realized standard and own input/output configurations.

3.1.4.1 The registry card *Time control*

Into registry card **Time control** special settings valid for offline operation can be made. The settings, which are made in these input fields, mainly are meaningful for **Time Recording**.
Into the registry card an overview of all offline-available identifier types is represented. These identifiers are linked by activation of the appropriate field ✓ with a defined property or by an entry of a characteristic number into the field *Display format (0..10)* with a certain display format on the reader display.
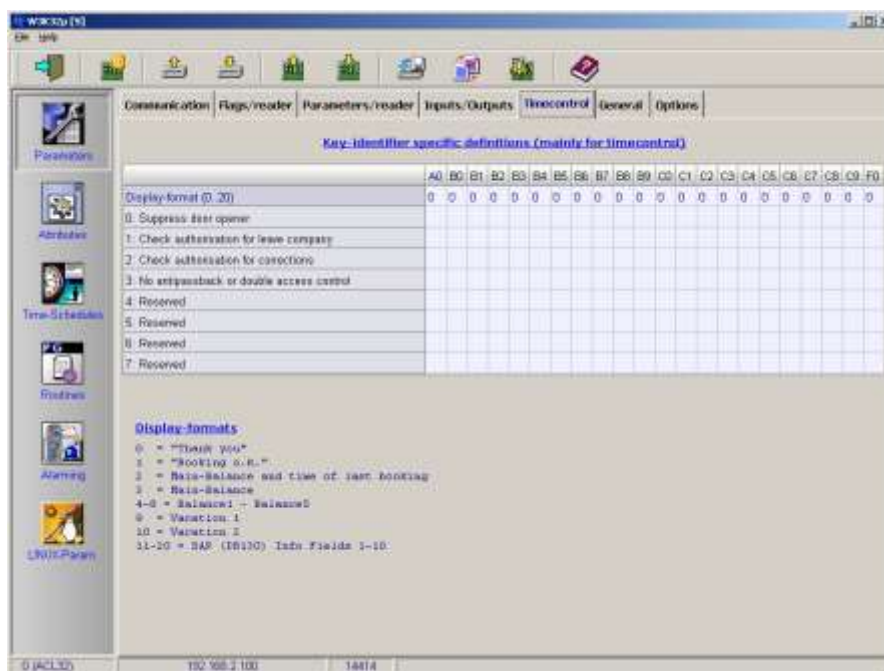

Fig. 6: Registry card **Time control**

Meaning of the input fields of the registry card *Time control*

Display-formats (0..10)	The entry of a code number into the appropriate field specifies the display format for the reader coupled with the identifier. The code numbers correspond to the following display formats: 0 = 'Thank you' 1 = 'Booking o.k.' 2 = Main-Balance and time of last booking 3 = Main-Balance 4 = Balance 1 5 = Balance 2 6 = Balance 3 7 = Balance 4 8 = Balance 5 9 = Vacation 1 10 = Vacation 2
0: Suppress door opener	Setting this flag suppresses the door opening in connection with this identifier. This is often used in connection with inquiry functions (B0 key).
1: Check authorization for leave company	With setting this flag in connection with this identifier the system checks if business errand is allowed.
2: Check authorization for corrections	With setting this flag in connection with this identifier the system checks if there is the authorization for corrections.
3: No Antipas back or double access control	With setting this flag in connection with this identifier the Antipas back and double access control will be suppressed.

3.1.5 The registry card *General*

In the registry card *General* the following definitions are made:
- definitions for the check of the company code,
- definitions for the multi-host-operation with the XMP-K32, not used in ACL32
- definitions for the code offset for BPA9 readers and
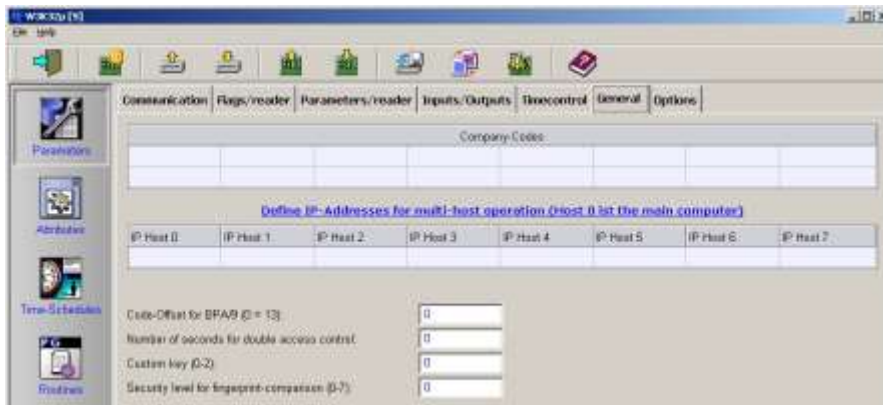- the time definition for double access control (offline).

Fig. 7: Registry card *General*

Meaning of the input fields of the registry card *General*

Company-Codes:	The company code is a customer specific code consisting of a defined character sequence. The positions on the badge where this code is read must be registered into the registry card *Communication* in the field Company-*Code*. The company code is always checked on the **XMP-K32**. Up to 16 different company codes can be defined.
Define IP-Addresses for multi-host operation (Host 0 is the main computer) (Attention: only possible for XMP-K32 and BABYLON!)	In the multiple host operation a **XMP-K32** is used by several control systems with several sets of personnel master data. The appropriate assignments of the feedbacks (bookings, alarms) to the respective BABYLON control system is realized in the **XMP-K32**. The master computer 0 (host 0) has a special position. On host 0 the reader parameters and periphery definitions (e.g. door opener, door contacts) of the XMP-K32 must be set. Hardware alarms (e.g. door breaking) and bookings with unauthorized badges are always forwarded to host 0. The IP address of host 0 must be entered into the first field. The IP addresses of further BABYLON master computers (maximum 7) - which also use this K32 for the Access Control/ Time Recording - must be entered into the remaining fields. For the hosts the 1..7 it is allowed to read attributes and upload parameter sets etc. into the XMP-K32, but for them it is not allowed to write changes for attributes, parameters, routines etc.. Master data and profiles are stored in separate files (pers0..7.sav, prof0..7.sav).

	Profile names may be used several times, however, badge data not. The badge data are not checked for repeated occurrence in the XMP-K32. The host with the lower IP number gets the priority. **Important: The multi-host mode for the XMP-K32 must be released with the necessary releasing code!** **The feature flag 1 (K32 system point SY 0 0 → FE attribute) must be set!**
Code-Offset for BPA/9 (0 = 13):	If a 0 is entered into this field 0, this is equivalent to an offset of 13. I.e., the position 14 of the characters transmitted by the reader contains the first character of the PIN code. For BPA/9 reader this offset can differ depending on telegram definition. This field offers the possibility of a correction. Example: 1 (→ Offset = 14)
Number of seconds for double access control:	For a double access control a certain time interval is specified. Within this interval two successive bookings with the same badge are forbidden. This applies also for all readers with activated double access control (i.e., if flag 6 is set). As the consequence of a successive booking within this time interval the badge is rejected and an alarm is generated. The time interval (in seconds) must be entered into this field. It is only valid if the XMP-K32 is in offline mode.
Custom key (0-2)	If the communication encryption mode between K32/K32lite and Host-PC is activated (Dipswitch 7 / SW3 of the K32/K32lite =ON) an additional defined custom key can be used as type of encryption. Important: The defined custom key will be activated after download of the parameter data and new warm start of the K32/K32lite.
Security level for fingerprint comparison (0-7)	Using fingerprint-readers with door controllers K32/K32lite the sensitivity of the fingerprint verification can be defined. A good setting is found if the fingerprints of all persons can be verified without failures. An undersized security level allows maybe some people to enter the building without authorization; an oversized security level can cause under influence of dirt many reading errors. A good value is a security level 4 or 5

3.1.6 The registry card *Options*

In the registry card *Options* special properties for the function of a **XMP-K32/K32lite** or properties of **XMP-K32/K32lite** together with other **XMP-K32/K32lite** integrated into the network can be defined.
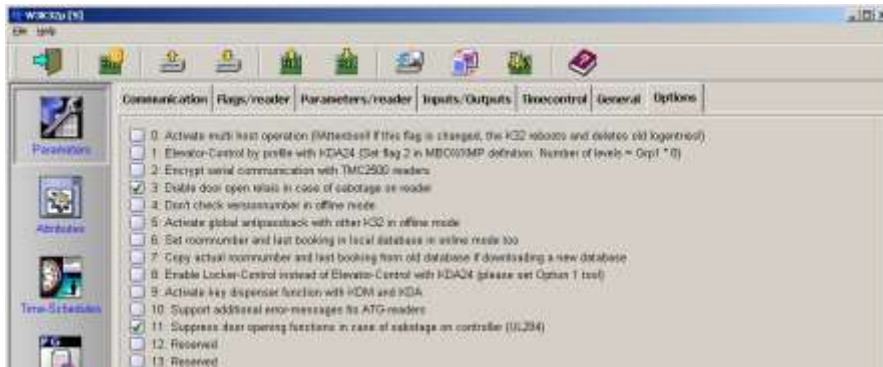

Fig. 8: Registry card *Options*

Meaning of the input fields of the registry card *Options*

0: Activate multi host operation (Attention: only possible for XMP-K32 and BABYLON !)	This option activates the multi-host-operation (see also 3.1.5 The registry card *General*). **Important: The change of this flag will boot the XMP-K32 and delete old log data!**
1: Elevator-Control by profile with KDA24 (Attention: only possible with BABYLON !)	Setting this flag activates the elevator control after profiles with the KDA24. By the access profiles of the person it is specified, which floors are allowed for the person and which not. **Important:** **Setting of the flag 1 ‚*Elevator-Control by profile with KDA'* and input into the field ‚*Number of elevator levels divided by 8 if Flag 1 set'* in the program W3port, registry card *XMP-Parameters***
2: Encrypt serial communication with TMC2500 readers	This flag activates the encrypted communication to the TMC2500. **Important:** **For the TMC2500 this option can be reset only by a power off.**
3: Disable door open relay in case of sabotage on reader	If this flag is set, in case of a sabotage at the reader the door opener relay will go into the state 'block'. As long as the XMP-K32 registers a sabotage condition for the reader the door will not open.
4: Don't check version number in offline mode	If this flag is set, the version number is not checked in offline mode.

5: Activate global Antipas back with other K32 in offline mode	For the operation of this option it is provided that the involved XMP-K32 are in offline mode after parameter download (i.e., there is no connection to the master computer), however, there must be a cross-linking between the individual XMP-K32s. The sense for a global double access control is: it refers not only to an individual door with card reader authorization, but to a whole series of doors with card reader authorization. For it the door controls can be realized by several XMP-K32. The K32 exchanges the necessary data among themselves. Example: A person A executes a booking at entrance 1 of a stadium and hands over the badge to a following person B. By the global double access control for the person B is not allowed to execute any repeated booking neither at reader (entrance 1) nor at any other reader (stadium entrance) of this network. A similar information exchange between the XMP-K32s also causes that the Antipas back mode can be realized in offline mode. The whereabouts of the persons are defined by the executed badge bookings.
6: Set room number and last booking in local database in online mode, too **(Attention: only possible with BABYLON !)**	The room number and the last booking will be forwarded to local master data also for online mode. It recommended to set this option if option 5 is set.
7: Copy actual room number and last booking from old database if downloading a new database	With the master data download also the current room number and the last booking are taken over from old master data. It recommended to set this option if option 5 is set.
8: Enable Locker-Control instead of Elevator-Control with KDA024	**(Attention: only possible with BABYLON !)**
9: Enable key dispenser function with KDM and KDA	**(Attention: only possible with BABYLON !)**
10: Support additional error-messages for ATG-readers	**(Attention: only possible with BABYLON !)**
11: Suppress door opening functions in case of sabotage on controller (UL294)	This feature disables the functionality of the output relays on the door controller if the sabotage alarm of this device is pending. UL installations don't allow access in case of sabotage alarms even on authorized bookings.

3.2 Attributes

The menu ***Attribute*** consists of two registry cards. Inside the first card all attributes of the depending **K32/K32lite** are listed. For easy finding attributes a search-string can be inserted on the bottom. **All attributes of a K32/K32lite can be uploaded and changed through clicking with the right mouse button on the attribute value! To activate the new setting and values the data must be downloaded into the K32/K32lite.**
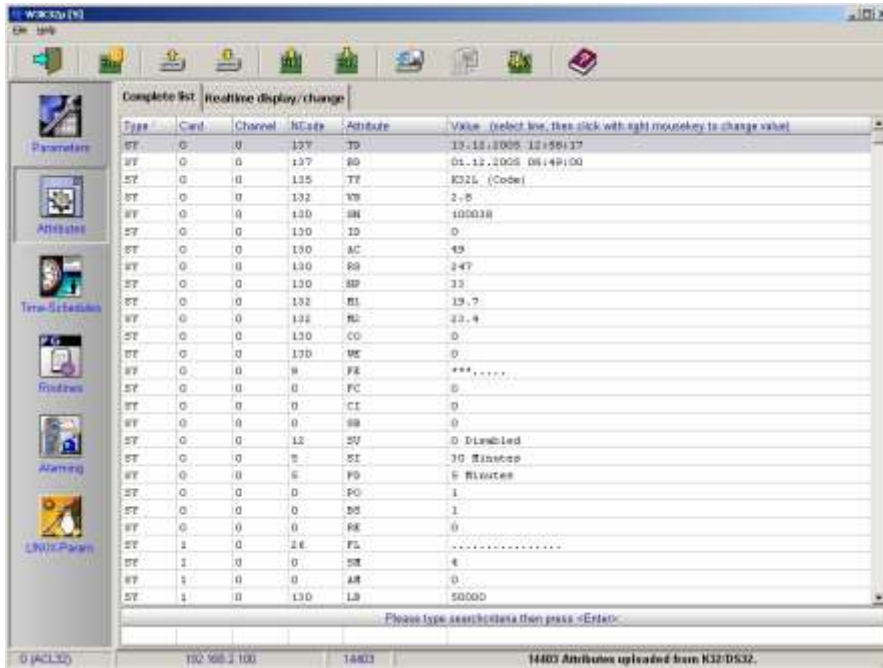

Fig. 9: The menu ***Attributes***

The second registry card shows a real time view of the attributes. All data and data-changes of attributes are displayed. Inserting search strings reduce the visualization of data.
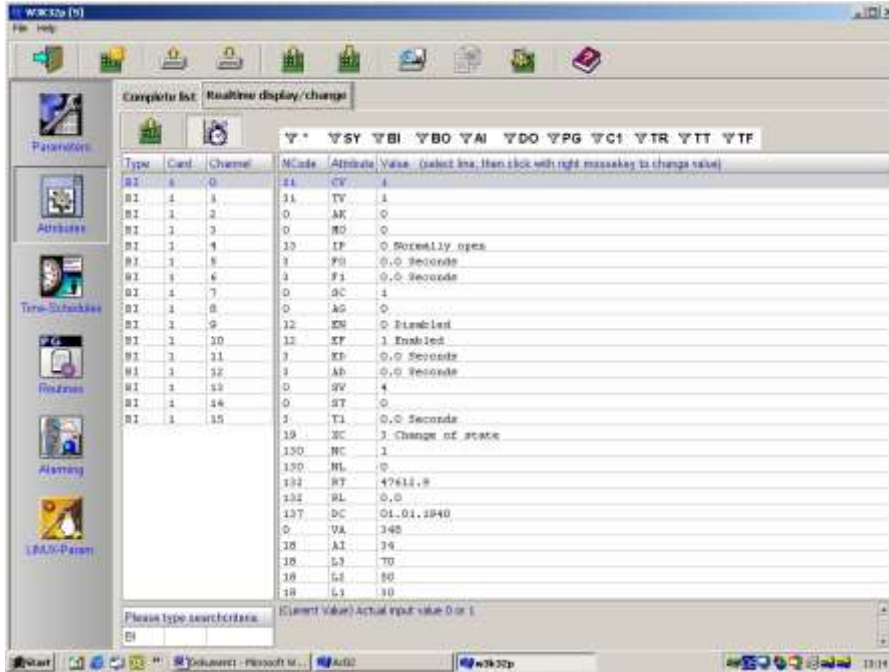

Fig. 10: Real-time view of **Attributes**

3.3 Time-Schedules

The menu *Time-Schedules* consists of 4 registry cards **(Set points, Time-Schedules, Trend-Definition, Display Trends)**.
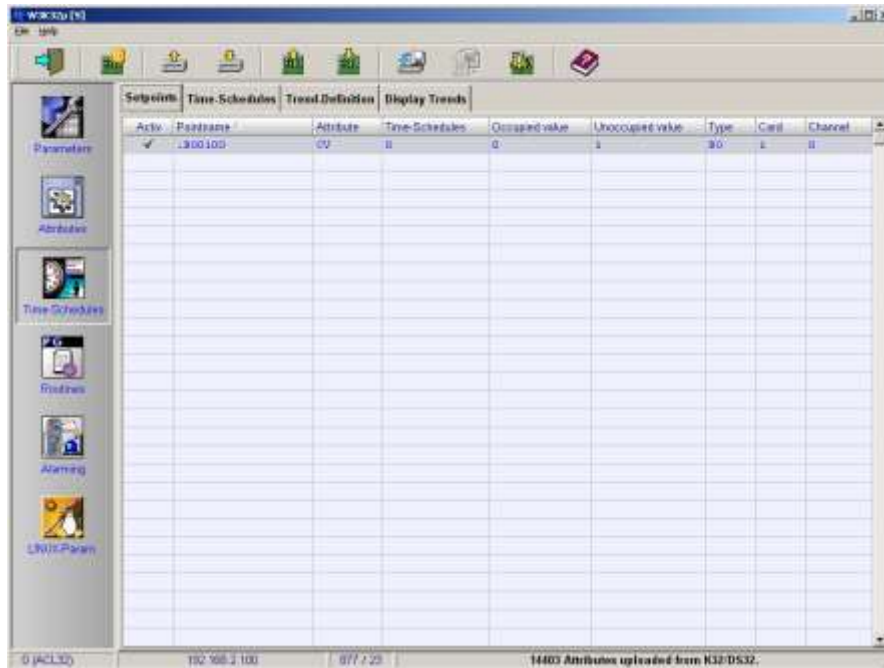

Fig. 11: The menu *Time-Schedules*

3.3.1 The registry card *Set points*

In registry card   *Set points*   the data points - which should be controlled by the schedule – can be selected and specified with its parameters.
Attention: Within the smart system ACL32 the Data points are addressed by their technical addresses.
Example: Output BO Card 1, Channel 0 is named **'BO0100'**

Meaning of the input fields of the registry card *Set points*__

Sell.	Setting a hook into the box the data point depending time schedule will be activated.
Point name :	Technical address of the data point that should be controlled by the schedule
Attribute :	The data point attribute that should be affected by the schedule is entered here.
Time-Schedules :	The number of the schedule which was defined for the time control of the data point must be entered here. The definition of the schedule with the appropriate schedule number is made into the registry card *Time-Schedules*.
Occupied value :	In dependence on the data point and attribute type the set point value for the ‚active' time window of the schedule must be entered here.
Unoccupied value :	In dependence on the data point and attribute type the set point value for the ‚non-active' time window of the schedule must be entered here.
Type :	Type of the selected data point (inserted by system)
Card :	Card, that is defined for the selected data point (inserted by system)
Channel :	Channel, that is defined for selected data point (inserted by system)

3.3.2 The registry card *Time-Schedules*

In the registry card *Time-Schedules* the actual schedule is defined by the setting of occupation times (‚active' times). The schedule is characterized by a number.

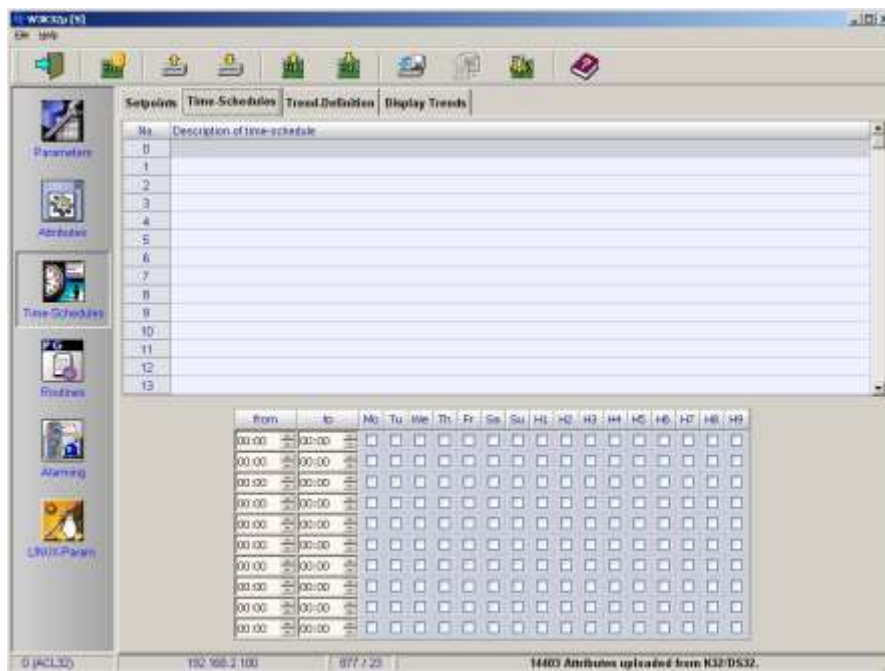Fig. 12: Registry card *Time-Schedules*

Meaning of the input fields of the registry card *Time-Schedules*

No. :	Number of the time-schedule [0..63]
Description of time-schedule :	A short description of the time-schedule can be inserted here.

By selection of an appropriate day-type (*Mo-So, H1-H9*) and setting of the ,active' time window (*from.. to..*) up to 10 different occupation times can be defined for a schedule.

Hint: By double-click on the time schedule number in the set-point value table it is possible to jump directly into the appropriate schedule.

3.3.3 The registry card *Trend-Definition*

In the registry card ***Trend-Definition*** each ***K32/K32lite*** up to 32 data points can be visualized by trend diagrams*.*

Fig. 13: Registry card ***Trend-Definition***

Meaning of the input fields of the registry card *Trend-Definition*

Nr. :	Number of trend [0..31]
Point name :	Technical address of the data point to be visualized.
Attribute :	Attribute of the data point that should be visualized.
Trigger :	A new trend value will be set if the attribute changes about this minimum value.
Type :	Type of selected data point (automatically set from system)
Card :	Card of the selected data point (automatically set from system)
Channel :	Channel of the selected data point (automatically set from system)

3.3.4 The registry card *Display Trends*

In the registry card *Display-Trends* the selected data points of the trend definition are visualized. For each trend up to 2048 values are displayed. The visualization can be defined in different types.
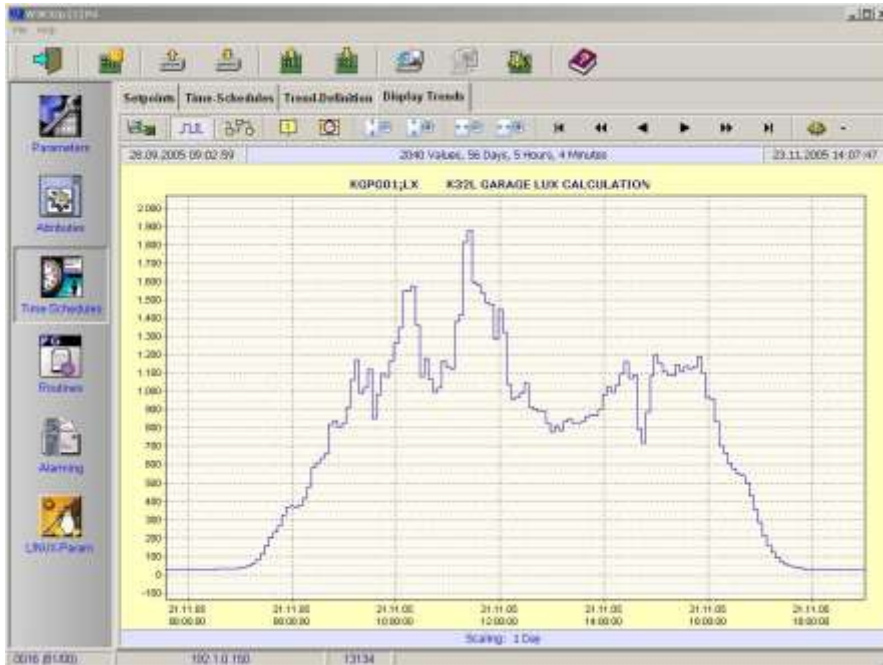

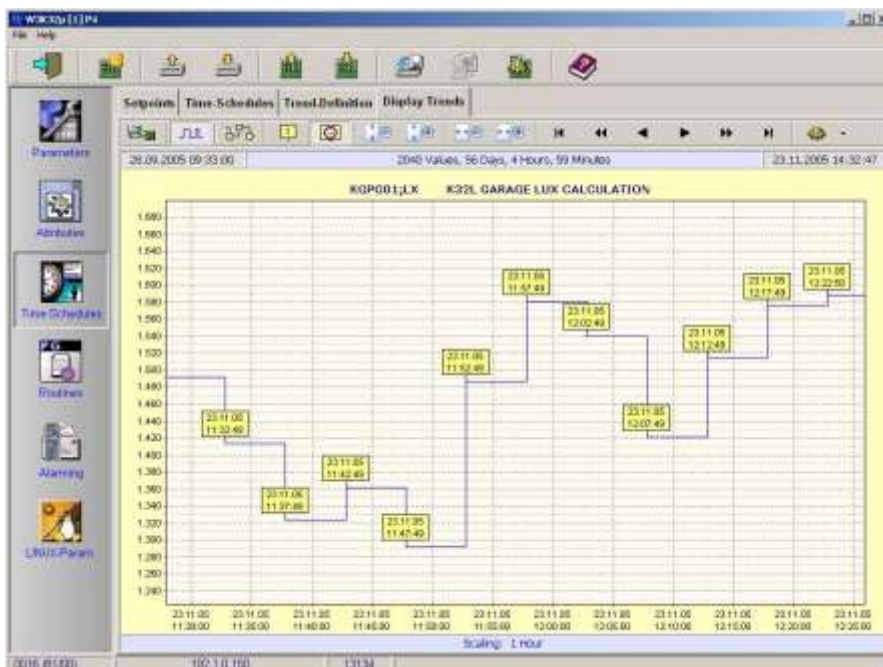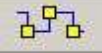Fig. 14: Registry card *Display Trends* (Example 1)
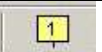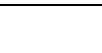

Fig. 15: Registry card *Display Trends* (Example 2)

Meaning of the menu symbols of the registry card *Display-Trends*

Upload actual trend values :	In the door controller K32/K32lite stored trend values will be load to the computer.
Display type (line / bar)	Changes display type from line to bar.
Display type (Marker)	Each maximum value will be marked by a rectangle.
Display type (Value)	Each maximum value will be marked by its value.
Display type (Date/Time)	Each maximum value will be marked by date and time.
Zoom Y	Zooms value range 'Y'
Zoom X	Zooms value range 'X'
Position backward	Moves displayed values backward
Position forward	Moves displayed values forward
Export trend	Export of displayed trends in 3 different file-formats. 1. BMP 2. WMF 3. CSV

3.4 Routines

In the menu option **Routines** up to 32 XMP routines can be created. With routines it is possible to control the periphery of the K32 according to a program sequence particularly specified by the user.
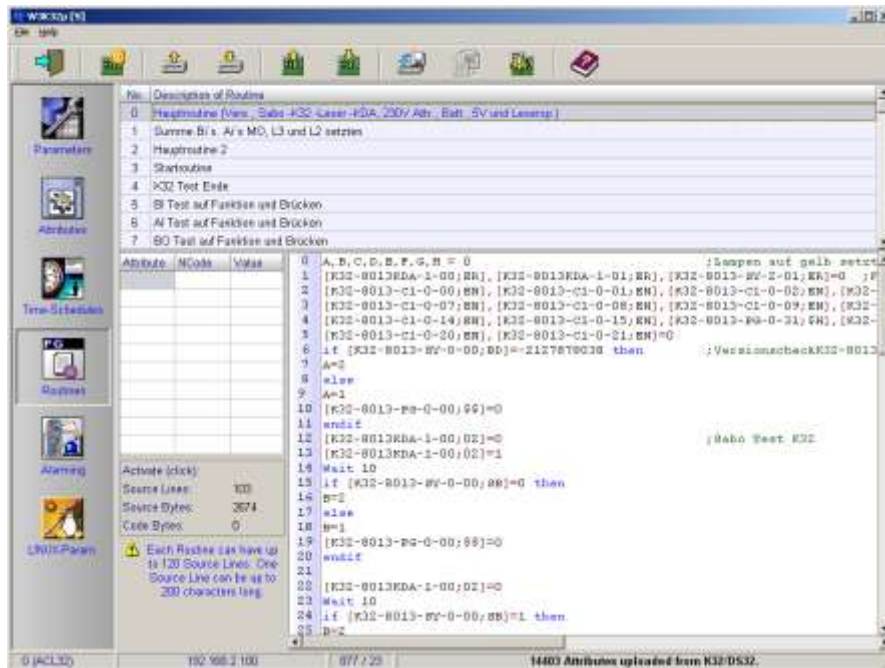

Fig. 16: The menu **Routines**

Meaning of the input fields of the menu program *Routines*

No. :	Number of the routine [0..31]
Description of Routine :	A short description of the routine can be inserted here.

The length of a routine can be up to 120 lines. The length of a line may be maximum 200 characters.

Commands which can be used in K32/K32Lite routines:

print [0..9],"format-string",expr1,expr2,...,expr10
>; 0..7 = Reader 0..7,
>; 8 = Universal reader port,
>; 9 = Universal KDM port,
>; C = Console
>; The structure of the format-string is the same as for the printf-
>; command in the programming language „C" !

wait expr   ; in 100ms Steps, i.e. 3.5 = 3.5 seconds

alarm expr   ; release an alarm
>; expr is the No from defmess~.txt

if expr **op** expr **then**   ; if– constructions
 ..
else
..
endif

if expr **op** expr **goto** nn
if 12 < A < 27 **then**   ; this constellation is allowed, too
goto nn   ; jump to line
>; return into last line not necessary
expr = expr   ; assignment of expressions

Meaning of defined **variables:**

cy = year   ; current year 2005
cm = month   ; current month
cd = mday   ; day of month
cw = wday   ; weekday incl. holidays (0..15) 0=Monday
wday2   ; weekday excluding holidays(0..6)
time   ; time in running minutes per day
time2   ; time in running seconds per day
date   ; date in PM format
wm   ; weekday-map
rand   ; random number
c100   ; internal 100ms counter

Operators, which can be used:
+ - * /
AND or **&**
OR or **|**
XOR or **^**
MOD or **%**
ROR, **ROL**
>> and **<<**
Hex constants can be inserted e.g. as 0xB4D3.

Examples for **technical hardware addresses** in K32-XMP routines
[.BO0100] = 1   or [.BI0100] = 0 ; !!cardnumber double-digit

3.5 Alarming

The menu *Alarming* can be used to send door controller alarms by EMAIL, SMS or TCP/IP- message (alarm printer). There are 4 identical registry cards to define up to 4 different types of alarming or receivers.

Hint

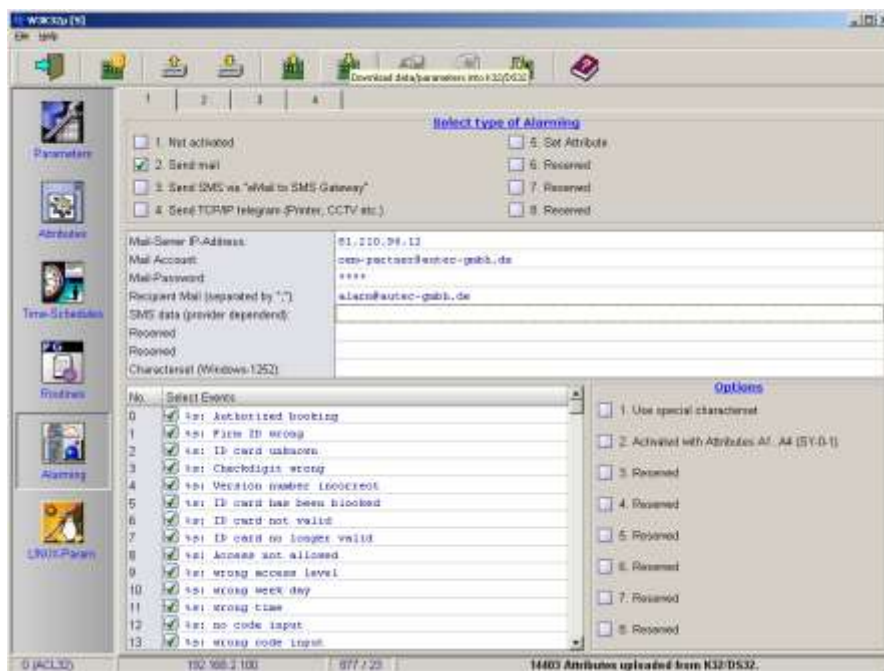The optional software feature 'alarming by email/sms' has to be activated on the door controller (Flag 3).

Fig. 17: The menu *Alarming*

Meaning of the input fields of the menu *Alarming*

Offline alarming by Mail and/or SMS : (Top)	Defining the type of alarming.
Offline alarming by Mail and/or SMS : (Middle)	Defining of receiver address and used character set.
Offline alarming by Mail and/or SMS : (Bottom)	Defining the types of alarms that will be send. (Pushing the button 'NR' all hooks are set.)

3.6 LINUX-Parameters

 The menu **Linux-Param** is used as a control window to monitor or modify files in the K32/K32lite.
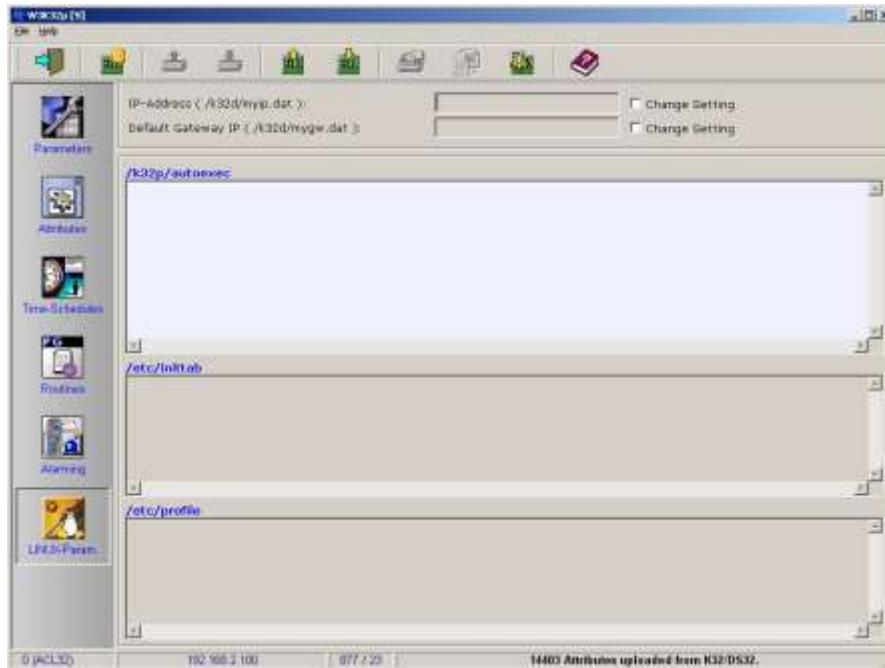

Fig. 18: The menu **LINUX-Parameters**

4 ACL32 download-files

All user defined values (definition of card readers, time schedules, routines and so on.) are stored from the system into K32-parameter-files. Each door controller the following files are stored with the corresponding hardware address (Example: K32A0 for K32 No. 0 ; K32A1 for K32 No. 1 …):

K32A.a32 => holds Attribute values
K32M.a32 => holds Mail addresses
K32P.a32 => holds Parameter values
K32R.a32 => holds Routines
K32S.a32 => holds Set points
K32T.a32 => holds Trend values
K32Z.a32 => holds Time schedules

5 Document history

24.05.07	Format and spelling

AUTEC Gesellschaft für Automationstechnik mbH
Bahnhofstraße 57-61b
55232 Framersheim
Tel.: +49 (0)6733-9201-0
Fax: +49 (0)6733-9201-99
Email: vk@autec-gmbh.de
Internet: www.autec-gmhb.de